kaspersky

Kaspersky Embedded Systems Security 4.0 for Windows

© 2025 AO Kaspersky Lab

Contenido

Kaspersky Embedded Systems Security para Windows
- Novedades
- Kit de distribución
- Requisitos de hardware y software
- Versiones compatibles de Kaspersky Security Center
- Requisitos funcionales y limitaciones
  - Instalación y eliminación de la aplicación
  - Control de integridad del sistema
  - Firewall
  - Limitaciones de las versiones obsoletas de Windows
  - Integración con Kaspersky Security Center
  - Otras limitaciones
- Compatibilidad con otras aplicaciones

Instalación y eliminación de la aplicación
- Planificación de la instalación
  - Selección de herramientas de administración
  - Selección del tipo de instalación
- Instalación y desinstalación de la aplicación mediante un asistente
  - Instalación mediante el asistente de instalación
    - Instalación de Kaspersky Embedded Systems Security
    - Instalación de la Consola de Kaspersky Embedded Systems Security
    - Configuración avanzada después de la instalación de la Consola de la aplicación en otro dispositivo
      - Permiso de acceso remoto anónimo a las aplicaciones COM
      - Permiso de conexión de red para el proceso de administración remota de Kaspersky Embedded Systems Security
    - Acciones para realizar después de la instalación de Kaspersky Embedded Systems Security
      - Iniciar y configurar la tarea Actualización de bases de datos y módulos de la aplicación
      - Análisis de áreas críticas
  - Modificación del conjunto de componentes y reparación de Kaspersky Embedded Systems Security
  - Desinstalación mediante el asistente de instalación
    - Desinstalación de Kaspersky Embedded Systems Security
    - Desinstalación de la Consola de Kaspersky Embedded Systems Security
- Instalación y desinstalación de la aplicación desde la línea de comandos
  - Acerca de la instalación y desinstalación de Kaspersky Embedded Systems Security desde la línea de comandos
  - Códigos de los componentes del software Kaspersky Embedded Systems Security para el servicio Windows Installer
    - Componentes de software de Kaspersky Embedded Systems Security
    - Componentes de software “Herramientas de administración”
  - Ajustes de instalación y recuperación y opciones de línea de comandos de Windows Installer
  - Comandos de ejemplo para la instalación de Kaspersky Embedded Systems Security
  - Acciones para realizar después de la instalación de Kaspersky Embedded Systems Security
  - Cómo agregar o eliminar componentes. Comandos de ejemplo
  - Desinstalación de Kaspersky Embedded Systems Security. Comandos de ejemplo
  - Códigos de devolución

Instalación y desinstalación de la aplicación mediante Kaspersky Security Center
Información general sobre la instalación mediante Kaspersky Security Center
Derechos para instalar o desinstalar Kaspersky Embedded Systems Security
Instalación de Kaspersky Embedded Systems Security a través de Kaspersky Security Center
Acciones para realizar después de la instalación de Kaspersky Embedded Systems Security
Instalación de la Consola de la aplicación mediante Kaspersky Security Center
Desinstalación de Kaspersky Embedded Systems Security a través de Kaspersky Security Center
Cambiar el conjunto de componentes de la aplicación con Kaspersky Security Center
Instalación y desinstalación de la aplicación a través de directivas de grupo de Active Directory
Instalación de Kaspersky Embedded Systems Security mediante directivas de grupo de Active Directory
Acciones para realizar después de la instalación de Kaspersky Embedded Systems Security
Desinstalación de Kaspersky Embedded Systems Security mediante políticas de grupo de Active Directory
Registros de instalación y desinstalación de Kaspersky Embedded Systems Security
Cambios en el sistema después de la instalación de Kaspersky Embedded Systems Security
Procesos de Kaspersky Embedded Systems Security
Verificación de funciones de Kaspersky Embedded Systems Security. Uso del virus de prueba EICAR
Acerca del virus de prueba EICAR
Verificación de las funciones Protección de archivos en tiempo real y Análisis a pedido
Actualización de versiones anteriores de Kaspersky Embedded Systems Security a la versión 4.0
Actualizar Kaspersky Embedded Systems Security
Actualización de las herramientas de administración de Kaspersky Embedded Systems Security
Migrar directivas y tareas
Migración de la configuración de la versión de la aplicación que se actualiza
Correspondencia de componentes y tareas en las versiones 3.4 y 4.0 de Kaspersky Embedded Systems Security
Interfaz de aplicación
Cómo usar el Complemento de administración
Administración de Kaspersky Embedded Systems Security mediante Kaspersky Security Center
Administración de las configuraciones de la aplicación
Navegación
Cómo abrir la configuración general en la ventana de propiedades de la aplicación
Cómo abrir la configuración general mediante la directiva
Configuración de las opciones generales de la aplicación en Kaspersky Security Center
Configuración de opciones de interfaz y análisis en Kaspersky Security Center
Configuración de opciones de seguridad en Kaspersky Security Center
Configuración de opciones de conexión mediante Kaspersky Security Center
Configurar el inicio programado de las tareas locales
Configurar Copia de seguridad en Kaspersky Security Center
Creación y configuración de directivas
Creación de una directiva
Configuración de directivas
Indicador del nivel de seguridad
Creación y configuración de tareas con Kaspersky Security Center
Acerca de la creación de tareas en Kaspersky Security Center
Creación de tareas mediante Kaspersky Security Center
Ir a los ajustes de una tarea local y a los ajustes generales de la aplicación para un equipo individual

Configuración de tareas de grupo en Kaspersky Security Center
Tarea Activar la aplicación
Tarea de actualización
Control de integridad de la aplicación
Administración de programaciones de tareas
Tareas de programación
Cómo habilitar y deshabilitar tareas programadas
Informes en Kaspersky Security Center
Cómo usar la Consola de Kaspersky Embedded Systems Security
Iniciar la Consola de la aplicación.
Interfaz de la Consola de Kaspersky Embedded Systems Security
Ventana Consola de Kaspersky Embedded Systems Security
Icono de la bandeja del sistema en el área de notificación
Ajustar la configuración general a través de la Consola de la aplicación
Administración de tareas de Kaspersky Embedded Systems Security
Categorías de tareas de Kaspersky Embedded Systems Security
Cómo iniciar, pausar, reanudar y detener tareas manualmente
Administración de programaciones de tareas
Configuración de las opciones de programación de tareas
Cómo habilitar y deshabilitar tareas programadas
Uso de cuentas de usuario para iniciar tareas
Acerca del uso de cuentas para iniciar tareas
Especificación de una cuenta de usuario para iniciar una tarea
Cómo importar y exportar la configuración
Acerca de la importación y exportación de la configuración
Exportación de la configuración
Importación de la configuración
Consultar el estado de protección e información de Kaspersky Embedded Systems Security
Trabajo con el complemento web desde Web Console y Cloud Console
Administración de Kaspersky Embedded Systems Security mediante Web Console y Cloud Console
Limitaciones del Complemento web
Administración de las configuraciones de la aplicación
Configuración de opciones generales de la aplicación en el Complemento web
Configuración de interfaz y análisis en el Complemento web
Configuración de seguridad y confiabilidad en el Complemento web
Ajustes de la configuración de conexión en el Complemento web
Configuración del inicio programado de tareas locales en el Complemento web
Configurar Copia de seguridad en el Complemento web
Creación y configuración de directivas
Creación y configuración de tareas con Kaspersky Security Center
Acerca de la creación de tareas en el Complemento web
Crear una tarea en el Complemento web
Configurar tareas de grupo en el Complemento web
Configurar la tarea Activar la aplicación en el Complemento web
Configurar la tarea de Actualización en el Complemento web

Administración de programaciones de tareas
Tareas de programación
Cómo habilitar y deshabilitar tareas programadas
Informes en Kaspersky Security Center
Licencia de la aplicación
Acerca del Contrato de licencia de usuario final
Acerca de la licencia
Acerca del certificado de licencia
Acerca de la clave
Acerca del archivo de clave
Acerca del código de activación
Comparación de la funcionalidad de la aplicación según el tipo de licencia
Activación de la aplicación con un archivo de clave
Activación de la aplicación con un código de activación
Ver información acerca de la licencia actual
Renovación de la licencia
Eliminación de la clave
Sobre la provisión de datos
Cumplimiento de la legislación de la Unión Europea (RGPD)
Cómo iniciar y detener Kaspersky Embedded Systems Security
Iniciar y detener la aplicación.
Suspensión y reanudación de la protección y control del equipo
Interfaz de diagnóstico compacto
Acerca de la Interfaz de diagnóstico compacto
Revisión del estado de Kaspersky Embedded Systems Security a través de la Interfaz de diagnóstico compacto
Revisión de estadísticas de eventos de seguridad
Revisión de la actividad de la aplicación actual
Configuración del seguimiento de la aplicación y el registro del volcado de memoria
Autoprotección de Kaspersky Embedded Systems Security
Habilitar y deshabilitar el componente Autoprotección
Compatibilidad con la tecnología AM-PPL
Protección de los servicios del sistema operativo
Configuración de permisos de usuario para administrar Kaspersky Embedded Systems Security
Configuración de permisos de acceso de usuarios para administrar el servicio de Kaspersky Security.
Acceso protegido por contraseña a funciones de Kaspersky Embedded Systems Security
Notificaciones de Secure Desktop
Zona de confianza
Cómo crear una exclusión de análisis
Selección de tipos de objetos detectables
Modificación de la lista de aplicaciones de confianza
Crear una zona de confianza local
Exportar e importar la zona de confianza
Uso de almacenamiento de certificados de sistema de confianza
Protección de archivos en tiempo real
Acerca del área de protección de la tarea y la configuración de seguridad
Áreas de protección predefinidas
Acerca de los niveles de seguridad predefinidos

- Extensiones de archivo analizadas de manera predeterminada en el componente Protección de archivos en tiempo real
- Configurar el componente Protección de archivos en tiempo real
- Configurar el alcance de la protección para el componente de Protección de archivos en tiempo real
- Configuración manual de las opciones de seguridad
- Análisis de contenedores

Uso de KSN
- Habilitar el uso de Kaspersky Security Network
- Estadísticas de uso de Kaspersky Security Network
- Limitaciones de Kaspersky Private Security Network
- Configuración del proxy de KSN

Prevención de exploits
- Modo de Prevención de exploits
- Habilitación y deshabilitación de la Prevención de exploits
- Habilitar y deshabilitar la protección de memoria
- Crear la lista de procesos protegidos

Motor de reparación

Detección de comportamiento
- Habilitar y deshabilitar la protección de cifrado para las carpetas locales
- Protección de carpetas compartidas contra cifrado externo
  - Habilitación y deshabilitación de la protección de carpetas compartidas contra el cifrado externo
  - Creación del área de protección
  - Agregar equipos de confianza para el cifrado de datos externo
  - Configurar el periodo de bloqueo de un equipo no confiable
  - Exportar e importar una lista de exclusiones de la protección de carpetas compartidas contra el cifrado externo

Protección contra amenazas de red

Escáner AMSI
- Habilitar y deshabilitar el Escáner AMSI
- Configuración del Escáner AMSI

Control de inicio de aplicaciones
- Acerca de las Reglas de Control de inicio de aplicaciones
- Acerca del control de distribución de software
- Acerca del Generador de reglas de control de inicio de aplicaciones
- Habilitar y configurar el Control de inicio de aplicaciones
- Configuración del Control de distribución de software
- Trabajar con las reglas de Control de inicio de aplicaciones
  - Agregar reglas de Control de inicio de aplicaciones
  - Agregar condiciones de activación para la regla de Control de inicio de aplicaciones
  - Agregar exclusiones del alcance de una regla de Control de inicio de aplicaciones
  - Habilitación del modo Habilitación predeterminada
  - Generar un archivo TXT con una selección de eventos bloqueados de la aplicación de Kaspersky Security Center
- Configurar una tarea de grupo de Generador de reglas de Control de inicio de aplicaciones
- Crear reglas con la tarea de grupo del Generador de reglas de Control de inicio de aplicaciones.

Control de dispositivos
- Reglas de acceso a dispositivos
- Control de acceso a dispositivos por tipo
- Control de conexiones Wi-Fi
- Control de impresión

- Control de dispositivos de entrada (HID)
- Supervisar el uso de unidades extraíbles
- Administrar el acceso a los dispositivos Bluetooth
- Diferenciación de los derechos de acceso del usuario a los dispositivos
- Auditoría de dispositivos externos
- Incorporación de dispositivos de confianza
- Exportar e importar la lista de dispositivos de confianza

Firewall
- Acerca de las reglas de firewall
- Configurar el firewall
  - Establecer la configuración general de firewall
  - Creación y configuración de reglas de Firewall
  - Habilitación y deshabilitación de Reglas de firewall

Prevención de ataques BadUSB

Control de integridad del sistema
- Acerca de las reglas de Control de integridad del sistema
- Control de integridad del sistema en tiempo real
- Comprobación de integridad del sistema a pedido
- Exportación e importación de las reglas de Control de integridad del sistema
- Visualización de los informes de Control de integridad del sistema

Inspección de registros
- Agregar reglas personalizadas
- Configuración de reglas predefinidas

Análisis a pedido
- Acerca de las tareas de Análisis a pedido
- Acerca del área del análisis de la tarea y la configuración de seguridad
- Áreas del análisis predefinidas
- Análisis de archivos almacenados en línea
- Acerca de los niveles de seguridad predefinidos
- Análisis de unidades extraíbles
- Configuración de tareas de Análisis a pedido
- Administrar las tareas de Análisis a pedido
  - Navegación
    - Cómo abrir el asistente de la tarea de Análisis a pedido
    - Cómo abrir la configuración de la tarea de Análisis a pedido
  - Creación de una tarea de Análisis a pedido
    - Ejecución de una tarea de Análisis a pedido en segundo plano
    - Registro de la ejecución de un Análisis de áreas críticas
  - Configurar el alcance del análisis en la tarea de Análisis a pedido
  - Establecer la configuración de la tarea de Análisis a pedido
  - Configuración del Análisis de unidades extraíbles
  - Selección de niveles de seguridad predefinidos para tareas de Análisis a pedido
  - Configuración manual de las opciones de seguridad
  - Estadísticas de la tarea de Análisis a pedido

Base de datos y actualización de módulos del programa de Kaspersky Embedded Systems Security
- Actualizar bases de datos y módulos de la aplicación
- Acerca de las tareas de Actualización

- Esquemas de actualización para las bases de datos y los módulos de Kaspersky Embedded Systems Security
- Configuración de tareas de Actualización
- Actualización SMU de la aplicación
- Reversión de actualizaciones de bases de datos de Kaspersky Embedded Systems Security
- Estadísticas de las tareas de actualización

Creación de copias de seguridad de los objetos

- Creación de copias de seguridad de los objetos. Copia de seguridad
  - Ver objetos en Copia de seguridad
    - Cómo ordenar archivos en Copia de seguridad
    - Filtrado de archivos en Copia de seguridad
  - Restauración de archivos desde copias de seguridad
  - Eliminación de archivos de Copia de seguridad
  - Envío de objetos probablemente infectados a Kaspersky para su análisis
  - Configuración de Copia de seguridad
  - Estadísticas de Copia de seguridad
- Bloqueo de acceso a los recursos de red. Sesiones en la red bloqueadas
  - Lista de sesiones de red bloqueadas
  - Administrar la lista de sesiones de red bloqueadas

Registro de eventos. Registros de Kaspersky Embedded Systems Security

- Modos de registrar eventos de Kaspersky Embedded Systems Security
- Configuración de los parámetros del registro
  - Ordenar eventos en el registro
  - Filtrado de eventos en el registro
  - Eliminar eventos del registro
  - Exportar información desde el registro
- Registro de auditoría del sistema
- Registros de tareas
  - Visualización de las estadísticas y la información acerca de una tarea de Kaspersky Embedded Systems Security en los registros de tareas
- Ver el registro de eventos de Kaspersky Embedded Systems Security en el Visor de eventos
- Acerca de la integración de SIEM
  - Configuración de las opciones de integración de SIEM
- Métodos de notificación de administrador y usuario
  - Configuración de notificaciones de administrador y usuario
  - Configuración de notificaciones de correo electrónico
- Configuración de la interacción con el servidor de administración

Managed Detection and Response

- Configuración de integración de MDR

Contacto con Soporte técnico

- Cómo acceder al Servicio de soporte técnico
- Soporte técnico mediante Kaspersky CompanyAccount
- Proporcionar información de diagnóstico extendida a los especialistas del Servicio de soporte técnico
- Seguimiento de la operación de aplicaciones
- Registrar volcados de memoria

Fuentes de información acerca de Kaspersky Embedded Systems Security

Glosario
- Actualización
- Analizador heurístico
- Archivo de almacenamiento
- Archivo infectable
- Bases de datos antivirus
- Clave activa
- Configuración de tareas
- Copia de seguridad
- Cuarentena
- Desinfección
- Directiva
- Estado de protección
- Falso positivo
- Importancia de un evento
- Kaspersky Security Network (KSN)
- Máscara de archivo
- Nivel de seguridad
- Objeto infectado
- Objeto OLE
- Objetos de inicio
- Periodo de vigencia de la licencia
- Servidor de administración
- SIEM
- Tarea
- Tarea local
- Vulnerabilidad

Información acerca de código de terceros

Avisos de marca registrada

Apéndices
- Extensiones de archivos para un análisis rápido
- Cuentas de usuario en las reglas del componente de la aplicación

Kaspersky Embedded Systems Security para Windows

Kaspersky Embedded Systems Security para Windows (en adelante, denominado también Kaspersky Embedded Systems Security), protege equipos y otros sistemas integrados que ejecutan Microsoft® Windows® (en adelante, denominados también dispositivos protegidos) 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.

La aplicación no está diseñada para utilizarse en procesos tecnológicos que involucren sistemas de control automatizados. Para proteger dispositivos en tales sistemas, se recomienda utilizar la aplicación Kaspersky Industrial CyberSecurity for Nodes.

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 dispositivo protegido donde está instalado Kaspersky Embedded Systems Security o en un dispositivo 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 dispositivos protegidos 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 de archivos 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 los archivos, la RAM y los objetos de ejecución automática del dispositivo protegido.

- **Control de inicio de aplicaciones**. Este componente atiende a los intentos del usuario de iniciar aplicaciones y regula el inicio de las aplicaciones en el dispositivo protegido.

- **Control de dispositivos**. El componente controla el registro y el uso de dispositivos externos a fin de proteger el dispositivo contra amenazas de seguridad informática que pueden surgir al intercambiar archivos con unidades flash conectadas mediante USB u otros tipos de dispositivos externos.

- **Firewall**. Según el modo, el componente hace lo siguiente: supervisar el filtrado de tráfico mediante el Firewall de Windows; registrar solo eventos sobre la actividad de red del equipo protegido en el registro del componente; o filtrar el tráfico de red de acuerdo con la configuración de 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 dispositivo 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 módulos de la aplicación**. 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, 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 motivos de seguridad, los objetos en la carpeta Cuarentena se almacenan en forma cifrada.

- **Copias de seguridad**. Kaspersky Embedded Systems Security almacena copias cifradas de los objetos clasificados como *Infectados* en *Copias de seguridad* antes de desinfectarlos o eliminarlos.

- **Notificaciones de administrador y usuario**. Puede hacer que la aplicación notifique al administrador y a los usuarios que accedan al dispositivo protegido sobre los eventos vinculados al funcionamiento de Kaspersky Embedded Systems Security y al estado de la protección antivirus del dispositivo.

- **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 dispositivo protegido y guardar los valores de ajuste configurados como plantilla. Esta plantilla se puede utilizar entonces para especificar 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 Windows**. 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 exclusiones de la protección o del alcance del análisis que Kaspersky Embedded Systems Security aplicará durante las tareas de Protección del equipo en tiempo real y a pedido.

- **Prevención de exploits**. La memoria de un proceso puede protegerse contra los exploits a través de un Agente de protección inyectado en el proceso.

Las funciones de actualización (incluidas la posibilidad de actualizar las firmas antivirus y el código del programa) y las funciones de KSN podrían no estar disponibles si el programa se utiliza en los EE. UU.

Novedades

Kaspersky Embedded Systems Security 4.0 ofrece las siguientes características y mejoras:

- Interfaz de usuario con una gran actualización de la Consola de la aplicación y los complementos para administrar la aplicación mediante Kaspersky Security Center.

- Compatibilidad con Windows 11 24H2.

- Ahora puede cambiar el puerto que usa la Consola de la aplicación para conectarse a un equipo con la aplicación instalada.

- En la *Zona de confianza*, puede hacer lo siguiente:

  - Configurar los procesos de confianza con mayor detalle.

  - Usar el almacén de certificados de confianza.

- Nueva configuración de derechos de usuario y grupo para administrar la aplicación.

- Nuevo componente *Anti-Rootkit*. De manera predeterminada, el componente está habilitado si *Protección de archivos en tiempo real* está habilitada. Puede deshabilitar el componente mientras instala la aplicación mediante la tarea *Cambiar los componentes de la aplicación Kaspersky Embedded Systems Security* o en las propiedades del paquete de instalación de la aplicación.

- En la configuración de *Prevención de exploits*, la aplicación ahora puede identificar automáticamente los procesos protegidos.

- Nuevo componente *Motor de reparación*.

- El componente Protección contra amenazas de red puede controlar el tráfico de la red para detectar el escaneo de puertos y las solicitudes de red de alta intensidad.

- La aplicación ahora es compatible con el Firewall de Windows. Ya no es necesario eliminar el Firewall de Windows para instalar la aplicación.

- El componente *Detección de comportamiento* supervisa las carpetas compartidas y las locales.
- Componente *Control de inicio de aplicaciones* rediseñado:
  - Cambios significativos en la estructura de la configuración de los componentes.
  - Para especificar las condiciones de activación y las exclusiones de regla de Control de inicio de aplicaciones, ahora puede usar el tipo de unidad, las categorías de KL y los grupos de KSN.
- Componente *Control de dispositivos* rediseñado:
  - De manera predeterminada, el componente *Control de dispositivos* está configurado para permitir la conexión de todos los dispositivos.
  - *Control de Wi-Fi* ya no es un componente separado y ahora es parte de Control de dispositivos.
  - Se agregó la posibilidad de controlar los dispositivos conectados en función del bus de conexión.
  - Se agregó la migración de la configuración para acceder a unidades extraíbles durante la actualización de versiones anteriores de la aplicación a la versión 4.0.
- El componente *Administración de firewall* se rediseñó para incluirse en el componente *Firewall*, que, además de interactuar con el firewall de Windows, ahora también funciona como firewall.
- La funcionalidad de los componentes *Monitor de integridad de archivos* y *Monitor de acceso al registro* se fusionaron en el nuevo componente *Control de integridad del sistema*. Esta mejora le permite realizar un seguimiento eficiente de los cambios en el sistema de archivos y el registro de Windows, lo que aumenta la protección contra la modificación no autorizada de datos.
- La aplicación no admite la programación de componentes individuales. Si los componentes están habilitados, continúan ejecutándose mientras se ejecuta la aplicación.
- Kaspersky Security Center Windows 15.1 ya es compatible.
- Tareas de grupo agregadas:
  - *Protección de la conexión del Servidor de administración*
  - *Cambiar el conjunto de componentes de Kaspersky Embedded Systems Security*
  - *Monitor comparativo de integridad del sistema* en lugar del *Monitor comparativo de integridad de archivos*
  - *Actualizar* en lugar de *Copia de actualizaciones*, *Actualización de bases de datos de la aplicación* y *Actualización de módulos del programa*
  - *Reversión de la actualización* en lugar de *Reversión de la actualización de la base de datos de la aplicación*
  - *Eliminar clave*
- La aplicación revisa la configuración de los componentes de control antes de guardar los ajustes. La revisión se implementó para los componentes Control de inicio de aplicaciones, Control de dispositivos y Control de integridad del sistema. Ahora, la aplicación muestra una advertencia si la configuración actual del componente de control podría aumentar la carga en la computadora o causar fallas en el sistema. Por ejemplo, en el caso del Control de inicio de aplicaciones, si seleccionó el modo que bloquea todas las aplicaciones excepto las permitidas y no agregó ninguna regla de autorización, la aplicación muestra una advertencia porque una configuración así podría causar fallas en el sistema.

- Se agregó la posibilidad de crear automáticamente reglas de autorización para el Control de inicio de aplicaciones y exportar estas reglas a un archivo. Para ello, ejecute la tarea *Generador de reglas de control de inicio de aplicaciones* y habilite la creación automática de reglas de autorización basadas en las aplicaciones en ejecución, así como la exportación de reglas de autorización. Puede usar el archivo resultante para hacer un inventario del software instalado en el dispositivo.

- Nuevo componente: *Prevención de ataques BadUSB*. El componente Prevención de ataques BadUSB impide que los dispositivos USB infectados que emulan un teclado se conecten al equipo. Cuando se conecta al equipo un dispositivo USB que el sistema operativo identifica como un teclado, la aplicación solicita al usuario que escriba en este teclado para autorizarlo.

- Se agregó el *Indicador de nivel de seguridad*. El Indicador de nivel de seguridad se muestra en la parte superior de la ventana de propiedades de la directiva y muestra el grado de cumplimiento de la configuración de seguridad con las recomendaciones de Kaspersky Lab. El Indicador de nivel de seguridad le permite configurar rápidamente la directiva y habilitar los componentes de protección necesarios.

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 la herramienta de eliminación de virus de Kaspersky.
- Leer sobre esta versión de Kaspersky Embedded Systems Security.
- Abrir la ayuda de Kaspersky Embedded Systems Security 4.0.
- Ir a la página de Kaspersky Embedded Systems Security en el sitio web de Kaspersky.
- Visitar el sitio web de Kaspersky.
- Visitar el sitio web del servicio de soporte técnico.

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

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 una unidad extraíble.
setupui.exe	Archivo de inicio de la pantalla de bienvenida de la aplicación.
ess_win.kud	Archivo en el formato definición Unicode de Kaspersky con una descripción del paquete de instalación para la instalación remota de la aplicación mediante Kaspersky Security Center.
\console\esstools.msi	Paquete de instalación de Windows Installer; instala Kaspersky Embedded Systems Security Console en los dispositivos protegidos.
\console\setup_esstool.exe	Archivo que permite iniciar un asistente para instalar un conjunto de componentes de Herramientas de administración (incluida la Consola de Kaspersky Embedded Systems Security). El archivo de paquete de instalación esstools.msi se inicia con los parámetros de instalación definidos en el asistente.
\console\license.txt	Archivo de texto del Contrato de licencia de usuario final y la Política de privacidad de la Consola de administración de Kaspersky Embedded Systems Security.

Archivo	Objetivo
\exec\bases.cab	Archivo de almacenamiento que contiene las bases de datos antivirus actuales al momento del lanzamiento de la aplicación.
\exec\cleaner_v2.cab \exec\cleanerapi_v2.cab	Archivos para eliminar software incompatible.
\exec\ess.cab	Archivos para la interfaz gráfica de la aplicación.
\exec\ess_win.kud	Archivo en el formato definición Unicode de Kaspersky con una descripción del paquete de instalación para la instalación remota de la aplicación mediante Kaspersky Security Center.
\exec\ess_win.msi	Paquete de instalación de Windows Installer: instala Kaspersky Embedded Systems Security en el dispositivo protegido.
\exec\incompatible.txt	Kaspersky no garantiza la compatibilidad de Kaspersky Embedded Systems Security con las aplicaciones que se indican en la lista.
\exec\installer.ini	Archivo installer.ini que contiene las configuraciones internas del kit de distribución.
\exec\klcfginst.msi	Instalador para el Complemento de administración de Kaspersky Embedded Systems Security disponible a través de Kaspersky Security Center. Instale el Complemento de administración en cada dispositivo protegido donde esté instalada la Consola de administración de Kaspersky Security Center si planea usarla para administrar Kaspersky Embedded Systems Security.
\exec\ksn_en.txt	Archivo con el texto de la Declaración de KSN.
\exec\license.txt	Archivo de texto del Contrato de licencia de usuario final de Kaspersky Embedded Systems Security.
\exec\package.kcat	Archivo con las firmas de los archivos del kit de distribución.
\exec\setup_ess.exe	El archivo que inicia el asistente para instalar Kaspersky Embedded Systems Security en el dispositivo protegido; inicia el archivo del paquete de instalación ess_win.msi con la configuración de instalación especificada en el asistente.
\kvrt\KVRT.exe	Instalador de la herramienta de eliminación de virus de Kaspersky.
\product_long_term\cleaner_v2.cab \product_long_term\cleanerapi_v2.cab	Archivos para eliminar software incompatible.
\product_long_term\ess.cab	Archivos para la interfaz gráfica de la aplicación.
\product_long_term\ess_win.kud	Archivo en el formato definición Unicode de Kaspersky con una descripción del paquete de instalación para la instalación remota de la aplicación mediante Kaspersky Security Center.
\product_long_term\ess_win.msi	Paquete de instalación de Windows Installer; instala Kaspersky Embedded Systems Security con la configuración **Proteger el equipo con la tecnología Default Deny** en el dispositivo protegido.
\product_long_term\incompatible.txt	Kaspersky no garantiza la compatibilidad de Kaspersky Embedded Systems Security con las aplicaciones que se indican en la lista.
\product_long_term\installer.ini	Archivo installer.ini que contiene las configuraciones internas del kit de distribución.
\product_long_term\klcfginst.exe	Instalador para el Complemento de administración de Kaspersky Embedded Systems Security disponible a través de Kaspersky Security Center. Instale el Complemento de administración en cada dispositivo protegido donde esté instalada la Consola de administración de Kaspersky Security Center si planea usarla para administrar Kaspersky Embedded Systems Security.
\product_long_term\ksn_en.txt	Archivo con el texto de la Declaración de KSN en ruso.
\product_long_term\license.txt	Archivo de texto del Contrato de licencia de usuario final de Kaspersky Embedded Systems Security.
\product_long_term\package.kcat	Archivo con las firmas de los archivos del kit de distribución.
\product_long_term\setup_ess.exe	El archivo que inicia el asistente para instalar Kaspersky Embedded Systems Security en el dispositivo protegido; inicia el archivo del paquete de instalación ess_win.msi con la configuración de instalación especificada en el asistente.
\setup\images	Carpeta con archivos de inicio de la pantalla de bienvenida de la aplicación.
\setup\setup.hta	Archivo de inicio de la pantalla de bienvenida de la aplicación.
\setup\SETUP_STRINGS.JS	Archivo con los recursos de texto de la aplicación.

Los archivos del kit de distribución se pueden ejecutar desde el CD de instalación. Si copió los archivos del paquete de distribución en la unidad local de antemano, asegúrese de que se haya conservado la estructura

de los archivos del kit de distribución.

Requisitos de hardware y software

Requisitos de software para el dispositivo protegido

Se requiere Windows Installer 3.1 para instalar y utilizar la aplicación en un dispositivo protegido que ejecute Microsoft Windows XP.

Para instalar y usar Kaspersky Embedded Systems Security en dispositivos protegidos que tengan sistemas operativos integrados, se requiere el componente Filter Manager.

Para el correcto funcionamiento de Kaspersky Embedded Systems Security, se requiere compatibilidad con SHA-2 en Microsoft Windows. Para obtener información detallada, consulte la base de conocimientos en el sitio web del Servicio de soporte técnico.

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

Estaciones de trabajo:

- Windows XP Professional SP2 y posterior (32 bits/64 bits)
- Windows Vista SP2 (32 bits/64 bits)
- Windows 7 SP1 y posterior Home/Pro/Education/Enterprise (32 bits/64 bits)
- Windows 8 Pro/Enterprise (32 bits/64 bits)
- Windows 8.1 Pro/Enterprise (32 bits/64 bits)
- Windows 10 TH1 Home/Pro/Pro for Workstations/Education/Enterprise (32 bits/64 bits)
- Windows 10 TH2 Home/Pro/Pro for Workstations/Education/Enterprise (32 bits/64 bits)
- Windows 10 RS1 Home/Pro/Pro for Workstations/Education/Enterprise (32 bits/64 bits)
- Windows 10 RS2 Home/Pro/Pro for Workstations/Education/Enterprise (32 bits/64 bits)
- Windows 10 RS3 Home/Pro/Pro for Workstations/Education/Enterprise (32 bits/64 bits)
- Windows 10 RS4 Home/Pro/Pro for Workstations/Education/Enterprise (32 bits/64 bits)
- Windows 10 RS5 Home/Pro/Pro for Workstations/Education/Enterprise (32 bits/64 bits)
- Windows 10 RS6 Home/Pro/Pro for Workstations/Education/Enterprise (32 bits/64 bits)

- Windows 10 19H2 Home/Pro/Pro for Workstations/Education/Enterprise (32 bits/64 bits)
- Windows 10 20H1 Home/Pro/Pro for Workstations/Education/Enterprise (32 bits/64 bits)
- Windows 10 20H2 Home/Pro/Pro for Workstations/Education/Enterprise (32 bits/64 bits)
- Windows 10 21H1 Home/Pro/Pro for Workstations/Education/Enterprise (32 bits/64 bits)
- Windows 10 21H2 Home/Pro/Pro for Workstations/Education/Enterprise (64 bits)
- Windows 10 22H2 Home/Pro/Pro for Workstations/Education/Enterprise (64 bits)
- Windows 11 21H2 Home/Pro/Pro for Workstations/Education/Enterprise (64 bits)
- Windows 11 22H2 Home/Pro/Pro for Workstations/Education/Enterprise (64 bits)
- Windows 11 23H2 Home/Pro/Pro for Workstations/Education/Enterprise (64 bits)
- Windows 11 24H2 Home/Pro/Pro for Workstations/Education/Enterprise (64 bits)

Sistemas operativos del servidor:

- Windows Server 2003 SP1 y posterior Standard/Enterprise (32 bits/64 bits)
- Windows Server 2003 R2 SP2 Standard/Enterprise (64 bits)
- Windows Server 2008 SP2 Standard/Enterprise (32 bits / 64 bits)
- Windows Server 2008 R2 SP2 y posterior Foundation/Standard/Enterprise (64 bits)

Sistemas integrados:

- Windows XP Embedded SP3 (POS Ready) (32 bits)
- Windows 7 Embedded (POS Ready) Standard (32 bits/64 bits)
- Windows 7 Embedded SP1 Standard (32 bits/64 bits)
- Windows 8.0 Embedded Standard (32 bits/64 bits)
- Windows 8.1 Embedded Industry/Pro (32 bits/64 bits)
- Windows 10 versión 1507 IoT Enterprise (32 bits/64 bits)
- Windows 10 versión 1607 IoT Enterprise (32 bits/64 bits)
- Windows 10 versión 1803 IoT Enterprise (32 bits/64 bits)
- Windows 10 versión 1809 IoT Enterprise (32 bits/64 bits)
- Windows 10 versión 1909 IoT Enterprise (32 bits/64 bits)
- Windows 10 versión 21H2 IoT Enterprise (32 bits / 64 bits)
- Windows 10 versión 22H2 IoT Enterprise (32 bits / 64 bits)

- Windows 11 versión 21H2 IoT Enterprise (64 bits)
- Windows 11 versión 22H2 IoT Enterprise (64 bits)
- Windows 11 versión 23H2 IoT Enterprise (64 bits)
- Windows 11 versión 24H2 IoT Enterprise (64 bits)

Requisitos de hardware para el dispositivo protegido

Requisitos de hardware para el dispositivo protegido

Tipo de sistema operativo	Nombre del sistema operativo	Requisitos mínimos	Requisitos recomendados
Estaciones de trabajo	Windows XP x86/x64	• Procesador: procesador de un núcleo de 1,4 GHz Pentium III (x32), Pentium IV (x64). • RAM: • Para instalar solo el componente del Control de inicio de aplicaciones: 256 MB. • Para instalar todos los componentes de la aplicación: 512 MB • Espacio libre en disco: • Para instalar solo el componente del Control de inicio de aplicaciones: 50 MB. • Para instalar todos los componentes de la aplicación: 2 GB	• Procesador: procesador de cuatro núcleos de 2,4 GHz. • RAM: 2 GB • Espacio libre en disco: • Para instalar solo el componente del Control de inicio de aplicaciones: 2 GB. • Para instalar todos los componentes de la aplicación: 4 GB
	Windows 7/8/10 x86	• Procesador: procesador de un núcleo de 1,4 GHz Pentium III (x32), Pentium IV (x64). • RAM: • Para instalar solo el componente del Control de inicio de aplicaciones: 256 MB. • Para instalar todos los componentes de la aplicación: 1 GB • Espacio libre en disco: • Para instalar solo el componente del Control de inicio de aplicaciones: 50 MB. • Para instalar todos los componentes de la aplicación: 2 GB	• Procesador: procesador de cuatro núcleos de 2,4 GHz. • RAM: 2 GB • Espacio libre en disco: • Para instalar solo el componente del Control de inicio de aplicaciones: 2 GB. • Para instalar todos los componentes de la aplicación: 4 GB
	Windows 7/8/10/11 x64	• Procesador: Procesador de un núcleo de 1,4 GHz Pentium IV (x64). • RAM: • Para instalar solo el componente del Control de inicio de aplicaciones: 1 GB. • Para instalar todos los componentes de la aplicación: 2 GB • Espacio libre en disco: • Para instalar solo el componente del Control de inicio de aplicaciones: 50 MB. • Para instalar todos los componentes de la aplicación: 2 GB	• Procesador: procesador de cuatro núcleos de 2,4 GHz. • RAM: • Para instalar solo el componente del Control de inicio de aplicaciones: 2 GB. • Para instalar todos los componentes de la aplicación: 4 GB • Espacio libre en disco: • Para instalar solo el componente del Control de inicio de aplicaciones: 2 GB. • Para instalar todos los componentes de la aplicación: 4 GB
Sistemas integrados	Windows XP Embedded	• Procesador: procesador de un núcleo de 1,4 GHz Pentium III (x32), Pentium IV (x64). • RAM: • Para instalar solo el componente del Control de inicio de aplicaciones: 256 MB. • Para instalar todos los componentes de la aplicación: 512 MB • Espacio libre en disco: • Para instalar solo el componente del Control de inicio de aplicaciones: 50 MB. • Para instalar todos los componentes de la aplicación: 2 GB	• Procesador: procesador de cuatro núcleos de 2,4 GHz. • RAM: 2 GB • Espacio libre en disco: • Para instalar solo el componente del Control de inicio de aplicaciones: 2 GB. • Para instalar todos los componentes de la aplicación: 4 GB

Tipo de sistema operativo	Nombre del sistema operativo	Requisitos mínimos	Requisitos recomendados
	Windows 7/8 Embedded Windows 10/11 IoT	• Procesador: Procesador de un núcleo de 1,4 GHz Pentium IV (x64). • RAM: 1 GB. • Espacio libre en disco: • Para instalar solo el componente del Control de inicio de aplicaciones: 50 MB. • Para instalar todos los componentes de la aplicación: 2 GB	• Procesador: procesador de cuatro núcleos de 2,4 GHz. • RAM: 2 GB • Espacio libre en disco: • Para instalar solo el componente del Control de inicio de aplicaciones: 2 GB. • Para instalar todos los componentes de la aplicación: 4 GB

Versiones compatibles de Kaspersky Security Center

Kaspersky Embedded Systems Security es compatible con las siguientes versiones de Kaspersky Security Center:

- Kaspersky Security Center Windows versiones 10.5 y 11. La administración de Kaspersky Embedded Systems Security instalado en equipos que ejecutan el sistema operativo Microsoft Windows XP SP2 es compatible con la Consola de administración de Kaspersky Security Center y con Kaspersky Security Center Web Console.
- Kaspersky Security Center Windows versiones 14.2 y 15.1. La administración de Kaspersky Embedded Systems Security es compatible con la Consola de administración de Kaspersky Security Center y Kaspersky Security Center Web Console.
- Kaspersky Security Center Linux versiones 15.0, 15.1, 15.2, 15.3, 15.4 y 16.0. La administración de Kaspersky Embedded Systems Security es compatible con Kaspersky Security Center Web Console.

Para administrar Kaspersky Embedded Systems Security a través de Kaspersky Security Center, se requiere el Agente de red de Kaspersky Security Center.

El Agente de red de Kaspersky Security Center no viene incluido en el kit de distribución de Kaspersky Embedded Systems Security. Puede obtenerlo de la página de descarga de aplicaciones; lo encontrará en la sección **Kaspersky Security Center**.

Requisitos funcionales y limitaciones

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

Instalación y eliminación de la aplicación

- Para el correcto funcionamiento de Kaspersky Embedded Systems Security, se requiere compatibilidad con SHA-2 en Microsoft Windows.

- Cuando instala la aplicación, puede aparecer una advertencia en la pantalla si la ruta especificada a la carpeta de instalación de Kaspersky Embedded Systems Security contiene más de 150 caracteres. La advertencia no afecta el proceso de instalación: puede instalar y ejecutar Kaspersky Embedded Systems Security.

- Si desea instalar el componente de compatibilidad con el protocolo SNMP, asegúrese de reiniciar el servicio SNMP si este se está ejecutando.

- Si desea instalar y ejecutar Kaspersky Embedded Systems Security en un dispositivo que se ejecuta en un sistema operativo integrado, asegúrese de instalar el componente de administración de filtros.

- No puede instalar las Herramientas de administración de Kaspersky Embedded Systems Security a través de las directivas de grupo Active Directory® de Microsoft.

- Si excluye el nodo Protección antivirus de la lista de componentes de la aplicación instalados, este nodo desaparece de la lista de componentes disponibles una vez que se completa la instalación. Para instalar los componentes del nodo Protección antivirus, inicie el Asistente de instalación desde el paquete de instalación, ya que este contiene una lista completa de los componentes.

- Si la Consola de administración de Kaspersky Embedded Systems Security está instalada, es posible que el Asistente de instalación le solicite reiniciar el equipo. En este caso, no es obligatorio reiniciarlo. Basta con finalizar la sesión del usuario que instaló la Consola de administración y volver a iniciar sesión en el sistema.

- Cuando instale la aplicación en un dispositivo con Windows XP o Windows Vista, es posible que deba instalar el certificado raíz DigiCert Assured ID Root CA para habilitar la verificación de la firma del controlador. De ser necesario, este certificado se instalará automáticamente en el almacén de certificados raíz de confianza del sistema operativo desde el paquete de instalación de la aplicación.

- Cuando instale la aplicación en dispositivos con Windows XP o Windows Vista, deberá verificar si se encuentra el certificado DigiCert High Assurance EV Root CA..

  Si este certificado raíz no está instalado, la aplicación puede funcionar de forma incorrecta. Le recomendamos que instale el certificado lo antes posible.

- La instalación de la aplicación finaliza con un error si la ruta de la carpeta de instalación es igual a la ruta de al menos una de las siguientes carpetas: carpeta de bases de datos de la aplicación, carpeta de Copia de seguridad, carpeta para restaurar objetos de Cuarentena, carpeta de archivos temporales.

- Si administra Kaspersky Embedded Systems Security con Kaspersky Security Center Cloud Console, no es posible actualizar la aplicación de forma local. Al actualizar la aplicación de forma local, no es posible aceptar el Contrato de procesamiento de datos de Kaspersky Security Center Cloud Console.

Control de integridad del sistema

De manera predeterminada, el componente Control de integridad del sistema no supervisa los cambios en las carpetas del sistema o en los archivos de limpieza del sistema de archivos para que los informes de tareas no estén saturados con información sobre los cambios de archivos rutinarios que el sistema operativo realiza constantemente. No puede incluir tales carpetas en el área de supervisión.

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 y otros).

Firewall

- Debe especificar más de una dirección. De lo contrario, no es posible trabajar con IPv6.
- Las reglas de Firewall predeterminadas admiten los escenarios básicos de interacción entre dispositivos protegidos y el Servidor de administración. Para hacer uso completo de las funciones de Kaspersky Security Center, debe configurar las reglas de puerto. Puede encontrar información sobre los números de puertos, los protocolos y sus funciones en la Base de conocimientos de Kaspersky Security Center.
- Una vez que se instala la aplicación y se configuran las reglas del Firewall, la aplicación supervisa los cambios en las reglas y en los grupos de reglas del Firewall de Windows cuando se ejecuta el componente Firewall. Para actualizar el estado y agregar las reglas necesarias del Firewall de Windows, reinicie el componente Firewall.
- Cuando inicia el componente Firewall, las reglas de denegación y las reglas que controlan el tráfico saliente se eliminan automáticamente de la configuración del Firewall de Windows.
- No se permite usar los caracteres `*` ni `?` en la ruta de la aplicación ni en el nombre de la regla de Firewall para las aplicaciones.
- En el sistema operativo Windows, en la configuración del Firewall (**Configuración → Actualización y seguridad → Seguridad de Windows → Firewall y protección de red**), el botón que habilita el Firewall de Kaspersky Embedded Systems Security solo habilita el Firewall, pero no lo cambia al modo *Bloquear* a menos que, antes de habilitar el firewall, tuviera el modo *Observar el estado del Firewall de Windows* del Firewall habilitado. El botón, que habilita el Firewall de Kaspersky Embedded Systems Security, dejará de mostrarse solo después de que el modo Firewall se cambie a *Bloquear*.

Limitaciones de las versiones obsoletas de Windows

- La versión de Windows XP SP2 no permite bloquear dispositivos remotos ni configurar la Lista de sesiones de red bloqueadas. En esta versión de Windows, está inactiva la opción **Bloquear acceso a recursos compartidos en la red para las sesiones que muestran actividad maliciosa**.
- Instalación de Kaspersky Embedded Systems Security:
  - En equipos que ejecutan Windows XP SP2 Professional (32 bits/64 bits), Windows Server 2003 y Windows Server 2003 R2, debe usar el kit de distribución de la aplicación o colocar el archivo ejecutable setup.exe del paquete de instalación estándar "Agente de red de Kaspersky Security Center 10.5 para Windows XP" en la carpeta del paquete de instalación de la aplicación de Kaspersky Security Center.
  - En equipos con Windows XP SP3 Professional (32 bits) y Windows XP Embedded SP3 (32 bits), es necesario utilizar el kit de distribución de la aplicación o colocar el archivo ejecutable setup.exe del paquete de instalación de la aplicación creado en Kaspersky Security Center versión 14 o del paquete de instalación estándar "Agente de red de Kaspersky Security Center 14 para Windows XP" en la carpeta del paquete de instalación de la aplicación de Kaspersky Security Center.

Cómo extraer el archivo setup.exe del paquete de instalación estándar de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione **Avanzado** → **Instalación remota** → **Paquetes de instalación**.
2. En el espacio de trabajo, haga clic en **Acciones adicionales** y seleccione **Ver versiones actuales de las aplicaciones de Kaspersky** de la lista desplegable.
3. Seleccione la aplicación necesaria de la lista. Por ejemplo, Agente de red de Kaspersky Security Center 10.5 para Windows XP.
4. Haga clic en el botón **Descargar y crear paquete de instalación**.

   El paquete de instalación creado se mostrará en la lista **Paquetes de instalación**.
5. Abra las propiedades del paquete de instalación creado.
6. En la sección **General**, copie la ruta a la carpeta del paquete de instalación.
7. Abra la carpeta del paquete de instalación.
8. Copie el archivo setup.exe.

- Para administrar Kaspersky Embedded Systems Security a través de Kaspersky Security Center:
  - En un equipo con Windows XP SP2 Professional (32 bits / 64 bits) o Windows Server 2003 o Windows Server 2003 R2, debe usar el Agente de red de Kaspersky Security Center (klnagent) versión 10.5.1781.
  - En un equipo con Windows XP SP3 Professional (32 bits) y Windows XP Embedded SP3 (32 bits), debe usar el Agente de red de Kaspersky Security Center (klnagent) versión 14.0.0.20023.
- En equipos con Windows XP, la telemetría no se puede enviar a un diodo de datos mediante el protocolo MQTT.

Integración con Kaspersky Security Center

- Cuando se reciben paquetes de actualización, el Servidor de administración verifica las actualizaciones de la base de datos antes de enviar las actualizaciones a los dispositivos protegidos en la red. El Servidor de administración de Kaspersky Security Center no verifica las actualizaciones del módulo de la aplicación.
- Asegúrese de que las casillas requeridas estén seleccionadas en la configuración de Interacción con Servidor de administración de Kaspersky Security Center al momento de utilizar los componentes que transmiten datos dinámicos a Kaspersky Security Center mediante las listas de la red (Cuarentena, Copia de seguridad).
- La versión 10.5 del Agente de red no envía información acerca de los componentes instalados al Servidor de administración de Kaspersky Security Center. Por este motivo, en la Consola de administración de Kaspersky Security Center, y Kaspersky Security Center Web Console, la configuración de un dispositivo con la versión 10.5 del Agente de red no muestra los componentes instalados de Kaspersky Embedded Systems Security y su configuración.
- Si se instala la versión 10.5 del Agente de red de Kaspersky Security Center en el dispositivo, no puede usar Kaspersky Security Center Web Console para descargar archivos en Copia de seguridad.

- Si se instala Kaspersky Embedded Systems Security con el modo de consumo de bajos recursos habilitado para el Agente de red de Kaspersky Security Center (predeterminado, `SKIP_KLNAG_FLAG_TEST_VM_PERF=0`) y, luego, se instala el Agente de red, Kaspersky Embedded Systems Security no crea una exclusión para el Agente de red en el Firewall de Windows; por lo tanto, el Firewall de Windows bloquea el Agente de red.

- Si se instala Kaspersky Embedded Systems Security con el modo de consumo de bajos recursos habilitado para el Agente de red de Kaspersky Security Center (predeterminado, `SKIP_KLNAG_FLAG_TEST_VM_PERF=0`), las modificaciones realizadas en las listas de redes se reflejan en la Consola de administración de Kaspersky Security Center con una demora de aproximadamente diez minutos.

Otras limitaciones

Análisis a pedido y Protección de archivos en tiempo real

- El análisis de dispositivos MTP conectados no está disponible.

- El análisis de archivos 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. El análisis de archivos SFX está disponible sin analizar los archivos.

- Si las casillas **Análisis profundo sobre los procesos de ejecución (se bloquea el inicio del proceso mientras dure el análisis)** y **Uso de KSN** están seleccionadas al mismo tiempo, se bloquearán los procesos ejecutados que reciban una dirección web URL como argumento, incluso si se seleccionó el modo "Informar". Para evitar el bloqueo del proceso, elija una de las opciones:

  - Deshabilite **Uso de KSN**.

  - Deshabilite la casilla **Análisis profundo sobre los procesos de ejecución (se bloquea el inicio del proceso mientras dure el análisis)**.

  Recomendamos que anule la selección de la casilla **Análisis profundo sobre los procesos de ejecución (se bloquea el inicio del proceso mientras dure el análisis)**.

Administración de licencias

- No puede activar la aplicación con una clave mediante el asistente de instalación si la clave se creó con el comando SUBST o si la ruta de acceso al archivo de clave es una ruta de acceso de red.

- Si planea usar un servidor proxy de Kaspersky Security Center para activar el producto en un dispositivo cliente, deshabilite la optimización para VDI en ese dispositivo cuando instale el Agente de red de Kaspersky Security Center.

Actualizaciones

- De manera predeterminada, el icono de la aplicación está oculto después de instalar las actualizaciones de los módulos críticos de Kaspersky Embedded Systems Security.
- KLRAMDISK no se admite en dispositivos protegidos que se ejecutan con los sistemas operativos Windows XP y Windows Server® 2003.
- Si no se pudo instalar el parche de Kaspersky Embedded Systems Security, el parche se revierte y se le pide que reinicie el sistema operativo.

Interfaz

- En la Consola de la aplicación, el filtrado en la Cuarentena, Copia de seguridad, Registro de auditoría del sistema o Registro de tareas distingue entre mayúsculas y minúsculas.
- Al configurar un área de análisis o de protección en la Consola de la aplicación, sólo puede utilizar una máscara y sólo al final de la ruta de acceso. A continuación, se muestran ejemplos de máscaras correctas: `C:\Temp\Temp*`, `C:\Temp\Temp???.doc` y `C:\Temp\Temp*.doc`. Esta limitación no afecta la configuración de la Zona de confianza.
- En la Consola de la aplicación, en la sección **Servidores de colección de telemetría**, no se muestra la hora de ejecución programada de las tareas. La columna **Hora de inicio** está vacía.

Seguridad

- Si el sistema operativo tiene habilitada la característica Control de cuentas de usuario, es necesario que la cuenta de usuario forme parte del grupo Administradores de ESS para poder abrir la Consola de la aplicación con un doble clic en el icono de la aplicación ubicado en el área de notificación de la bandeja. De lo contrario, será necesario iniciar sesión como usuario que cuenta con permiso para abrir la Interfaz de diagnóstico compacto o el complemento de Microsoft Management Console.
- Si el Control de la cuenta de usuario está habilitado, no puede desinstalar la aplicación a través de la ventana Programas y características de Microsoft Windows.

Prevención de exploits

- Prevención de exploits no está disponible si las bibliotecas apphelp.dll no están cargadas en la configuración del entorno actual.
- El componente Prevención de exploits es incompatible con la utilidad EMET de Microsoft en dispositivos protegidos que ejecutan el sistema operativo Microsoft Windows 10. Kaspersky Embedded Systems Security bloquea EMET si el componente Prevención de exploits se instala en un dispositivo protegido que tenga instalada la utilidad EMET.
- El componente Prevención de exploits no es compatible con el motor de bases de datos SQL Server® 2012. Si instala Kaspersky Embedded Systems Security en el equipo con MS SQL Server 2012 instalado, debe agregar la biblioteca sqlos.dll del servidor de bases de datos a la lista de exclusiones en la tarea Prevención de exploits.

Detection and Response

- Si en el transcurso del proceso de respuesta a amenazas, se produce un error de acceso a la carpeta compartida, el error no se refleja en el historial de respuestas a amenazas (Kaspersky Security Center Web Console → propiedades del host con la aplicación instalada → sección **Detection and Response** - **Historial de respuestas**).

- La configuración de [KESS+KEA+agente integrado] no es compatible. Esa configuración interrumpe la interacción entre las aplicaciones y la solución de Detección y respuesta que se implementa en su organización. Además, el uso de Kaspersky Endpoint Agent y el agente integrado en la misma computadora puede provocar la duplicación de la telemetría y una mayor carga en la computadora y la red.

  El instalador le permite implementar Kaspersky Endpoint Agent en una computadora con Kaspersky Embedded Systems Security y el agente integrado instalados. Kaspersky Endpoint Agent y el agente integrado también se pueden instalar en una computadora como resultado de la tarea *Cambiar componentes de la aplicación*. El comportamiento depende de las versiones de Kaspersky Embedded Systems Security y Kaspersky Endpoint Agent.

Configuración de eventos

La configuración del evento *Operación de archivo no controlada en área controlada* que se puede establecer en la sección **Configuración de eventos** de la directiva de Kaspersky Security Center también se aplica a los siguientes eventos:

- *Operación de archivo permitida en un área controlada realizada por un usuario de confianza*.
- *Operación de archivo no permitida en área controlada*.
- *Solo estadísticas: operación de archivo no permitida en área controlada*.
- *Operación de archivo no controlada en área controlada*.

Interfaz de diagnóstico compacto

En equipos con Windows XP, la Interfaz de diagnóstico compacta requiere que el Servicio de terminal esté funcionando.

Compatibilidad con otras aplicaciones

Kaspersky Embedded Systems Security en configuración de *Funcionalidad completa* no es compatible con aplicaciones que forman parte de sistemas de protección de endpoints de terceros (Plataforma de protección de endpoints, EPP). Kaspersky Embedded Systems Security también puede no ser compatible con otras aplicaciones y algunas aplicaciones de Kaspersky. Para determinar la compatibilidad, Kaspersky Embedded Systems Security verifica una lista de software que elaboró Kaspersky. Esta lista se encuentra en el archivo incompatible.txt. El archivo está incluido en el kit de distribución.

Si se detecta una aplicación de la lista incompatible.txt, el instalador aborta la instalación de Kaspersky Embedded Systems Security. Debe eliminar la aplicación antivirus de terceros. El instalador puede eliminar automáticamente algunas aplicaciones de la lista.

Si el Firewall de Windows está instalado en el equipo, el instalador lo desactiva para continuar con la instalación de Kaspersky Embedded Systems Security.

Si, a pesar de los riesgos, necesita instalar Kaspersky Embedded Systems Security junto con una aplicación de la lista incompatible.txt, puede omitir la verificación de aplicaciones antivirus de terceros instaladas. Para hacerlo, pase el parámetro `SKIPINCOMPATIBLESW= 1` al instalador.

Ejemplo:

```
setup_ess.exe /s EULA=1 PRIVACYPOLICY=1 /p  SKIPINCOMPATIBLESW= 1
```

Instalación y eliminación de la aplicación

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

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, desde la línea de comandos, mediante Kaspersky Security Center y mediante directivas de grupos de Active Directory.

Si instala Kaspersky Embedded Systems Security después de eliminar Kaspersky Industrial CyberSecurity for Nodes o Kaspersky Endpoint Security para Windows, debe reiniciar el equipo.

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.
3. Elija el método de instalación.

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 puede administrarse mediante la Consola de la aplicación instalada en el dispositivo protegido o en cualquier otro dispositivo 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 dispositivos con Kaspersky Embedded Systems Security instalado.

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 dispositivo 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 dispositivos, 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 dispositivo protegido.

- **Agente de red de Kaspersky Security Center**. Instale este componente en todos los dispositivos protegidos. Este componente admite la interacción entre la instancia de Kaspersky Embedded Systems Security instalada en el dispositivo protegido 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**. Además, puede instalar el Complemento de administración para gestionar Kaspersky Embedded Systems Security a través de la Consola de administración en el dispositivo protegido 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, \exec\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, 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.

- Si la configuración de instalación será la misma para todos los dispositivos protegidos o específica para cada dispositivo protegido.

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 dispositivo protegido 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 dispositivos protegidos. 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:

- Los componentes de Kaspersky Embedded Systems Security en el dispositivo protegido. Para esto se debe hacer clic en el vínculo correspondiente de la aplicación de bienvenida, la cual se abre mediante el archivo setupui.exe, o se puede usar directamente el archivo \exec\setup_ess.exe del kit de distribución.

- La Consola de Kaspersky Embedded Systems Security en el dispositivo protegido o en otro dispositivo de la LAN. Para esto se debe hacer clic en el vínculo correspondiente de la aplicación de bienvenida, la cual se abre mediante el archivo setupui.exe, o se puede usar directamente el archivo \exec\setup_esstools.exe del kit de distribución.

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 dispositivo protegido y/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.

Instalación centralizada mediante Kaspersky Security Center

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

Los dispositivos protegidos en los que quiera instalar Kaspersky Embedded Systems Security mediante Kaspersky Security Center 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 dispositivo protegido. La Consola de la aplicación puede instalarse en el dispositivo protegido o en la estación de trabajo del administrador.

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

Los dispositivos protegidos en los cuales se instala Kaspersky Embedded Systems Security mediante directivas de grupo de Active Directory deben estar ubicados en el mismo dominio y en la misma unidad organizacional. La instalación se lleva a cabo al iniciar el dispositivo protegido, 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.

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:

1. Instale Kaspersky Embedded Systems Security en el dispositivo protegido.
2. Instale la Consola de la aplicación en los dispositivos desde los que administrará Kaspersky Embedded Systems Security.
3. Si instaló la Consola de la aplicación en un dispositivo de la red que no es el dispositivo protegido, realice las acciones de configuración necesarias 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.

Instalación de Kaspersky Embedded Systems Security

Antes de instalar Kaspersky Embedded Systems Security, realice lo siguiente:

1. Asegúrese de que no haya otros aplicaciones antivirus instalados en el dispositivo protegido. Debe eliminar Kaspersky Anti-Virus 8.0 para Windows Servers Enterprise Edition. No necesita eliminar Kaspersky Security 10 para Windows Server para instalar Kaspersky Embedded Systems Security.
2. Asegúrese de que la cuenta con la que planee ejecutar el asistente de instalación pertenezca al grupo de administradores del dispositivo 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 (desinstalación).

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

1. Ejecute el archivo setupui.exe en el dispositivo protegido.
2. En la ventana que se abre, en la sección **Instalación"**, haga clic en el vínculo **Proteger el equipo con la tecnología de denegación predeterminada"** o el vínculo **Proteger el equipo con bases antivirus"**.

   Cuando se selecciona la configuración **Proteger el equipo con bases antivirus"**, de manera predeterminada, se incluyen todos los componentes de Kaspersky Embedded Systems Security, excepto los componentes Firewall y Contadores de rendimiento.

   Cuando se instala la configuración **Proteger el equipo con bases antivirus"** de Kaspersky Embedded Systems Security sobre una versión de la aplicación que no depende del análisis de firmas y el uso de bases de datos antivirus para proteger el equipo, el conjunto de componentes de la aplicación se extiende automáticamente con los siguientes componentes:

   - Protección de archivos en tiempo real
   - Análisis a pedido.
   - Protección contra amenazas de red.

   Los componentes que habilitan las actualizaciones no se incluyen en la configuración **Proteger el equipo con la tecnología de denegación predeterminada"**.

   Si se selecciona la configuración **Proteger el equipo con la tecnología de denegación predeterminada"**, los siguientes componentes se incluyen de manera predeterminada:

   - Core
   - Prevención de exploits
   - Control de inicio de aplicaciones
   - Icono de la bandeja del sistema

   Cuando se instala la configuración **Proteger el equipo con la tecnología de denegación predeterminada"** de Kaspersky Embedded Systems Security sobre una versión de la aplicación que usa el análisis de firmas y las bases de datos antivirus para proteger el equipo, el conjunto de componentes de la aplicación se reduce automáticamente al eliminar los siguientes componentes:

   - Protección de archivos en tiempo real
   - Análisis a pedido.
   - los componentes que permiten actualizaciones

   Esta configuración se recomienda para proteger dispositivos con recursos limitados. En este caso, puede activar la aplicación a largo plazo y el componente Control de inicio de aplicaciones proporciona protección al equipo.

3. En la pantalla bienvenida del Asistente de instalación de Kaspersky Embedded Systems Security, haga clic en el botón **Siguiente >**.

   Se abre la ventana **Contrato de licencia de usuario final**.

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, marque las casillas **Confirmo que he leído y que comprendo y acepto en su totalidad los términos y las condiciones de estos contratos de licencia de usuario final** y **Reconozco y acepto el hecho de que mis datos se manejarán y transmitirán (incluso a otros países) según lo descrito en la Política de privacidad. Confirmo que he leído y que comprendo en su totalidad la Política de privacidad**.

   Si no acepta el Contrato de licencia de usuario final y/o la Política de privacidad, la instalación se cancelará.

6. Haga clic en **Siguiente >**.

   Se abre la ventana **Instalación personalizada**.

7. Seleccione los componentes que quiera instalar.

   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 dispositivo protegido.

8. Para cancelar todos los cambios, haga clic en el botón **Restablecer** en la ventana **Instalación personalizada**. Haga clic en **Siguiente >**.

9. En la ventana **Seleccionar la carpeta de destino**, haga lo siguiente:

   - 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 **Siguiente >**.

10. En la ventana **Configurar**, puede excluir objetos y carpetas del alcance de la protección y configurar la Protección de archivos en tiempo real.

11. En la ventana **Importar opciones de configuración del archivo de configuración**, especifique una ruta para el archivo de configuración, si desea importar la configuración de Kaspersky Embedded Systems Security de un archivo de configuración existente creado con una versión anterior de la aplicación.

12. 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 guardó previamente un archivo de clave en la carpeta \exec 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.

El asistente de instalación no permite activar la aplicación con un código de activación. Si desea activar la aplicación con un código de activación, puede especificar uno después de instalar la aplicación.

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 **Siguiente >** para agregar el archivo de clave a la aplicación.

13. En la sección **Configuración del acceso remoto**, de ser necesario, cambie los números de puertos TCP que usa la Consola de la aplicación para la conexión remota a un equipo con la aplicación instalada.

    El número de puerto predeterminado para la conexión con las credenciales de Windows es 13032. El número de puerto predeterminado para la conexión con las credenciales de los usuarios creados manualmente es 13031. Intervalo de posibles números de puerto: 1-65535.

    Para evitar la conexión con las credenciales de cuentas de usuario creadas manualmente, borre la casilla de verificación **Utilizando las credenciales de usuarios creados manualmente**.

14. En la ventana **Preparado para instalar**, puede deshabilitar la opción **Proteger el proceso de instalación de la aplicación** si es necesario. El mecanismo de protección impide reemplazar el paquete de distribución con una aplicación maliciosa, bloquea el acceso a la carpeta de instalación de Kaspersky Embedded Systems Security e impide el acceso a la sección del Registro en la que se encuentran las claves de la aplicación. Sin embargo, si no se puede instalar la aplicación (por ejemplo, al realizar una instalación remota con la ayuda de Windows Remote Desktop), se recomienda que desactive la protección del proceso de instalación.

15. En caso de ser necesario, puede agregar la ruta del archivo kavshell.exe a la variable de sistema %PATH% para facilitar el uso de la interfaz de línea de comandos.

16. Haga clic en **Instalar**.

17. Una vez que termine la instalación, se abrirá la ventana **Instalación terminada**.

18. Haga clic en el botón **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:

1. Asegúrese de que la cuenta que utiliza para ejecutar el asistente de instalación pertenezca al grupo de administradores del dispositivo.

2. Ejecute el archivo setupui.exe en el dispositivo protegido.

   Se abre la ventana de bienvenida.

3. Haga clic en el vínculo **Instalar la Consola de Kaspersky Embedded Systems Security para Windows"**.

   Se abre la ventana de bienvenida del asistente de instalación. Haga clic en **Siguiente >**.

4. Si acepta los términos y condiciones del Contrato de licencia de usuario final y la Política de privacidad, marque las casillas **Confirmo que he leído y que comprendo y acepto en su totalidad los términos y las condiciones de estos contratos de licencia de usuario final** y **Reconozco y acepto el hecho de que mis datos se manejarán y transmitirán (incluso a otros países) según lo descrito en la Política de privacidad. Confirmo que he leído y que comprendo en su totalidad la Política de privacidad**. Haga clic en **Siguiente >**.

5. Especifique una carpeta en la que se deben guardar los archivos que se están instalando en la ventana **Seleccionar la carpeta de destino**.

6. Haga clic en **Siguiente >**.

7. Haga clic en el botón **Instalar** de la ventana **Preparado para instalar**.

   El asistente comenzará a instalar los componentes seleccionados.

8. Haga clic en **Finalizar**.

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

Si instaló las Herramientas de administración en un dispositivo de la red que no sea el protegido, configure los ajustes avanzados.

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

Si la Consola de la aplicación se instaló en cualquier dispositivo de la red que no sea el dispositivo protegido, realice las siguientes acciones para que los usuarios pueden administrar Kaspersky Embedded Systems Security de forma remota:

- Utilice una cuenta de usuario que tenga permiso para conectarse de forma remota en la configuración de la aplicación. De forma predeterminada, todos los usuarios de los administradores y los grupos de administradores de ESS tienen este permiso.

- En el dispositivo remoto, en la configuración del Firewall de Windows, abra el puerto TCP 13032 para la conexión mediante las cuentas de usuario del sistema de Windows y el puerto TCP 13031 para la conexión mediante las cuentas de usuario creadas manualmente en la configuración de la aplicación. También debe permitir las conexiones de red para el archivo ejecutable del proceso de administración remota de Kaspersky Embedded Systems Security: avp.exe. Puede administrar esta configuración con la opción `ADDWFEXCLUSION=1` al instalar la aplicación desde la línea de comandos.

Si necesita ejecutar Kaspersky Embedded Systems Security de forma remota, haga lo siguiente:

La cuenta de usuario que iniciará la aplicación de forma remota debe ser parte del grupo de administradores.

- En el dispositivo remoto, en la configuración del Firewall de Windows, habilite la regla **Uso compartido de archivos e impresoras (SMB de entrada)** (puerto TCP 445). También recomendamos abrir el puerto TCP 135 para permitir la conexión con el dispositivo.

- En el caso de dispositivos remotos que ejecutan Windows Vista o una versión posterior que no forman parte de un dominio o se administran mediante una cuenta de usuario local, **deshabilite el control remoto de cuentas de usuario (UAC).**

  1. Abra el editor de registro en el equipo.

  2. En el editor de registro, abra la clave HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System.

  3. Abra el valor LocalAccountTokenFilterPolicy.

     Si falta el valor LocalAccountTokenFilterPolicy en esta clave, cree un valor DWORD (32 bits) con este nombre (para obtener más información, consulte el Sitio web de soporte técnico de Microsoft).

  4. Configúrelo en `1` y haga clic en **Aceptar**.

     Deshabilitar el UAC remoto no afecta el UAC local.

- Si el dispositivo en el que se instaló la Consola de la aplicación o el dispositivo protegido cuentan con Windows 8.1 o una versión anterior de Windows, **habilite la compatibilidad con el acceso compartido a archivos SMB 1.0/CIFS en dispositivos con Windows 10 o una versión posterior.**

  - En la aplicación "Características de Windows":

    1. Seleccione **Inicio** → **Panel de control** → **Programas y características** → **Activar o desactivar las características de Windows**.

    2. En la ventana **Características de Windows**, seleccione la casilla de verificación **Compatibilidad con el protocolo para compartir archivos SMB 1.0/CIFS**.

    3. Haga clic en **Aceptar**.

- En Windows PowerShell:

  1. Ejecute Windows PowerShell como administrador.
  2. Ejecute el siguiente comando:

     ```
     Enable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
     ```

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

Si la Consola de la aplicación está abierta mientras usted configura la conexión entre el dispositivo protegido y el dispositivo 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 avp.exe de Kaspersky Embedded Systems Security.
3. Reinicie la consola de la aplicación.

   Se aplicará la nueva configuración de conexión.

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:

1. En el dispositivo remoto donde se encuentra instalada la Consola de Kaspersky Embedded Systems Security, abra la consola de **Servicios de componentes**. Para hacerlo:

   a. Seleccione **Iniciar** → **Ejecutar**.

   b. Ejecute el comando `dcomcnfg`.

   c. Se abre la consola de **Servicios del componente**.
2. Amplíe el nodo **Equipos** en la consola de **Servicios de componentes** en su dispositivo protegido.
3. Abra el menú contextual en el nodo **Mi equipo**.
4. Seleccione **Propiedades**.
5. 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**.
6. 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**.
7. 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:

1. Cierre la Consola de Kaspersky Embedded Systems Security en el dispositivo remoto.
2. Realice una de las siguientes acciones:
   - 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 **Inicio** → **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 aplicación**. 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**).

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 la casilla **Habilitar Protección de archivos en tiempo real después de instalar la aplicación (recomendado)** durante la instalación de Kaspersky Embedded Systems Security, la aplicación analizará los objetos del sistema de archivos del dispositivo cuando acceda a ellos. Si se instaló el componente Supervisión de scripts como parte de la instalación personalizada, Kaspersky Embedded Systems Security analiza el código fuente de todos los scripts cuando se inician. 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 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 dispositivo si no había ningún software antivirus con protección de archivos en tiempo real instalado en el dispositivo antes de la instalación de Kaspersky Embedded Systems Security.

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

Iniciar y configurar la tarea Actualización de bases de datos y módulos de la aplicación

Para actualizar la base de datos de la aplicación después de la instalación:

1. En la tarea Actualización de bases de datos y módulos de la aplicación, configure la conexión al origen de actualizaciones.

2. Inicie la tarea Actualización de bases de datos y módulos de la aplicación.

Es posible que Web Proxy Auto-Discovery Protocol (WPAD) no se pueda 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:

1. Abra el menú contextual del nodo **Kaspersky Embedded Systems Security**.

2. Seleccione **Propiedades de la aplicación**.

3. En la ventana que se abre, seleccione la pestaña **Configuración de red**.

4. En la sección **Configuración del servidor proxy**, haga clic en **Configuración** y, en la ventana que se muestra, marque la casilla **Usar el servidor proxy especificado**.

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:

   - **Autenticación NTLM** si el servidor proxy admite la autenticación NTLM integrada en Microsoft Windows. Kaspersky Embedded Systems Security utilizará la cuenta especificada en la configuración de la tarea para acceder al servidor proxy. De manera predeterminada, la tarea se inicia con la cuenta de usuario del sistema (SYSTEM).

   - **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.

   - **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**.

Para ejecutar la tarea Actualización de bases de datos y módulos de la aplicación:

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 **Inicio**.

   Se inicia la tarea Actualización de bases de datos y módulos de la aplicación.

   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 resultados del nodo **Kaspersky Embedded Systems Security**.

Análisis de áreas críticas

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

Para ejecutar la tarea Análisis de áreas críticas:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Análisis a pedido**.

2. En el menú contextual del nodo secundario **Análisis de áreas críticas**, seleccione el comando **Inicio**.

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

Para ver el registro de tareas,

En el panel de resultados del nodo **Análisis de áreas críticas**, haga clic en el vínculo **Abrir 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 **Panel de control** de Windows, seleccione **Aplicaciones y funciones**. Se abre la ventana **Modificar o eliminar**.
2. Haga clic con el botón secundario en **Kaspersky Embedded Systems Security** y seleccione **Editar**.

   Se abre el asistente de configuración **Modificar, reparar o eliminar la aplicación**.
3. Seleccione **Modificar**.

   Se abre la ventana **Instalación personalizada**. Seleccione **Todas las funcionalidades** y haga clic en **Siguiente >**.
4. 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:
     - **Esta función se instalará en el disco duro local**, si desea instalar un componente;
     - **Esta función y todas las subfunciones se instalarán en el disco duro local**, si desea instalar el grupo de componentes;
   - Para eliminar los componentes instalados previamente, haga clic en el botón situado junto al nombre del componente seleccionado. En el menú contextual, seleccione **Esta función no estará disponible**.

   Haga clic en **Siguiente >**.
5. En la ventana **Preparado para instalar**, confirme la selección de componentes de la aplicación al hacer clic en **Instalar**.
6. Haga clic en el botón **Finalizar** 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 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:

1. En el **Panel de control** de Windows, seleccione **Aplicaciones y funciones**. Se abre la ventana **Modificar o eliminar**.
2. Haga clic con el botón secundario en **Kaspersky Embedded Systems Security** y seleccione **Editar**.
3. Se abre el asistente de configuración **Modificar, reparar o eliminar la aplicación**.
4. Seleccione la opción **Reparar**.

   Se abre la ventana **Reparar Kaspersky Embedded Systems Security**. Haga clic en **Siguiente >**.
5. Espere hasta que se complete la operación de restauración y, en la ventana que se abre, haga clic en **Finalizar**.

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 dispositivo protegido con el Asistente de instalación/desinstalación.

Desinstalación de Kaspersky Embedded Systems Security

Los archivos de volcado y rastreo no se eliminan al desinstalar Kaspersky Embedded Systems Security. Puede eliminar manualmente los archivos de volcado y rastreo de la carpeta especificada durante la configuración de la escritura de los archivos de volcado y rastreo.

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

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

Después de desinstalar Kaspersky Embedded Systems Security de un dispositivo protegido, es posible que deba reiniciarlo. El reinicio se puede posponer.

La desinstalación, reparación e instalación de la aplicación no está disponible a través del Panel de control de Windows.

Kaspersky Embedded Systems Security solicita las credenciales de la cuenta del usuario cuando el usuario intenta eliminar o modificar el conjunto de componentes en el Asistente de instalación. Debe ingresar las credenciales de un usuario con los derechos necesarios. Si se configura una contraseña de Windows vacía para la cuenta de usuario que realiza la eliminación, deshabilite la funcionalidad **Solicitar contraseña para confirmar acciones críticas** antes de iniciar la eliminación.

Para desinstalar Kaspersky Embedded Systems Security.

1. En el **Panel de control** de Windows, seleccione **Aplicaciones y funciones**. Se abre la ventana **Modificar o eliminar**.
2. Haga clic con el botón secundario en **Kaspersky Embedded Systems Security** y seleccione **Editar**.
3. Se abre el asistente de configuración **Modificar, reparar o eliminar la aplicación**.
4. Seleccione **Eliminar**.

   Se abre la ventana **Guardar objetos**.
5. Si es necesario, en la ventana **Guardar objetos**, haga lo siguiente:

   En **Guardar objetos**, especifique los objetos o la configuración que desea conservar. De manera predeterminada, las casillas no están activadas.

   - Seleccione la casilla de verificación **Datos de activación**.
   - Seleccione la casilla de verificación **Archivos de Copias de seguridad**.
   - Seleccione la casilla de verificación **Configuración de operación de la aplicación**.

   En **Exportar objetos**, especifique los objetos que desea exportar. De manera predeterminada, las casillas no están activadas.

   - 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 no está activada.
   - 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 no está activada.
   - Haga clic en el botón **Guardar** y seleccione la carpeta a la cual desea exportar los objetos. De forma predeterminada, los objetos se exportarán a %ProgramData%\Kaspersky Lab\KESS.4.0\QB.

     Haga clic en **Siguiente**.
6. En la ventana **Preparado para desinstalar**, confirme la eliminación al hacer clic en **Eliminar**.
7. Haga clic en el botón **Finalizar** en la ventana que se abre una vez completada la desinstalación.

Kaspersky Embedded Systems Security se desinstalará del dispositivo protegido.

Desinstalación de la Consola de Kaspersky Embedded Systems Security

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

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

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

Para desinstalar la Consola de la aplicación:

1. En el **Panel de control** de Windows, seleccione **Aplicaciones y funciones**. Se abre la ventana **Modificar o eliminar**.
2. Haga clic con el botón secundario en la **Consola de Kaspersky Embedded Systems Security** y seleccione **Editar**.

   Se abre la ventana del asistente **Modificar, reparar o eliminar la aplicación**.
3. Seleccione **Eliminar**.

   Se abre la ventana **Preparado para desinstalar**. Haga clic en **Desinstalar**.
4. Haga clic en el botón **Aceptar** en la ventana que se abre una vez completada la desinstalación.

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.

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

Los archivos de volcado y rastreo no se eliminan al desinstalar Kaspersky Embedded Systems Security. Puede eliminar manualmente los archivos de volcado y rastreo de la carpeta especificada durante la configuración de la escritura de los archivos de volcado y rastreo.

Para instalar o desinstalar Kaspersky Embedded Systems Security para Windows y agregar o eliminar sus componentes, puede ejecutar el archivo de paquete de instalación \exec\ess_win.msi desde la línea de comandos, tras especificar los parámetros de instalación con las respectivas opciones en la línea de comandos.

El conjunto de "Herramientas de administración" puede instalarse en el dispositivo protegido o en otro dispositivo 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 dispositivo protegido en el que se instalará la aplicación.

Si ejecuta el archivo \exec\ess_win.msi en el dispositivo protegido sin especificar ninguna opción adicional en la línea de comandos, Kaspersky Embedded Systems Security se instalará con los parámetros de instalación predeterminados.

Puede asignar el conjunto de componentes que se instalará con la opción de la línea de comandos ADDLOCAL y enumerando los códigos de los componentes o conjuntos de componentes seleccionados.

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

El archivo \product_long_term\ess_win.msi está diseñado para instalar la configuración **Proteger el equipo con la tecnología de denegación predeterminada** de Kaspersky Embedded Systems Security, y el archivo \exec\ess_win.msi file está diseñado para instalar la configuración **Proteger el equipo con bases antivirus** de Kaspersky Embedded Systems Security.

Cuando se selecciona la configuración **Proteger el equipo con bases antivirus"**, de manera predeterminada, se incluyen todos los componentes de Kaspersky Embedded Systems Security, excepto los componentes Firewall y Contadores de rendimiento.

Cuando se instala la configuración **Proteger el equipo con bases antivirus"** de Kaspersky Embedded Systems Security sobre una versión de la aplicación que no depende del análisis de firmas y el uso de bases de datos antivirus para proteger el equipo, el conjunto de componentes de la aplicación se extiende automáticamente con los siguientes componentes:

- Protección de archivos en tiempo real
- Análisis a pedido.
- Protección contra amenazas de red.

Los componentes que habilitan las actualizaciones no se incluyen en la configuración **Proteger el equipo con la tecnología de denegación predeterminada"**.

Si se selecciona la configuración **Proteger el equipo con la tecnología de denegación predeterminada"**, los siguientes componentes se incluyen de manera predeterminada:

- Core
- Prevención de exploits

- Control de inicio de aplicaciones
- Icono de la bandeja del sistema

Cuando se instala la configuración **Proteger el equipo con la tecnología de denegación predeterminada"** de Kaspersky Embedded Systems Security sobre una versión de la aplicación que usa el análisis de firmas y las bases de datos antivirus para proteger el equipo, el conjunto de componentes de la aplicación se reduce automáticamente al eliminar los siguientes componentes:

- Protección de archivos en tiempo real
- Análisis a pedido.
- los componentes que permiten actualizaciones

Esta configuración se recomienda para proteger dispositivos con recursos limitados. En este caso, puede activar la aplicación a largo plazo y el componente Control de inicio de aplicaciones proporciona protección al equipo.

El archivo \console\esstools.msi instala todos los componentes de software que forman parte de las 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.

Componentes de software de Kaspersky Embedded Systems Security

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

Descripción de los componentes del software de Kaspersky Embedded Systems Security

Componente	Código	Funciones del componente
Protección de archivos en tiempo real	`FileThreatProtection`	Este componente realiza análisis de virus en archivos en el dispositivo protegido cuando se accede a estos archivos.
Escáner AMSI	`AMSI`	Este componente está diseñado para admitir la interfaz de análisis antimalware de Microsoft. La interfaz de análisis antimalware AMSI permite que las aplicaciones de terceros envíen a Kaspersky Embedded Systems Security aquellos objetos que precisan analizar (por ejemplo, scripts de PowerShell). Una vez que el análisis se completa, el resultado se devuelve a la aplicación que originó la solicitud.
Detección de comportamiento	`BehaviorDetection`	Este componente completa la lista de hosts bloqueados con los nombres de los dispositivos remotos que muestran actividades maliciosas.
Prevención de exploits	`ExploitPrevention`	Este componente permite administrar la configuración para proteger la memoria que utilizan los procesos en la memoria de un dispositivo.
Motor de reparación	`RemediationEngine`	Este componente permite a Kaspersky Embedded Systems Security deshacer acciones realizadas por el malware en el sistema operativo.
Firewall	`Firewall`	Este componente permite administrar el firewall de Windows a través de la interfaz gráfica de usuario de Kaspersky Embedded Systems Security.
Protección contra amenazas de red	`NetworkThreatProtection`	Este componente analiza el tráfico de red entrante en busca de actividad típica de los ataques de red. Al detectar un intento de ataque de red que apunta a su equipo, Kaspersky Embedded Systems Security bloquea la actividad de red del equipo atacante.
Control de inicio de aplicaciones	`ApplicationControl`	Este componente supervisa los intentos del usuario de iniciar aplicaciones y permite o deniega el inicio de aplicaciones de acuerdo con las reglas especificadas de Control de inicio de aplicaciones.

Componente	Código	Funciones del componente
Control de dispositivos	`DeviceControl`	Este componente rastrea los intentos de conectar dispositivos externos a un dispositivo protegido y permite o deniega el uso de estos de acuerdo con las reglas especificadas de Control de dispositivos.
Módulo de integración con el Agente de red de Kaspersky Security Center	`AdminKitConnector`	Este componente brinda una conexión entre Kaspersky Embedded Systems Security para Windows y el Agente de red de Kaspersky Security Center. Puede instalar este componente en el dispositivo protegido si planea 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.
Control de integridad del sistema	`SystemIntegrityMonitor`	Este componente incluye todas las funciones de Monitor de integridad de archivos y, además, permite supervisar los cambios del registro y la conexión de los dispositivos externos.
Prevención de ataques BadUSB	`BadUSBAttackPrevention`	El componente impide que los dispositivos USB infectados que emulan un teclado se conecten al equipo.
Managed Detection and Response	`MDR`	El componente facilita la interacción con la solución Kaspersky Managed Detection and Response.

Componentes de software “Herramientas de administración”

La siguiente tabla contiene código y la descripción del componente de software de las "Herramientas de administración".

Descripción del componente de software "Herramientas de administración"

Componente	Código	Funciones del componente
Componente de Kaspersky Embedded Systems Security	MmcSnapin	Este componente instala el complemento Microsoft Management Console para administrar la aplicación mediante la Consola de Kaspersky Embedded Systems Security. MmcSnapin se instala automáticamente; no es necesario indicarlo en los parámetros del comando de instalación.

Ajustes de instalación y recuperación y opciones de línea de comandos de Windows Installer

Esta sección describe la configuración de instalación y recuperación de Kaspersky Embedded Systems Security. También se enumeran las claves con las que se pueden cambiar las opciones de instalación y los valores que puede tener cada una. 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 línea de comandos de Windows Installer

- Aceptación de los términos del Contrato de licencia de usuario final.

  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.

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.

- Instalar Kaspersky Embedded Systems Security y conservar la configuración de la versión anterior durante la actualización.

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

  - `0`: durante la actualización, se transferirán a la nueva versión todos los datos de la versión anterior (valor predeterminado).
  - `1`: durante la actualización, se migrará a la nueva versión únicamente el archivo que contiene los datos de activación y las claves privadas ([unidad]:\ProgramData\Kaspersky Lab\<producto>\<versión>\Data\product.dat). Se eliminarán todos los demás datos de la versión anterior, incluidos los ajustes, las bases de datos antivirus, los informes, los objetos en cuarentena y los objetos de copia de seguridad.

- Instalar Kaspersky Embedded Systems Security y conservar los informes de la versiones anteriores durante la actualización.

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

  - `0`: durante la actualización, se migrarán a la nueva versión todos los datos de la versión anterior, excepto los informes ([unidad]:\ProgramData\Kaspersky Lab\<producto>\<versión>\Reports). Los informes se eliminarán.
  - `1`: durante la actualización, se migrarán a la nueva versión todos los datos de la versión anterior, incluidos los ajustes, las bases de datos antivirus, los informes, los objetos en cuarentena y los objetos de copia de seguridad (valor predeterminado).

- 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 de la carpeta >` son los siguientes:

  - Para la versión de 32 bits de Microsoft Windows:
    - Kaspersky Embedded Systems Security: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security.4.0.0
    - Consola de Kaspersky Embedded Systems Security: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools.4.0.0
  - Para la versión de 64 bits de Microsoft Windows: %ProgramFiles(x86)% y de manera similar a las rutas para las versiones de 32 bits de Microsoft Windows.

- Iniciar la tarea Protección de archivos en tiempo real inmediatamente después de que se inicie Kaspersky Embedded Systems Security.

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

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

- Ruta de acceso al archivo de clave (`LICENSEKEYPATH`). De forma predeterminada, Windows Installer busca el archivo con la extensión .key en la carpeta \exec del kit de distribución. Si la carpeta \exec contiene más de un archivo de clave, Windows Installer selecciona el archivo de clave con la fecha de caducidad más lejana en el futuro. Puede guardar de antemano el archivo de clave en la carpeta \exec o en cualquier otra ruta que especifique mediante el parámetro `LICENSEKEYPATH`.

  `LICENSEKEYPATH` puede tener los valores siguientes:

  - Ruta completa al archivo de clave, incluido su nombre.
  - Ruta a la carpeta en la que se almacenan los archivos de 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 >`.

- Modo *Análisis al inicio del sistema operativo* (SCANSTARTUP_BLOCKING). Si Kaspersky Embedded Systems Security se instaló sin una clave SCANSTARTUP_BLOCKING, el parámetro **Alcance del análisis** de la tarea *Análisis al inicio del sistema operativo* se configurará de la siguiente manera:

  - Acción que se realizará con los objetos infectados y otros objetos: **Informar**.
  - Acción que se realizará con los objetos probablemente infectados: **Informar**.

  Si Kaspersky Embedded Systems Security se instaló con una clave SCANSTARTUP_BLOCKING, el parámetro **Alcance del análisis** de la tarea *Análisis al inicio del sistema operativo* se configurará de la siguiente manera:

  - Acción que se realizará con los objetos infectados y otros objetos: **Realizar la acción recomendada**.
  - Acción que se realizará con los objetos probablemente infectados: **Realizar la acción recomendada**.

  La tarea *Análisis al inicio del sistema operativo* se crea automáticamente. El **Informar** modo está aplicado de manera predeterminada. En este caso, después de implementar Kaspersky Embedded Systems Security en los dispositivos, puede habilitar la tarea *Análisis al inicio del sistema operativo* si no se descubrieron problemas con los servicios del sistema durante el análisis. Si la aplicación detecta servicios críticos del sistema como objetos infectados o probablemente infectados, el modo **Informar** le da tiempo para averiguar el motivo y resolver el problema. Si la aplicación aplica el modo **Realizar la acción recomendada**, se realiza la acción **Desinfectar; eliminar si falla la desinfección**. Desinfectar o eliminar archivos del sistema puede provocar problemas críticos en el inicio del sistema operativo.

- Deshabilitación de la verificación de software incompatible. Utilice esta configuración para habilitar o deshabilitar la verificación de software incompatible durante la instalación en segundo plano de la aplicación en el dispositivo protegido. Independientemente del valor de esta configuración, durante la instalación de Kaspersky Embedded Systems Security, la aplicación siempre advierte sobre otras versiones de la aplicación instaladas en el dispositivo protegido.

  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.

- Deshabilitar la verificación para la actualización del sistema operativo KB5007186.

  Después de instalar la actualización KB5007186, la aplicación sigue funcionando normalmente, la seguridad del sistema no está en riesgo, pero resulta imposible instalar actualizaciones menores de las aplicaciones. Antes de instalar la aplicación, el instalador verifica las actualizaciones del sistema operativo instaladas. Si se detecta la actualización KB5007186, el instalador anula la instalación. Puede usar la clave `SKIPKB5007186CHECK` en la línea de comandos a fin de habilitar o deshabilitar la verificación para la actualización del sistema operativo KB5007186.

  Los valores posibles para la opción de la línea de comandos `SKIPKB5007186CHECK=< valor >` son los siguientes:

  - `0`: El instalador verifica si se instaló la actualización del sistema operativo KB5007186.
  - `1`: El instalador no verifica si se instaló la actualización del sistema operativo KB5007186.

  De manera predeterminada, no se establece la clave, que corresponde a 0.

- Configurar la funcionalidad de protección de los servicios del sistema operativo.

  Si se habilita esta función, las aplicaciones de terceros no pueden actuar sobre los procesos del sistema operativo. Los valores posibles para la opción de la línea de comandos `PROTECTOSSERVICES=< valor >` son los siguientes:

  - `1` significa que la protección de los servicios del sistema operativo está habilitada (valor predeterminado).
  - `0` significa que la protección de los servicios del sistema operativo está deshabilitada.

- Configuración de los puertos usados para la conexión remota de la Consola de la aplicación al equipo en el que está instalada la aplicación:

  Para configurar el puerto para conectarse con las credenciales de Windows, puede usar el parámetro `UIPORT=< número de puerto >`. Intervalo de posibles números de puerto: 1-65535. Si el número está fuera del intervalo especificado, se usa el número de puerto predeterminado. El valor predeterminado es 13032.

  Si es necesario, puede cerrar el puerto para conectarse con las credenciales de los usuarios creados manualmente usando el parámetro `ENABLEUIKLPORT=< valor >`:

  - `1` abre el puerto (valor predeterminado).
  - `0` cierra el puerto.

  El valor predeterminado para este puerto es 13031. Puede cambiar el número de puerto especificando el parámetro `UIKLPORT=< valor >`. El intervalo de posibles números de puerto es 1-65535.

- Configuración para habilitar las conexiones de red para la administración remota de Kaspersky Embedded Systems Security usando la Consola de la aplicación instalada en un equipo diferente.

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

- `1`. Si se especifica este valor, los puertos TCP configurados para la conexión remota de la Consola de la aplicación a un equipo con la aplicación instalada (los parámetros `UIPORT=< valor >` y `UIKLPORT= < valor >`) se abren en el Firewall de Windows y se permiten conexiones de red para el archivo ejecutable del proceso de administración remota de Kaspersky Embedded Systems Security, avp.exe.

  Obtenga información también sobre la configuración adicional al instalar la aplicación en otro dispositivo.

- `0`. Si se especifica este valor, no ocurre nada.

Configuración de recuperación y opciones de línea de comandos de 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 \QB.

- 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 \QB.

- Ingrese la contraseña actual para confirmar la restauración (si la protección con contraseña está habilitada).

  No está especificado el valor predeterminado de `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 de la carpeta >` es %ALLUSERSPROFILE%\Program Data\Kaspersky Lab\KESS.4.0.0\QB\Restored

Comandos de ejemplo para la instalación de Kaspersky Embedded Systems Security

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

Ejecute el archivo ess_win.msi desde el kit de distribución en el dispositivo protegido.

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_ess.exesetup_ess.exe

Para instalar Kaspersky Embedded Systems Security con la configuración de instalación recomendada y sin la participación del usuario:

```
\exec\setup_ess.exe EULA=1 PRIVACYPOLICY=1
```

Para instalar componentes como Control de dispositivos:

```
\exec\setup_ess.exe /p ADDLOCAL=DevCtrl /p RUNRTP=0 /p ADDMSEXCLUSION=0
```

Si necesita instalar Kaspersky Embedded Systems Security en equipos con dispositivos de red o dispositivos SCSI que ocasionan un bloqueo del sistema tras la instalación, puede usar las siguientes opciones adicionales con este comando:

```
/p SKIP_NETWORK_UPPERFILTERS=<1|0>
```

Habilita (`1`) o deshabilita (`0`) la interceptación de conexiones de adaptadores de red.

```
/p SKIP_SCSIADAPTER_UPPERFILTERS=<1|0>
```

Habilita (`1`) o deshabilita (`0`) la interceptación de conexiones de adaptadores SCSI.

Para instalar y activar Kaspersky Embedded Systems Security utilizando el archivo de clave:

```
setup_ess.exe /s EULA=1 PRIVACYPOLICY=1 /p LICENSEKEYPATH=C:\0000000A.key
```

Para cambiar el puerto usado para la conexión remota de la Consola de la aplicación al equipo en el que está instalada la aplicación con credenciales de usuario de Windows:

```
setup_ess.exe /pUIPORT=<número de puerto>
```

Intervalo de posibles números de puerto: 1-65535. El valor predeterminado es 13032.

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

Para instalar Kaspersky Embedded Systems Security con la configuración de instalación recomendada y sin la participación del usuario:

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

Para instalar Kaspersky Embedded Systems Security con los parámetros de instalación recomendados y mostrar la interfaz de instalación:

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

Para instalar Kaspersky Embedded Systems Security con las opciones de instalación recomendadas y habilitar la rotación de archivos de seguimiento cuando el número de archivos de seguimiento alcance el número máximo especificado:

```
msiexec /i ess_win.msi TRACE_FOLDER=C:\Traces TRACE_MAX_ROLL_COUNT=50 /qn EULA=1
PRIVACYPOLICY=1
```

El parámetro `TRACE_FOLDER` es obligatorio.

El parámetro `TRACE_MAX_ROLL_COUNT` está sujeto a las siguientes reglas:

- Si especifica este parámetro, se habilitará la rotación de archivos de seguimiento cuando el número de archivos de seguimiento alcance el número máximo definido en el parámetro. Intervalo de valores posible para el parámetro: de 1 a 999.

- Si se indica 0 como número máximo de archivos de seguimiento, la rotación de archivos de seguimiento quedará deshabilitada.

- Si se indica un valor para el parámetro, pero dicho valor no es válido o no pertenece al intervalo de valores posibles (de 1 a 999), se habilitará la rotación de archivos de seguimiento con el número máximo predeterminado (5 archivos de seguimiento).

- Si no se especifica este parámetro, ocurrirá lo siguiente:

  - Si la rotación de archivos de seguimiento ya se encuentra configurada en el dispositivo, la configuración no se modificará. La aplicación ignorará los parámetros ingresados.

  - Si la rotación de archivos de seguimiento no está configurada en el dispositivo, se habilitará la opción de rotación con el número máximo predeterminado (5 archivos de seguimiento).

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

```
msiexec /i ess_win.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:

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

Para instalar Kaspersky Embedded Systems Security en la carpeta de instalación C:\KESS:

```
msiexec /i ess_win.msi INSTALLDIR=C:\KESS/qn EULA=1 PRIVACYPOLICY=1
```

Para instalar Kaspersky Embedded Systems Security y guardar un archivo llamado ess.log con el registro de la instalación en la carpeta donde se encuentra el archivo msi de Kaspersky Embedded Systems Security:

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

Para instalar la Consola de Kaspersky Embedded Systems Security:

```
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:

```
msiexec /i ess_win.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:

```
msiexec /p "<nombre del archivo msp con ruta>" UNLOCK_PASSWORD=<contraseña>
```

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 la casilla **Habilitar Protección de archivos en tiempo real después de instalar la aplicación (recomendado)** durante la instalación de Kaspersky Embedded Systems Security, la aplicación analizará los objetos del sistema de archivos del dispositivo cuando acceda a ellos. Si se instaló el componente Supervisión de scripts como parte de la instalación personalizada, Kaspersky Embedded Systems Security analiza el código fuente de todos los scripts cuando se inician. 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 que actualice 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 iniciar la tarea Actualización de bases de datos 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. La conexión a un origen de actualizaciones se establece a través de un servidor proxy (dirección del servidor proxy: proxy.company.com, puerto: 8080) y utiliza la autenticación NTLM incorporada de Windows para acceder al servidor con una cuenta (nombre de usuario: inetuser; contraseña: 123456).

- Realice un Análisis de áreas críticas del dispositivo si no había ningún software antivirus con protección de archivos en tiempo real instalado en el dispositivo antes de la instalación de Kaspersky Embedded Systems Security.

Para iniciar la tarea Análisis de áreas críticas desde 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

Para instalar el componente Análisis a pedido, ejecute el siguiente comando:

```
msiexec /i ess_win.msi ADDLOCAL=Oas,Ods /qn
```

o

```
\exec\setup_ess.exe /s /p ADDLOCAL=Oas,Ods
```

Después de agregar los componentes a la lista, Kaspersky Embedded Systems Security reinstala los componentes existentes e instala los componentes especificados.

Para eliminar los componentes instalados, ejecute el siguiente comando:

```
msiexec /i ess_win.msi REMOVE=Firewall,PerfMonCounters EULA=1 PRIVACYPOLICY=1 /qn
```

Para instalar nuevos componentes, ejecute el siguiente comando:

```
msiexec /i ess_win.msi
ADDLOCAL=AKIntegration,AVProtection,AntiExploit,AppCtrl,DevCtrl,Fim,Ksn,LogInspector,Oas
EULA=1 PRIVACYPOLICY=1 /qn
```

Una vez que haya enumerado los componentes que desee instalar y eliminar, Kaspersky Embedded Systems Security para Windows instalará y eliminará los componentes correspondientes.

Desinstalación de Kaspersky Embedded Systems Security. Comandos de ejemplo

Para desinstalar Kaspersky Embedded Systems Security desde el dispositivo protegido en modo No Molestar, ejecute el siguiente comando:

```
msiexec /x ess_win.msi KLLOGIN=<user name> KLPASSWD=<password> /qn
```

o

```
msiexec /x {70579418-34B7-49A8-A1EB-CF309F4D032B} KLLOGIN=<user name> KLPASSWD=<password>
/qn
```

o

```
setup_ess.exe /pKLLOGIN=<user name> /pKLPASSWD=<password> /s /x
```

donde `<user name>` es el nombre y el nombre de usuario de un usuario con suficientes derechos para desinstalar.

Si se configura una contraseña de Windows vacía para la cuenta de usuario que realiza la eliminación, deshabilite la funcionalidad **Solicitar contraseña para confirmar acciones críticas** antes de iniciar la eliminación.

Para desinstalar la Consola de Kaspersky Embedded Systems Security en modo No Molestar, ejecute el siguiente comando:

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

o

```
msiexec /x {D66EC1A9-A456-46FF-8B49-308A23FEBF88} /qn
```

Códigos de devolución

El instalador de la aplicación puede devolver los códigos de retorno descritos en este articulo.

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

Códigos de devolución

Código	Descripción
27100	Se detectaron en el equipo unidades con el Agente de autenticación instalado en el modo de prueba.
27101	Se detectaron en el equipo unidades con el Agente de autenticación instalado en el modo de prueba.
27102	No se pudieron encontrar discos cifrados.
27200	No se pudo descargar la aplicación de la RAM.
27201	Se produjo un error al iniciar el proceso AVP.exe. Es posible que el equipo esté infectado.
27204	No se pudo almacenar en caché el paquete distributivo.
27205	No se pudo migrar la información de la licencia.
27206	No se pudo eliminar la información de la licencia.
27207	No se pudo eliminar el software incompatible.
27208	No se pudo comprobar el software incompatible.
27209	No se pudieron extraer los archivos del gabinete.
27210	No se pudo configurar la Autoprotección.
27211	No se pudo habilitar la Autoprotección.
27212	No se pudo obtener información de la versión del sistema operativo.
27213	No se pudo obtener el directorio de inicio.
27214	No se pudo verificar el directorio de instalación.
27215	No se pudo configurar el servicio.
27216	No se pudo configurar la actualización de klcp.
27217	No se pudo actualizar klcp.
27218	No se pudieron configurar los parámetros del controlador kl1.
27219	No se pudieron configurar los parámetros del controlador klelam.
27220	No se pudieron configurar los parámetros del controlador klwfp.
27221	No se pudo configurar el modo de compatibilidad del controlador.
27222	No se pudo eliminar la clave del registro.
27223	No se pudo reiniciar el sistema operativo.
27224	No se pudo instalar el controlador.
27225	No se pudo migrar la configuración del controlador.
27226	No se pudo detener el controlador.
27227	No se pudo bloquear el inicio del controlador.
27228	No se pudo verificar la firma del archivo.
27230	No se pudo preparar la configuración del controlador kldl.
27231	No se pudo configurar el controlador kldl.
27300	Se produjo un error al instalar el controlador.

Código	Descripción
27301	Se produjo un error al eliminar el controlador.
27302	Se produjo un error al instalar componentes de red.
27303	La información de registro del controlador no es consistente o está incompleta. Reinicie el sistema operativo y vuelva a intentarlo.
27305	Se produjo un error al deshabilitar el controlador.
27310	No se pudo instalar el archivo de catálogo firmado digitalmente.
27311	No se pudo desinstalar el archivo de catálogo firmado digitalmente.
27312	No se pudieron instalar los certificados.
27313	No se pudieron eliminar los certificados.
27320	No se pudo configurar el servicio.
27321	No se pudo quitar la protección del servicio.
27350	El parche <nombre del parche> no está diseñado para la localización de la aplicación <nombre de la aplicación>.
27352	No se puede eliminar el parche de cifrado de disco completo.
27353	El parche <nombre del parche 1> solo se puede instalar junto con el parche <nombre del parche 2>.
27354	El equipo debe reiniciarse para aplicar los parches antes de que modificar o restaurar la aplicación.
27355	No se pudo bloquear la administración de Cifrado de disco completo. No se pudo bloquear la administración de Cifrado de disco completo. Debe finalizar el cifrado para instalar una actualización de Cifrado de disco completo.
27356	No se puede instalar el parche.
27357	Se encontraron parches recuperados en el paquete de instalación. Se anulará la instalación.
27360	No se puede registrar el parche.
27361	No se pudieron establecer los parámetros de instalación del parche.
27363	El parche contiene bibliotecas de cifrado incompatibles con las bibliotecas de cifrado instaladas.
27370	Se produjo un error al iniciar la descompresión de .NET 8.0.
27371	Se produjo un error al descomprimir .NET 8.0.
27372	Se eliminó la información de registro sobre la versión anterior de la aplicación. Reinicie la instalación.
27373	No se pudo eliminar la información de registro sobre la versión anterior de la aplicación.
27374	La aplicación se está actualizando. Vuelva a intentarlo más tarde.
27375	El nombre de usuario o la contraseña de desinstalación no se especificaron o no son correctos.
27376	No se pudo desinstalar Kaspersky Endpoint Agent. Desinstálelo usted mismo o deshabilite la protección con contraseña en la configuración. Luego reinicie la instalación de la aplicación.
27377	No se pudo desinstalar Kaspersky Security for Windows Server. Desinstálelo usted mismo o deshabilite la protección con contraseña en la configuración. Luego reinicie la instalación de la aplicación.
27378	No hay espacio suficiente en disco.
27379	No se pudo instalar la aplicación porque se seleccionaron los componentes incompatibles. Cambie el conjunto de componentes y reinicie la instalación.
27380	Se seleccionó un archivo de configuración no válido.
27381	Se seleccionó una clave de licencia no válida.
27382	Se produjo un error al crear el grupo de administración de aplicaciones.
27383	Seleccionó una carpeta no válida. El nombre de la carpeta de destino no puede superar los 160 caracteres.
27384	Seleccionó una carpeta o unidad no válida. La aplicación debe estar instalada en un disco duro local.
27385	Seleccionó una carpeta no válida. La aplicación no se puede instalar en la carpeta raíz.
27386	Seleccionó una carpeta no válida. La aplicación no se puede instalar en la carpeta de Windows o las subcarpetas.
27387	Seleccionó una carpeta no válida. La aplicación no se puede instalar en una carpeta que contenga una subcarpeta Temp.
27388	Seleccionó una carpeta no válida. La aplicación no se puede instalar directamente en la carpeta Archivos de programa.

Código	Descripción
27389	Seleccionó una carpeta no válida. La aplicación no se puede instalar en un disco virtual.
27390	Seleccionó una carpeta o unidad no válida. La aplicación no se puede instalar en la carpeta donde está instalada la versión anterior de la aplicación.
27391	La carpeta o unidad seleccionada ya contiene archivos. La aplicación no se puede instalar en una carpeta que contenga otros datos, ya que estos datos pueden dejar de estar disponibles una vez que se habilita la Autoprotección.
27392	La aplicación no se puede instalar en una carpeta que contenga puntos de reanálisis. Seleccione otra carpeta de instalación.
27393	La aplicación no se puede instalar en una carpeta que contenga un punto y coma (;) en su nombre. Seleccione otra carpeta de instalación.
27394	Seleccionó una carpeta no válida. No se puede especificar la carpeta raíz.
27395	Seleccionó una carpeta no válida. No se puede especificar la carpeta de Windows o las subcarpetas.
27396	Seleccionó una carpeta no válida. No se puede especificar directamente la carpeta Archivos de programa.
27397	Seleccionó una carpeta no válida. No se puede especificar una carpeta que contenga una subcarpeta Temp.
27400	Se produjo un error al inicializar las actualizaciones de archivos.
27450	No se pudo instalar el archivo CAB.
27451	Se produjo un error al eliminar.
27452	Se produjo un error al eliminar archivos.
27453	Se produjo un error al mover archivos.
27454	No se pudieron crear los archivos de registro.
27455	No se pudo obtener información de la versión del sistema operativo.
27456	No se pudieron programar los valores del registro de reversión.
27457	No se pudieron obtener identificadores de seguridad (SID) conocidos.
27460	Se produjo un error al crear descriptores de seguridad.
27461	Se produjo un error al restaurar descriptores de seguridad.
27462	No se pudieron crear reglas para el Firewall de Microsoft Windows.
27463	No se pudieron eliminar reglas del Firewall de Microsoft Windows.

Instalación y desinstalación de la aplicación mediante Kaspersky Security Center

En esta sección, encontrará información sobre la instalación de Kaspersky Embedded Systems Security a través de Kaspersky Security Center, una descripción del procedimiento para instalar y desinstalar Kaspersky Embedded Systems Security a través de Kaspersky Security Center y una descripción de las acciones que se deben realizar cuando concluye la instalación de Kaspersky Embedded Systems Security.

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 dispositivos protegidos.

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

Puede crear una tarea que instale Kaspersky Embedded Systems Security de forma remota en un grupo de dispositivos protegidos que no pertenecen al mismo grupo de administración. Al crear esta tarea, debe generar una lista de los dispositivos protegidos 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 dispositivos 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 dispositivos protegidos en los que se instalará Kaspersky Embedded Systems Security (independientemente del dominio en que estén los dispositivos protegidos o si pertenecen a alguno).

  > Si el Agente de red todavía no está instalado en los dispositivos protegidos, 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 dispositivos protegidos.

- Todos los dispositivos protegidos en los que desea instalar Kaspersky Embedded Systems Security pertenecen al mismo dominio que el Servidor de administración, y el Servidor de administración se ha registrado como cuenta de **Administrador de dominio** (si esta cuenta dispone de derechos de administrador local en los dispositivos protegidos 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 dispositivos protegidos bajo el modo de instalación/desinstalación forzada, la cuenta debe disponer de los siguientes derechos en el dispositivo protegido:

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

Los dispositivos 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 utilizando una tarea de instalación remota de Kaspersky Security Center:

1. Abra la Consola de administración de Kaspersky Security Center.
2. En la Consola de administración de Kaspersky Security Center, expanda el nodo **Avanzado**.
3. Expanda el nodo secundario **Instalación remota**.
4. En el panel de resultados del nodo secundario **Paquetes de instalación**, haga clic en el botón **Crear paquete de instalación**.
5. Seleccione la opción **Crear un paquete de instalación para una aplicación de Kaspersky**.
6. Ingrese el nombre del nuevo paquete de instalación.
7. Elija el archivo ess_win.kud del kit de distribución de Kaspersky Embedded Systems Security como archivo del paquete de instalación.

   Si tiene la intención de instalar la aplicación mediante la configuración de **Proteger el equipo con bases antivirus"** sobre la configuración de la aplicación que no utiliza el análisis de firmas ni las bases de datos antivirus para proteger el equipo, o viceversa, primero debe especificar el nombre de usuario y la contraseña de la cuenta que tiene permisos para instalar la aplicación en el archivo ess_win.kud. Para ello, abra el archivo ess_win.kud en un editor de texto y agregue los siguientes parámetros en la línea `Params: /pKLLOGIN=<nombre de usuario>` y `/pKLPASSWD=<contraseña>.`

   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, marque las casillas **Confirmo que he leído y que comprendo y acepto en su totalidad los términos y las condiciones de este Contrato de licencia de usuario final** y **Entiendo y acepto que mis datos se manipularán y transmitirán (incluso a otros países) conforme se describe en la Política de privacidad. Confirmo que he leído completamente y entiendo la Política de privacidad**.

   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 y las opciones de instalación predeterminadas en el paquete de instalación:

   a. En la Consola de administración de Kaspersky Security Center, expanda el nodo **Instalación remota**.

   b. En el panel de resultados 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>**, abra la sección **Configuración**.

   d. Seleccione el tipo de instalación.

   e. Especifique la lista de exclusiones para sistemas industriales al hacer clic en el botón **Configurar**.

   f. En la sección **Selección de componentes**, seleccione las casillas situadas junto a los nombres de los componentes de Kaspersky Embedded Systems Security que quiera instalar.

   g. En la sección **Modo Protección de archivos en tiempo real**, seleccione la casilla de verificación **Habilitar Protección de archivos en tiempo real después de instalar la aplicación (recomendado)** y especifique el nivel de seguridad.

   h. Si es necesario, cambie los números de puertos TCP que usa la Consola de la aplicación para la conexión remota al equipo con la aplicación instalada.

      El número de puerto predeterminado para la conexión con las credenciales de Windows es 13032. El número de puerto predeterminado para la conexión con las credenciales de los usuarios creados manualmente es 13031. Intervalo de posibles números de puerto: 1-65535.

      Para evitar la conexión con las credenciales de cuentas de usuario creadas manualmente, borre la casilla de verificación **Utilizando credenciales de usuarios creados manualmente**.

   i. Para indicar una carpeta de instalación que no sea la predeterminada, especifique el nombre y la ruta de la carpeta en la sección **Configurar rutas de instalación de aplicaciones** al hacer clic en el botón **Configuración**.

   j. Especifique el archivo de configuración si corresponde.

   k. Guarde los cambios.

10. En el nodo **Paquetes de instalación**, cree una tarea para instalar Kaspersky Embedded Systems Security de forma remota en los dispositivos protegidos 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 dispositivos protegidos 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 dispositivos y realice un Análisis de áreas críticas de los dispositivos en caso de que estos no hayan tenido instaladas aplicaciones antivirus con protección en tiempo real habilitada antes de la instalación de Kaspersky Embedded Systems Security.

Si los dispositivos protegidos 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 dispositivos protegidos 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 Análisis a pedido con el estado *Análisis de áreas críticas*. Kaspersky Security Center evalúa el estado de seguridad de cada uno de los dispositivos protegidos del grupo de acuerdo con los resultados de esta tarea, no en función de los resultados de la tarea *Análisis de áreas críticas*.

3. Cree una nueva directiva para el grupo de dispositivos protegidos. En las propiedades de la directiva, en la sección **Configuración de la aplicación**, desactive el inicio programado de las tareas locales de análisis a pedido del sistema y actualización de bases de datos en los dispositivos protegidos del grupo de administración en la configuración de la subsección **Ejecutar tareas locales 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. Cree un paquete de instalación:

   a. En el panel de resultados del nodo secundario **Paquetes de instalación**, haga clic en el botón **Crear paquete de instalación**.

   b. En la ventana **Asistente de paquete nuevo**, seleccione **Crear un paquete de instalación para el archivo ejecutable especificado** como un tipo de paquete.

   c. Ingrese el nombre del nuevo paquete de instalación.

d. Seleccione el archivo \client\setup_esstool.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**.

e. En el campo **Configuración de ejecución de archivos ejecutables (opcional)**, especifique los valores del parámetro EULA=1 y PRIVACYPOLICY=1. De lo contrario, es imposible instalar componentes.

```
/s /p "EULA=1 PRIVACYPOLICY=1"
```

f. De ser necesario, en el campo **Configuración de inicio del archivo ejecutable (opcional)**, puede definir el parámetro de línea de comandos ADDLOCAL para modificar el conjunto de componentes que se instalarán y el parámetro de línea de comandos INSTALLDIR para indicar una carpeta de destino distinta de la predeterminada. Por ejemplo, para realizar una instalación independiente de la Consola de la aplicación en la carpeta C:\KasperskyConsole, use la siguiente opción de línea de comandos:

```
/s /p "INSTALLDIR=C:\KasperskyConsole EULA=1 PRIVACYPOLICY=1"
```

4. En el nodo secundario **Paquetes de instalación**, cree una tarea para instalar la Consola de la aplicación de forma remota en los dispositivos protegidos seleccionados (grupo de administración).

5. 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.

6. Ejecute la tarea de instalación remota.

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

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

Los archivos de volcado y rastreo no se eliminan al desinstalar Kaspersky Embedded Systems Security. Puede eliminar manualmente los archivos de volcado y rastreo de la carpeta especificada durante la configuración de la escritura de los archivos de volcado y rastreo.

Si la administración de Kaspersky Embedded Systems Security en dispositivos 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 de los dispositivos en los cuales la contraseña introducida se corresponda con el valor establecido. Kaspersky Embedded Systems Security no se desinstalará de los otros dispositivos protegidos.

Para desinstalar Kaspersky Embedded Systems Security.

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 dispositivos protegidos. Kaspersky Embedded Systems Security solo puede desinstalarse con la configuración de desinstalación predeterminada.

Cambiar el conjunto de componentes de la aplicación con Kaspersky Security Center

Para cambiar el conjunto de componentes de Kaspersky Embedded Systems Security después de instalar la aplicación, puede usar la tarea *Cambiar componentes de la aplicación*.

Cómo modificar el conjunto de componentes de la aplicación en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Nueva tarea**.

Se inicia el Asistente de tareas. Siga las instrucciones del Asistente.

Paso 1. Selección del tipo de tarea

Seleccione **Kaspersky Embedded Systems Security para Windows (4.0)** → **Cambiar componentes de la aplicación**.

Paso 2. Configuración de la tarea para cambiar los componentes de la aplicación

Seleccione los componentes que estarán disponibles en el equipo del usuario. Defina la configuración avanzada para la tarea (consulte la tabla a continuación).

Paso 3. Selección de los dispositivos a los que se asignará la tarea

Seleccione los equipos en los que se ejecutará la tarea. Las siguientes opciones están disponibles:

- Asignar la tarea a un grupo de administración. En este caso, la tarea se asigna a los equipos incluidos en un grupo de administración creado anteriormente.
- Seleccione los equipos no detectados por el Servidor de Administración en la red - *dispositivos no asignados*. Los dispositivos específicos pueden incluir dispositivos en grupos de administración, así como dispositivos no asignados.
- Especifique direcciones de dispositivo manualmente o importe direcciones de una lista. Puede especificar los nombres NetBIOS, las direcciones IP y las subredes IP de los dispositivos a los que desea asignar la tarea.

Paso 4. Programación de la tarea

Programe la ejecución de la tarea. La tarea puede iniciarse manualmente o cuando el equipo está inactivo, por ejemplo.

Paso 5. Nombre de la tarea

Escriba el nombre que se le dará a la tarea, por ejemplo *Agregar el componente Control de aplicaciones*.

Paso 6. Completar creación de la tarea

Complete el asistente. Si es necesario, seleccione la casilla **Ejecutar la tarea al finalizar el asistente**. Podrá ver el progreso de la tarea en las propiedades de la misma.

Cómo cambiar el conjunto de componentes de la aplicación en Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Tareas**.
   Se abre la lista de tareas.
2. Haga clic en **Agregar**.

Se inicia el Asistente de tareas. Siga las instrucciones del Asistente.

Paso 1. Configuración de los parámetros generales de una tarea

Configure los parámetros generales de la tarea:

1. En la lista desplegable **Aplicación**, seleccione **Kaspersky Embedded Systems Security 4.0.0**.
2. En la lista desplegable **Tipo de tarea**, seleccione **Cambiar componentes de Kaspersky Embedded Systems Security**.
3. En el campo **Nombre de la tarea**, escriba una descripción breve (por ejemplo, *Agregar el componente Control de aplicaciones*).
4. En el bloque **Dispositivos a los que se asignará la tarea**, seleccione el alcance de la tarea.

Paso 2. Selección de los dispositivos a los que se asignará la tarea

Seleccione los equipos en los que se ejecutará la tarea. Por ejemplo, seleccione un grupo de administración separado o cree una selección.

Paso 3. Completar creación de la tarea

1. Seleccione la casilla de verificación **Abrir los detalles de la tarea cuando se complete la creación** y finalice el asistente.
2. En Propiedades de la tarea, seleccione la pestaña **Configuración de la aplicación**.
3. Seleccione los componentes que estarán disponibles en el equipo del usuario. Defina la configuración avanzada para la tarea (consulte la tabla a continuación).

El conjunto de componentes de Kaspersky Embedded Systems Security se modificará en los equipos de los usuarios de manera silenciosa.

Configuración avanzada de la tarea

Parámetro	Descripción
Zona de confianza	En el caso de la tarea Cambiar componentes de la aplicación, solo puede agregar exclusiones de análisis y aplicaciones de confianza a la zona de confianza.
Usar una contraseña para modificar el conjunto de componentes de la aplicación	Los administradores suelen habilitar la protección con contraseña para restringir el acceso a Kaspersky Embedded Systems Security. Es decir, para modificar la selección de componentes de la aplicación, debe ingresar credenciales de un usuario que tenga permiso para **Eliminar, modificar o restaurar la aplicación**. Por ejemplo, puede utilizar la cuenta KLAdmin.

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

En esta sección, se describe cómo instalar y desinstalar Kaspersky Embedded Systems Security a través de las directivas de grupo de Active Directory y se brinda información sobre las acciones que se deben realizar después de instalar Kaspersky Embedded Systems Security mediante directivas de grupo.

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

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

Los dispositivos protegidos 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 dispositivos protegidos en los que desea instalar Kaspersky Embedded Systems Security con 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 el paquete de instalación de ess_win.msi. Para instalar la Consola de la aplicación, use el paquete 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 ess_win.msi en una carpeta compartida del controlador de dominio.
2. Guarde el archivo de clave en la misma carpeta pública en el controlador de dominio.

3. En la misma carpeta compartida en el controlador de dominio, cree un archivo install_props.json que contenga las líneas que se indican a continuación. Esto significa que acepta los términos del Contrato de licencia de usuario final y de 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 dispositivos protegidos.

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 dispositivos protegidos del grupo después de que se hayan reiniciado.

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

Después de instalar Kaspersky Embedded Systems Security en los dispositivos protegidos, se recomienda actualizar inmediatamente las bases de datos de la aplicación y ejecutar un Análisis de áreas críticas. Puede realizar estas acciones 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

Los archivos de volcado y rastreo no se eliminan al desinstalar Kaspersky Embedded Systems Security. Puede eliminar manualmente los archivos de volcado y rastreo de la carpeta especificada durante la configuración de la escritura de los archivos de volcado y rastreo.

Si utilizó una directiva del grupo de Active Directory para instalar Kaspersky Embedded Systems Security (o la Consola de la aplicación) en el grupo de dispositivos protegidos, 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 dispositivos protegidos 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 dispositivos protegidos después de que se hayan reiniciado y antes de iniciar sesión en Microsoft Windows.

Registros de instalación y desinstalación de Kaspersky Embedded Systems Security

Si instala (o desinstala) Kaspersky Embedded Systems Security o la Consola de la aplicación con la ayuda del asistente de instalación (o desinstalación), el servicio Windows Installer crea un registro de instalación (o desinstalación). Se guardará un archivo de registro llamado kl-install-<uid>.log (donde <uid> es un identificador único de registro formado por ocho caracteres) en la carpeta %temp% del usuario cuya cuenta se haya utilizado para iniciar el archivo setup_ess.exe o setup_esstool.exe.

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:\:, ejecute el siguiente comando:

```
msiexec /i ess_win.msi /l*v C:\<log_name>.log /qn EULA=1 PRIVACYPOLICY=1
```

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 realiza las siguientes modificaciones en el dispositivo protegido:

- Se crean las carpetas de Kaspersky Embedded Systems Security en el dispositivo protegido y en el dispositivo protegido en el que 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.
- Se crea la tarea de detección de actualizaciones del SO de Kaspersky Embedded Systems Security que se muestra en el Programador de tareas de Windows.

Estos cambios se describen a continuación.

Carpetas de Kaspersky Embedded Systems Security en un dispositivo protegido

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

- Carpeta de instalación predeterminada de Kaspersky Embedded Systems Security que contiene los archivos ejecutables de Kaspersky Embedded Systems Security. La siguiente carpeta de instalación se utiliza de manera predeterminada:

  %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security.4.0.0

- 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:

  %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security.4.0.0\mibs

- Archivos de servicio de Kaspersky Embedded Systems Security:

  - %ProgramData%\Kaspersky Lab\KESS.4.0\Data
  - %ProgramData%\Kaspersky Lab\KESS.4.0\Settings
  - %ProgramData%\Kaspersky Lab\KESS.4.0\Dskm

- Archivos con configuración para orígenes de actualizaciones:

  %ProgramData%\Kaspersky Lab\KESS.4.0\Data

- Actualizaciones de bases de datos y módulos del programa descargados mediante la tarea *Actualización* (la carpeta se crea la primera vez que se descargan actualizaciones con la tarea *Actualización*).

  %ProgramData%\Kaspersky Lab\KESS.4.0\Update distribution

- Registros de tareas y registro de auditoría del sistema:
  %ProgramData%\Kaspersky Lab\KESS.4.0\Reports
- Conjunto de bases de datos actualmente en uso:
  %ProgramData%\Kaspersky Lab\KESS.4.0\Bases
- Copias de seguridad de bases de datos; se sobrescriben cada vez que se actualizan las bases de datos:
  %ProgramData%\Kaspersky Lab\KESS.4.0\QB
- Archivos temporales creados durante la ejecución de tareas de actualización:
  %ProgramData%\Kaspersky Lab\KESS.4.0\Data\temp\temporaryFolder
- Objetos en cuarentena (carpeta predeterminada):
  %ProgramData%\Kaspersky Lab\KESS.4.0\QB
- Objetos en copia de seguridad (carpeta predeterminada):
  %ProgramData%\Kaspersky Lab\KESS.4.0\QB
- Objetos restaurados desde la copia de seguridad y la cuarentena (carpeta predeterminada para los objetos restaurados):
  %ProgramData%\Kaspersky Lab\KESS.4.0\QB\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. La siguiente carpeta de instalación se utiliza de manera predeterminada:

%ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools.4.0.0.

Grupo de Kaspersky Embedded Systems Security

"Administradores de ESS" es un grupo que se crea en el dispositivo protegido. Sus usuarios tienen 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:

- Configuración de Kaspersky Embedded Systems Security:
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AVP.ESS.4.0]
- Configuración del registro de eventos de Kaspersky Embedded Systems Security (Registro de eventos de Kaspersky):
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Embedded Systems Security]
- Configuración del archivo de rastreo:
  [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KESS.4.0\Trace]

- Configuración para las tareas y funciones de la aplicación:
  [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KESS.4.0\environment]

Tarea del sistema Kaspersky Embedded Systems Security OS Upgrade Detect

Durante la instalación de la aplicación, el servicio Windows Installer crea una tarea Kaspersky Embedded Systems Security OS Upgrade Detect. La tarea se inicia en forma inmediata una vez creada y vuelve a iniciarse cada vez que se inicia el sistema operativo. La tarea analiza la versión de los controladores utilizados por la aplicación: si la versión del sistema operativo se ha actualizado, la aplicación actualiza los controladores a la versión que corresponda para el sistema operativo.

Esta tarea no afecta a la aplicación y se puede eliminar. Recomendamos tener presente el escenario de actualización del sistema operativo.

Procesos de Kaspersky Embedded Systems Security

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

Procesos de Kaspersky Embedded Systems Security

Nombre del archivo	Objetivo
avp.exe	Flujo de trabajo de Kaspersky Embedded Systems Security
avpsus.exe	Este proceso permite instalar y revertir actualizaciones de módulos de aplicaciones críticas y aprobadas.

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 de archivos en tiempo real y Análisis a pedido de Kaspersky Embedded Systems Security.

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 dispositivo, 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. Puede descargarse del sitio web de EICAR.

Antes de guardar el archivo en una carpeta en el disco duro de su dispositivo, 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 tal fin, abra el archivo con un editor de texto y, al comienzo de la línea de texto del archivo, agregue uno de los prefijos enumerados en la tabla a continuación. Hecho esto, guarde el archivo con un nuevo nombre, como 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 del equipo en tiempo real y Análisis a pedido de Kaspersky Embedded Systems Security.

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.
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 de archivos en tiempo real y Análisis a pedido

Después de instalar Kaspersky Embedded Systems Security, puede verificar que Kaspersky Embedded Systems Security sea capaz de detectar objetos que contengan código malicioso. Para tal fin, utilice el virus de prueba EICAR.

Para verificar la función Protección de archivos en tiempo real:

1. Descargue el archivo eicar.com en el sitio web de EICAR. Guárdelo en una carpeta compartida en el disco local de cualquier dispositivo 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 el funcionamiento de las notificaciones del usuario de red, asegúrese de que el servicio Windows Messenger de Microsoft esté habilitado tanto en el dispositivo protegido como en el dispositivo donde guardó el archivo eicar.com.

3. Abrir la Consola de la aplicación en el dispositivo protegido.

4. Copie el archivo eicar.com guardado en el disco local del dispositivo 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 dispositivo protegido después de conectarlo al dispositivo protegido 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 dispositivo para copiar el archivo eicar.com del dispositivo 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 dispositivo protegido.

- En la Consola de la aplicación, se le asigna el estado *Críticos* al registro de tareas. El registro tiene una nueva línea con información sobre una amenaza en el archivo eicar.com.

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

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

Para verificar la función de Análisis a pedido:

1. Descargue el archivo eicar.com en el sitio web de EICAR. Guárdelo en una carpeta compartida en el disco local de cualquier dispositivo 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 y expanda el nodo **Análisis a pedido** en el árbol de la Consola de la aplicación.

3. Seleccione el nodo secundario **Análisis de áreas críticas**.

4. Agregue **Todas las unidades de red** al alcance de la tarea Análisis a pedido.

5. 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 dispositivo.

- En la Consola de la aplicación, se le asigna el estado *Críticos* al registro de tareas. El registro de tareas de Análisis a pedido tiene una nueva línea con información sobre una amenaza en el archivo eicar.com.

Actualización de versiones anteriores de Kaspersky Embedded Systems Security a la versión 4.0

Al actualizar una versión anterior de Kaspersky Embedded Systems Security a la versión 4.0, siga estas recomendaciones:

- Planifique con anticipación y programe la actualización. Elija un momento en el que los servidores estén funcionando con la carga más ligera, por ejemplo, durante el fin de semana.
- Después de la actualización, active los componentes de la aplicación uno por uno. Es decir, comience habilitando solo el componente Protección de archivos en tiempo real, luego habilite otros componentes de protección, luego habilite los componentes de control y así sucesivamente. Recomendamos probar la aplicación en cada paso.
- Realice la actualización paso a paso. Primero actualice un solo equipo, luego varios equipos, luego actualice todos los equipos de la organización.

Pasos del procedimiento de actualización

Actualice Kaspersky Embedded Systems Security a la versión 4.0 en el siguiente orden:

1. **Actualice Kaspersky Security Center**

   Actualice todos los componentes de Kaspersky Security Center a la versión 14.2 o superior, incluido el Agente de red en las computadoras de los usuarios y en Kaspersky Security Center Web Console.

2. **Actualice el complemento web de Kaspersky Embedded Systems Security**

   En Kaspersky Security Center Web Console, actualice el complemento web de Kaspersky Embedded Systems Security a la versión 4.0.

3. **Migrar de tareas y directivas de Kaspersky Embedded Systems Security**

   Después de migrar las directivas y las tareas, debe configurar los parámetros que el asistente de migración no puede migrar y que no existían en versiones anteriores de la aplicación. También recomendamos verificar si el asistente de migración migró correctamente todos los parámetros.

4. **Instale Kaspersky Embedded Systems Security 4.0**

   Kaspersky Embedded Systems Security versión 4.0 usa el protocolo HTTPS en lugar del protocolo DCOM. Por lo tanto, antes de instalar la nueva versión de Kaspersky Embedded Systems Security, es necesario configurar el dispositivo en el que se actualizará la aplicación para habilitar el inicio remoto del servicio de KESS. Si no se realiza dicha configuración, el inicio del servicio remoto no estará disponible.

   Puede instalar Kaspersky Embedded Systems Security 4.0 después de eliminar una versión anterior de la aplicación o sobre ella.

   Cuando se instala sobre una versión anterior de la aplicación, se instala el mismo conjunto de componentes de la aplicación, teniendo en cuenta que posee nuevos nombres y contenidos de algunos componentes.

Cuando se realiza una instalación remota, el instalador incluye los componentes que selecciona en las propiedades del paquete de instalación.

5. **Si es necesario, active Kaspersky Embedded Systems Security 4.0**

   Cuando se instala Kaspersky Embedded Systems Security 4.0 sobre una versión anterior de la aplicación, la licencia actual se aplica automáticamente a la aplicación y los nuevos componentes y tareas de la aplicación están completamente disponibles. El plazo de la licencia no se modificará.

6. **Asegúrese de que el servidor esté funcionando**

   Después de actualizar Kaspersky Embedded Systems Security, asegúrese de que la aplicación funcione correctamente. Asegúrese de que no se informen errores para la aplicación, también verifique la hora de la última conexión con el Servidor de administración, la hora de la última actualización y el estado de protección del equipo.

   Preste atención a la migración de listas de exclusión, aplicaciones de confianza, reglas de Control de dispositivos y reglas de Control de inicio de aplicaciones.

Actualizar Kaspersky Embedded Systems Security

La mejora a Kaspersky Embedded Systems Security 4.0 es compatible con las versiones 2.3, 3.1 o posteriores. Para actualizar versiones anteriores de la aplicación, debe eliminar la versión instalada e instalar la versión 4.0.

Para actualizar la aplicación, debe instalarse la versión nueva sobre la versión instalada. No es necesario reiniciar el equipo tras la operación.

De manera predeterminada, la aplicación crea una nueva carpeta de instalación con el nombre de la nueva versión de la aplicación, tomando como base la ruta a la carpeta de instalación de la versión existente. Puede especificar manualmente una nueva ruta para la carpeta de instalación de la aplicación.

Al actualizar Kaspersky Embedded Systems Security a la versión 4.0, la versión instalada anteriormente se elimina automáticamente.

Si necesita actualizar una instalación de Kaspersky Embedded Systems Security que se encuentre protegida con contraseña, use uno de estos métodos para brindarle la contraseña al instalador:

- Si va a instalar la aplicación en forma local utilizando la interfaz del Asistente de instalación o el modo CLI interactivo, ingrese la contraseña cuando le sea solicitada.
- Si va a instalar la aplicación en forma local usando el modo CLI no interactivo, indique la contraseña a través de la clave `UNLOCK_PASSWORD`.
- Si va a realizar la instalación utilizando directivas de grupo de Active Directory, use el valor de la clave `UNLOCK_PASSWORD` en el archivo de configuración install_props.json.

Cuando la aplicación que está actualizando de forma remota a través de Kaspersky Security Center está protegida con contraseña, primero debe deshabilitar la protección con contraseña utilizando una directiva de Kaspersky Security Center.

Cuando actualice la aplicación, la licencia que esté utilizando se aplicará automáticamente a la versión 4.0 de Kaspersky Embedded Systems Security. Podrá seguir usando los componentes y las tareas de la nueva aplicación sin restricciones. El plazo de la licencia no se modificará.

Si actualiza la aplicación y la licencia está caducada, la nueva versión de la aplicación se ejecutará en modo de funcionalidad limitada después de la instalación (con ello, por ejemplo, no podrá actualizar las bases de datos de la aplicación).

Actualización de las herramientas de administración de Kaspersky Embedded Systems Security

Puede actualizar el Complemento de administración para administrar la aplicación con Kaspersky Security Center a la versión 4.0 a partir de las versiones 2.3, 3.1, 3.2, 3.3, 3.4 o posteriores. Para actualizar versiones anteriores del Complemento de administración y la Consola de la aplicación, debe eliminar la versión instalada y luego instalar la versión 4.0.

Durante la actualización, se instala una nueva versión del Complemento de administración sobre la versión instalada anteriormente. No es necesario reiniciar el equipo tras esta operación.

Para obtener información sobre cómo migrar la configuración del complemento de administración, consulte este artículo.

Migrar directivas y tareas

Puede migrar la configuración de directivas y tareas de versiones anteriores de la aplicación a la versión 4.0 de las siguientes maneras:

- Usando el Asistente de conversión por lotes de directivas y tareas (solo disponible en la Consola de administración de Kaspersky Security Center).
- Usando el Asistente de migración de directivas y tareas de Kaspersky Embedded Systems Security 4.0 (disponible solo en Kaspersky Security Center Web Console).

Se recomienda comenzar con la migración de directivas y tareas de Kaspersky Embedded Systems Security en un solo equipo, luego hacerlo en un grupo de equipos, y finalmente completar la migración en todos los equipos de la organización.

Cómo usar el Asistente de conversión por lotes de directivas y tareas para migrar la configuración de directivas y tareas

1. En la Consola de administración de Kaspersky Security Center, seleccione el Servidor de administración y haga clic con el botón derecho para abrir el menú contextual.
2. Seleccione **Todas las tareas** → **Asistente de conversión por lotes de directivas y tareas**.

Se iniciará el Asistente de conversión por lotes de directivas y tareas. Siga las instrucciones del Asistente.

Paso 1. Seleccionar la aplicación para la que desea convertir directivas y tareas

Seleccione Kaspersky Embedded Systems Security 4.0. Vaya al siguiente paso.

Paso 2. Conversión de directivas

Seleccione las directivas de la versión de la aplicación que se actualiza que desea crear para Kaspersky Embedded Systems Security 4.0. Vaya al siguiente paso.

Paso 3. Conversión de tareas

Seleccione las tareas de la versión de la aplicación que se actualiza que desea crear para Kaspersky Embedded Systems Security 4.0.

Las tareas que no son de grupo (tareas asignadas a dispositivos individuales) no se muestran en el paso actual.

Para convertir tareas que no son de grupo de su versión de la aplicación a Kaspersky Embedded Systems Security 4.0:

1. Haga clic en **Siguiente**.

   Se abre la ventana **Migración adicional de programaciones y tareas**.

2. Seleccione la casilla de verificación **Migrar las tareas que no son de grupo**.

3. Especifique la configuración de conexión para el Servidor de administración de Kaspersky Security Center.

4. Haga clic en **Aceptar**.

Paso 4. Fin del Asistente

Complete el asistente. Como resultado, el asistente hace lo siguiente:

- Se crean nuevas directivas para Kaspersky Embedded Systems Security 4.0.

  Las nuevas directivas contienen la configuración de las directivas de Kaspersky Embedded Systems Security seleccionadas y también la nueva configuración que se ingresaron en Kaspersky Embedded Systems Security 4.0. Los nombres de las nuevas directivas son los mismos que los nombres de las directivas de Kaspersky Embedded Systems Security antes de la conversión y se agrega la palabra " (convertido)". Las nuevas directivas tienen el estado *Directiva inactiva*.

- Se crean nuevas tareas para Kaspersky Embedded Systems Security 4.0.

  Las nuevas tareas contienen la configuración de las tareas de Kaspersky Embedded Systems Security seleccionadas y también la nueva configuración que se ingresaron en Kaspersky Embedded Systems Security 4.0. Los nombres de las nuevas tareas son los mismos que los nombres de las tareas de Kaspersky Embedded Systems Security antes de la conversión y se agrega la palabra "(conversión)".

- Las directivas y las tareas seleccionadas para la conversión no se modifican.

[Cómo usar el asistente de migración para migrar la configuración de directivas y tareas]

En la ventana principal de Web Console, seleccione **Operaciones → Migración a KESS 4.0.0**.

Esto ejecuta el Asistente de migración de tareas y directivas. Siga las instrucciones del Asistente.

Paso 1. Migración de la directiva

Seleccione las directivas de Kaspersky Embedded Systems Security que desee crear para Kaspersky Embedded Systems Security 4.0. Vaya al siguiente paso.

Paso 2. Migración de la tarea

En la lista de tareas, seleccione las tareas de Kaspersky Embedded Systems Security que desee crear para Kaspersky Embedded Systems Security 4.0. Vaya al siguiente paso.

Paso 3. Fin del Asistente

Complete el asistente. Como resultado, el asistente hace lo siguiente:

- Se crean nuevas directivas para Kaspersky Embedded Systems Security 4.0.

  Las nuevas directivas contienen la configuración de las directivas de Kaspersky Embedded Systems Security migradas y también la nueva configuración que se ingresaron en Kaspersky Embedded Systems Security 4.0. Los nombres de las nuevas directivas son los mismos que los nombres de las directivas de Kaspersky Embedded Systems Security antes de la fusión y se agrega la frase "copiado de KESS". Las nuevas directivas tienen el estado *Directiva inactiva*.

- Se crean nuevas tareas para Kaspersky Embedded Systems Security 4.0.

  Las nuevas tareas contienen la configuración de las tareas de Kaspersky Embedded Systems Security migradas y también la nueva configuración que se ingresaron en Kaspersky Embedded Systems Security 4.0. Los nombres de las nuevas tareas son los mismos que los nombres de las tareas de Kaspersky Embedded Systems Security antes de la migración y se agrega la frase "copiado de KESS".

Migración de la configuración de la versión de la aplicación que se actualiza

Los siguientes valores se migran sin cambios después de la actualización de la aplicación y sus complementos de administración a la versión 4.0:

- Configuración de componentes y tareas, excepto aquellos que se restablecen a los valores predeterminados y aquellos que se incluyen en "Limitaciones de la configuración y la migración de componentes"
- Registros de tareas y registros de auditoría del sistema, así como registros en el Registro de eventos de Windows
- Configuración de notificaciones de tareas
- Cuentas de usuarios con las que se inician las tareas

- Permisos de acceso de usuario para administrar la aplicación
- Contraseña de la conexión del servidor proxy
- Estado de los atributos

La siguiente configuración se restablece o toma los valores predeterminados de la nueva versión después de que se actualizan la aplicación y sus complementos a la versión 4.0:

- Todos los contadores, incluidos los estados de la base de datos antivirus
- Datos sobre las actualizaciones instaladas para los módulos de la aplicación y las bases de datos antivirus
- Estados de las tareas
- Permisos para administrar Kaspersky Security Service
- Configuración de la aplicación y de las tareas a través del Registro
- Configuraciones de la aplicación y de las tareas que se hayan modificado al instalar correcciones críticas
- Configuración de eventos
- Configuración de la transferencia de datos al Servidor de administración de Kaspersky Security Center; de manera predeterminada, la transferencia de todos los datos está habilitada
- Configuración de seguimiento y volcado
- Configuración de las tareas locales de la aplicación, ubicadas en la pestaña **Notificaciones**

La configuración que no existía en la versión de la aplicación que está actualizando se completa con valores predeterminados.

Limitaciones en la configuración y la migración de componentes

- El contenido de la cuarentena de la versión que se actualiza se mueve a la copia de seguridad de la versión 4.0. Al mismo tiempo, el tamaño máximo de la copia de seguridad aumenta a 400 MB y el umbral de espacio disponible aumenta a 100 MB.
- La siguiente configuración de Kaspersky Embedded Systems Security versión 3.4 no existe en Kaspersky Embedded Systems Security versión 4.0 y posteriores, por lo tanto, no se migran: **Carpeta de cuarentena**, **Carpeta de respaldo** y **Carpeta para restaurar objetos**. Tampoco se migran otras configuraciones que existan en la versión anterior, pero no en la versión nueva.
- La lista de sesiones de red bloqueadas de los equipos cliente no se migra. Al mismo tiempo, la configuración para desbloquear automáticamente el acceso a los recursos de archivos en red bloqueados no se modifican cuando se actualiza la aplicación.
- La configuración de la protección con contraseña no se migra. En Kaspersky Embedded Systems Security 4.0, la protección con contraseña sufrió cambios significativos. Si es necesario, active Protección con contraseña y establezca una contraseña.

- Zona de confianza:
  - El método de selección de objetos de la zona de confianza se modificó en Kaspersky Embedded Systems Security 4.0. Las exclusiones definidas como archivos individuales o rutas de archivo o carpeta se pueden migrar. Las exclusiones definidas como un alcance predefinido (por ejemplo, discos duros) o una URL de script no se migran. Después de la migración, debe agregar estas exclusiones manualmente.
  - Las exclusiones de análisis y las aplicaciones de confianza predefinidas que ayudan a configurar la aplicación en los servidores se agregaron a la zona de confianza.
- Los componentes Control de aplicaciones y Control de dispositivos se rediseñaron significativamente. La configuración de los componentes de la versión que se actualiza se migra teniendo en cuenta la nueva estructura de configuración en Kaspersky Embedded Systems Security 4.0.
- La configuración de los componentes Monitor de integridad de archivos y Monitor de acceso al registro de la versión de la aplicación que se actualiza se migra a la configuración del componente Control de integridad del sistema.
- El componente Administración de firewall se rediseñó para incluirse en el componente Firewall, que, además de interactuar con el firewall de Windows, ahora también funciona como firewall. Después de completar la migración, debe configurar el modo de componente desde cero.
- Para usar KSN, debe leer y aceptar la Declaración de KSN nuevamente.
- Las versiones 4.0 y posteriores de la aplicación no admiten la programación de componentes individuales. Si los componentes están habilitados, continúan ejecutándose mientras se ejecuta la aplicación.
- Cuando se migran tareas, la hora de inicio programada para la tarea se desplaza el número de horas que coincide con el número de la zona horaria configurada en la configuración del sistema operativo del equipo en el que se realiza la migración. Por ejemplo, suponga que la hora de inicio de la tarea en la versión anterior de la aplicación es las 7:00 y la zona horaria configurada para el sistema operativo es UTC +3:00. Después de migrar la tarea, la hora de inicio cambia a las 10:00.
- La sección para configurar las acciones que se realizarán con los objetos probablemente infectados se eliminó de la configuración del componente Protección de archivos en tiempo real y las tareas de Análisis a pedido. Esta configuración no se migra a la versión más reciente de la aplicación.
- Kaspersky Security Center Web Console o la Consola de administración de Kaspersky Security Center no se pueden usar para enviar objetos en Copia de seguridad a Kaspersky para analizar si se migraron después de actualizar la versión 3.4 o anteriores a la versión 4.0 o posteriores.
- Al migrar las tareas de Análisis a pedido, el nivel de seguridad predeterminado para los alcances de análisis predefinidos cambia de *Informar* a *Personalizado*.

Correspondencia de componentes y tareas en las versiones 3.4 y 4.0 de Kaspersky Embedded Systems Security

Cuando se actualiza Kaspersky Embedded Systems Security 3.4 a la versión 4.0, el conjunto de componentes y tareas se migra solo si la aplicación se instaló localmente.

Correspondencia de los componentes en las versiones 3.4 y 4.0 de Kaspersky Embedded Systems Security

Componente de Kaspersky Embedded Systems Security 3.4	Componente de Kaspersky Embedded Systems Security 4.0
Zona de confianza	Zona de confianza
Protección de archivos en tiempo real	Protección de archivos en tiempo real
Uso de KSN	Uso de KSN
Prevención de exploits	Prevención de exploits
Escáner AMSI	Protección vía AMSI
Control de inicio de aplicaciones	Control de inicio de aplicaciones
Control de dispositivos	Control de dispositivos
Administración de firewall	Firewall El Firewall de Windows actúa como el firewall de Kaspersky Embedded Systems Security 3.4, mientras que la aplicación administra el Firewall de Windows. En Kaspersky Embedded Systems Security 4.0, un componente separado es responsable de la funcionalidad del Firewall.
Protección contra amenazas de red	Protección contra amenazas de red
Monitor de integridad de archivos	Control de integridad del sistema La funcionalidad de los componentes Monitor de integridad de archivos y Monitor de acceso al registro se fusionó en el componente Control de integridad del sistema.
Inspección de registros	Inspección de registros
Monitor de acceso al registro	Control de integridad del sistema La funcionalidad de los componentes Monitor de integridad de archivos y Monitor de acceso al registro se fusionó en el componente Control de integridad del sistema.
(ninguno)	Detección de comportamiento
(ninguno)	Motor de reparación
Tarea de Kaspersky Embedded Systems Security 3.4	**Tarea de Kaspersky Embedded Systems Security 4.0**
Activación de la aplicación	Activar la aplicación
Copia de actualizaciones	Actualización La funcionalidad de la tarea Copiar actualizaciones se fusionó con la tarea Actualización.
Monitor comparativo de integridad de archivos	Monitor comparativo de integridad del sistema
Actualización de bases de datos	Actualización La funcionalidad de la tarea Actualización de la base de datos se fusionó con la tarea Actualización.
Actualización de módulos del programa	Actualización La funcionalidad de la tarea Actualización de módulos de software se fusionó con la tarea Actualización.
Reversión de la actualización de la bases de datos de la aplicación	Reversión de la actualización
Análisis a pedido	Análisis a pedido
Control de integridad de la aplicación	Control de integridad de la aplicación
Generador de reglas de Control de inicio de aplicaciones	Generador de reglas de Control de inicio de aplicaciones
Generador de reglas para Control de dispositivos	Generador de reglas para Control de dispositivos
(ninguno)	Protección de la conexión del Servidor de administración
(ninguno)	Cambiar componentes de Kaspersky Embedded Systems Security
(ninguno)	Restablecimiento del estado de integridad del sistema

Interfaz de aplicación

Puede controlar Kaspersky Embedded Systems Security mediante las siguientes interfaces:

- Consola de la aplicación.
- Consola de administración de Kaspersky Security Center.
- Kaspersky Security Center Web Console,

Consola de administración de Kaspersky Security Center

Kaspersky Security Center le permite instalar y desinstalar, iniciar y detener Kaspersky Embedded Systems Security de forma remota, configurar la configuración de la aplicación, cambiar el grupo de componentes de la aplicación disponibles, agregar claves e iniciar y detener tareas.

La aplicación puede administrarse a través de Kaspersky Security Center mediante el complemento de administración de Kaspersky Embedded Systems Security. Consulte la información detallada sobre la interfaz de Kaspersky Security Center en la Ayuda de *Kaspersky Security Center*.

Kaspersky Security Center Web Console

Kaspersky Security Center Web Console (de ahora en más denominada Web Console) es una aplicación web destinada a realizar, de forma centralizada, tareas principales para administrar y mantener el sistema de seguridad de la red de una organización. Kaspersky Security Center Web Console es un componente de Kaspersky Security Center que proporciona una interfaz de usuario. Para obtener información detallada sobre Kaspersky Security Center Web Console, consulte la *Ayuda de Kaspersky Security Center*.

Las siguientes acciones están disponibles para Web Console:

- Supervisar el estado del sistema de seguridad de su organización.
- Instalar aplicaciones de Kaspersky en los dispositivos conectados a la red.
- Administrar las aplicaciones instaladas.
- Ver informes sobre el estado del sistema de seguridad.

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 dispositivo protegido o en un grupo de dispositivos.

Administración de Kaspersky Embedded Systems Security mediante Kaspersky Security Center

Si ha instalado Kaspersky Embedded Systems Security en una serie de dispositivos protegidos que forman parte de un mismo grupo de administración, puede administrarlos en forma centralizada mediante el Complemento de administración de Kaspersky Embedded Systems Security. Kaspersky Security Center también permite configurar individualmente los ajustes de cada dispositivo protegido incluido en el grupo de administración.

Un *grupo de administración* se crea manualmente a través de Kaspersky Security Center. El grupo incluye varios dispositivos 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 solo dispositivo protegido no está disponible si el funcionamiento de Kaspersky Embedded Systems Security en el dispositivo protegido está controlado por una directiva de Kaspersky Security Center activa.

No se requiere ninguna acción avanzada para iniciar el Complemento de administración de Kaspersky Embedded Systems Security en Kaspersky Security Center. Una vez que el Complemento de administración se instala en el dispositivo protegido del administrador, se inicia junto con cualquier tipo de Consola de administración de Kaspersky Security Center.

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 dispositivos. La configuración de la tarea especificada en la directiva activa tiene prioridad sobre la configuración de la tarea definida de forma local en la Consola de la aplicación o remotamente en la ventana **Propiedades: <Nombre del dispositivo protegido>** de Kaspersky Security Center.

  Las directivas se pueden usar para establecer la configuración general de la aplicación, la configuración de las tareas de protección del equipo en tiempo real, las tareas de control de actividades en los dispositivos, las tareas de protección de almacenamiento de la red y la configuración que regula el inicio programado de tareas del sistema local.

- **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 dispositivos.

  Puede usar tareas de grupo para activar la aplicación, configurar la tarea Análisis a pedido, actualizar la configuración de tareas y configurar la tarea Generador de reglas de 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 dispositivos protegidos que no pertenecen a ningún grupo de administración.

- **Utilización de la ventana de propiedades de un solo dispositivo**. En la ventana **Propiedades: <Nombre del dispositivo protegido>**, puede configurar remotamente la configuración de la tarea para un dispositivo protegido específico que forme parte de un grupo de administración. También puede establecer tanto la configuración general de la aplicación como la configuración para todas las tareas de Kaspersky Embedded Systems Security si el dispositivo protegido seleccionado no está controlado por una directiva de Kaspersky Security Center activa.

Administración de las configuraciones de la aplicación

Esta sección contiene información acerca de cómo ajustar la configuración general de Kaspersky Embedded Systems Security en la Consola de administración de Kaspersky Security Center.

Navegación

Obtenga información sobre cómo dirigirse a la configuración de la tarea requerida a través de la interfaz que elija.

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 dispositivo 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 ficha **Dispositivos**.

4. Abra la ventana **Propiedades: <Nombre del dispositivo protegido>** con uno de los siguientes métodos:

   - Haga doble clic en el nombre del dispositivo protegido.

   - Abra el menú contextual del nombre del dispositivo protegido y seleccione el elemento **Propiedades**.

   Se abre la ventana **Propiedades: <Nombre del dispositivo protegido>**.

5. En la sección **Aplicaciones**, seleccione **Kaspersky Embedded Systems Security**.

6. Haga clic en **Propiedades**.

   Se abre la ventana **Configuración** de **Kaspersky Embedded Systems Security**.

7. Vaya a la sección **Configuración de la aplicación**.
8. Haga clic en el botón **Configuración**, en la subsección de la configuración que desee ajustar.

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 ficha **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, vaya a **Configuración de la aplicación**.
6. Haga clic en el botón **Configuración**, en la subsección de la configuración que desee ajustar.

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 dispositivos protegidos o para un dispositivo protegido.

Configuración de opciones de interfaz y análisis 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 dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Properties: <Nombre de directiva>**.
   - Para configurar los ajustes de una tarea o aplicación para un dispositivo protegido específico, seleccione la pestaña **Dispositivos** y vaya a la configuración de la tarea local o a la configuración de la aplicación.
4. En la sección **Configuración de la aplicación**, haga clic en el botón **Configuración** de la subsección **Configuración de la interfaz**.

5. En la ventana **Configuración de la interfaz**, en la pestaña **General**, configure las siguientes opciones:

   - En la sección **Interacción con el usuario**, configure si se mostrará el ícono de bandeja del sistema en la barra de tareas después del inicio de cada aplicación.

     - **Mostrar interfaz del usuario**. En el equipo cliente, hay un ícono disponible en la bandeja de Windows. El usuario podrá interactuar con Kaspersky Embedded Systems Security a través del menú contextual del icono. Kaspersky Embedded Systems Security también mostrará notificaciones por encima del icono. El menú contextual del ícono en la bandeja del sistema de Windows le permite abrir la Interfaz de diagnóstico compacto. Al hacer clic en un vínculo en la Interfaz de diagnóstico compacto, se abre la Consola de la aplicación.

     - **No mostrar interfaz del usuario**. No habrá ninguna indicación en el equipo cliente de que Kaspersky Embedded Systems Security está en funcionamiento. El ícono del área de notificación de Windows no estará disponible y tampoco se mostrará ninguna notificación.

   - En la sección **Estados**, puede especificar las advertencias que desea ver en el ícono de bandeja del sistema de Kaspersky Embedded Systems Security.

6. Haga clic en **Aceptar**.

Se guarda la configuración de la aplicación.

Configuración de opciones de seguridad en Kaspersky Security Center

Para configurar las opciones de seguridad manualmente:

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 dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Properties: <Nombre de directiva>**.

   - Para configurar los ajustes de una tarea o aplicación para un dispositivo protegido específico, seleccione la pestaña **Dispositivos** y vaya a la configuración de la tarea local o a la configuración de la aplicación.

4. En la sección **Configuración de la aplicación**, haga clic en el botón **Configuración** de la subsección **Seguridad y confiabilidad**.

5. En la ventana **Configuración de seguridad**, en la pestaña **Seguridad**, configure las siguientes opciones:

   - En la sección **General**, recomendamos dejar **Iniciar la aplicación al arrancar el equipo (recomendado)** habilitado (predeterminado).

   - En la sección **Autoprotección**, habilite o deshabilite la funcionalidad **Proteger los procesos de la aplicación de amenazas externas**.

- En la sección **Acciones al pasar a usar alimentación de respaldo (UPS)**, especifique limitaciones de la carga del dispositivo protegido creadas por Kaspersky Embedded Systems Security después de cambiar a la alimentación de UPS:
  - **No iniciar las tareas de análisis programadas**
  - **Detener las tareas de análisis en ejecución**
- En la sección **Estado del equipo cuando se aplique la configuración**, configure la visualización del estado de los equipos cliente que tienen la aplicación instalada si se producen errores durante la aplicación de una directiva o la ejecución de una tarea.
- En la sección **Configuración de compatibilidad**, configure la opción **Compatible con software de administración remota**.

  Si el uso de Kaspersky Embedded Systems Security junto con las herramientas de administración remota (RAT) causa problemas, puede habilitar el modo de compatibilidad. Los problemas pueden estar relacionados con la incompatibilidad de las RAT con la funcionalidad de Escritorio seguro de la aplicación. El propósito de esta funcionalidad es confirmar las acciones que potencialmente pueden reducir el nivel de seguridad del equipo. Esta funcionalidad permite que una aplicación muestre un cuadro de diálogo de confirmación aislado de otros procesos. Esta funcionalidad utiliza derechos de alto nivel para proteger la solicitud. De esta forma, solo el usuario puede confirmar la acción y no el malware.

  Si se selecciona la casilla, se habilita el modo de compatibilidad con la RAT. La aplicación muestra un cuadro de diálogo de confirmación sin esta funcionalidad. Esto puede reducir el nivel de seguridad del equipo. No recomendamos habilitar el modo de compatibilidad si Kaspersky Embedded Systems Security no está causando problemas con la RAT.

  Si cancela la selección de la casilla de verificación, se deshabilita el modo de compatibilidad con la RAT. De forma predeterminada, la casilla no está activada.

  Por ejemplo: si se utiliza el navegador en modo RemoteApp, es posible que Kaspersky Embedded Systems Security no muestre una ventana de confirmación cuando se visita un sitio web con un certificado no confiable, ya que RemoteApp no admite la funcionalidad de Escritorio seguro de la aplicación. Esto puede hacer que el navegador deje de responder. Para que el navegador funcione correctamente en el modo RemoteApp, debe habilitar el modo de compatibilidad.

  También puede intentar habilitar el modo de compatibilidad si tiene problemas con la funcionalidad de Escritorio Seguro al utilizar otro software de terceros.

6. En la pestaña **Configuración de análisis**, establezca la siguiente configuración:

   - **Restringir el uso de CPU para las tareas del análisis**. Kaspersky Embedded Systems Security limita el uso de CPU del dispositivo protegido durante las tareas de análisis a pedido al valor especificado en el campo **Límite superior**. La activación de esta opción puede afectar negativamente el rendimiento de Kaspersky Embedded Systems Security.

   - Conceder recursos a otras aplicaciones. Es posible que el consumo de recursos del equipo por parte de Kaspersky Embedded Systems Security al analizar el equipo aumente la carga de la CPU y de los subsistemas del disco duro. Esto puede ralentizar otras aplicaciones. Para optimizar el rendimiento, Kaspersky Embedded Systems Security proporciona un modo para transferir recursos a otras aplicaciones. En este modo, el sistema operativo puede dar menos prioridad a los subprocesos de la tarea de análisis de Kaspersky Embedded Systems Security cuando la carga de la CPU sea alta. Esto permite redistribuir los recursos del sistema operativo a otras aplicaciones. De este modo, las tareas de análisis recibirán menos tiempo de CPU. Por consiguiente, Kaspersky Embedded Systems Security tardará más tiempo en analizar el equipo. Por defecto, la aplicación está configurada para dispensar recursos para otras aplicaciones.

7. 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 dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Properties: <Nombre de directiva>**.

   - Para configurar los ajustes de una tarea o aplicación para un dispositivo protegido específico, seleccione la pestaña **Dispositivos** y vaya a la configuración de la tarea local o a la configuración de la aplicación.

4. En la sección **Configuración de la aplicación**, haga clic en el botón **Configuración** de la subsección **Configuración de conexión**.

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

5. En la ventana **Configuración de conexión**, configure las siguientes opciones:

   - En la sección **Servidor proxy**, especifique la configuración del servidor proxy haciendo clic en el botón **Configuración**:

     - No usar un servidor proxy.

     - **Detectar automáticamente la configuración del servidor proxy**

- Usar el servidor proxy especificado.
- **La dirección IP o el nombre simbólico del servidor proxy y el número de puerto**
- No usar el servidor proxy para las direcciones locales.
- 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.
  - **Autenticación NTLM**: la autenticación se realiza usando el protocolo de autenticación de red NTLM desarrollado por Microsoft. Este modo está seleccionado en forma predeterminada.
- Escriba el nombre de usuario y la contraseña, de ser necesario.
- En la sección **Licencias**, seleccione o desactive la casilla de verificación **Usar Kaspersky Security Center como servidor proxy al activar la aplicación**.

- En la sección **Puertos vigilados**, especifique los puertos de red vigilados:
  - **Vigilar todos los puertos de red**. En este modo de supervisión de puertos de red, los componentes de protección controlan los flujos de datos que se transmiten a través de cualquier puerto de red abierto del equipo.
  - **Vigilar solo los puertos de red seleccionados**. Cuando se selecciona este modo, los componentes de protección vigilan los puertos de red seleccionados y la actividad de red de las aplicaciones seleccionadas. La lista de puertos de red que normalmente se utilizan para transmitir correo electrónico y otras clases de tráfico se configura siguiendo las recomendaciones de los expertos de Kaspersky.

  Haga clic en **Configuración** y especifique la siguiente configuración**:**
  - **Vigilar todos los puertos de las aplicaciones que aparecen en la lista recomendada por Kaspersky**. En este modo, se utiliza una lista predefinida con las aplicaciones a las que están asociados los puertos que Kaspersky Embedded Systems Security vigilará. La lista incluye aplicaciones como Google Chrome, Adobe Reader y Java.
  - **Vigilar todos los puertos de las aplicaciones especificadas**. La lista de aplicaciones cuyos puertos de red supervisa Kaspersky Embedded Systems Security.

6. Haga clic en **Aceptar**.

Los parámetros de conexión configurados se guardan.

Configurar el inicio programado de las tareas locales

Puede utilizar directivas para permitir o bloquear el inicio de la tarea Análisis a pedido y la tarea Actualización del sistema local. Esto se hace de acuerdo con la programación configurada localmente en cada dispositivo protegido 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 dispositivo protegido 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, la directiva prohíbe el inicio de tareas locales del sistema.

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

Si no utiliza las tareas de actualización de grupo o de análisis a pedido, permita que las tareas locales del sistema se inicien en la directiva: Kaspersky Embedded Systems Security realizará las actualizaciones de bases de datos y del módulo, e iniciará todas tareas locales de análisis a pedido del sistema 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 al inicio del sistema operativo*, *Comprobación de integridad de la aplicación* y *Monitor comparativo de integridad del sistema*.
- Tareas de actualización: *Actualización de bases de datos y módulos de la aplicación*, *Actualización de aplicación*.

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

Para permitir o bloquear la administración de la programación de inicio para las tareas locales de la aplicación en una directiva:

1. En el árbol de la Consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados**, expanda el grupo relevante y, en el panel de resultados, seleccione la pestaña **Directivas**.
2. En la pestaña **Directivas**, en el menú contextual de la directiva para la que desee programar tareas del sistema local de Kaspersky Embedded Systems Security del grupo de dispositivos protegidos, seleccione **Propiedades**.
3. En la ventana de propiedades de la directiva, seleccione la sección **Configuración de la aplicación**.
4. Haga clic en **Configuración** en la subsección **Ejecutar tareas locales del sistema**.
5. Seleccione la casilla de verificación **Permitir el uso de tareas locales**.
6. Use la casilla de verificación **Permitir la administración de programaciones** para permitir o bloquear la administración de la programación de inicio para las tareas locales de la aplicación.

Configurar 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 dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Properties: <Nombre de directiva>**.
   - Para configurar los ajustes de una tarea o aplicación para un dispositivo protegido específico, seleccione la pestaña **Dispositivos** y vaya a la configuración de la tarea local o a la configuración de la aplicación.
4. Vaya a la sección **Adicional**.
5. Haga clic en el botón **Configuración** de la subsección **Depósitos**.
6. Configure las opciones que se describen en la tabla a continuación.

Configuración de almacenamiento

Parámetro	Descripción
En la pestaña **Informes**, especifique la configuración de informes:	
Conservar informes como máximo	Si la casilla está seleccionada, los informes se conservarán solo por el tiempo definido como máximo. Por defecto, el plazo máximo de almacenamiento de informes es de 30 días. Después de ese plazo, Kaspersky Embedded Systems Security elimina automáticamente las entradas más antiguas del archivo del informe.
Limitar el tamaño del archivo de los informes a	Si la casilla está seleccionada, el tamaño máximo del archivo de informes se limitará al valor definido. Por defecto, el tamaño máximo del archivo es de 1024 MB. Para evitar que se exceda el tamaño máximo del archivo del informe, Kaspersky Embedded Systems Security elimina automáticamente las entradas más antiguas de este archivo cuando alcanza el tamaño máximo.
En la pestaña **Copias de seguridad**, especifique la configuración de Copia de seguridad:	
Conservar objetos como máximo	Si la casilla está seleccionada, los archivos se conservarán solo por el tiempo definido como máximo. Por defecto, el plazo máximo de almacenamiento de archivos es de 30 días. Al caducar el plazo de almacenamiento máximo, Kaspersky Embedded Systems Security elimina los archivos más antiguos de Copia de seguridad.
Limitar el tamaño de Copia de seguridad a	Si la casilla está seleccionada, el espacio de almacenamiento se limitará al tamaño definido como máximo. Por defecto, el tamaño máximo es de 400 MB. Cuando se alcanza el valor definido, Kaspersky Embedded Systems Security elimina automáticamente los archivos más antiguos para evitar que el límite se exceda.
Valor umbral para el espacio disponible	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 de 100 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 **Valor umbral para el espacio disponible** está activada si la casilla **Limitar el tamaño de Copia de seguridad a** está seleccionada.

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 dispositivos protegidos.

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

Una directiva implementa la configuración, las funciones y las tareas especificadas de Kaspersky Embedded Systems Security en todos los dispositivos 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 **Inspección de registros**.

Kaspersky Security Center ofrece una manera de aplicar directivas en dispositivos protegidos: *Prohibir la edición de la configuración*. Después de aplicar una directiva, Kaspersky Embedded Systems Security utiliza los valores de configuración para los cuales especificó en las propiedades de la directiva que **Modificación no permitida** . En este caso, Kaspersky Embedded Systems Security no utiliza los valores de configuración vigentes antes de que se aplicara la directiva. Kaspersky Embedded Systems Security no aplica los valores de configuración de la directiva activa para los cuales especificó en las propiedades de la directiva que **Modificación permitida** .

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 configuraciones pueden editarse en la Consola de la aplicación.

Las opciones de configuración definidas en la directiva activa y marcadas con el icono no pueden modificarse para un dispositivo protegido en particular a través de la ventana **Propiedades: <Nombre del dispositivo protegido>** de Kaspersky Security Center.

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

Si una directiva define la configuración de una tarea de Protección del equipo en tiempo real o una tarea de Protección de depósitos conectados a la red que se encuentra en ejecución, la configuración definida por la directiva cambiará en cuanto se aplique la directiva. Si la tarea no está en ejecución, la configuración se implementará cuando se inicie.

Creación de una directiva

Antes de crear una directiva, necesita instalar el complemento de administración klcfginst.exe.

Para crear una directiva para un grupo de dispositivos protegidos en los que la aplicación esté instalada y en ejecución:

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 dispositivos protegidos para los que desea crear una directiva.

2. En el panel de resultados del grupo de administración seleccionado, seleccione la pestaña **Directivas** y haga clic en el vínculo **Crear una directiva** para iniciar el Asistente de nueva directiva.

   Se abre la ventana **Asistente de nueva directiva**.

3. En la ventana **Seleccionar la aplicación para la cual desea crear una directiva de grupo**, seleccione Kaspersky Embedded Systems Security.

4. Haga clic en **Siguiente**.

5. Ingrese un nombre de la directiva de grupo en el campo **Nombre**.

   El nombre de la directiva no puede contener los siguientes símbolos: `" * < : > ? \ |` .

6. Para aplicar una configuración de directiva que se utilizó en una versión anterior de la aplicación:

   a. Seleccione la casilla de verificación **Usar la configuración de la directiva creada para una versión más antigua de la aplicación**.

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

   c. Seleccione la directiva que desea aplicar.

   d. Haga clic en **Siguiente**.

7. En la ventana **Selección del tipo de operación**, en **Configuración de Protección de archivos en tiempo real**, marque la casilla **Habilitar Protección de archivos en tiempo real** y especifique un nivel de seguridad.

   Si no se selecciona el modo de ejecución de la tarea, no puede continuar con el siguiente paso del Asistente de nueva directiva.

8. Configure la Protección del equipo en tiempo real.

9. Configure las exclusiones de análisis y aplicaciones de confianza.

10. Seleccione uno de los siguientes estados de la directiva en la ventana **Crear la directiva de grupo para la aplicación**:

    - **Directiva activa**, si desea que la directiva se aplique inmediatamente después de su creación. Si ya existiera una directiva activa en el grupo, se la desactivará y se aplicará la directiva nueva.

    - **Directiva inactiva**, si no desea aplicar la directiva creada inmediatamente. En este caso, la directiva se puede activar más tarde.

- Una directiva **fuera de la oficina** se activa cuando un equipo sale del perímetro de la red de la organización.
- 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**.

11. 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.

Cuando se crea una nueva directiva, se crea también un conjunto de reglas de autorización para evitar que las aplicaciones se bloqueen y garantizar que continúen funcionando sin interrupciones. Puede ver las reglas predeterminadas en la configuración de tareas. Encontrará los detalles y las limitaciones más abajo.

De manera predeterminada, cuando se crea una nueva directiva, Kaspersky Embedded Systems Security para Windows crea un conjunto de reglas para el tráfico de red entrante:

- Dos reglas de autorización para el proceso de compartir el escritorio de Windows mediante el Agente de red de Kaspersky Security Center, el cual se encuentra en las carpetas %Program Files% y %Program Files (x86)%. Estado: habilitado. Direcciones externas permitidas: todas. Protocolos: TCP y UDP, una regla por protocolo.
- Dos reglas de autorización para el puerto local 15000. Estado: habilitado. Direcciones externas permitidas: todas. Protocolos: TCP y UDP, una regla por protocolo.

De manera predeterminada, cuando se crea una nueva directiva, Kaspersky Embedded Systems Security para Windows crea un conjunto de reglas para el tráfico de red saliente:

- Dos reglas de autorización para el servicio de Kaspersky Embedded Systems Security para Windows, el cual se encuentra en las carpetas %Program Files% y %Program Files (x86)%. Estado: habilitado. Direcciones externas permitidas: todas. Protocolos: TCP y UDP, una regla por protocolo.
- Dos reglas de autorización para el proceso de trabajo de Kaspersky Embedded Systems Security, el cual se encuentra en las carpetas %Program Files% y %Program Files (x86)%. Estado: habilitado. Direcciones externas permitidas: todas. Protocolos: TCP y UDP, una regla por protocolo.
- Dos reglas de autorización para el puerto local 13000. Estado: habilitado. Direcciones externas permitidas: todas. Protocolos: TCP y UDP, una regla por protocolo.

Configuración de directivas

Para establecer la configuración de la directiva:

1. En el árbol de la Consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados**.
2. Expanda el grupo de administración para el cual desee configurar las opciones de la directiva asociada y abra la pestaña **Directivas** en el panel de detalles.
3. Haga clic en el nombre de la directiva que desea configurar.

Abra la ventana **Propiedades: <Nombre de la directiva>** con uno de los siguientes métodos:

- Al seleccionar la opción **Propiedades** en el menú contextual de la directiva.
- Al hacer 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 dispositivos protegidos dentro del grupo de administración seleccionado.
   - **Directiva para fuera de la oficina**, la directiva se activa cuando un equipo sale del perímetro de la red de la organización.
   - **Directiva inactiva**, si desea activar la directiva más tarde en todos los dispositivos protegidos dentro del grupo de administración seleccionado.
5. Configure los parámetros de la aplicación en otras secciones de la directiva.

   Puede habilitar o deshabilitar la ejecución de cualquier tarea en todos los dispositivos protegidos 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 dispositivos protegidos en red para cada componente de la aplicación particular.

6. Haga clic en **Aceptar**.

La configuración establecida se aplica en la directiva.

Indicador del nivel de seguridad

El indicador del nivel de seguridad se muestra en la parte superior de la ventana de propiedades de la directiva. El indicador puede tener uno de los valores siguientes:

- **Nivel de protección alto**. El indicador toma este valor y el color cambia a verde si todos los componentes pertenecientes a las siguientes categorías están habilitados y marcados con :
  - **Críticos**. Esta categoría incluye los siguientes componentes:
    - Protección de archivos en tiempo real.
    - Detección de comportamiento.
    - Prevención de exploits.

- Motor de reparación.
- Habilitar las notificaciones de Secure Desktop.

- **Importantes**. Esta categoría incluye el componente Uso de KSN.

- **Nivel de protección medio**. El indicador toma este valor y el color cambia a amarillo si un componente importante está deshabilitado o marcado con .
- **Nivel de protección bajo**. El indicador toma este valor y el color cambia a rojo si un componente crítico o varios están deshabilitados o marcados con .

Si el indicador muestra los valores **Nivel de protección medio** o **Nivel de protección bajo**, con el vínculo que se encuentra a la derecha del indicador se abre la ventana **Componentes de protección recomendados**. En esta ventana, puede habilitar cualquiera de los componentes de protección recomendados y evitar que se deshabiliten.

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.

Acerca de la creación de tareas en Kaspersky Security Center

Puede crear tareas de grupo para grupos de administración y conjuntos de dispositivos protegidos. Puede crear los siguientes tipos de tareas a través de Kaspersky Security Center:

- *Activar la aplicación*
- *Protección de la conexión del Servidor de administración*
- *Cambiar componentes de Kaspersky Embedded Systems Security*
- *Monitor comparativo de integridad del sistema*
- *Actualización*
- *Reversión de la actualización*
- *Análisis a pedido*
- *Comprobación de integridad de la aplicación*
- *Eliminar una clave*
- *Generador de reglas de 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 dispositivo protegido individual en la sección **Tareas**.
- Para un grupo de administración: en el panel de detalles del nodo del grupo seleccionado de dispositivos protegidos en la pestaña **Tareas**.
- Para un conjunto de dispositivos protegidos: en el panel de detalles del nodo **Selecciones de dispositivos**.

Puede usar directivas para deshabilitar programaciones de las tareas del sistema local *Actualización* y *Análisis a pedido* en todos los dispositivos 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 tareas 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 y seleccione el grupo al cual pertenezca el servidor protegido.
     b. En el panel de resultados, en la pestaña **Dispositivos**, abra el menú contextual del dispositivo protegido y seleccione **Propiedades**.
     c. En la ventana que se abre, en la sección **Tareas**, haga clic en el botón **Agregar**.
   - 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 resultados, abra la pestaña **Tareas** y seleccione **Nueva tarea**.

   Se abre la ventana del asistente de tareas.
2. En la ventana **Seleccione el tipo de tarea**, en el encabezado **Kaspersky Embedded Systems Security**, seleccione el tipo de tarea que se creará.

3. Es posible que varíe la configuración según el tipo de tarea:

   - Cree una tarea de Análisis a pedido.Cree una tarea de Análisis a pedido.
   - Para crear una tarea de actualización, configure los valores de la tarea según sus requisitos:

     a. Puede especificar el Servidor de administración de Kaspersky Security Center o los Servidores de actualizaciones de Kaspersky como un origen de actualizaciones de la aplicación en el bloque **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 si los servidores personalizados manualmente no están disponibles.

     b. Ajuste la configuración para una función que reduce la carga en el subsistema del disco:

     c. Puede especificar las acciones que Kaspersky Embedded Systems Security realizará cuando se necesiten actualizaciones críticas para los módulos de la aplicación y cuando se complete la instalación de tales actualizaciones. También puede indicar si Kaspersky Embedded Systems Security recibirá información sobre las actualizaciones programadas disponibles.

     d. Especifique el conjunto de actualizaciones que desea copiar y una ruta a la carpeta que Kaspersky Embedded Systems Security utilizará para almacenar las actualizaciones copiadas.

   - Para crear la tarea *Activar la aplicación*:

     a. En la ventana **Configuración de la activación**, especifique el archivo de clave o el código de activación 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 Generador de reglas de Control de inicio de aplicaciones.
   - Cree la tarea Generador de reglas para Control de dispositivos.

4. Configure la programación de la tarea.

5. Haga clic en **Aceptar**.

6. Si la tarea se crea para un conjunto de dispositivos protegidos, seleccione la red (o el grupo) de los dispositivos protegidos en los que se ejecutará esta tarea.

7. En la ventana **Seleccione una cuenta con la que ejecutar la tarea**, especifique la cuenta que desee utilizar para ejecutar la tarea.

8. En la ventana **Defina el nombre de la tarea**, ingrese el nombre de la tarea (100 caracteres como máximo y no debe contener los símbolos `" * < > ? \ | :`).

   Le recomendamos agregar el tipo de tarea al nombre de la tarea (por ejemplo, "Análisis a pedido de carpetas compartidas").

9. En la ventana **Finalizar la creación de la tarea**, haga lo siguiente:

    a. Seleccione la casilla de verificación **Ejecutar la tarea al finalizar el asistente** si desea que la tarea se inicie tan pronto como se cree.

    b. Haga clic en **Finalizar**.

La tarea creada se mostrará en la lista **Tareas**.

Ir a los ajustes de una tarea local y a los ajustes generales de la aplicación para un equipo individual

Si una aplicación se encuentra sujeta a una directiva de Kaspersky Security Center y dicha directiva no permite cambiar los ajustes de la aplicación, no podrá modificar esos ajustes para un equipo puntual.

Para ir a los ajustes de una tarea local para un equipo puntual:

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 dispositivo protegido.
3. En el panel de resultados, seleccione la pestaña **Dispositivos**.
4. Abra la ventana **Propiedades: <Nombre del dispositivo protegido>** con uno de los siguientes métodos:
    - Haga doble clic en el nombre del dispositivo protegido.
    - En el menú contextual del nombre del dispositivo protegido, seleccione **Propiedades**.

    Se abre la ventana **Propiedades: <Nombre del dispositivo protegido>**.
5. Vaya a la sección **Tareas**.
6. En la lista de tareas, realice alguna de estas acciones para seleccionar la tarea local que desee configurar:
    - haga doble clic en el nombre de la tarea
    - seleccione la tarea en la lista y haga clic en el botón **Propiedades**
    - en el menú contextual del nombre de la tarea, seleccione **Propiedades**

    Se abre la ventana **Propiedades: <Nombre de la tarea>**.

Para ir a los ajustes generales de la aplicación para un equipo puntual:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo al cual pertenezca el dispositivo protegido.
2. En el panel de resultados, seleccione la pestaña **Dispositivos**.

3. Abra la ventana **Propiedades: <Nombre del dispositivo protegido>** con uno de los siguientes métodos:

   - Haga doble clic en el nombre del dispositivo protegido.
   - En el menú contextual del nombre del dispositivo protegido, seleccione **Propiedades**.

   Se abre la ventana **Propiedades: <Nombre del dispositivo protegido>**.

4. Vaya a la sección **Aplicaciones**.

5. En la lista de aplicaciones instaladas, realice alguna de las siguientes acciones para seleccionar Kaspersky Embedded Systems Security:

   - haga doble clic en el nombre de Kaspersky Embedded Systems Security
   - seleccione Kaspersky Embedded Systems Security en la lista y haga clic en el botón **Propiedades**
   - en el menú contextual del nombre de Kaspersky Embedded Systems Security, seleccione el elemento **Propiedades**

   Se abre la ventana **Configuración** de **Kaspersky Embedded Systems Security**.

Configuración de tareas de grupo en Kaspersky Security Center

Para configurar una tarea de grupo para varios dispositivos protegidos:

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 desee 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.

4. 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**.

5. En la sección **Notificación**, establezca la configuración 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*.

6. Según el tipo de tarea configurada, realice una de las siguientes acciones:

   - Para configurar la tarea *Análisis a pedido*:
     - En la sección **Alcance del análisis**, configure un área del análisis.
     - En la sección **Configuración**, configure el nivel de prioridad de la tarea y la integración con otros componentes del programa.

- Para configurar la tarea *Actualización*:
  - Vaya a la sección **Configuración** y especifique **Configuración de actualización de módulos y bases de datos de la aplicación**.
  - Elija una acción a realizar: copiar e instalar actualizaciones críticas de módulos del programa o solo buscarlas.
- Para configurar la tarea *Activar la aplicación*:
  - En la sección **Configuración**, especifique el archivo de clave o código de activación que desea usar 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 tarea *Generador de reglas para Control de dispositivos*, en la sección **Configuración**, especifique la configuración que desee usar para crear la lista de reglas de Control de dispositivos.

7. Configure la programación de tareas en la sección **Programación**.
8. En la sección **Cuenta**, especifique la cuenta cuyos derechos se utilizarán para ejecutar la tarea. Para obtener información sobre la configuración de opciones en esta sección, consulte la *Ayuda de Kaspersky Security Center*.
9. 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*.
10. Haga clic en el botón **Aceptar** de la ventana **Propiedades: <Nombre de la tarea>**.

Se guardan las opciones de la tarea de grupo recientemente configuradas.

Debajo se enumera la configuración ajustable de las tareas de grupo.

- Generador de reglas de Control de inicio de aplicaciones

  Al configurar la tarea *Generador de reglas de Control de inicio de aplicaciones*, puede seleccionar cómo desea crear las reglas de autorización en la pestaña **Reglas**:

  - **Crear reglas de autorización para las aplicaciones en ejecución**.
  - **Crear reglas de autorización para las aplicaciones de las carpetas**.

  Puede especificar las siguientes acciones para que se lleven a cabo durante la creación de las reglas de autorización del Control de inicio de aplicaciones en la pestaña **Configuración**:

  - **Usar certificado digital**
  - **Usar sujeto y huella digital del certificado digital**
  - **De no haber un certificado, usar**
  - **Usar hash SHA256**
  - **Generar reglas para usuarios 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 finalizar la tarea.

Puede configurar las opciones para iniciar la tarea en base a una programación.

- Generador de reglas para Control de dispositivos
  - Seleccione el modo de operación: tener en cuenta los datos del sistema sobre todos los dispositivos externos que se hayan conectado o tener en cuenta solo los dispositivos externos conectados actualmente.
  - Ajuste la configuración para archivos de configuración con listas de reglas de autorización que Kaspersky Embedded Systems Security crea después de finalizar la tarea.
  - Puede configurar las opciones para iniciar la tarea en base a una programación.
- Activar la aplicación
  - Para activar la aplicación o renovar la licencia, puede agregar un archivo de clave o código de activación.
  - Puede configurar las opciones para iniciar la tarea en base a una programación.
- Actualización de bases de datos y módulos de la aplicación
  - Puede especificar el Servidor de administración de Kaspersky Security Center o los servidores de actualización de Kaspersky como origen de actualización de aplicaciones en el bloque de configuración **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 si los servidores personalizados manualmente no están disponibles.
  - Puede configurar para una función que reduce la carga en el subsistema del disco:
    - **Reducir la carga de lectura y escritura en disco**
    - **RAM usada para la optimización, MB**.
  - Puede especificar las acciones que Kaspersky Embedded Systems Security realizará cuando se necesiten actualizaciones críticas para los módulos de la aplicación y cuando se complete la instalación de tales actualizaciones. También puede indicar si Kaspersky Embedded Systems Security recibirá información sobre las actualizaciones programadas disponibles.
  - Puede especificar el conjunto de actualizaciones que desea copiar y una ruta a la carpeta que Kaspersky Embedded Systems Security utilizará para almacenar las actualizaciones copiadas.
  - Puede configurar las opciones para iniciar la tarea en base a una programación.
- Análisis a pedido
  - Puede especificar un área del análisis para la tarea de Análisis a pedido y configurar las opciones del nivel de seguridad.
  - En el bloque de opciones del **Analizador heurístico**, puede habilitar o deshabilitar el uso del analizador heurístico en la tarea Análisis a pedido y definir, mediante un control deslizante, el nivel de análisis que se usará.

- En el bloque **Integración con otros componentes**, puede establecer la siguiente configuración:
  - Inicie la tarea de análisis en modo de segundo plano.
  - Considerar la tarea como análisis de áreas críticas.
  - Deshabilitar el inicio simultáneo de varias tareas de análisis.
- Puede configurar las opciones para iniciar la tarea en base a una programación.

- Comprobación de integridad de la aplicación
  - Puede configurar las opciones para iniciar la tarea en base a una programación.
- Monitor comparativo de integridad del sistema
  - Puede configurar el modo de monitoreo y reglas que especifiquen las acciones que se deben tomar en los archivos, el registro y los dispositivos.
  - Puede configurar las opciones para iniciar la tarea en base a una programación.

Tarea Activar la aplicación

Para configurar la tarea Activar 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.
4. 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.
   - Abra el menú contextual del nombre de la tarea en la lista de tareas creadas y seleccione el elemento **Propiedades**.

   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. Active la casilla **Usar como clave adicional** si desea agregar una clave para renovar la licencia.
6. En la sección **Programación**, configure las opciones de programación de la tarea.
7. 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*.

8. Haga clic en el botón **Aceptar** de la ventana **Propiedades: <Nombre de la tarea>**.

   Se guardan las opciones de la tarea de grupo recientemente configuradas.

Tarea de actualización

Para configurar la tarea Actualización:

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.
4. 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.
   - Abra el menú contextual del nombre de la tarea en la lista de tareas creadas y seleccione el elemento **Propiedades**.
5. 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*.
6. En la sección **Configuración**, haga lo siguiente:
   a. Elija un origen de actualizaciones con el botón **Configuración** en la sección **Configuración de actualización de módulos y bases de datos de la aplicación**:
      - Servidor de administración de Kaspersky Security Center.
      - Servidores de actualizaciones de Kaspersky.
      - Servidores FTP o HTTP personalizados o carpetas de red.

      Para usar una carpeta compartida de SMB como origen de actualizaciones, debe especificar una cuenta de usuario para iniciar una tarea.

      Puede especificar el uso de Servidores de actualizaciones de Kaspersky si los servidores personalizados manualmente no están disponibles.

   b. Ajuste la configuración para una función que reduce la carga en el subsistema del disco:
      - **Reducir la carga de lectura y escritura en disco**. Esta casilla de verificación habilita o deshabilita el proceso mediante el cual el subsistema del disco se optimiza a través del almacenamiento de archivos de actualización en una unidad virtual en RAM. De forma predeterminada, la casilla no está activada.
      - **RAM usada para la optimización, MB**.

c. Especifique las acciones que Kaspersky Embedded Systems Security debe realizar cuando hay actualizaciones críticas de módulos de la aplicación disponibles o cuando hay información acerca de actualizaciones planificadas.

d. Especifique la configuración para la copia de actualizaciones.

7. Configure la programación de la tarea en la sección **Programación** (puede configurar una programación para todos los tipos de tareas excepto Reversión de la actualización).

8. En la sección **Cuenta**, especifique la cuenta cuyos derechos se utilizarán para ejecutar 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**.

Para la tarea *Reversión de la actualización*, 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 Comprobación 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 desee configurar la tarea Control de integridad 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 de Control de integridad de la aplicación que desea configurar.

4. 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.

   - Abra el menú contextual del nombre de la tarea en la lista de tareas creadas y seleccione el elemento **Propiedades**.

5. 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*.

6. En la sección **Dispositivos**, seleccione los dispositivos para los cuales desea configurar la tarea Control de integridad de la aplicación.

7. En la sección **Programación**, configure las opciones de programación de la tarea.

8. En la sección **Cuenta**, especifique la cuenta cuyos derechos se utilizarán para ejecutar la tarea.

9. 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*.

10. Haga clic en el botón **Aceptar** de la ventana **Propiedades: <Nombre de la tarea>**.

Administración de programaciones de tareas

Puede programar tareas de Kaspersky Embedded Systems Security.

Tareas de programación

Puede programar las tareas personalizadas y las tareas locales del sistema en la Consola de la aplicación. No puede programar tareas de grupo en la Consola de la aplicación.

Para programar tareas de grupo mediante el Complemento de administración, realice lo siguiente:

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 dispositivo protegido.
3. En el panel de resultados, 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 la lista desplegable **Inicio programado**, seleccione los parámetros de inicio:

   Los campos con la configuración de programación para las tareas análisis a pedido y actualización no estarán disponibles si una directiva de Kaspersky Security Center bloquea la programación de estas tareas.

   - **Cada N horas** si desea que la tarea se ejecute periódicamente cada pocas horas; ingrese el número de horas en el campo **Intervalo de inicio (h)**.
   - **Cada N días** si desea que la tarea se ejecute periódicamente cada pocos días; ingrese el número de días en el campo **Intervalo de inicio (días)**.
   - **Cada N minutos** si desea que la tarea se ejecute periódicamente cada pocos minutos; ingrese el número de minutos en el campo **Intervalo de inicio (minutos)**.

- **Semanal** si desea que la tarea se ejecute un día específico de la semana; especifique también la hora de ejecución deseada.
- **Mensual** si desea que la tarea se ejecute un día específico del mes; especifique también la hora de ejecución deseada.
- **Una vez** si desea que la tarea se ejecute una vez en una fecha y hora especificadas.
- **Manual** si desea ejecutar la tarea manualmente.
- **Al inicio de la aplicación** si desea que la tarea se ejecute cada vez que se inicia Kaspersky Embedded Systems Security.
- **Al descargar nuevas actualizaciones al repositorio** si desea que la tarea se ejecute cada vez que se descarguen actualizaciones en el repositorio.
- **Ante brotes de virus** si desea que la tarea se ejecute si se detecta un ataque de virus.
- **Al completarse otra tarea** si desea que la tarea se ejecute al finalizar otra tarea.

a. Especifique la hora del primer inicio de la tarea en el campo **Hora de inicio**.

b. En el campo **Planificación para**, especifique la fecha de inicio de la programación.

Luego de programar la hora de inicio, fecha y frecuencia de la tarea, se muestra el tiempo estimado hasta el próximo inicio.

Vaya a la pestaña **Programación** y abra la ventana **Configuración de la tarea**. En el campo **Próximo inicio** en la parte superior de la ventana, se muestra la hora de inicio estimada. Cada vez que abre la ventana, la hora estimada de inicio se actualiza y se muestra.

El campo **Próximo inicio** muestra el valor **Bloqueado por directiva** si la configuración de la directiva activa de Kaspersky Security Center prohíbe el inicio de tareas locales del sistema programadas.

7. Seleccione la casilla de verificación **Ejecutar tareas no realizadas** para habilitar el inicio de las tareas omitidas.

8. Si se selecciona la casilla **Utilizar retardo aleatorio automático para el inicio de la tarea**, la tarea no se ejecuta estrictamente según lo programado, sino aleatoriamente dentro de un cierto intervalo, es decir, se distribuyen las horas de inicio de la tarea.

9. Haga clic en **Avanzado** para configurar las siguientes opciones de programación de acuerdo con sus requisitos:

- **Encender dispositivos mediante la función Wake-on-LAN antes de iniciar la tarea**. Si se selecciona la casilla, el sistema operativo del equipo recibe un tiempo de espera especificado para completar el inicio antes de que se ejecute la tarea. El tiempo de espera predeterminado es de 5 minutos.
- **Apagar dispositivos cuando se complete la tarea**. Si se selecciona la casilla, los dispositivos se desactivarán una vez que se completa la tarea.
- **Detener la tarea si tarda más de**. Si se selecciona la casilla, la tarea se detendrá si se ejecuta durante más tiempo que el especificado.

10. Haga clic en **Aceptar**.

11. Haga clic en el botón **Aplicar** para guardar la configuración de inicio de la tarea.

Si desea establecer la configuración de la aplicación para una sola tarea con Kaspersky Security Center, consulte la sección "Configuración de tareas locales en la ventana de configuración de la aplicación de Kaspersky Security Center".

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:

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 dispositivo 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. Seleccione la configuración para ejecutar una tarea programada en la lista desplegable **Inicio programado** si desea habilitar el inicio de la tarea programada.

7. Seleccione **Manual** en la lista desplegable si desea deshabilitar el inicio de la tarea programada.

La programación configurada para la tarea no se eliminará y se aplicará la próxima vez que habilite el inicio de una tarea programada.

8. Haga clic en **Aceptar**.

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 de estado de los componentes de Kaspersky Embedded Systems Security

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*, *Suspendido*, *Detenido* o *Sin cobertura por la licencia*.

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 un conjunto especificado 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**.
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 Servidor de administración>** en el árbol de la Consola de administración.
2. Seleccione 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 el estado, la versión, el dispositivo y el grupo del componente.

Informes sobre aplicaciones prohibidas en los modos activo y de prueba

En base a los resultados 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 modo Activo) y un informe sobre las aplicaciones prohibidas en modo de prueba (si la tarea se inició en modo Solo estadísticas). Estos informes muestran información sobre las aplicaciones bloqueadas en los dispositivos protegidos de la red. Cada informe se genera para todos los grupos de administración y acumula datos de todas las aplicaciones de Kaspersky instaladas en los dispositivos protegidos.

Para revisar un informe sobre aplicaciones prohibidas en el modo Informar:

1. Ejecute la tarea Control de inicio de aplicaciones en el modo Informar.
2. Seleccione el nodo **Servidor de administración <nombre del Servidor de administración>** en el árbol de la Consola de administración.
3. Seleccione la pestaña **Informes**.
4. Haga doble clic en el elemento **Informe sobre aplicaciones prohibidas en modo de prueba**.

   Se genera un informe.
5. Revise los siguientes detalles del informe:

   - Diagrama gráfico que muestra las diez primeras aplicaciones con el mayor número de inicios bloqueados.
   - Una tabla que resume los bloqueos de aplicaciones, donde se especifican el nombre del archivo ejecutable, el motivo, el tiempo de bloqueo y el número de dispositivos donde se bloqueó.
   - 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. Ejecute la tarea Control de inicio de aplicaciones en el modo Activo.
2. Seleccione el nodo **Servidor de administración <nombre del Servidor de administración>** en el árbol de la Consola de administración.
3. Seleccione la pestaña **Informes**.
4. Haga doble clic en el elemento **Informe sobre aplicaciones prohibidas**.

   Se genera un informe.

Este informe consiste en los mismos datos sobre bloqueos que el informe sobre aplicaciones prohibidas en 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 dispositivo protegido o en otro dispositivo.

Iniciar la Consola de la aplicación.

Para iniciar la Consola de la aplicación:

1. Abra la Interfaz de diagnóstico compacto de una de las siguientes maneras:

   - Ejecute el archivo avpui.exe de la carpeta de instalación de la aplicación en el dispositivo protegido. De forma predeterminada, el archivo se encuentra en C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.0.0.

   - Haga clic en el ícono de la aplicación en el área de notificaciones de la barra de tareas.

2. En la ventana de la Interfaz de diagnóstico compacto que se abre, haga clic en el vínculo **Consola de Kaspersky Embedded Systems Security**.

   Si ya configuró una conexión con el dispositivo protegido, se abre la Consola de la aplicación.

   Si inicia la Consola de la aplicación por primera vez, se lo llevará a la ventana **Seleccionar dispositivo protegido**, en la que debes **configurar la conexión de la Consola de la aplicación al equipo protegido**.

   a. Si Kaspersky Embedded Systems Security y la Consola de la aplicación están instalados en el mismo equipo, seleccione **Equipo local (el equipo en el que se ejecuta la Consola de aplicaciones)**.

   b. Si Kaspersky Embedded Systems Security y la Consola de la aplicación están instalados en diferentes equipos, siga estos pasos:

      1. Seleccione **Otro dispositivo**.

      2. Haga clic en **Examinar** y especifique el nombre del equipo donde está instalada la aplicación.

      3. Ingrese el puerto para conectarse al equipo con la aplicación instalada.

   c. Seleccione o borre la selección de la casilla de verificación **Conectarse como usuario** para habilitar o deshabilitar el uso de permisos de cuenta de usuario al conectar la Consola de la aplicación al equipo con la aplicación instalada.

d. Si habilita la conexión como usuario, ingrese el nombre y la contraseña del usuario. El usuario especificado debe ser miembro del grupo de administradores de ESS en el equipo donde está instalada la aplicación.

El nombre de usuario distingue entre mayúsculas y minúsculas.

e. Haga clic en **Conectar**.

Interfaz de la Consola de Kaspersky Embedded Systems Security

En esta sección se describen los elementos principales de la interfaz de la aplicación.

Ventana Consola de Kaspersky Embedded Systems Security

Una vez que se establece conexión con una copia de Kaspersky Embedded Systems Security instalada en un dispositivo protegido diferente, el nombre del nodo se complementa con el nombre del dispositivo protegido en el que se instaló la aplicación y el nombre de la cuenta de usuario con la que se estableció la conexión: **Kaspersky Embedded Systems Security <nombre del dispositivo> como <nombre de la cuenta>**. Cuando la conexión se establece con una copia de Kaspersky Embedded Systems Security que se encuentra instalada en el mismo dispositivo protegido que la Consola de Kaspersky Embedded Systems Security, el nombre del nodo es Kaspersky Embedded Systems Security.

Árbol de la Consola

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** permite configurar las siguientes tareas:
  - **Protección de archivos en tiempo real**
  - **Kaspersky Security Network**
  - **Prevención de exploits**
  - **Protección contra amenazas de red**
  - **Detección de comportamiento**
  - **Motor de reparación**
  - **Protección vía AMSI**.

- **Control del equipo**: control de las aplicaciones que se ejecutan en el dispositivo protegido y en los dispositivos conectados.
  - **Control de inicio de aplicaciones**
  - **Control de dispositivos**
  - **Firewall**.
- **Generación automática 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 de Control de inicio de aplicaciones**
  - **Generador de reglas para Control de dispositivos**
  - Tareas de grupo de generación de reglas **<Nombres de las tareas>** (si corresponde)

    Las tareas del grupo se crean mediante Kaspersky Security Center. No puede administrar tareas de grupo a través de la Consola de Kaspersky Embedded Systems Security.
- **Inspección del sistema**: configuración de las opciones de Control de integridad del sistema y el análisis de registros de eventos de Windows.
  - **Inspección de registros**
  - **Control de integridad del sistema**.
- **Análisis a pedido**: administra las tareas de Análisis a pedido. Hay un nodo independiente para cada tarea:
  - **Análisis de áreas críticas**
  - **Control de integridad de la aplicación**
  - **Análisis de unidades extraíbles**
  - **Análisis completo**
  - Tareas personalizadas **<Nombres de las tareas>** (si corresponde)

  El nodo muestra tareas del sistema que se crean cuando la aplicación se instala, tareas personalizadas y tareas de grupo de análisis a pedido creadas y enviadas a un dispositivo protegido mediante Kaspersky Security Center.
- **Actualización**: administra las actualizaciones para las bases de datos y los módulos de la aplicación de Kaspersky Embedded Systems Security y proporciona la posibilidad de revertir la última actualización:
  - **Actualización de bases de datos y módulos de la aplicación**
  - **Reversión de la última actualización**
  - **Actualización de aplicación**.

  El nodo muestra todas las tareas personalizadas y de actualización de grupo creadas y enviadas a un dispositivo protegido mediante Kaspersky Security Center.

- **Depósitos**: administra la configuración de Copia de seguridad y la lista de sesiones de red bloqueadas.
  - **Copias de seguridad**
  - **Sesiones de red bloqueadas**.
- **Registros y notificaciones**: administra los registros de tareas locales y el registro de auditoría del sistema de Kaspersky Embedded Systems Security.
  - **Auditoría del sistema**
  - **Control de inicio de aplicaciones**
  - **Control de dispositivos**
  - **Control de integridad de la aplicación**
  - **Inspección de registros**
  - **Control de integridad del sistema**
  - **Protección contra amenazas de red**
  - **Análisis a pedido**
  - **Firewall**
  - **Prevención de exploits**
  - **Detección de comportamiento**
  - **Escáner AMSI**
  - **Actualización**
  - **Protección de archivos en tiempo real**
  - **Copias de seguridad**.
- **Licencias**: permite agregar y eliminar claves de Kaspersky Embedded Systems Security y ver los 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 dispositivo e información sobre Kaspersky Embedded Systems Security, el estado de protección de sus componentes funcionales y el estado de la clave.

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:

- **Suspender protección**.
- **Configurar Zona de confianza**. Consulte y configure las opciones de la Zona de confianza.
- **Análisis de unidades extraíbles**. Configure el análisis de unidades extraíbles conectadas al dispositivo protegido a través del puerto USB.
- **Permisos de acceso de usuario para administrar la aplicación**. Consulte y configure los permisos para acceder a las funciones de Kaspersky Embedded Systems Security.
- **Permisos de acceso de usuario para la administración del servicio de Kaspersky Security**. Vea y configure los derechos de usuario para administrar el servicio de Kaspersky Security.
- **Depósitos**
- **Exportar configuración**. Guarde la configuración de la aplicación en un archivo de configuración con formato XML. 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. También puede realizar esta operación en los menús contextuales de las tareas de la aplicación.
- **Actualizar**. Actualice el contenido de la ventana de la Consola de Kaspersky Embedded Systems Security. También puede realizar esta operación en los menús contextuales de las tareas de la aplicación.
- **Propiedades de la aplicación**. 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.

- **Ayuda**. Consulte la información en 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 las tareas de la aplicación con los menús contextuales disponibles para cada tarea en el árbol de la Consola de Kaspersky Embedded Systems Security.

Puede usar los elementos del menú contextual para realizar las siguientes operaciones:

- **Reanudar/Pausar**. Reanudar o pausar la ejecución de tareas. 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.
- **Crear tarea**. Cree una nueva tarea personalizada.
- **Eliminar tarea**. Elimine la tarea personalizada.

- **Exportar configuración/Importar configuración**. Exporte o importe la configuración de la tarea.
- **Propiedades**. Abra la ventana de configuración de tareas.
- **Ayuda**. Abra el tema de la ayuda en línea correspondiente.

Icono de la bandeja del sistema en el área de notificación

Inmediatamente después de instalar Kaspersky Embedded Systems Security, aparece el icono de la aplicación en el área de notificación de la barra de tareas de Microsoft Windows.

Si el ícono de la aplicación en el área de notificación de la barra de tareas está oculto, el administrador deshabilitó la visualización de la interfaz de la aplicación en la directiva.

El icono tiene las siguientes finalidades:

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

El funcionamiento de la aplicación se representa a través de los siguientes iconos de estado:

- El icono indica que los componentes de protección críticos están habilitados. El icono de advertencia aparece cuando Kaspersky Embedded Systems Security necesita que el usuario realice alguna acción (por ejemplo, reiniciar el equipo tras una actualización del software).
- El icono indica que uno o más componentes de protección críticos están deshabilitados o han tenido problemas de funcionamiento. Los problemas de funcionamiento pueden deberse a un error en la aplicación, por ejemplo, o al hecho de que la licencia haya caducado. Kaspersky Embedded Systems Security mostrará una advertencia ( ) junto con una descripción del inconveniente de protección.

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 para mostrar ventanas de aplicaciones (consulte la tabla a continuación).

Comandos del menú contextual en el icono de la bandeja del sistema

Comando	Descripción
Abrir la Consola de la aplicación	Abre la Consola de Kaspersky Embedded Systems Security (si está instalada).
Abrir Interfaz de diagnóstico compacto	Abre la Interfaz de diagnóstico compacto.
Acerca de	Abre la ventana **Acerca de** que contiene información acerca de Kaspersky Embedded Systems Security. Para los usuarios registrados de Kaspersky Embedded Systems Security, la ventana **Acerca de** 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 volver a mostrar el Icono de la bandeja del sistema,

en el menú **Inicio** de Microsoft Windows, seleccione **Todos los programas** > **Kaspersky Embedded Systems Security**. El ícono aparecerá en el área de notificaciones de la barra de tareas de Microsoft Windows.

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

Ajustar la configuración general a través de 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 operativas para la aplicación. Este parámetro le permite controlar el número de procesos de trabajo que utiliza Kaspersky Embedded Systems Security, habilitar la recuperación de las tareas de Kaspersky Embedded Systems Security después de una cancelación anormal, mantener el registro, habilitar la creación de archivos de volcado de los procesos de Kaspersky Embedded Systems Security después de una cancelación anormal y configurar otros parámetros generales.

Los ajustes de la aplicación no se pueden configurar en Kaspersky Embedded Systems Security Console si la directiva activa de Kaspersky Security Center bloquea los cambios en estas opciones.

Para ajustar la configuración general 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 resultados del nodo.
   - Seleccione **Propiedades de la aplicación** en el menú contextual del nodo.

   Se abre la ventana **Propiedades de la aplicación**.

2. En la sección **Interfaz**, puede especificar las advertencias que desea ver en el ícono de bandeja del sistema de Kaspersky Embedded Systems Security.

3. En la pestaña **Configuración de seguridad**, establezca la siguiente configuración:

   - En la sección **General**, configure la opción **Iniciar la aplicación al arrancar el equipo (recomendado)**.
   - En **Autoprotección**, configure la protección de los módulos de la aplicación y los servicios del sistema operativo.
   - En la sección **Acciones al pasar a usar alimentación de respaldo (UPS)**, especifique limitaciones de la carga del dispositivo protegido creadas por Kaspersky Embedded Systems Security después de cambiar a la alimentación de UPS:
     - **No iniciar las tareas de análisis programadas**.
     - **Detener las tareas de análisis en ejecución**.

- En la sección **Configuración de compatibilidad**, configure la opción **Compatible con software de administración remota**.

  Si el uso de Kaspersky Embedded Systems Security junto con las herramientas de administración remota (RAT) causa problemas, puede habilitar el modo de compatibilidad. Los problemas pueden estar relacionados con la incompatibilidad de las RAT con la funcionalidad de Escritorio seguro de la aplicación. El propósito de esta funcionalidad es confirmar las acciones que potencialmente pueden reducir el nivel de seguridad del equipo. Esta funcionalidad permite que una aplicación muestre un cuadro de diálogo de confirmación aislado de otros procesos. Esta funcionalidad utiliza derechos de alto nivel para proteger la solicitud. De esta forma, solo el usuario puede confirmar la acción y no el malware.

  Si se selecciona la casilla, se habilita el modo de compatibilidad con la RAT. La aplicación muestra un cuadro de diálogo de confirmación sin esta funcionalidad. Esto puede reducir el nivel de seguridad del equipo. No recomendamos habilitar el modo de compatibilidad si Kaspersky Embedded Systems Security no está causando problemas con la RAT.

  Si cancela la selección de la casilla de verificación, se deshabilita el modo de compatibilidad con la RAT. De forma predeterminada, la casilla no está activada.

  Por ejemplo: si se utiliza el navegador en modo RemoteApp, es posible que Kaspersky Embedded Systems Security no muestre una ventana de confirmación cuando se visita un sitio web con un certificado no confiable, ya que RemoteApp no admite la funcionalidad de Escritorio seguro de la aplicación. Esto puede hacer que el navegador deje de responder. Para que el navegador funcione correctamente en el modo RemoteApp, debe habilitar el modo de compatibilidad.

  También puede intentar habilitar el modo de compatibilidad si tiene problemas con la funcionalidad de Escritorio Seguro al utilizar otro software de terceros.

- En la sección **Configuración de análisis**, configure la **restricción de uso de CPU para las tareas de análisis** y habilite la opción Conceder recursos a otras aplicaciones.

  Kaspersky Embedded Systems Security limita el uso de CPU del dispositivo protegido durante las tareas de análisis a pedido al valor especificado en el campo **Límite máximo**.

  > Sin embargo, la aplicación puede usar mucho más tiempo de CPU debido a otros componentes.

  La activación de esta funcionalidad puede afectar negativamente el rendimiento de Kaspersky Embedded Systems Security.

  De manera predeterminada, esta función está deshabilitada.

4. En la pestaña **Configuración de red**, establezca la siguiente configuración:

   - En la sección **Servidor proxy**, especifique la configuración del servidor proxy: tipo de autenticación y detalles requeridos para la autenticación en el servidor proxy.

   - En **Puerto para conexión remota**, de ser necesario, cambie los puertos que usa la Consola de la aplicación para conectarse a un equipo con la aplicación instalada.

     El número de puerto predeterminado para la conexión con las credenciales de Windows es 13032. El número de puerto predeterminado para la conexión con las credenciales de los usuarios creados manualmente es 13031. Intervalo de posibles números de puerto: 1-65535.

El números de puerto guardados anteriormente se utiliza hasta que se reinicia la aplicación.

5. En la pestaña **Diagnóstico de mal funcionamiento**, haga clic en **Configuración** y configure el seguimiento y el volcado de memoria de la aplicación.

1. Seleccione la ficha **Configuración de volcado de la aplicación**.
2. Seleccione o desactive la casilla **Crear archivo de volcado** para habilitar o deshabilitar el volcado de memoria en caso de mal funcionamiento.

   De manera predeterminada, los archivos de volcado de memoria se almacenan en la siguiente carpeta: %ProgramData%\Kaspersky Lab\KESS.4.0\Traces. Puede especificar otra ruta.

El campo **Carpeta de archivos de seguimiento** contiene la ruta completa a la carpeta local en la que Kaspersky Embedded Systems Security guarda los archivos de rastreo de manera predeterminada. Puede especificar otra ruta.

1. En la lista desplegable **Nivel de detalle**, seleccione el nivel de detalle de la información para depuración:

   - **Crítico** significa que el archivo de rastreo guarda solo los mensajes acerca de errores fatales.
   - **Diagnóstico** significa que el archivo de rastreo guarda mensajes acerca de todos los errores y las advertencias.
   - **Importante** significa que el archivo de rastreo guarda mensajes acerca de todos los errores, advertencias e información adicional.
   - **Normal** significa que el archivo de rastreo guarda mensajes acerca de todos los errores, advertencias, así como información acerca del funcionamiento normal de la aplicación (predeterminado).
   - **Detallado** significa que el archivo de rastreo guarda toda la información acerca del funcionamiento de la aplicación.

   El nivel de detalle que se requiere para solucionar cualquier posible problema es determinado por un especialista del servicio de soporte técnico.

   El nivel de detalle predeterminado es **Normal**.

2. Especifique el **Tamaño máximo de los archivos de seguimiento (MB)**.

   Valores disponibles: de 1 a 4095 MB. De forma predeterminada, el tamaño máximo de los archivos de seguimiento es de 100 MB.

3. Para que los archivos de seguimiento antiguos se eliminen cuando se alcance el número máximo de archivos, seleccione la casilla **Eliminar los archivos de seguimiento más antiguos**.

4. Especifique el **Cantidad máxima de archivos para un registro de seguimiento**.

   Valores disponibles: de 1 a 999. De manera predeterminada, el número máximo de archivos es 5. El campo está disponible si la casilla de verificación **Eliminar los archivos de seguimiento más antiguos** está seleccionada.

Kaspersky Embedded Systems Security escribe la información en los archivos de seguimiento y el archivo de volcado de memoria en formato no cifrado. La carpeta donde se guardan los archivos, administrada por la configuración del sistema operativo y la configuración de Kaspersky Embedded Systems Security. Puede configurar los permisos de acceso y permitir que solo los usuarios necesarios puedan acceder a los registros, los archivos de rastreo y los archivos de volcado.

6. Haga clic en **Aceptar**.

Se guarda la configuración de Kaspersky Embedded Systems Security.

Administración de tareas de Kaspersky Embedded Systems Security

En esta sección, encontrará información sobre cómo crear, configurar, iniciar y detener tareas de Kaspersky Embedded Systems Security.

Categorías de tareas de Kaspersky Embedded Systems Security

Las funciones Protección del equipo en tiempo real, Control del equipo, Generación automática de reglas, Inspección del sistema, Análisis a pedido, Protección de red industrial, Administración de almacenamiento y Actualización en Kaspersky Embedded Systems Security se implementan como tareas.

Puede administrar estas tareas con el menú contextual de la tarea en el árbol de la Consola de Kaspersky Embedded Systems Security y el panel de resultados. Puede consultar información sobre el estado de la tarea en el panel de resultados. 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 pueden ejecutarse en el dispositivo protegido para el que fueron creadas. Según el método de inicio, existen los siguientes tipos de tareas locales:

- **Tareas locales del sistema**. Estas tareas se crean automáticamente durante la instalación de Kaspersky Embedded Systems Security. Puede cambiar la configuración de todas las tareas locales del sistema, excepto la tarea *Reversión de la actualización*. Las tareas locales del sistema no se pueden renombrar o eliminar. Puede ejecutar al mismo tiempo tareas de análisis a pedido personalizadas y locales del sistema.

- **Tareas locales personalizadas**. En la Consola de la aplicación, puede crear las tareas Análisis a pedido, Actualización y Monitor comparativo de integridad del sistema. En Kaspersky Security Center, puede crear tareas de Análisis a pedido, tareas de Actualización, etc. Puede cambiar el nombre, configurar o eliminar tareas personalizadas. Puede ejecutar varias tareas personalizadas simultáneamente.

Tareas de grupo

Puede administrar tareas de grupo y tareas para grupos de dispositivos protegidos desde Kaspersky Security Center. Todas las tareas de grupo son tareas personalizadas. Las tareas de grupo también se muestran en la Consola de la aplicación. En la Consola de la aplicación, solo puede ver el estado de las tareas de grupo. No puede usar la Consola de la aplicación para administrar o configurar tareas de grupo.

Cómo iniciar, pausar, reanudar y detener tareas manualmente

Puede iniciar, pausar, reanudar o detener tareas manualmente. Estas opciones no están disponibles para todas las tareas de Kaspersky Embedded Systems Security.

Para iniciar, pausar, reanudar o detener una tarea, realice lo siguiente:

1. En la Consola de la aplicación, abra el menú contextual de la tarea.
2. Seleccione uno de los siguientes comandos: **Inicio** o **Pausar**.

La operación se realiza y se registra en el Registro de auditoría del sistema.

Administración de programaciones de tareas

Puede programar tareas de Kaspersky Embedded Systems Security.

Configuración de las opciones de programación de tareas

En la Consola de la aplicación, puede programar el tiempo de inicio de tareas locales del sistema y tareas personalizadas. Sin embargo, no puede programar el tiempo de inicio de tareas de grupo.

Para programar una tarea, realice lo siguiente:

1. En el árbol de la Consola, seleccione la tarea para la cual desea configurar la programación.
2. En el panel de resultados, haga clic en **Modo de ejecución** o **Propiedades**.
3. En la sección **Modo de ejecución**, seleccione **Mediante programación**.
4. Siga estos pasos para especificar la configuración de programación:
    a. En la lista desplegable **Frecuencia**, seleccione una de las siguientes opciones:
        - **Minutos** si desea que la tarea se ejecute periódicamente cada pocos minutos; ingrese el número de minutos en el campo **Ejecutar cada <número> minuto(s)**.
        - **Horas** si desea que la tarea se ejecute periódicamente cada pocas horas; ingrese el número de horas en el campo **Ejecutar cada <número> hora(s)**.

- **Días** si desea que la tarea se ejecute periódicamente cada pocos días; ingrese el número de días en el campo **Ejecutar cada <número> día(s)**.
- **En el momento especificado** si desea que la tarea se ejecute una vez en una fecha y hora especificadas.
- **Cada mes** si desea que la tarea se ejecute cada mes. Especifique los días del mes y la hora en las que desea que la tarea se ejecute (de manera predeterminada, la tarea se ejecuta el primer día de cada mes).
- **Después de iniciar la aplicación** si desea que la tarea se ejecute cada vez que se inicia Kaspersky Embedded Systems Security.

b. Especifique el periodo o la fecha y hora del primer inicio de la tarea según la opción seleccionada en el primer paso.

c. También puede especificar el tiempo que desea retrasar la ejecución de la tarea después de iniciar la aplicación.

d. Especifique el nombre de usuario y la contraseña para ejecutar la tarea.

5. Haga clic en **Aceptar**.

Se guarda la configuración de programación 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 el inicio de una tarea programada, realice lo siguiente:

1. Seleccione la tarea necesaria en el árbol de la Consola de la aplicación.
2. En el panel de resultados, haga clic en el vínculo **Modo de ejecución**.

   Se abre la ventana **Programación y modo de ejecución**.
3. En la ventana que se abre, en la pestaña **Modo de ejecución**, realice una de las siguientes acciones:
   - Seleccione la casilla de verificación **Manual** si desea deshabilitar el inicio programado de la tarea.
   - Seleccione la casilla de verificación **Mediante programación** si desea habilitar el inicio programado de la tarea.
4. Haga clic en **Aceptar**.

Se guarda la configuración de programación de la tarea.

Uso de cuentas de usuario para iniciar tareas

Puede iniciar tareas con la cuenta de sistema o bien especificar una cuenta diferente.

Acerca del uso de cuentas para iniciar tareas

Puede especificar la cuenta para ejecutar las siguientes tareas de Kaspersky Embedded Systems Security:

- Generador de reglas de Control de inicio de aplicaciones
- Generador de reglas para Control de dispositivos
- Inspección de registros
- Comprobación de integridad de la aplicación
- Actualización de bases de datos y módulos de la aplicación
- 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:

- Tarea **Actualización**: si definió una carpeta compartida de otro dispositivo de la red como origen de actualizaciones.
- Tarea **Actualización**: si utiliza un servidor proxy con autenticación NTLM de Windows incorporada para acceder al origen de actualizaciones.
- Tarea **Generador de reglas de Control de inicio de aplicaciones**: si las reglas generadas se exportan a un archivo de configuración al cual la cuenta de sistema no puede acceder (por ejemplo, en una carpeta compartida en el dispositivo protegido).

Puede iniciar las tareas enumeradas con los privilegios de la cuenta del sistema. Kaspersky Embedded Systems Security realiza estas tareas y accede a las carpetas compartidas en otro dispositivo en la red si este dispositivo está registrado en el mismo dominio que el dispositivo protegido. En este caso, la cuenta del sistema debe tener permisos de acceso a estas carpetas. Kaspersky Embedded Systems Security accede al dispositivo mediante los permisos de la cuenta **<nombre de dominio \ nombre_de_dispositivo>**.

Especificación de una cuenta de usuario para iniciar una tarea

La opción para especificar una cuenta en la Consola de la aplicación no está disponible para todas las tareas.

Para especificar una cuenta para iniciar una tarea:

1. En el árbol de la Consola de la aplicación, seleccione la tarea que desea iniciar con los derechos de una cuenta específica.
2. En el panel de resultados, haga clic en el vínculo **Modo de ejecución**.

   Se abre la ventana **Programación y modo de ejecución**.

3. En la ventana que se abre, en la sección **Usuario**, realice las siguientes operaciones:

   a. Seleccione la opción **Ejecutar la tarea como**.

   b. Escriba el nombre de usuario y la contraseña de la cuenta que desea usar.

   El usuario seleccionado debe estar registrado en el dispositivo protegido o en el mismo dominio que este equipo.

4. Haga clic en **Aceptar**.

La configuración modificada se guarda.

Cómo importar y exportar la configuración

En esta sección, se explica cómo exportar la configuración de Kaspersky Embedded Systems Security. También aprenderá cómo exportar una configuración de componentes específicos de la aplicación a un archivo de configuración XML y cómo importarla desde un archivo de configuración a la aplicación.

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
- Prevención de exploits
- Protección contra amenazas de red
- Detección de comportamiento.
- Motor de reparación
- Escáner AMSI
- Control de inicio de aplicaciones
- Control de dispositivos
- Firewall
- Generador de reglas de Control de inicio de aplicaciones

- Generador de reglas para Control de dispositivos
- Inspección de registros
- Control de integridad del sistema
- Análisis de áreas críticas
- Comprobación de integridad de la aplicación
- Análisis de unidades extraíbles
- Análisis completo
- Actualización de bases de datos y módulos de software de la aplicación
- Reversión de la última actualización
- Actualización

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 la tarea de grupo.

Kaspersky Embedded Systems Security exporta todas las contraseñas usadas por la aplicación, por ejemplo, la configuración de la cuenta de usuario 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 dispositivo protegido 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 dispositivo protegido diferente. Tras importar la configuración en el dispositivo protegido, deberá introducir todas las contraseñas manualmente.

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 ajustes de un archivo de configuración que contenga ajustes para componentes individuales de Kaspersky Embedded Systems Security (por ejemplo, de un archivo creado en una copia de Kaspersky Embedded Systems Security que se ha instalado con un juego de componentes incompleto). 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:

1. Para exportar toda la configuración de Kaspersky Embedded Systems Security, en el menú contextual del nodo **Kaspersky Embedded Systems Security**, seleccione el comando **Exportar configuración**.

Para exportar la configuración de un componente individual, haga clic en **Exportar configuración** en el panel de resultados.

> La configuración de Kaspersky Security Network no se puede exportar. Kaspersky Security Network debe configurarse manualmente.

2. En la ventana que se abre, escriba el nombre del archivo XML en el que se exportará la lista de configuraciones. Seleccione también la carpeta en la que se guardará este archivo.

   Puede usar variables de entorno del sistema cuando especifica la ruta, pero no puede usar variables de entorno de usuarios.

   > Si una directiva de Kaspersky Security Center está activa en el momento de la exportación, la aplicación exporta la configuración usada por esa directiva.

3. Guarde el archivo.

4. Haga clic en el botón **Aceptar** de la ventana **Se completó correctamente la exportación de la configuración**.

   Kaspersky Embedded Systems Security exportará la lista de configuraciones al archivo XML.

Para exportar la lista de aplicaciones de confianza:

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Kaspersky Embedded Systems Security**.

2. Seleccione **Configurar Zona de confianza**.

3. Se abre la ventana **Configurar Zona de confianza**.

4. Vaya a la sección **Aplicaciones de confianza** y haga clic en **Configuración**.

   Esto abre una ventana que contiene una lista de las aplicaciones de confianza.

5. Seleccione las aplicaciones de confianza que desea exportar.

   Si no selecciona ninguna aplicación de confianza, Kaspersky Embedded Systems Security exporta todas las aplicaciones de confianza.

6. Haga clic en la flecha y, en la lista desplegable, seleccione **Exportar**.

7. En la ventana que se abre, ingrese el nombre del archivo XML en el que se exportará la lista de aplicaciones de confianza. Seleccione la carpeta en la que se guardará este archivo.

8. Guarde el archivo.

   Kaspersky Embedded Systems Security exportará la lista de aplicaciones de confianza al archivo XML.

Importación de la configuración

Para importar configuraciones desde un archivo de configuración guardado:

1. Para importar toda la configuración de Kaspersky Embedded Systems Security, en el menú contextual del nodo **Kaspersky Embedded Systems Security**, seleccione el comando **Importar configuración**.

Para importar la configuración de un componente individual, haga clic en **Importar configuración** en el panel de resultados.

Después de importar la configuración general de Kaspersky Embedded Systems Security o la configuración funcional de los componentes en el dispositivo protegido, no puede volver a la configuración anterior.

La configuración de Kaspersky Security Network no se puede importar. Kaspersky Security Network debe configurarse manualmente.

2. En la ventana que se muestra, seleccione el archivo de configuración XML desde el cual desea importar la configuración y haga clic en **Abrir**.
3. Haga clic en el botón **Aceptar** de la ventana **Se completó correctamente la importación de la configuración**.
4. En la barra de tareas de la Consola de la aplicación, haga clic en el botón **Actualización**.

La ventana de la Consola de la aplicación muestra la configuración importada.

Kaspersky Embedded Systems Security no importa contraseñas (credenciales de la cuenta utilizada para iniciar tareas o establecer conexión con el servidor proxy) de un archivo creado en otro dispositivo protegido o en el mismo dispositivo protegido después de que Kaspersky Embedded Systems Security se haya reinstalado o actualizado. Después de finalizar la importación, las contraseñas deben ingresarse manualmente.

Para importar la lista de aplicaciones de confianza:

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Kaspersky Embedded Systems Security**.
2. Seleccione **Configurar Zona de confianza**.
3. Se abre la ventana **Configurar Zona de confianza**.
4. Vaya a la sección **Aplicaciones de confianza** y haga clic en **Configuración**.
5. Haga clic en la flecha y, en la lista desplegable, seleccione **Importar**.
6. En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de aplicaciones de confianza.
7. Abra el archivo.

   Cuando ya exista una lista de aplicaciones de confianza en el equipo, Kaspersky Embedded Systems Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas nuevas del archivo XML.
8. La lista se muestra en la pestaña **Aplicaciones de confianza**. Haga clic en **Aceptar**.

Consultar el estado de protección e información de Kaspersky Embedded Systems Security

Para consultar información sobre el estado de protección del dispositivo de Kaspersky Embedded Systems Security,

seleccione el nodo **Kaspersky Embedded Systems Security** en el árbol de la Consola de Kaspersky Embedded Systems Security.

De manera predeterminada, la información en el panel de detalles de la Consola de Kaspersky Embedded Systems Security se actualiza automáticamente:

- Cada 10 segundos en caso de una conexión local.
- Cada 15 segundos en caso de una conexión remota.

La información se puede actualizar en forma manual.

*Para actualizar la información del nodo **Kaspersky Embedded Systems Security** de forma manual,*

seleccione el comando **Actualizar** del 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 Kaspersky Embedded Systems Security:

- Estado de Uso de Kaspersky Security Network.
- Estado de Protección del dispositivo.
- Información sobre las actualizaciones del módulo de aplicación y la base de datos.
- Datos de diagnóstico reales.
- Datos sobre las tareas de control de dispositivos protegidos.
- Información sobre la licencia.
- Estado de integración con Kaspersky Security Center: los detalles del servidor que tiene Kaspersky Security Center instalado y al cual se ha conectado la aplicación e información sobre las tareas de la aplicación que se encuentran controladas por la directiva activa.

El estado de protección se representa mediante el siguiente esquema de colores:

- *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 KSN** muestra el estado actual de la tarea, por ejemplo, *En ejecución*, *Detenido* o *Nunca ejecutada*. El indicador puede tener los siguientes valores:

- Color verde del panel: significa que la tarea **Uso de KSN** se está ejecutando y las solicitudes de estado de archivos están enviando a KSN.
- Color amarillo del panel: 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.
- Color rojo del panel: significa que se produjo un error en la tarea.

Protección del equipo

La sección **Protección del equipo** (consulte la siguiente tabla) muestra información acerca del estado actual de la protección del dispositivo.

Información sobre el estado de protección del dispositivo

Sección	Información
Indicador del estado de protección del dispositivo	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: • Color verde del panel: se muestra de manera predeterminada y significa que el componente Protección de archivos en tiempo real está instalado y la tarea está en ejecución. • Color amarillo del panel: significa que el componente Protección de archivos en tiempo real no está instalado y que hace mucho tiempo que no se realiza la tarea *Análisis de áreas críticas*. • Color rojo del panel: significa que las tareas de Protección de archivos en tiempo real no se están ejecutando.
Protección de archivos en tiempo real	**Estado**: estado actual del componente, por ejemplo, *En ejecución* o *Deshabilitado*.
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 ejecutada*: evento que ocurre cuando la tarea *Análisis de áreas críticas* no se ejecutó durante 30 días o más (valor predeterminado). Se puede cambiar el umbral para la generación de este evento.
Protección contra amenazas de red	**Estado**: estado actual del componente, por ejemplo, *En ejecución* o *Deshabilitado*.
Prevención de exploits	**Estado**: estado actual del componente, por ejemplo, *En ejecución* o *Deshabilitado*. **Modo de operación**: uno de los dos modos disponibles para la tarea Prevención de exploits; **Bloquear** o **Informar**.
Detección de comportamiento	**Estado**: estado actual del componente, por ejemplo, *En ejecución* o *Deshabilitado*. **Modo de operación**: uno de los tres modos disponibles para la tarea Detección de comportamiento; **Eliminar**, **Bloquear** o **Informar**.

Actualización

La sección **Actualización** (consulte la siguiente tabla) muestra qué tan actuales son las bases de datos antivirus y los módulos de la aplicación.

Información sobre el estado de los módulos y las bases de datos de Kaspersky Embedded Systems Security

Sección	Información
Indicador del estado de las bases de datos y los módulos de la aplicación	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: • Color verde del panel: se muestra de manera predeterminada, y significa que las bases de datos de la aplicación están actualizadas y que la última tarea de actualización de bases de datos y módulos se completó correctamente. • Color amarillo del panel: significa que las bases de datos están desactualizadas o que se produjo un error en la última tarea de actualización de bases de datos y módulos. • Color rojo del panel: significa que se produjo el evento *Las bases de datos están obsoletas* o *Las bases de datos están actualizadas*.
Actualización de bases de datos	**Estado de las bases de datos**: evaluación del estado de actualización de las bases de datos. La opción puede tener los siguientes valores: • **Las bases de datos están actualizadas**: las bases de datos de la aplicación se actualizaron en los siete días anteriores (predeterminado). • **Las bases de datos están desactualizadas**: las bases de datos de la aplicación se actualizaron en los siete a 14 días anteriores (predeterminado). • **Las bases de datos están obsoletas**: las bases de datos de la aplicación se actualizaron hace más de 14 días (predeterminado). Se puede cambiar el umbral para la generación de los eventos *Las bases de datos están desactualizadas* y *Las bases de datos están obsoletas*. **Fecha de las bases de datos**: fecha y hora en que se publicó la actualización de bases de datos más reciente. La fecha y la hora se especifican en formato UTC. **Estado de la última tarea de 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 dispositivo protegido. El valor del campo aparece de color rojo si se produce el evento *Error*.

Control

La sección **Control** (consulte la tabla a continuación) muestra información sobre las tareas Control de inicio de aplicaciones, Control de dispositivos y Firewall.

Información sobre el estado de control de dispositivos protegidos

Sección	Información
Indicador de estado para el control de dispositivos protegidos	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: • Color verde del panel: se muestra de manera predeterminada y significa que se instalaron todos los componentes del Control de inicio de aplicaciones y se está ejecutando la tarea en el modo Activo; la funcionalidad Prevención de exploits está instalada y activa. • El panel es amarillo bajo una o más de las siguientes condiciones: Prevención de exploits no se está ejecutando; Control de inicio de aplicaciones se está ejecutando en el modo Informar; Prevención de exploits se está ejecutando en el modo Activo, y Control de inicio de aplicaciones no se está ejecutando o falló. • Color rojo del panel: significa que la tarea de Control de inicio de aplicaciones no se está ejecutando o falló, y la Prevención de exploits no se está ejecutando o está en el modo **Informar**.
Control de inicio de aplicaciones	**Estado**: estado actual del componente, por ejemplo, *En ejecución* o *Deshabilitado*. **Modo de operación**: uno de los dos modos disponibles para la tarea Control de inicio de aplicaciones: **$EntAppControl_OperatingMode_Active** o **$EntAppControl_OperatingMode_StatisticsOnly**.
Control de dispositivos	**Estado**: estado actual del componente, por ejemplo, *En ejecución* o *Deshabilitado*. **Modo de operación**: uno de los dos modos disponibles para la tarea Control de dispositivos: **Por reglas** o **Informar**.
Firewall	**Estado**: estado actual del componente, por ejemplo, *En ejecución* o *Deshabilitado*.

Diagnóstico

La sección **Diagnóstico** (consulte la tabla a continuación) muestra información sobre las tareas Inspección de registros y Monitor de integridad de archivos.

Información sobre estado de inspección del sistema

Sección	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: se muestra de manera 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; ocurre el evento *Sin ejecutar*. • Rojo: una de las tareas tuvo un error.
Control de integridad del sistema	**Estado**: estado actual del componente, por ejemplo, *En ejecución* o *Deshabilitado*.
Inspección de registros	**Estado**: estado actual del componente, por ejemplo, *En ejecución* o *Deshabilitado*.

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.

Puede conectarse a otro dispositivo protegido a través del vínculo Conectarse a un equipo remoto.

Trabajo con el complemento web desde Web Console y Cloud Console

Esta sección proporciona información sobre el Complemento de administración de Kaspersky Embedded Systems Security para Web Console y describe cómo administrar la aplicación instalada en un dispositivo protegido o en un grupo de dispositivos protegidos.

Administración de Kaspersky Embedded Systems Security mediante Web Console y Cloud Console

Si instaló Kaspersky Embedded Systems Security en una serie de dispositivos protegidos que forman parte de un mismo grupo de administración, puede administrarlos en forma centralizada mediante el Complemento de web de Kaspersky Embedded Systems Security. Kaspersky Security Center Web Console y Cloud Console también permiten configurar por separado cada dispositivo protegido incluido en un grupo de administración.

Un *grupo de administración* se crea manualmente en Kaspersky Security Center Web Console. El grupo incluye varios dispositivos 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 solo dispositivo protegido no está disponible si el funcionamiento de Kaspersky Embedded Systems Security en el dispositivo protegido está controlado por una directiva de Kaspersky Security Center activa.

Kaspersky Embedded Systems Security puede administrarse desde Kaspersky Security Center Web Console 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 dispositivos. La configuración de la tarea especificada en la directiva activa tiene prioridad sobre las configuración de la tarea definida de forma local en la Consola de la aplicación o remotamente en la ventana Propiedades: <Nombre del dispositivo protegido> de Kaspersky Security Center Web Console. Las directivas se pueden usar para establecer la configuración general de la aplicación, la configuración de las tareas de protección del equipo en tiempo real, las tareas de control de actividades en los dispositivos, las tareas de protección de almacenamiento de la red y la configuración que regula el inicio programado de tareas del sistema local.

- **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 dispositivos. Puede usar tareas de grupo para activar la aplicación, configurar la tarea Análisis a pedido, actualizar la configuración de tareas y configurar la tarea Generador de reglas de 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 dispositivos protegidos que no pertenecen a ningún grupo de administración.

- **Utilización de la ventana de propiedades de un solo dispositivo**. En la ventana de propiedades del dispositivo, puede configurar remotamente las opciones de tareas para un solo dispositivo protegido incluido en un grupo de administración. También puede establecer tanto la configuración general de la aplicación como la configuración para todas las tareas de Kaspersky Embedded Systems Security si el dispositivo protegido seleccionado no está controlado por una directiva de Kaspersky Security Center activa.

Kaspersky Security Center Web Console y Cloud Console le permiten establecer la configuración de la aplicación y las funciones avanzadas, y trabajar con registros y notificaciones. Puede configurar estos parámetros tanto para un grupo de dispositivos protegidos, como para dispositivos protegidos individuales.

Limitaciones del Complemento web

El Complemento web de Kaspersky Embedded Systems Security tiene las siguientes limitaciones en comparación con el Complemento de administración de Kaspersky Embedded Systems Security:

- No se pueden crear reglas de la tarea Control de inicio de aplicaciones con un certificado digital ni con eventos de Kaspersky Security Center.

- No se pueden generar reglas de la tarea Control de dispositivos según los dispositivos conectados ni los datos del sistema.

Administración de las configuraciones de la aplicación

Esta sección contiene información acerca de cómo ajustar la configuración general de Kaspersky Embedded Systems Security en la Consola de administración de Kaspersky Security Center.

Configuración de opciones generales de la aplicación en el Complemento web

Puede establecer la configuración general de Kaspersky Embedded Systems Security desde el Complemento web para un grupo de dispositivos protegidos o para un dispositivo protegido.

Configuración de interfaz y análisis en el Complemento web

Para configurar los parámetros de la interfaz:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.

2. Haga clic en el nombre de la directiva que desea configurar.

3. En la ventana **<Nombre de directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Seleccione la sección **Configuración de la aplicación**.
5. Haga clic en **Configurar** en la subsección **Configuración de la interfaz**.
6. Configure las opciones que se describen en la tabla a continuación.

Configuración de interacción del usuario y configuración de análisis

Parámetro	Descripción
Interacción con el usuario	**No mostrar interfaz del usuario**. No habrá ninguna indicación en el equipo cliente de que Kaspersky Embedded Systems Security está en funcionamiento. El ícono del área de notificación de Windows no estará disponible y tampoco se mostrará ninguna notificación. **Mostrar interfaz del usuario**. En el equipo cliente, hay un ícono disponible en la bandeja de Windows. El usuario podrá interactuar con Kaspersky Embedded Systems Security a través del menú contextual del icono. Kaspersky Embedded Systems Security también mostrará notificaciones por encima del icono. El menú contextual del ícono en la bandeja del sistema de Windows le permite abrir la Interfaz de diagnóstico compacto. Al hacer clic en un vínculo en la Interfaz de diagnóstico compacto, se abre la Consola de la aplicación.
Mostrar el estado de la aplicación en el área de notificaciones	Seleccione las casillas que se encuentran frente a las categorías de eventos de los que quiere ver notificaciones en el área de notificación de Microsoft Windows.

Configuración de seguridad y confiabilidad en el Complemento web

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

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva que desea configurar.
3. En la ventana **<Nombre de directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Seleccione la sección **Configuración de la aplicación**.
5. Haga clic en **Configurar** en la subsección **Seguridad y confiabilidad**.
6. Configure las opciones que se describen en la tabla a continuación.

Configuración de seguridad y confiabilidad

Parámetro	Descripción
Iniciar la aplicación al arrancar el equipo (recomendado)	Cuando se selecciona esta casilla, Kaspersky Embedded Systems Security se inicia después de cargado el sistema operativo y protege al equipo durante toda la sesión. Cuando se desactiva esta casilla, Kaspersky Embedded Systems Security no se inicia después de cargado el sistema operativo, sino cuando el usuario lo inicia manualmente. La protección del equipo está desactivada y los datos del usuario pueden estar expuestos a amenazas.
Proteger los procesos de la aplicación de amenazas externas	Cuando se selecciona esta casilla, Kaspersky Embedded Systems Security impide la alteración y la eliminación de archivos de aplicaciones en el disco duro, procesos de memoria y entradas en el registro del sistema.
Proteger los servicios del sistema operativo	Si se habilita la protección de los servicios del sistema operativo, las aplicaciones de terceros no pueden actuar sobre los procesos del sistema operativo. Si se deshabilita la protección de los servicios del sistema operativo, las aplicaciones de terceros pueden actuar sobre los procesos del sistema operativo.

Parámetro	Descripción
Posponer las tareas programadas cuando el equipo funciona con carga de batería	Si se selecciona la casilla, se habilita el modo de ahorro de energía. Kaspersky Embedded Systems Security pospone las tareas programadas. Las tareas de análisis y actualización podrán iniciarse manualmente cuando sea necesario. Cuando el modo de ahorro de energía está activado y el equipo está funcionando con alimentación de la batería, las siguientes tareas no se ejecutan, incluso si estuvieran programadas: • *Actualización de bases de datos y módulos de la aplicación* • *Análisis completo* • *Análisis de áreas críticas* • *Análisis personalizado* • *Comprobación de integridad de la aplicación* • *Análisis de IOC*.
Estado del equipo cuando se aplique la configuración	Opciones para mostrar, en Web Console, los estados de los equipos cliente con Kaspersky Embedded Systems Security instalado cuando ocurran errores al aplicar una directiva o ejecutar una tarea. Los siguientes estados están disponibles: *Aceptar*, *Advertencia* y *Crítico*.
Compatible con software de administración remota	Si el uso de Kaspersky Embedded Systems Security junto con las herramientas de administración remota (RAT) causa problemas, puede habilitar el modo de compatibilidad. Los problemas pueden estar relacionados con la incompatibilidad de las RAT con la funcionalidad de Escritorio seguro de la aplicación. El propósito de esta funcionalidad es confirmar las acciones que potencialmente pueden reducir el nivel de seguridad del equipo. Esta funcionalidad permite que una aplicación muestre un cuadro de diálogo de confirmación aislado de otros procesos. Esta funcionalidad utiliza derechos de alto nivel para proteger la solicitud. De esta forma, solo el usuario puede confirmar la acción y no el malware. Si se selecciona la casilla, se habilita el modo de compatibilidad con la RAT. La aplicación muestra un cuadro de diálogo de confirmación sin esta funcionalidad. Esto puede reducir el nivel de seguridad del equipo. No recomendamos habilitar el modo de compatibilidad si Kaspersky Embedded Systems Security no está causando problemas con la RAT. Si cancela la selección de la casilla de verificación, se deshabilita el modo de compatibilidad con la RAT. De forma predeterminada, la casilla no está activada. Por ejemplo: si se utiliza el navegador en modo RemoteApp, es posible que Kaspersky Embedded Systems Security no muestre una ventana de confirmación cuando se visita un sitio web con un certificado no confiable, ya que RemoteApp no admite la funcionalidad de Escritorio seguro de la aplicación. Esto puede hacer que el navegador deje de responder. Para que el navegador funcione correctamente en el modo RemoteApp, debe habilitar el modo de compatibilidad. También puede intentar habilitar el modo de compatibilidad si tiene problemas con la funcionalidad de Escritorio Seguro al utilizar otro software de terceros.
Restringir el uso de CPU para las tareas del análisis	Kaspersky Embedded Systems Security limita el uso de CPU del dispositivo protegido durante las tareas de análisis a pedido al valor especificado en el campo **Límite máximo**. Sin embargo, la aplicación puede usar mucho más tiempo de CPU debido a otros componentes. La activación de esta funcionalidad puede afectar negativamente el rendimiento de Kaspersky Embedded Systems Security. De manera predeterminada, esta función está deshabilitada.
Conceder recursos a otras aplicaciones	Es posible que el consumo de recursos del equipo por parte de Kaspersky Embedded Systems Security al analizar el equipo aumente la carga de la CPU y de los subsistemas del disco duro. Esto puede ralentizar otras aplicaciones. Para optimizar el rendimiento, Kaspersky Embedded Systems Security proporciona un modo para transferir recursos a otras aplicaciones. En este modo, el sistema operativo puede dar menos prioridad a los subprocesos de la tarea de análisis de Kaspersky Embedded Systems Security cuando la carga de la CPU sea alta. Esto permite redistribuir los recursos del sistema operativo a otras aplicaciones. De este modo, las tareas de análisis recibirán menos tiempo de CPU. Por consiguiente, Kaspersky Embedded Systems Security tardará más tiempo en analizar el equipo. Por defecto, la aplicación está configurada para dispensar recursos para otras aplicaciones.

Ajustes de la configuración de conexión en el Complemento web

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. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva que desea configurar.
3. En la ventana **<Nombre de directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Seleccione la sección **Configuración de la aplicación**.
5. Haga clic en **Configurar** en la subsección **Configuración de conexión**.
6. Configure las opciones que se describen en la tabla a continuación.

Configuración de conexión

Parámetro	Descripción
Limitar el tráfico en conexiones de uso medido	Si esta casilla está seleccionada, la aplicación limita su propio tráfico de red cuando la conexión a Internet está limitada. Kaspersky Embedded Systems Security identifica las conexiones de Internet móviles de alta velocidad como limitadas, y las conexiones Wi-Fi como ilimitadas. Redes basadas en costos funciona en equipos con Windows 8 o posterior.
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.
Detectar la configuración del servidor proxy automáticamente	Si esta opción está seleccionada, Kaspersky Embedded Systems Security define la configuración del servidor proxy automáticamente.
Usar el servidor proxy especificado	Si esta opción está seleccionada, Kaspersky Embedded Systems Security se conecta al KSN con la configuración del servidor proxy especificada manualmente.
No usar el servidor proxy para las direcciones locales	Esta casilla de verificación habilita o deshabilita el uso de un servidor proxy al acceder a dispositivos ubicados en la misma red que el dispositivo protegido con Kaspersky Embedded Systems Security instalado. Si esta casilla de verificación está seleccionada, se accede a los dispositivos directamente desde la red que aloja el dispositivo protegido con Kaspersky Embedded Systems Security instalado. No se utiliza ningún servidor proxy. Si la casilla de verificación está desactivada, se utiliza un servidor proxy para la conexión a dispositivos locales. De forma predeterminada, la casilla está activada.
Configuración de autenticación del servidor proxy	Especifique la configuración de autenticación
No usar autenticación	La autenticación no se realiza.
Autenticación NTLM	La autenticación se realiza usando el protocolo de autenticación de red NTLM desarrollado por Microsoft. Este modo está seleccionado en forma predeterminada.
Autenticación NTLM con nombre de usuario y contraseña	La autenticación se realiza con un nombre de usuario y contraseña usando el protocolo de autenticación de red NTLM desarrollado por Microsoft.
Nombre de usuario y contraseña	La autenticación se realiza usando el nombre de usuario y la contraseña.
Vigilar todos los puertos de red	En este modo de supervisión de puertos de red, los componentes de protección controlan los flujos de datos que se transmiten a través de cualquier puerto de red abierto del equipo.

Parámetro	Descripción
Vigilar solo los puertos de red seleccionados	Cuando se selecciona este modo, los componentes de protección vigilan los puertos de red seleccionados y la actividad de red de las aplicaciones seleccionadas. La lista de puertos de red que normalmente se utilizan para transmitir correo electrónico y otras clases de tráfico se configura siguiendo las recomendaciones de los expertos de Kaspersky.
Usar Kaspersky Security Center como servidor proxy al activar la aplicación	Especifique si Kaspersky Security Center se usará como un servidor proxy para la activación de la aplicación.

Configuración del inicio programado de tareas locales en el Complemento web

Puede utilizar directivas para permitir o bloquear el inicio de la tarea Análisis a pedido y la tarea Actualización del sistema local. Esto se hace de acuerdo con la programación configurada localmente en cada dispositivo protegido 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 dispositivo protegido 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, la directiva prohíbe el inicio de tareas locales del sistema.

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

Si no utiliza las tareas de actualización de grupo o de análisis a pedido, permita que las tareas locales del sistema se inicien en la directiva: Kaspersky Embedded Systems Security realizará las actualizaciones de bases de datos y del módulo, e iniciará todas tareas locales de análisis a pedido del sistema 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 al inicio del sistema operativo*, *Comprobación de integridad de la aplicación* y *Monitor comparativo de integridad del sistema*.
- Tareas de actualización: Actualización de bases de datos y módulos de la aplicación, Actualización de aplicación.

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

Para autorizar o bloquear el inicio programado de tareas locales del sistema de Kaspersky Embedded Systems Security en una directiva realice lo siguiente:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva que desea configurar.
3. En la ventana **<Nombre de directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.

4. Seleccione la sección **Configuración de la aplicación**.

5. Haga clic en **Configurar** en la subsección **Ejecutar tareas locales del sistema**.

6. Configure las opciones que se describen en la tabla a continuación.

Configuración para ejecutar tareas locales

Parámetro	Descripción
Permitir el uso de tareas locales	Si se selecciona la casilla, las tareas locales se muestran en la interfaz local de Kaspersky Embedded Systems Security. Cuando no haya restricciones adicionales de la directiva, el usuario puede configurar y ejecutar tareas. Sin embargo, la configuración del programa de ejecución de tareas no está disponible para el usuario. El usuario puede ejecutar tareas solo manualmente. Si la casilla de verificación se desactiva, el uso de tareas locales se detiene. En este modo, las tareas locales no se ejecutan según la programación. Las tareas no pueden iniciarse o configurarse en la interfaz local de Kaspersky Embedded Systems Security, o al funcionar con la línea de comandos.
Permitir la administración de programaciones	La casilla está disponible si la casilla **Permitir el uso de tareas locales** está seleccionada. Si se selecciona la casilla, la administración de la programación está disponible en las propiedades de la tarea local en la Consola de la aplicación. De forma predeterminada, la casilla no está activada.
Permitir que se muestren las tareas de grupo	Si se selecciona la casilla, las tareas de grupo se muestran en la interfaz local de Kaspersky Embedded Systems Security. El usuario podrá ver la lista de tareas completa a través de la Consola de la aplicación. Si se desactiva esta casilla, Kaspersky Embedded Systems Security mostrará una lista de tareas vacía.
Permitir la administración de tareas de grupo	Si se selecciona esta casilla, los usuarios podrán iniciar y detener las tareas de grupo que se creen en Kaspersky Security Center. Los usuarios pueden iniciar y detener tareas en la Consola de la aplicación o en la interfaz de la aplicación simplificada. Si se desactiva esta casilla, Kaspersky Embedded Systems Security iniciará las tareas programadas automáticamente. El administrador también podrá iniciar estas tareas manualmente a través de Kaspersky Security Center.

Configurar Copia de seguridad en el Complemento web

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

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.

2. Haga clic en el nombre de la directiva que desea configurar.

3. En la ventana **<Nombre de directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.

4. Seleccione la sección **Adicional**.

5. Haga clic en **Configurar** en la subsección **Depósitos**.

6. Configure las opciones que se describen en la tabla a continuación.

Configuración de almacenamiento

Parámetro	Descripción
En la pestaña **Informes**, especifique la configuración de informes:	
Conservar informes como máximo	Si la casilla está seleccionada, los informes se conservarán solo por el tiempo definido como máximo. Por defecto, el plazo máximo de almacenamiento de informes es de 30 días. Después de ese plazo, Kaspersky Embedded Systems Security elimina automáticamente las entradas más antiguas del archivo del informe.
Limitar el tamaño del archivo de los informes a	Si la casilla está seleccionada, el tamaño máximo del archivo de informes se limitará al valor definido. Por defecto, el tamaño máximo del archivo es de 1024 MB. Para evitar que se exceda el tamaño máximo del archivo del informe, Kaspersky Embedded Systems Security elimina automáticamente las entradas más antiguas de este archivo cuando alcanza el tamaño máximo.
En la pestaña **Copias de seguridad**, especifique la configuración de Copia de seguridad:	

Parámetro	Descripción
Conservar objetos como máximo	Si la casilla está seleccionada, los archivos se conservarán solo por el tiempo definido como máximo. Por defecto, el plazo máximo de almacenamiento de archivos es de 30 días. Al caducar el plazo de almacenamiento máximo, Kaspersky Embedded Systems Security elimina los archivos más antiguos de Copia de seguridad.
Limitar el tamaño de Copia de seguridad a	Si la casilla está seleccionada, el espacio de almacenamiento se limitará al tamaño definido como máximo. Por defecto, el tamaño máximo es de 400 MB. Cuando se alcanza el valor definido, Kaspersky Embedded Systems Security elimina automáticamente los archivos más antiguos para evitar que el límite se exceda.
Valor umbral para el espacio disponible	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 de 100 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 **Valor umbral para el espacio disponible** está activada si la casilla **Limitar el tamaño de Copia de seguridad a** está seleccionada. De forma predeterminada, la casilla está activada.

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 dispositivos protegidos.

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

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

Se pueden crear e implementar por turnos varias directivas para un grupo de administración. En Web Console, 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 **Registros y notificaciones**.

Kaspersky Security Center ofrece una manera de aplicar directivas en dispositivos protegidos: *prohibir la modificación de la configuración*. Después de aplicar una directiva, Kaspersky Embedded Systems Security utiliza la configuración para los cuales seleccionó el icono en las propiedades de la directiva en dispositivos protegidos. En este caso, se utiliza la configuración seleccionada en lugar de la configuración vigente antes de que se aplicara la directiva. Kaspersky Embedded Systems Security no aplica la configuración de la directiva activa para los cuales seleccionó 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.

Las opciones de configuración definidas en la directiva activa y marcadas con el icono no pueden modificarse para un dispositivo protegido en particular a través de la ventana **Propiedades: <Nombre del dispositivo protegido>** de Kaspersky Security Center.

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

Si una directiva define la configuración de alguna tarea de protección del equipo en tiempo real o tarea de protección de almacenamiento de red que se encuentra en ejecución, la configuración definida por la directiva cambiará en cuanto se aplique la directiva. Si la tarea no está en ejecución, la configuración se implementará cuando se inicie.

Cómo crear una directiva en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en **Agregar**.
3. Se abre la ventana **Nueva directiva**.
4. En la sección **Seleccionar aplicación**, seleccione Kaspersky Embedded Systems Security.
5. Especifique los modos de Kaspersky Embedded Systems Security en los dispositivos protegidos.
6. Si es necesario, especifique archivos o carpetas, así como nombres de objetos (según la Enciclopedia de virus), que desea excluir del análisis por todos o algunos de los componentes de la aplicación.
7. En la pestaña **General**, puede realizar las siguientes acciones:
   - Cambiar el nombre de la directiva.

     El nombre de la directiva no puede contener los siguientes símbolos: `" * < : > ? \ | .`
   - Seleccionar el estado de la directiva:
     - **Activa**. Después de la próxima sincronización, la directiva se usará como directiva activa en el equipo.
     - **Inactiva**. Directiva de reserva. Puede convertirse en la directiva activa cuando resulta necesario.
     - **Fuera de la oficina**. La directiva se activa cuando un equipo sale del perímetro de la red de la organización.
   - Configurar la herencia de configuración:
     - **Heredar configuración de la directiva primaria**. Si activa este interruptor, los valores de configuración de la directiva se tomarán de la directiva de mayor nivel jerárquico. La configuración de la directiva no se puede editar si está establecida para la directiva principal.
     - **Forzar la herencia de configuración en las directivas secundarias**. Si el botón de alternar está activado, los valores de la configuración de la directiva se propagan a las directivas secundarias. En la configuración de la directiva secundaria, la casilla **Heredar configuración de la directiva primaria** se selecciona automáticamente. La configuración de la directiva secundaria se hereda de la directiva principal, excepto la configuración marcada con . La configuración de la directiva secundaria no se puede editar si está establecida para la directiva principal.
8. En la pestaña **Configuración de la aplicación**, configure las opciones de directiva según sea necesario.
9. Haga clic en **Guardar**.

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

Cuando se crea una nueva directiva, se crea también un conjunto de reglas de autorización para evitar que las aplicaciones se bloqueen y garantizar que continúen funcionando sin interrupciones. Puede ver las reglas predeterminadas en la configuración de tareas. Encontrará los detalles y las limitaciones más abajo.

De manera predeterminada, cuando se crea una nueva directiva, Kaspersky Embedded Systems Security para Windows crea un conjunto de reglas para el tráfico de red entrante:

- Dos reglas de autorización para el proceso de compartir el escritorio de Windows mediante el Agente de red de Kaspersky Security Center, el cual se encuentra en las carpetas %Program Files% y %Program Files (x86)%. Estado: habilitado. Direcciones externas permitidas: todas. Protocolos: TCP y UDP, una regla por protocolo.
- Dos reglas de autorización para el puerto local 15000. Estado: habilitado. Direcciones externas permitidas: todas. Protocolos: TCP y UDP, una regla por protocolo.

De manera predeterminada, cuando se crea una nueva directiva, Kaspersky Embedded Systems Security para Windows crea un conjunto de reglas para el tráfico de red saliente:

- Dos reglas de autorización para el servicio de Kaspersky Embedded Systems Security para Windows, el cual se encuentra en las carpetas %Program Files% y %Program Files (x86)%. Estado: habilitado. Direcciones externas permitidas: todas. Protocolos: TCP y UDP, una regla por protocolo.
- Dos reglas de autorización para el proceso de trabajo de Kaspersky Embedded Systems Security, el cual se encuentra en las carpetas %Program Files% y %Program Files (x86)%. Estado: habilitado. Direcciones externas permitidas: todas. Protocolos: TCP y UDP, una regla por protocolo.
- Dos reglas de autorización para el puerto local 13000. Estado: habilitado. Direcciones externas permitidas: todas. Protocolos: TCP y UDP, una regla por protocolo.

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.

Acerca de la creación de tareas en el Complemento web

Puede crear tareas de grupo y locales de las siguientes maneras:

- Para un único dispositivo protegido: en la ventana **<Nombre del dispositivo protegido>** en la sección **Tareas**.
- Para un grupo de administración: en el panel de detalles del nodo del grupo seleccionado de dispositivos protegidos en la pestaña **Tareas**.
- Para un conjunto de dispositivos protegidos: en el panel de detalles del nodo **Selecciones de dispositivos**.

Puede usar directivas para deshabilitar programaciones de las tareas del sistema local *Actualización* y *Análisis a pedido* en todos los dispositivos protegidos desde el mismo grupo de administración.

Se proporciona información general sobre tareas en Kaspersky Security Center en la *Ayuda de Kaspersky Security Center*.

Crear una tarea en el Complemento web

Para crear una tarea nueva en Kaspersky Security Center Web Console:

1. Inicie el asistente de tareas de una de las siguientes maneras:
   - Para crear una tarea local:
     a. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Dispositivos administrados**.
     b. Haga clic en el nombre del dispositivo protegido.
     c. En la ventana que se abre **<Nombre de dispositivo>**, seleccione la pestaña **Tareas**.
     d. Haga clic en **Agregar**.
   - Para crear una tarea de grupo:
     a. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Tareas**.
     b. Haga clic en **Agregar**.

   Se abre la ventana del asistente de tareas.
2. En la lista desplegable **Aplicación**, seleccione **Kaspersky Embedded Systems Security**.
3. En la lista desplegable **Tipo de tarea**, seleccione el tipo de tarea que se creará.

4. Según el tipo de tarea seleccionado, realice una de las siguientes acciones:

   - Cree una tarea de Análisis a pedido.
   - Para crear una tarea de actualización, configure los valores de la tarea según sus requisitos:

     a. Puede especificar el Servidor de administración de Kaspersky Security Center o los Servidores de actualizaciones de Kaspersky como un origen de actualizaciones de la aplicación en el bloque **Orígenes 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 si los servidores personalizados manualmente no están disponibles.

     b. Ajuste la configuración para una función que reduce la carga en el subsistema del disco:

     c. Puede especificar las acciones que Kaspersky Embedded Systems Security realizará cuando se necesiten actualizaciones críticas para los módulos de la aplicación y cuando se complete la instalación de tales actualizaciones. También puede indicar si Kaspersky Embedded Systems Security recibirá información sobre las actualizaciones programadas disponibles.

     d. Especifique el conjunto de actualizaciones que desea copiar y una ruta a la carpeta que Kaspersky Embedded Systems Security utilizará para almacenar las actualizaciones copiadas.

   - Para crear la tarea Activar la aplicación:

     a. En la ventana **Seleccionar una clave de licencia**, especifique el archivo de clave o el código de activación que desea usar para activar la aplicación.

     b. Seleccione la casilla de verificación **Utilizar como clave de reserva** si desea crear una tarea para renovar la licencia.

   - Cree y configure la tarea Generador de reglas de Control de inicio de aplicaciones.
   - Cree y configure la tarea Generador de reglas para Control de dispositivos.

5. Haga clic en **Siguiente**.

6. Si la tarea se crea para un conjunto de dispositivos protegidos, seleccione la red (o el grupo) de los dispositivos protegidos en los que se ejecutará esta tarea.

7. Haga clic en **Siguiente**.

8. En la ventana **Finalizar la creación de la tarea**, seleccione la casilla **Abrir los detalles de la tarea cuando se complete la creación** si desea ajustar la configuración de la tarea.

9. Haga clic en **Finalizar**.

La tarea creada se mostrará en la lista **Tareas**.

Configurar tareas de grupo en el Complemento web

Para configurar una tarea de grupo para varios dispositivos protegidos:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Tareas**.
2. Haga clic en el nombre de la tarea en la lista de tareas de Kaspersky Security Center.

   Se abre la ventana **<Nombre de la tarea>**.
3. Vaya a la pestaña **Configuración de la aplicación**.
4. Según el tipo de tarea configurada, realice una de las siguientes acciones:
   - Para configurar la tarea *Análisis a pedido*:
     a. En la sección **Alcance del análisis**, configure un área del análisis.
     b. En la sección **Opciones**, configure el nivel de análisis heurístico y la integración con otros componentes de la aplicación.
   - Para configurar una tarea *Actualización*, ajuste la configuración de la tarea según sus requisitos:
     a. En la sección **Orígenes de actualizaciones**, configure las opciones del origen de actualizaciones.
     b. En la sección **Configuración de actualización**, administre la configuración de optimización del subsistema del disco, especifique las acciones que desea que Kaspersky Embedded Systems Security realice si hay actualizaciones críticas de los módulos de la aplicación disponibles o si hay información acerca de actualizaciones planificadas disponible; especifique la configuración para copiar actualizaciones.
   - Para configurar la tarea *Activar la aplicación*, aplique el archivo de clave o el código de activación que desee 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 reglas de autorización para el Control de dispositivos, especifique la configuración que se utilizará para crear la lista de reglas de autorización.
5. Configure la programación de la tarea en la sección **Programación** (puede configurar una programación para todos los tipos de tareas excepto *Reversión de la actualización*).
6. En la pestaña **Configuración** de la sección **Cuenta**, especifique la cuenta cuyos derechos se utilizarán para ejecutar la tarea. Para obtener información sobre la configuración de opciones en esta sección, consulte la *Ayuda de Kaspersky Security Center*.
7. Haga clic en **Guardar**.

Se guardan las opciones de la tarea de grupo recientemente configuradas.

Configurar la tarea Activar la aplicación en el Complemento web

Para configurar la tarea Activar la aplicación:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Tareas**.
2. Haga clic en el nombre de la tarea en la lista de tareas de Kaspersky Security Center.

   Se abre la ventana **<Nombre de la tarea>**.
3. En la sección **Configuración de la aplicación**, especifique el archivo de clave que desea usar para activar la aplicación. Active la casilla **Utilizar como clave de reserva** si desea agregar una clave para renovar la licencia.
4. Configure la programación de tareas en la sección **Programación**.
5. En la ventana **<Nombre de la tarea>**, haga clic en **Guardar**.

Configurar la tarea de Actualización en el Complemento web

Para configurar la tarea Actualización:

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Tareas**.
2. Haga clic en el nombre de la tarea en la lista de tareas de Kaspersky Security Center.

   Se abre la ventana <Nombre de la tarea>.
3. Seleccione la ficha **Configuración de la aplicación**.
4. En la sección **Orígenes de actualizaciones**, configure las opciones del origen de actualizaciones:

   a. Especifique el Servidor de administración de Kaspersky Security Center o los servidores de actualizaciones de Kaspersky como un 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 si los servidores personalizados manualmente no están disponibles.

   b. Ajuste la configuración para una función que reduce la carga en el subsistema del disco:

   - Reducir la carga de lectura y escritura en disco
   - RAM usada para la optimización, MB

   c. Especifique las acciones que Kaspersky Embedded Systems Security debe realizar cuando hay actualizaciones críticas de módulos de la aplicación disponibles o cuando hay información acerca de actualizaciones planificadas.

   d. Especifique la configuración para la copia de actualizaciones.

5. Configure la programación de la tarea en la sección **Programación** (puede configurar una programación para todos los tipos de tareas excepto *Reversión de la actualización*).

6. En la ventana **<Nombre de la tarea>**, haga clic en **Aceptar**.

Administración de programaciones de tareas

Puede programar tareas de Kaspersky Embedded Systems Security.

Tareas de programación

Puede programar las tareas personalizadas y las tareas locales del sistema en la Web Console.

Para programar tareas de grupo mediante Web Console:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Tareas**.

2. Haga clic en el nombre de la tarea en la lista de tareas de Kaspersky Security Center.

   Se abre la ventana **<Nombre de la tarea>**.

3. Vaya a la sección **Programación** y configure la programación necesaria.

   Los campos con la configuración de programación para las tareas análisis a pedido y actualización no estarán disponibles si una directiva de Kaspersky Security Center bloquea la programación de estas tareas.

   a. En la lista desplegable **Iniciar tarea**, seleccione una de las siguientes opciones:

   - **Cada N horas** si desea que la tarea se ejecute periódicamente cada pocas horas; ingrese el número de horas en el campo **Intervalo**.
   - **Cada N días** si desea que la tarea se ejecute periódicamente cada pocos días; ingrese el número de días en el campo **Intervalo**.
   - **Cada N minutos** si desea que la tarea se ejecute periódicamente cada pocos minutos; ingrese el número de minutos en el campo **Intervalo**.
   - **Por días de la semana** si desea que la tarea se ejecute un día específico de la semana; especifique también la hora de ejecución deseada.

     En Kaspersky Security Center 15.1, puede ejecutar tareas a intervalos de varias semanas (el parámetro **Periodo**). Kaspersky Embedded Systems Security no admite la ejecución de tareas en intervalos de varias semanas. Si tiene una tarea programada de Kaspersky Embedded Systems Security para ejecutarse en un intervalo de varias semanas, la aplicación ejecuta la tarea cada semana en el día y la hora especificados.

   - **Mensual** si desea que la tarea se ejecute un día específico del mes; especifique también la hora de ejecución deseada.

- **Una vez** si desea que la tarea se ejecute una vez en una fecha y hora especificadas.
- **Manual** si desea ejecutar la tarea manualmente.
- **Al inicio de la aplicación** si desea que la tarea se ejecute cada vez que se inicia Kaspersky Embedded Systems Security.
- **Al descargar nuevas actualizaciones al repositorio** si desea que la tarea se ejecute cada vez que se descarguen actualizaciones en el repositorio.
- **Ante brotes de virus** si desea que la tarea se ejecute si se detecta un ataque de virus.
- **Al completarse otra tarea** si desea que la tarea se ejecute al finalizar otra tarea.

b. En los campos **Hora de inicio** y **Fecha**, especifique la hora de inicio de la primera tarea.

4. En el bloque **Configuración adicional**:
   - Seleccione la casilla de verificación **Ejecutar tareas no realizadas** para habilitar el inicio de las tareas omitidas.
   - Si se selecciona la casilla **Utilizar retardo aleatorio automático para el inicio de la tarea**, la tarea no se ejecuta estrictamente según lo programado, sino aleatoriamente dentro de un cierto intervalo, es decir, se distribuyen las horas de inicio de la tarea.
   - **Encender dispositivos mediante la función Wake-on-LAN antes de iniciar la tarea**. Si se selecciona la casilla, el sistema operativo del equipo recibe un tiempo de espera especificado para completar el inicio antes de que se ejecute la tarea. El tiempo de espera predeterminado es de 5 minutos.
   - **Apagar dispositivos cuando se complete la tarea**. Si se selecciona la casilla, los dispositivos se desactivarán una vez que se completa la tarea.
   - **Detener la tarea si tarda más de**. Si se selecciona la casilla, la tarea se detendrá si se ejecuta durante más tiempo que el especificado.
5. Haga clic en el botón **Guardar** para guardar la configuración de inicio de la tarea.

Cómo habilitar y deshabilitar tareas programadas

Puede deshabilitar las tareas programadas después de establecer la configuración de programación.

Para deshabilitar la programación de inicio de tareas:

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Tareas**.
2. Haga clic en el nombre de la tarea en la lista de tareas de Kaspersky Security Center.

   Se abre la ventana **<Nombre de la tarea>**.
3. Vaya a la sección **Configuración de la aplicación**.
4. Seleccione la sección **Programación**.
5. Seleccione la configuración para ejecutar una tarea programada en la lista desplegable **Inicio programado** si desea habilitar el inicio de la tarea programada.

6. Seleccione **Manual** en la lista desplegable si desea deshabilitar el inicio de la tarea programada.

7. Haga clic en el botón **Guardar**.

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 de estado de los componentes de Kaspersky Embedded Systems Security

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*, *Suspendido*, *Detenido* o *Sin cobertura por la licencia*.

El estado *No instalado* hace referencia al componente, no a la aplicación. Si la aplicación no se instala, Kaspersky Security Center Web Console asigna el estado N/D (No disponible).

Puede crear selecciones de componentes y utilizar filtros para mostrar dispositivos de red con un conjunto especificado 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 ver el estado de los componentes en Kaspersky Security Center Web Console:

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Dispositivos administrados**.

2. Haga clic en el nombre del dispositivo y vaya a la sección **Aplicaciones**.

3. Haga clic en el nombre de la aplicación de Kaspersky Embedded Systems Security.

4. En la ventana que se abre, en la pestaña **General**, vaya a la sección **Componentes**.
5. Revise la tabla de estado.

Para revisar un informe estándar en Kaspersky Security Center Web Console:

1. Seleccione **Supervisión e informes** → **Informes**.
2. Seleccione el elemento de lista **Informe sobre el estado de componentes de la aplicación** y haga clic en él.
   Se genera un informe.
3. 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 el estado, la versión, el dispositivo y el grupo del componente.

Informes sobre aplicaciones prohibidas en los modos activo y de prueba

En base a los resultados 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 modo Activo) y un informe sobre las aplicaciones prohibidas en modo de prueba (si la tarea se inició en modo Informar). Estos informes muestran información sobre las aplicaciones bloqueadas en los dispositivos protegidos de la red. Cada informe se genera para todos los grupos de administración y acumula datos de todas las aplicaciones de Kaspersky instaladas en los dispositivos protegidos.

Para revisar un informe sobre aplicaciones prohibidas en el modo Informar:

1. Ejecute la tarea Control de inicio de aplicaciones en el modo Informar.
2. Seleccione **Supervisión e informes** → **Informes**.
3. Seleccione el elemento de lista **Informe sobre aplicaciones prohibidas en modo de prueba** y haga clic en él.
   Se genera un informe.
4. Revise los siguientes detalles del informe:
   - Diagrama gráfico que muestra las diez primeras aplicaciones con el mayor número de inicios bloqueados.
   - Una tabla que resume los bloqueos de aplicaciones, donde se especifican el nombre del archivo ejecutable, el motivo, el tiempo de bloqueo y el número de dispositivos donde se bloqueó.
   - 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. Ejecute la tarea Control de inicio de aplicaciones en el modo Activo.
2. Seleccione **Supervisión e informes** → **Informes**.

3. Seleccione el elemento de la lista **Informe sobre aplicaciones prohibidas** y haga clic en él.

   Se genera un informe.

Este informe consiste en los mismos datos sobre bloqueos que el informe sobre aplicaciones prohibidas en modo de prueba.

Licencia de la aplicación

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

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 leer los términos del Contrato de licencia de usuario final y de la Política de privacidad, que describen el procesamiento y la transmisión de datos, de las siguientes maneras:

- Durante la instalación de Kaspersky Embedded Systems Security.
- Durante la instalación de Kaspersky Embedded Systems Security Console.
- Leyendo el documento de archivo license.txt incluido en el kit de distribución.
- En el sitio web de Kaspersky (https://latam.kaspersky.com/business/eula).

Al confirmar que está de acuerdo con el Contrato de licencia de usuario final al instalar la aplicación, usted indica que acepta 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 otorga conforme al Contrato de licencia de usuario final.

Una licencia válida le da derecho a recibir el uso de la aplicación de acuerdo con los términos del Contrato de licencia de usuario final, así como a recibir soporte técnico cuando sea necesario.

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

Puede activar la aplicación de dos maneras:

- Con un archivo de clave, que le otorga el uso con la licencia comercial.
- Con un código de activación para comprar una licencia comercial.

Una vez que caduca la licencia comercial, solo los siguientes componentes y tareas de la aplicación permanecen disponibles sin actualizaciones de la base de datos:

- Protección de archivos en tiempo real
- Control de integridad del sistema
- Tareas de Análisis a pedido

Para seguir usando todas las funciones de Kaspersky Embedded Systems Security, debe renovar su licencia comercial. Se recomienda extender el período de validez de validez antes de su fecha de caducidad para garantizar la máxima protección.

Si se elimina la clave de licencia, la aplicación continuará ejecutándose. El componente Control de integridad del sistema permanece disponible y el resto de los componentes, las tareas y las actualizaciones de la base de datos de Kaspersky Embedded Systems Security dejan de estar disponibles. Lo mismo ocurre si Kaspersky agrega su licencia a la lista de rechazadas.

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.

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

- Identificador de licencia o 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 de unidades con licencia (por ejemplo, la cantidad de dispositivos en los cuales se puede usar la aplicación con la licencia)
- 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 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 puede agregar una clave a la lista de rechazadas si hay infracciones del Contrato de licencia. Si se bloquea su clave, se debe agregar una clave diferente para que funcione la aplicación.

Existen dos tipos de claves: activa y de reserva.

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

La *clave de reserva* es una clave que confirma el derecho de usar la aplicación pero que actualmente no se encuentra en uso. La clave de reserva se activa automáticamente cuando expira la licencia asociada con la clave activa actual. Para poder agregar una clave de reserva, es necesario que haya una clave activa disponible.

Acerca del archivo de clave

Un *archivo de clave* es un archivo con la extensión .key suministrado por Kaspersky. El propósito del archivo de clave es añadir una clave de licencia que active la aplicación.

Recibirá un archivo de clave en la dirección de correo electrónico que indique al momento de comprar Kaspersky Embedded Systems Security.

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

Puede recuperar el archivo de clave si se ha eliminado por error. Es posible que necesite un archivo de clave para registrarse en Kaspersky CompanyAccount, por ejemplo.

Para recuperar un archivo de clave, lleve a cabo una de las siguientes acciones:

- Comuníquese con el vendedor de la licencia.
- Obtenga un archivo de clave en el sitio web de Kaspersky según su código de activación existente.

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 un código de activación en la dirección de correo electrónico que indique al momento de comprar Kaspersky Embedded Systems Security.

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

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, comuníquese con el socio de Kaspersky Lab a quien le compró la licencia.

Comparación de la funcionalidad de la aplicación según el tipo de licencia

El conjunto de funcionalidades de Kaspersky Embedded Systems Security depende del tipo de licencia (consulte la siguiente tabla).

Comparación de las características de Kaspersky Embedded Systems Security

Característica	Kaspersky Embedded Systems Security	Kaspersky Embedded Systems Security Compliance Edition
Protección de archivos en tiempo real	✓	✓
Análisis a pedido	✓	✓
Control de inicio de aplicaciones	✓	✓
Control de dispositivos	✓	✓
Firewall	✓	✓
Monitor de integridad de archivos	–	✓
Inspección de registros	–	✓

Activación de la aplicación con un archivo de clave

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

Para activar Kaspersky Embedded Systems Security con un archivo de clave:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Licencias**.
2. Haga clic en el vínculo **Agregar clave** en el panel de resultados del nodo **Licencias**.
3. Haga clic en el botón **Examinar** en la ventana que se abre.

4. Seleccione un archivo de clave con la extensión .key.

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

5. Haga clic en **Aceptar**.

Se aplicará el archivo de clave seleccionado. En este caso:

- Si ya se agregó una clave activa para activar la aplicación y se agrega otra clave como clave activa, la nueva clave sustituye a la clave agregada anteriormente. La clave agregada previamente se elimina.
- Si ya se agregó una clave de reserva para activar la aplicación y se agrega otra clave como clave de reserva, la nueva clave sustituye a la clave agregada anteriormente. La clave de reserva agregada anteriormente se elimina.
- Si ya se agregó una clave activa y una clave de reserva para activar la aplicación y se agrega una nueva clave como clave activa, la nueva clave sustituye a la clave activa agregada anteriormente y la clave de reserva no se elimina.

La información sobre la clave agregada estará disponible en el nodo **Licencias**.

Activación de la aplicación con un código de activación

> Para activar la aplicación utilizando un código de activación, el dispositivo protegido 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 indica que debe ponerse en contacto con el Servicio de soporte técnico.

Puede activar Kaspersky Embedded Systems Security con un código de activación mediante la Consola de la aplicación o si crea la tarea de grupo *Activar la aplicación* mediante el complemento de administración o el complemento web.

Para activar Kaspersky Embedded Systems Security con un código de activación mediante la Consola de la aplicación, realice lo siguiente:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Licencias**.
2. Haga clic en el vínculo **Agregar código de activación** en el panel de resultados del nodo **Licencias**.
3. En la ventana que se abre, ingrese el código de activación en el campo **Código de activación**.
   - Si desea usar el código de activación como una clave de reserva, active la casilla **Usar como clave adicional**.
   - Para ver información sobre una licencia, haga clic en el botón **Ver información de licencia**. La información se mostrará en el bloque **Información de 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.

Ver información acerca de la licencia actual

Visualización del estado de la licencia

Puede ver información sobre el estado de la licencia actual en el panel de detalles del nodo **Kaspersky Embedded Systems Security** de la Consola de la aplicación. El estado de la licencia puede tener los siguientes valores:

- **Comprobando el estado de la clave**: Kaspersky Embedded Systems Security está verificando el archivo de clave adicional y esperando una respuesta sobre el estado actual.
- **Fecha de caducidad**: Kaspersky Embedded Systems Security está activo hasta la fecha especificada. El estado se resalta en amarillo en los siguientes casos:
  - La licencia caducará en 30 días y no se agregó ninguna clave de reserva.
  - La clave agregada se ha añadido a la lista de rechazadas y se bloqueará.
- **La aplicación no está activada**: Kaspersky Embedded Systems Security no está activado porque no agregó la clave. El estado se resalta en rojo.
- **La licencia caducó**: Kaspersky Embedded Systems Security no se activa porque la licencia ha caducado. El estado se resalta en rojo.
- **Se infringió el 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. El estado se resalta en rojo.
- **La clave está en la lista de rechazadas**: el archivo de clave agregado se bloqueó y Kaspersky lo agregó a la lista de rechazados, por ejemplo, en el caso de que terceros utilicen la clave para activar la aplicación ilegalmente. El estado se resalta en rojo.

Ver información acerca de la licencia actual

Para ver 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).

Información general acerca de la licencia en el nodo Licencia

Campo	Descripción
Estado del código de activación o estado de la clave	Estado del código de activación o estado de la clave: *Clave activa* o *De reserva*.
Fecha de caducidad	La fecha y hora de caducidad de la licencia asociada con una clave activa.
Tipo de licencia	Tipo de licencia: *Licencia comercial*.
Estado de activación	La información del estado de activación puede tomar los siguientes valores: • **Aplicada**: si activó la aplicación con una clave. • **Activar la aplicación**: 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 **Aplicada** después de la activación de la aplicación y la actualización de 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	El número de la clave que usó para activar la aplicación.

Para ver información detallada acerca de la licencia:

En el panel de detalles del nodo **Licencia**, abra el menú contextual de la licencia que desea visualizar y seleccione **Propiedades**.

Información detallada de la licencia en la ventana Propiedades <número de clave>

Campo	Descripción
Clave	El número de la clave que usó para activar la aplicación.
Aplicación	El nombre de la aplicación que se activó con la clave agregada.
Tipo de licencia	Tipo de licencia: comercial o de prueba.
Plazo de la licencia	La cantidad de días, a partir de la fecha de activación de la aplicación, durante los cuales la licencia es válida.
Fecha de activación	Fecha en la que se agregó la clave a la aplicación.
Fecha de caducidad	La fecha de caducidad de la licencia asociada con una clave activa. Si la aplicación se activa con una suscripción ilimitada, el valor del campo es *Ilimitado*. Si Kaspersky Embedded Systems Security no puede determinar la fecha de caducidad de la licencia, el valor del campo es *Desconocido*.
Días hasta la fecha de caducidad	Cantidad de días restantes hasta la caducidad de la licencia asociada con la clave activa.
Brinda acceso a soporte técnico	Información sobre si Kaspersky o sus socios proporcionarán servicio de soporte técnico a los clientes de acuerdo con los términos de la licencia.
Información de soporte	Información de contacto de Kaspersky o del socio que brinda 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 cliente de la licencia: el nombre del cliente y el nombre de la organización para la cual se adquirió la licencia.
Información de la licencia	Número y tipo de licencia actual.
Características	Funciones de la aplicación que la licencia permite usar.

Renovación de la licencia

De forma predeterminada, Kaspersky Embedded Systems Security notifica cuando la licencia está a 30 días de caducar.

Puede renovar la licencia antes de la fecha de caducidad mediante una clave de reserva. Esto asegura que su dispositivo 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:

1. Adquiera un nuevo código de activación o un archivo de clave.
2. En el árbol de la Consola de la aplicación, seleccione el nodo **Licencias**.
3. En el panel de resultados del nodo **Licencias**, realice una de las siguientes acciones:
   - Si desea renovar la licencia con un archivo de clave:
     a. Haga clic en el vínculo **Agregar clave**.
     b. Haga clic en el botón **Examinar** en la ventana que se abre.
     c. Seleccione un nuevo archivo de clave con la extensión .key.
     d. 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 de reserva se agregará y se aplicará automáticamente cuando venza la licencia actual de Kaspersky Embedded Systems Security.

Eliminación de la clave

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

Para eliminar la clave agregada anteriormente:

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

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 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.

Puede acceder a los términos del Contrato de licencia y la Política de privacidad durante la instalación de Kaspersky Embedded Systems Security como parte del kit de distribución y desde el menú **Inicio** (**Todos los programas** > **Kaspersky Embedded Systems Security** > **Contrato de licencia de usuario final y Política de privacidad**) después de la instalación.

Durante la desinstalación de Kaspersky Embedded Systems Security se eliminan todos los datos almacenados por Kaspersky Embedded Systems Security en el dispositivo protegido.

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

- 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: 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 (identificador y 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, que indique 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.

Procesamiento de datos local

Al ejecutar las funciones principales de la aplicación descritas en esta Guía, Kaspersky Embedded Systems Security procesa y almacena de forma local un conjunto de datos en el dispositivo protegido.

La siguiente tabla contiene información sobre el procesamiento y almacenamiento local que realiza Kaspersky Embedded Systems Security de los datos contenidos en los informes.

Procesamiento y almacenamiento de datos contenidos en informes

Área funcional	Registro de eventos
Tipo de uso	Kaspersky Embedded Systems Security almacena los datos de forma local y los envía al Servidor de administración. La base de datos del Servidor de administración almacena información sobre eventos de aplicaciones que ocurren en los dispositivos protegidos administrados.
Depósito	• %ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Security for Windows Server\<versión del producto>\Reports • %SystemRoot%\System32\Winevt\Logs\Kaspersky Security.evtx • Base de datos del Servidor de administración
Medidas de seguridad	Lista de control de acceso.
Periodo de almacenamiento	Kaspersky Embedded Systems Security almacena los datos hasta su desinstalación. Durante la desinstalación de Kaspersky Embedded Systems Security se eliminan todos los datos almacenados por Kaspersky Embedded Systems Security en el dispositivo protegido.
Objetivo	Proporcionar funcionalidad primaria.

Kaspersky Embedded Systems Security no elimina ningún evento del Registro de eventos de Windows, ni siquiera aquellos registrados durante la desinstalación de Kaspersky Embedded Systems Security.

Para proporcionar la funcionalidad de registro de eventos, Kaspersky Embedded Systems Security procesa los siguientes datos en forma local:

- Nombres, sumas de verificación (MD5, SHA-256) y atributos de archivos procesados y rutas completas a ellos en los medios analizados.
- Acciones tomadas en archivos analizados por Kaspersky Embedded Systems Security.
- Acciones realizadas por el usuario con los archivos analizados en el dispositivo protegido.
- Información sobre cuentas de usuarios que realizan acciones en la red protegida o el dispositivo protegido.
- Valores de la Ruta de acceso a la instancia del dispositivo para los dispositivos agregados a las reglas de Control de dispositivos.
- Información sobre procesos y scripts que se ejecutan en el sistema: sumas de verificación (MD5, SHA-256) y rutas completas a archivos ejecutables, información sobre certificados digitales.
- Configuración del firewall de Windows.
- Entradas del Registro de eventos de Windows.
- Nombres de las cuentas de usuario que realizan acciones con los archivos analizados en el dispositivo protegido.
- Instancias de archivos ejecutables que se inician y los tipos, nombres, sumas de verificación y atributos de estos archivos.

- Información sobre la actividad de red:
  - Las direcciones IP de los dispositivos externos bloqueados.
  - Direcciones IP procesadas.
- Información sobre el estado del Windows USN Journal.

La siguiente tabla contiene información sobre los datos de servicio procesados por Kaspersky Embedded Systems Security. Los datos de servicio incluyen lo siguiente: parámetros del programa, archivos en cuarentena y en copia de seguridad, información en las bases de datos de servicio del programa, datos de la licencia.

La siguiente tabla contiene información sobre el procesamiento y almacenamiento local que realiza Kaspersky Embedded Systems Security de datos sobre parámetros especificados por un usuario.

Procesamiento y almacenamiento de datos sobre parámetros especificados por un usuario

Área funcional	Toda la funcionalidad de Kaspersky Embedded Systems Security
Tipo de uso	Kaspersky Embedded Systems Security almacena los datos de forma local y los envía al Servidor de administración. Los datos se almacenan en la base de datos del Servidor de administración. Los datos que la aplicación procesa localmente no se envían automáticamente a Kaspersky ni a otros sistemas de terceros.
Depósito	• %ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Security for Windows Server\<versión del producto>\ • Base de datos del Servidor de administración
Medidas de seguridad	Lista de control de acceso.
Periodo de procesamiento	Kaspersky Embedded Systems Security almacena los datos hasta su desinstalación. Durante la desinstalación de Kaspersky Embedded Systems Security se eliminan todos los datos almacenados por Kaspersky Embedded Systems Security en el dispositivo protegido. Kaspersky Embedded Systems Security no elimina los datos sobre los parámetros exportados al archivo de configuración. Kaspersky Embedded Systems Security no elimina los objetos en cuarentena y en copia de seguridad si las casillas de verificación **Exportar objetos de Cuarentena** y **Exportar objetos de Copia de seguridad** están seleccionadas en el Asistente de configuración.
Objetivo	Proporcionar funcionalidad primaria.

Kaspersky Embedded Systems Security procesa de forma local los siguientes datos para los objetivos especificados.

- Objetos colocados en cuarentena o copia de seguridad.
- Información sobre las cuentas de usuario (nombres de usuario y contraseñas) con las que Kaspersky Embedded Systems Security ejecuta las tareas.
- Contraseña de Kaspersky Embedded Systems Security.
- Direcciones IP e identificadores de sesiones bloqueadas.
- Configuración del Firewall de Windows y configuración de reglas del Firewall de Windows.
- Sumas de verificación (MD5, SHA-256) y rutas de acceso a archivos ejecutables agregados a las reglas de la tarea Control de inicio de aplicaciones.
- Valores de la Ruta de acceso a la instancia del dispositivo para los dispositivos agregados a las reglas de Control de dispositivos.
- Información sobre archivos y carpetas incluidas en las áreas de las tareas de Kaspersky Embedded Systems Security.

- Direcciones IP incluidas o excluidas del alcance de protección.
- Información sobre eventos en el Registro de eventos de Windows.
- Información sobre detecciones con el uso de la tecnología iSwift o iChecker.
- Sumas de verificación (MD5, SHA-256), rutas completas y máscaras especificadas en la configuración de exclusiones.
- Información sobre procesos agregados a la Zona de confianza.
- Información sobre claves de licencia agregadas.
- Información sobre certificados digitales.
- Archivos desempaquetados de un archivo de almacenamiento u otro objeto compuesto durante el análisis.

Kaspersky Embedded Systems Security procesa y almacena datos como parte de la funcionalidad básica de la aplicación, lo cual incluye registrar eventos de la aplicación 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 protección para los datos procesados localmente. Puede cambiar los privilegios del usuario para acceder a los datos procesados, cambiar los 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 en la que se registran los datos.

Los datos que la aplicación procesa localmente no se envían automáticamente a Kaspersky ni a otros sistemas de terceros.

De forma predeterminada, todos los datos que la aplicación procesa localmente mientras está en funcionamiento se eliminan tras desinstalar Kaspersky Embedded Systems Security del dispositivo protegido.

Quedan exceptuados los archivos con información de diagnóstico (archivos de seguimiento y de volcado), los eventos que la aplicación almacena en el Registro de eventos de Windows y los archivos a los que se pueda haber exportado la configuración de Kaspersky Embedded Systems Security. Recomendamos que elimine 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.

Para eliminar los archivos del Registro de eventos de Windows que contienen eventos de la aplicación Kaspersky Embedded Systems Security, puede usar las herramientas 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 dispositivo incluso si Kaspersky Embedded Systems Security no está instalado en él. Los componentes auxiliares son los siguientes:

- Consola de la aplicación. Este componente forma parte de las Herramientas de administración de Kaspersky Embedded Systems Security. Es un complemento para 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 dispositivo protegido 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 dispositivo protegido que tiene instalado Kaspersky Embedded Systems Security (dirección IP o nombre de dominio) y al que se conectó por última vez la Consola de la aplicación de forma remota; parámetros de visualización 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 dispositivo protegido que tiene instalada la aplicación Kaspersky Embedded Systems Security y con el cual se estableció la conexión remota, y el nombre de la cuenta de usuario que se usó para establecer la conexión remota.

- El Complemento de administración puede procesar y almacenar temporalmente ciertos datos procesados por Kaspersky Embedded Systems Security (por ejemplo, los ajustes configurados para las tareas y los componentes de la aplicación, los ajustes de las directivas de Kaspersky Security Center y los datos enviados en las listas de red).

La siguiente tabla contiene información sobre el procesamiento y almacenamiento local que realiza Kaspersky Embedded Systems Security de los datos escritos en archivos de volcado y seguimiento.

Kaspersky Embedded Systems Security procesa y almacena de forma local los siguientes datos escritos en archivos de volcado y seguimiento:

- Información sobre acciones realizadas por Kaspersky Embedded Systems Security en el dispositivo protegido.

- Información sobre los objetos procesados por Kaspersky Embedded Systems Security.

- Información sobre la actividad en el dispositivo protegido que es procesada por Kaspersky Embedded Systems Security.

- Información sobre errores que ocurrieron durante la ejecución de Kaspersky Embedded Systems Security.

Los datos que los componentes auxiliares procesan no se envían automáticamente a Kaspersky 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.

La excepción son los archivos de seguimiento de los componentes auxiliares de la aplicación. Recomendamos que elimine estos archivos manualmente.

Datos en archivos de seguimiento y volcado

Kaspersky Embedded Systems Security puede, de acuerdo con la configuración, escribir información de depuración en archivos de rastreo con fines de soporte técnico durante la operación de Kaspersky Embedded Systems Security.

Los archivos de volcado de Kaspersky Embedded Systems Security son generados por el sistema operativo cuando la aplicación deja de funcionar y se sobrescriben la próxima vez que sucede.

Los archivos de seguimiento y volcado pueden incluir datos personales de un usuario o datos confidenciales de su organización.

No utilice Kaspersky Embedded Systems Security en dispositivos para los que la directiva de su organización prohíbe el envío de datos.

De forma predeterminada, Kaspersky Embedded Systems Security no registra información de depuración.

Los archivos de seguimiento y volcado no se envían automáticamente más allá del host en el que se generaron. El contenido de los archivos de seguimiento se puede visualizar con visores de archivos de texto estándar. Los archivos de seguimiento y de volcado se guardan indefinidamente y no se eliminan al desinstalar Kaspersky Embedded Systems Security.

La información de depuración puede ser útil para el Servicio de soporte técnico.

No se proporcionan mecanismos especiales para limitar el acceso a los archivos de seguimiento y volcado. El administrador puede configurar que estos datos se escriban en una carpeta protegida.

La ruta a la carpeta de archivos de seguimiento y volcado no está configurada de manera predeterminada. Para usar la carpeta de seguimiento y volcado, el administrador debe especificarla.

Los datos en los archivos de seguimiento y volcado pueden contener:

- Información sobre acciones realizadas por Kaspersky Embedded Systems Security en el dispositivo protegido.
- Información sobre objetos procesados por Kaspersky Endpoint Agent.
- Errores que surgen durante la operación de Kaspersky Endpoint Agent.

Cumplimiento de la legislación de la Unión Europea (RGPD)

Kaspersky Embedded Systems Security puede transmitir datos a Kaspersky en las siguientes situaciones:

- Al usar Kaspersky Security Network.
- Al activar la aplicación con un código de activación nuevo.
- Al actualizar módulos de aplicaciones y bases de datos antivirus.
- Hacer clic en vínculos en la Consola de la aplicación.

Independientemente de la clasificación de datos y el territorio desde el que se reciben los datos, Kaspersky respeta altos estándares de seguridad de datos y emplea diversas medidas legales, organizativas y técnicas para proteger los datos de los usuarios, garantizar la seguridad y confidencialidad de los datos, y también garantizar el cumplimiento de los derechos de los usuarios garantizados por la legislación vigente. El texto de la Política de privacidad se incluye en el kit de distribución de la aplicación y está disponible en el sitio web de Kaspersky.

Antes de usar Kaspersky Embedded Systems Security, lea atentamente la descripción de los datos transmitidos en el Contrato de licencia de usuario final y la Declaración de Kaspersky Security Network (incluidos en la Declaración de Kaspersky Security Network). Si los datos específicos transmitidos desde Kaspersky Embedded Systems Security en cualquiera de las situaciones descritas pueden clasificarse como datos personales de acuerdo con su legislación o norma local, debe asegurarse de que dichos datos se procesen legalmente y de obtener el consentimiento de los usuarios finales para la recopilación y la transmisión de tales datos.

Puede leer el Contrato de licencia de usuario final y visitar el sitio web de Kaspersky para obtener más información sobre cómo recibiremos, procesaremos, almacenaremos y destruiremos la información sobre el uso de la aplicación una vez que acepte el Contrato de licencia de usuario final y acepte la Declaración de Kaspersky Security Network. Los archivos license.txt y ksn_<identificador del idioma>.txt contienen el Contrato de licencia de usuario final y la Declaración de Kaspersky Security Network y están incluidos en el kit de distribución.

Si no desea transmitir datos a Kaspersky, puede deshabilitar el suministro de datos.

Uso de Kaspersky Security Network

Al usar Kaspersky Security Network, acepta proporcionar automáticamente los datos indicados en la Declaración de Kaspersky Security Network. Si no acepta proporcionar estos datos a Kaspersky, utilice Kaspersky Private Security Network (KPSN) o deshabilite el uso de KSN.

Activación de la aplicación con un código de activación

Al usar un código de activación, acepta proporcionar automáticamente los datos en el Contrato de licencia de usuario final. Si no está de acuerdo en suministrar estos datos con Kaspersky, utilice un archivo de clave para activar Kaspersky Embedded Systems Security.

Actualizar módulos de aplicaciones y bases de datos antivirus

Al usar los servidores de Kaspersky, acepta proporcionar automáticamente los datos en el Contrato de licencia de usuario final. Kaspersky requiere esta información para verificar que Kaspersky Embedded Systems Security se esté utilizando legítimamente. Si no acepta proporcionar esta información a Kaspersky, utilice Kaspersky Security Center para la actualización de las bases de datos.

Hacer clic en vínculos en la Consola de la aplicación.

Al usar vínculos en la Consola de la aplicación, acepta proporcionar automáticamente los datos en el Contrato de licencia de usuario final. La lista precisa de datos transmitidos en cada vínculo específico depende de dónde se encuentra el vínculo en la Consola de la aplicación y del problema que pretende resolver. Si no acepta proporcionar esta información a Kaspersky, deshabilite la visualización de la interfaz de la aplicación.

Cómo iniciar y detener Kaspersky Embedded Systems Security

Esta sección contiene información acerca de cómo iniciar y detener Kaspersky Embedded Systems Security, así como iniciar la Consola de Kaspersky Embedded Systems Security y el Complemento de administración para la Consola de administración de Kaspersky Security Center.

Iniciar y detener la aplicación.

Cuando termina de instalarse en el equipo de un usuario, Kaspersky Embedded Systems Security se abre automáticamente. De forma predeterminada, Kaspersky Embedded Systems Security se inicia después del inicio del sistema operativo. No es posible configurar la autoejecución de la aplicación en el sistema operativo.

Dependiendo de las prestaciones del equipo, las bases de datos antivirus de Kaspersky Embedded Systems Security pueden tardar hasta dos minutos en descargarse tras el inicio del sistema operativo. Durante este tiempo, el nivel de protección del equipo se reduce. Cuando Kaspersky Embedded Systems Security se inicia en un sistema operativo que ya está en funcionamiento, descargar las bases de datos no afecta el nivel de protección.

Cómo configurar el inicio automático de la aplicación en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Configuración de la aplicación** → **Seguridad y confiabilidad** y haga clic en **Configuración**.
4. En la pestaña **Seguridad**, seleccione o anule la selección de la casilla **Iniciar la aplicación al arrancar el equipo (recomendado)** para habilitar o deshabilitar el inicio automático de la aplicación.
5. Guarde los cambios.

Cómo configurar el inicio automático de la aplicación en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.

4. Vaya a **Configuración de la aplicación → Seguridad y confiabilidad**.
5. Haga clic en **Configurar**.

   Se abre la ventana **Seguridad y confiabilidad**.
6. Use la casilla **Iniciar la aplicación al arrancar el equipo (recomendado)** para habilitar o deshabilitar el inicio automático de la aplicación.
7. Guarde los cambios.

Cómo configurar el inicio automático de la aplicación en la Consola de la aplicación

1. seleccione el nodo **Kaspersky Embedded Systems Security** en el árbol de la Consola de la aplicación.
2. Seleccione **Propiedades de la aplicación** en el menú contextual del nodo.
3. En la ventana que se abre, seleccione la pestaña **Configuración de seguridad**.
4. Use la casilla **Iniciar la aplicación al arrancar el equipo (recomendado)** para habilitar o deshabilitar el inicio automático de la aplicación.
5. Guarde los cambios.

Puede iniciar y detener Kaspersky Embedded Systems Security si es miembro del grupo de Administradores en el dispositivo protegido.

Cómo iniciar o detener la aplicación en la Consola de administración de Kaspersky Security Center

1. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
2. En el espacio de trabajo, seleccione la ficha **Dispositivos**.
3. Haga doble clic en un equipo para abrir su ventana de propiedades.
4. En la ventana de propiedades del equipo, elija la sección **Aplicaciones**.
5. En la lista de aplicaciones de Kaspersky instaladas en el equipo, seleccione **Kaspersky Embedded Systems Security para Windows (4.0.0)**.
6. Realice una de las siguientes acciones:
   - Para iniciar la aplicación, haga clic en el botón  , que encontrará a la derecha de la lista de aplicaciones de Kaspersky.
   - Para detener la aplicación, haga clic en el botón  , que encontrará a la derecha de la lista de aplicaciones de Kaspersky.

Cómo iniciar o detener la aplicación en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Dispositivos administrados**.
2. Haga clic en el nombre del equipo en el que desea iniciar o detener Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades del equipo.
3. Seleccione la ficha **Aplicaciones**.
4. Seleccione la casilla opuesta **Kaspersky Embedded Systems Security para Windows (4.0.0)**.
5. Haga clic en los botones **Iniciar** o **Detener**.

Cómo iniciar o detener la aplicación en la Consola de la aplicación

1. En el árbol de la Consola de la aplicación, en el espacio de trabajo del nodo de **Kaspersky Embedded Systems Security**, haga clic en **Conectarse a un equipo remoto**.
2. En el mensaje de reinicio de la aplicación, haga clic en **Sí**.
3. En la ventana **Seleccionar dispositivo protegido**, junto a **Administración de servicio**, realice una de las siguientes acciones:
   - Si desea detener la aplicación, haga clic en el botón **Detener**.
   - Si desea iniciar la aplicación, haga clic en el botón **Inicio**.

La aplicación se detendrá o iniciará.

También se muestra la ventana **Seleccionar dispositivo protegido** si la conexión con el equipo en el que está instalada la aplicación se pierde o si el servicio KESS falla. Puede restaurar el servicio KESS haciendo clic en el botón **Inicio**.

Cómo iniciar o detener la aplicación a través de la línea de comandos

1. Abra el símbolo del sistema (cmd.exe) como administrador.
2. Con el comando `cd`, vaya a la carpeta donde se encuentran los archivos klpsm.exe y kavshell.exe.

   Por ejemplo: `cd C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.0.0`

3. Para iniciar la aplicación desde la línea de comandos, ejecute uno de los siguientes comandos:

   - `klpsm.exe start_avp_service`

   - `KAVSHELL start [/login:<nombre de la cuenta de usuario actual>] [/PWD:</contraseña de inicio de sesión o contraseña de KLAdmin si /no se especifica el nombre de usuario>]`

4. Para detener la aplicación desde la línea de comandos, ejecute uno de los siguientes comandos:

   - `klpsm.exe stop_avp_service`

   - `KAVSHELL stop [/login:<nombre de la cuenta de usuario actual>] [/PWD:</contraseña de inicio de sesión o contraseña de KLAdmin si /no se especifica el nombre de usuario>]`

Suspensión y reanudación de la protección y control del equipo

Suspender la protección y control del equipo significa deshabilitar todos los componentes de protección y control de Kaspersky Embedded Systems Security durante un tiempo.

El estado de aplicación se muestra por medio del ícono de la aplicación en el área de notificación de la barra de tareas.

- El icono  significa que la protección y control del equipo están suspendidos.

- El icono  significa que la protección y control del equipo están habilitados.

Suspender o reanudar el control y la protección del equipo no afecta las tareas de análisis o actualización.

Si hay conexiones de red ya establecidas cuando suspende o reanuda la protección y control del equipo, se muestra una notificación que informa que estas conexiones de red se han interrumpido.

Para pausar la protección y control del equipo:

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Kaspersky Embedded Systems Security**.

2. Seleccione **Suspender protección**.

3. Seleccione una de las siguientes opciones:

- **Suspender durante el tiempo especificado <periodo>**: las funciones de protección y control del equipo se reactivarán cuando haya transcurrido el tiempo que indique en la lista desplegable de abajo.
- **Pausar hasta reiniciar**: las funciones de protección y control del equipo se reactivarán luego de que cierre y vuelva a abrir la aplicación, o bien cuando se reinicie el sistema operativo. Para utilizar esta opción, debe habilitarse el inicio automático de la aplicación.
- **Pausar**: las funciones de protección y control del equipo se reactivarán cuando usted lo decida.

Kaspersky Embedded Systems Security pausará todos los componentes de protección y control que no estén marcados con un candado (🔒) en la directiva.

Para reanudar la protección y control del equipo:

1. Abra el menú contextual del ícono de la aplicación, ubicado en el área de notificación de la barra de tareas.
2. En el menú contextual, seleccione **Reanudar protección**.

Puede reanudar la protección y control del equipo en cualquier momento, sin importar la opción que seleccionó previamente para suspender la protección y control.

Interfaz de diagnóstico compacto

En esta sección se describe el uso de la Interfaz de diagnóstico compacto.

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 dispositivo protegido. Para iniciar la Interfaz de diagnóstico compacto, puede usar el icono de la bandeja del sistema o puede ejecutar el archivo avpui.exe, ubicado en la carpeta de la aplicación en el dispositivo protegido.

La Interfaz de diagnóstico compacto permite hacer lo siguiente:

- Abra la ventana **Acerca de** con la lista de actualizaciones instaladas y parches disponibles.
- Ver información sobre el estado general de la aplicación.
- Ver los incidentes de seguridad que han ocurrido.
- Revisar la actividad actual del dispositivo protegido.
- Iniciar o detener la escritura de los archivos de volcado y de rastreo.
- Abra la Consola de la aplicación.

La Interfaz de diagnóstico compacto está disponible incluso si el acceso a las funciones de Kaspersky Embedded Systems Security está protegido con contraseña. No se requiere contraseña.

El componente Interfaz de diagnóstico compacto no puede configurarse mediante Kaspersky Security Center.

Revisión del estado de Kaspersky Embedded Systems Security a través de la Interfaz de diagnóstico compacto

Para revisar el estado de la aplicación a través de la Interfaz de diagnóstico compacto, siga estos pasos:

1. Abra la Interfaz de diagnóstico compacto de una de las siguientes maneras:
   - Ejecute el archivo avpui.exe de la carpeta de instalación de la aplicación en el dispositivo protegido. De forma predeterminada, el archivo se encuentra en C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.0.0.
   - Haga clic en el ícono de la aplicación en el área de notificaciones de la barra de tareas.

2. Revise el estado actual de las tareas clave de Protección del equipo en tiempo real y de Actualización en la sección **Estado de la protección**. Se utilizan diferentes colores para notificar al usuario sobre el estado de protección (consulte la tabla a continuación).

Indicación de colores en la ventana Interfaz de diagnóstico compacto

Sección	Estado
Estado de la protección en tiempo real	El panel es *verde* para cualquiera de los siguientes escenarios (si se cumple alguna de las 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 **Bloquear** 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.
	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 **Informar**. • Prevención de exploits y la tarea Control de inicio de aplicaciones se iniciaron en modo **Informar**.
	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 **Informar**.
Licencias	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 30 días y no se ha agregado ninguna clave adicional ni código de activación.* • *La clave agregada se agregó a la lista de rechazadas y se bloqueará.*
	Un panel *rojo* significa que ha ocurrido uno de los siguientes eventos: • *La aplicación no está activada.* • *La licencia caducó.* • *Se infringió el Contrato de licencia de usuario final.* • *La clave está en la lista de rechazadas.*
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 son obsoletas.

Revisión de estadísticas de eventos de seguridad

En la sección **Estadísticas** se muestran 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 ver las estadísticas:

1. Abra la Interfaz de diagnóstico compacto de una de las siguientes maneras:

   - Ejecute el archivo avpui.exe de la carpeta de instalación de la aplicación en el dispositivo protegido. De forma predeterminada, el archivo se encuentra en C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.0.0.

   - Haga clic en el ícono de la aplicación en el área de notificaciones de la barra de tareas.

2. Vaya a la sección **Estadísticas**.

3. Revise los incidentes de seguridad para las tareas de protección.

Revisión de la actividad de la aplicación actual

Para revisar la actividad de la aplicación actual en el dispositivo protegido:

1. Abra la Interfaz de diagnóstico compacto de una de las siguientes maneras:

   - Ejecute el archivo avpui.exe de la carpeta de instalación de la aplicación en el dispositivo protegido. De forma predeterminada, el archivo se encuentra en C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.0.0.

   - Haga clic en el ícono de la aplicación en el área de notificaciones de la barra de tareas.

2. Vaya a la sección **Actividad de aplicaciones actual**.

Los diferentes colores se usan para indicar el estado de la actividad de la aplicación:

- En la sección **Tareas**:

  - *Verde*. Ninguna condición requiere rojo o amarillo.

  - *Amarillo*. Las áreas críticas no se han analizado durante un periodo prolongado.

  - *Rojo*. Al menos una de las siguientes condiciones es verdadera:

    - 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.

Configuración del seguimiento de la aplicación y el registro del volcado de memoria

Para configurar el seguimiento de la aplicación y el registro del volcado de memoria:

1. Abra la Interfaz de diagnóstico compacto de una de las siguientes maneras:

   - Ejecute el archivo avpui.exe de la carpeta de instalación de la aplicación en el dispositivo protegido. De forma predeterminada, el archivo se encuentra en C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.0.0.

   - Haga clic en el ícono de la aplicación en el área de notificaciones de la barra de tareas.

2. Vaya a la sección **Diagnóstico de mal funcionamiento**.

3. Use la casilla **Escribir información de depuración en el archivo de seguimiento** para habilitar o deshabilitar el seguimiento del funcionamiento de la aplicación.

4. Si es necesario, haga clic en el botón **Examinar** para especificar la carpeta donde Kaspersky Embedded Systems Security guardará los archivos de rastreo.

   La carpeta debe crearse de antemano y es necesario que la cuenta SYSTEM pueda escribir en ella. La ruta no puede hacer referencia a una unidad, una carpeta de red o una variable de entorno.

5. En la lista desplegable **Nivel de detalles**, seleccione el nivel de detalle de la información para depuración.

   - **Crítico** significa que el archivo de rastreo guarda solo los mensajes acerca de errores fatales.

   - **Diagnóstico** significa que el archivo de rastreo guarda mensajes acerca de todos los errores y las advertencias.

   - **Importante** significa que el archivo de rastreo guarda mensajes acerca de todos los errores, advertencias e información adicional.

   - **Normal** significa que el archivo de rastreo guarda mensajes acerca de todos los errores, advertencias, así como información acerca del funcionamiento normal de la aplicación (predeterminado).

   - **Detallado** significa que el archivo de rastreo guarda toda la información acerca del funcionamiento de la aplicación.

   El nivel de detalle que se requiere para solucionar cualquier posible problema es determinado por un especialista del servicio de soporte técnico.

   El nivel de detalle predeterminado es **Normal**.

6. Especifique el **Tamaño máximo de un archivo de seguimiento (MB)**.

   Valores disponibles: de 1 a 4095 MB. De forma predeterminada, el tamaño máximo de los archivos de seguimiento es de 100 MB.

7. Para que los archivos de seguimiento antiguos se eliminen cuando se alcance el número máximo de archivos, seleccione la casilla **Eliminar los archivos de seguimiento más antiguos**.

8. Especifique el **Cantidad máxima de archivos de seguimiento**.

   Valores disponibles: de 1 a 999. De manera predeterminada, el número máximo de archivos es 5. El campo está disponible si la casilla de verificación **Eliminar los archivos de seguimiento más antiguos** está seleccionada.

9. Si es necesario, configure volcados de memoria:

   a. Seleccione o desactive la casilla **Crear una archivo de volcado por mal funcionamiento en la carpeta** para habilitar o deshabilitar el volcado de memoria en caso de mal funcionamiento.

   b. Si es necesario, haga clic en el botón **Examinar** para especificar la carpeta donde Kaspersky Embedded Systems Security guardará los archivos de volcado de memoria. De manera predeterminada, los archivos de volcado de memoria se almacenan en la siguiente carpeta: %ProgramData%\Kaspersky Lab\KESS.4.0\Traces.

   > La carpeta debe crearse de antemano y es necesario que la cuenta SYSTEM pueda escribir en ella. La ruta no puede hacer referencia a una unidad, una carpeta de red o una variable de entorno.

10. Haga clic en **Aplicar**.

Autoprotección de Kaspersky Embedded Systems Security

Autoprotección evita que otras aplicaciones realicen acciones que puedan interferir con el funcionamiento de Kaspersky Embedded Systems Security. La aplicación tiene mecanismos de autoprotección que protegen la aplicación contra la modificación o eliminación de sus carpetas, los procesos de memoria y las entradas de registro del sistema. Kaspersky Embedded Systems Security es compatible con la tecnología de protección de procesos Antimalware Protected Process Light (AM-PPL) de Microsoft, que protege los procesos de las aplicaciones de actividades maliciosas. Además, la aplicación permite administrar los permisos de acceso de los usuarios a la funcionalidad de la aplicación y por separado al servicio de la aplicación.

Habilitar y deshabilitar el componente Autoprotección

Kaspersky Embedded Systems Security impide la alteración y la eliminación de los archivos de la aplicación en el disco duro, los procesos de memoria y las entradas en el registro del sistema.

La tecnología bloquea el acceso a los siguientes componentes de la aplicación:

- Archivos en la carpeta de instalación de Kaspersky Embedded Systems Security y otros archivos de la aplicación.
- Claves de registro con informes pertenecientes a la aplicación
- Procesos que la aplicación ejecuta

El mecanismo de Autoprotección de Kaspersky Embedded Systems Security está habilitado de manera predeterminada.

Cómo habilitar o deshabilitar la autoprotección en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de las propiedades de la directiva, vaya a la sección **Configuración de la aplicación**.
4. En el bloque **Seguridad y confiabilidad**, haga clic en el botón **Configuración**.
5. En la ventana que se abre, seleccione la pestaña **Seguridad**.
6. En el bloque **Autoprotección**, use la casilla **Proteger los procesos de la aplicación de amenazas externas** para habilitar o deshabilitar la Autoprotección.
7. Cierre el candado para aplicar la directiva en los equipos.
8. Haga clic en **Aceptar** para guardar los cambios.

Cómo habilitar o deshabilitar la autoprotección en la Consola de la aplicación

1. En el árbol de la Consola de aplicaciones, seleccione el nodo **Kaspersky Embedded Systems Security** y, en el panel de resultados, haga clic en el vínculo **Propiedades de la aplicación**.
2. En la ventana que se abre, seleccione la pestaña **Configuración de seguridad**.
3. En el bloque **Autoprotección**, use la casilla **Proteger los procesos de la aplicación de amenazas externas** para habilitar o deshabilitar la Autoprotección.
4. Haga clic en **Aceptar** para guardar los cambios.

Cómo habilitar o deshabilitar la autoprotección en Kaspersky Security Center Administration Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Seleccione la sección **Configuración de la aplicación**.
5. En el bloque **Seguridad y confiabilidad**, haga clic en el botón **Configurar**.
   Se abre la ventana **Seguridad y confiabilidad**.
6. En el bloque **Autoprotección**, use la casilla **Proteger los procesos de la aplicación de amenazas externas** para habilitar o deshabilitar la Autoprotección.
7. Cierre el candado para aplicar la directiva en los equipos.
8. Haga clic en **Aceptar** para guardar los cambios.

Compatibilidad con la tecnología AM-PPL

Kaspersky Embedded Systems Security es compatible con una tecnología de Microsoft denominada Antimalware Protected Process Light (en adelante, "AM-PPL"). AM-PPL evita que los procesos de Kaspersky Embedded Systems Security se vean afectados por acciones malintencionadas; puede impedir, por ejemplo, el cierre de la aplicación. AM-PPL no permite que un proceso se ejecute si no es de confianza. Los procesos de Kaspersky Embedded Systems Security, al estar firmados como lo exigen los requisitos de seguridad de Windows, se consideran de confianza. Para más información sobre la tecnología AM-PPL, visite el sitio web de Microsoft. La tecnología AM-PPL está habilitada por defecto.

Kaspersky Embedded Systems Security también cuenta con mecanismos propios para proteger sus procesos. Si opta por utilizar AM-PPL, la protección de los procesos quedará en manos del sistema operativo. Con ello, se reducirá el uso de recursos del equipo y aumentará la velocidad de la aplicación.

La aplicación registra los servicios Kaspersky Embedded Systems Security (AVP) y Kaspersky Seamless Update Service (AVPSUS). La tecnología AM-PPL protege solo el servicio AVP.

La tecnología AM-PPL siempre debe estar activa. La tecnología AM-PPL es un componente importante de la defensa del sistema operativo. Es admisible deshabilitar AM-PPL solo en un entorno de prueba independiente con el fin de solucionar problemas de la aplicación.

La tecnología AM-PPL está disponible en Windows 10 versión 1703 (RS2) y posteriores, así como en Windows Server 2019.

Para habilitar o deshabilitar la tecnología AM-PPL:

1. Desactive el mecanismo de Autoprotección de la aplicación.

   El mecanismo de Autoprotección evita que los procesos de la aplicación se modifiquen o se eliminen de la memoria del equipo. Una de las acciones contra las que protege es la modificación del estado de AM-PPL.

2. Abra el símbolo del sistema (cmd) como administrador.

3. Vaya a la carpeta en la que se encuentre el archivo ejecutable de Kaspersky Embedded Systems Security.

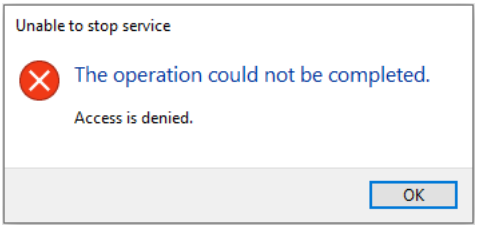
4. En la línea de comandos, escriba lo siguiente:

   - `klpsm.exe enable`: habilitar la compatibilidad con la tecnología AM-PPL.
   - `klpsm.exe disable`: deshabilitar la compatibilidad con la tecnología AM-PPL.

5. Reinicie Kaspersky Embedded Systems Security.

6. Reactive el mecanismo de Autoprotección de la aplicación.

Como consecuencia, cuando un usuario intente detener el servicio AVP, aparecerá una ventana del sistema con un mensaje de error. El usuario solo puede administrar los servicios de aplicación desde la interfaz de Kaspersky Embedded Systems Security.



Error de acceso a los servicios de la aplicación

Protección de los servicios del sistema operativo

Puede usar la funcionalidad *Proteger los servicios del sistema operativo* para permitir o prohibir que las aplicaciones de terceros actúen sobre los servicios del sistema operativo.

Cómo habilitar o deshabilitar la protección de los servicios del sistema operativo en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de las propiedades de la directiva, vaya a la sección **Configuración de la aplicación**.
4. En el bloque **Seguridad y confiabilidad**, haga clic en el botón **Configuración**.
5. En la ventana que se abre, seleccione la pestaña **Seguridad**.
6. Use la casilla **Proteger los servicios del sistema operativo** para habilitar o deshabilitar la protección de los servicios del sistema operativo.

   Si se habilita la protección de los servicios del sistema operativo, las aplicaciones de terceros no pueden actuar sobre los procesos del sistema operativo.

   Si se deshabilita la protección de los servicios del sistema operativo, las aplicaciones de terceros pueden actuar sobre los procesos del sistema operativo.

   Después de habilitar o deshabilitar la función, debe reiniciar el equipo para aplicar los cambios.
7. Cierre el candado para aplicar la directiva en los equipos.
8. Haga clic en **Aceptar** para guardar los cambios.

Cómo habilitar o deshabilitar la protección de los servicios del sistema operativo en la Consola de la aplicación

1. En el árbol de la Consola de aplicaciones, seleccione el nodo **Kaspersky Embedded Systems Security** y, en el panel de resultados, haga clic en el vínculo **Propiedades de la aplicación**.
2. En la ventana que se abre, seleccione la pestaña **Configuración de seguridad**.
3. Use la casilla **Proteger los servicios del sistema operativo** para habilitar o deshabilitar la protección de los servicios del sistema operativo.

   Si se habilita la protección de los servicios del sistema operativo, las aplicaciones de terceros no pueden actuar sobre los procesos del sistema operativo.

   Si se deshabilita la protección de los servicios del sistema operativo, las aplicaciones de terceros pueden actuar sobre los procesos del sistema operativo.

   Después de habilitar o deshabilitar la función, debe reiniciar el equipo para aplicar los cambios.
4. Haga clic en **Aceptar** para guardar los cambios.

Cómo habilitar o deshabilitar la protección de servicios del sistema operativo en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Seleccione la sección **Configuración de la aplicación**.
5. En el bloque **Seguridad y confiabilidad**, haga clic en el botón **Configurar**.

   Se abre la ventana **Seguridad y confiabilidad**.
6. Use la casilla **Proteger los servicios del sistema operativo** para habilitar o deshabilitar la protección de los servicios del sistema operativo.

   Si se habilita la protección de los servicios del sistema operativo, las aplicaciones de terceros no pueden actuar sobre los procesos del sistema operativo.

   Si se deshabilita la protección de los servicios del sistema operativo, las aplicaciones de terceros pueden actuar sobre los procesos del sistema operativo.

   Después de habilitar o deshabilitar la función, debe reiniciar el equipo para aplicar los cambios.
7. Cierre el candado para aplicar la directiva en los equipos.
8. Haga clic en **Aceptar** para guardar los cambios.

Configuración de permisos de usuario para administrar Kaspersky Embedded Systems Security

De forma predeterminada, tienen acceso a todas las funciones de Kaspersky Embedded Systems Security los miembros del grupo de Administradores del dispositivo protegido, los miembros del grupo de administradores de ESS creado en el dispositivo protegido durante la instalación de Kaspersky Embedded Systems Security y el grupo SYSTEM.

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 permitir o bloquear el acceso a funciones específicas de Kaspersky Embedded Systems Security para usuarios o grupos de usuarios en particular.

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

Derechos de usuario	Descripción
Administrar tareas	Capacidad para iniciar/detener/pausar/reanudar tareas de Kaspersky Embedded Systems Security.
Crear y eliminar tareas	Capacidad para crear y eliminar tareas de Análisis a pedido.
Editar configuración	Capacidad para: • Importar ajustes de Kaspersky Embedded Systems Security desde un archivo de configuración. • Editar la configuración de la aplicación.

Derechos de usuario	Descripción
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 depósitos	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.
Leer estadísticas	Capacidad para ver estadísticas por cada tarea de Kaspersky Embedded Systems Security.
Administrar la 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.
Modificar 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.
Conexión remota a la aplicación	Capacidad para conectarse de forma remota a la aplicación mediante la Consola de la aplicación. Para el acceso remoto, el usuario también debe tener los derechos de acceso a la funcionalidad **Leer configuración** .
Salir de la aplicación	Capacidad para salir de la aplicación con la Consola de la aplicación.
Deshabilitar la directiva de Kaspersky Security Center	Capacidad de deshabilitar la directiva de Kaspersky Security Center.
Exportar configuración	Capacidad de exportar la configuración de Kaspersky Embedded Systems Security.

Cómo configurar los permisos de usuario para administrar Kaspersky Embedded Systems Security en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de propiedades de la directiva, seleccione **Adicional**.
4. En la sección **Permisos de acceso de usuario para administrar la aplicación**, haga clic en **Configuración**.
5. Esto abre una ventana; en esa ventana, seleccione la casilla de verificación **Permitir la confirmación de acciones con la aplicación usando credenciales de usuarios creados manualmente** y establezca una contraseña para la cuenta de usuario KLAdmin. La cuenta de usuario se agrega automáticamente a la lista de cuentas de usuarios.

6. Si es necesario, agregue las cuentas de usuario a las que desea otorgar acceso a la administración de la aplicación. Para hacerlo, haga clic en **Agregar** en la tabla de cuentas de usuarios.

   Se abre el formulario para configurar los permisos de acceso de los usuarios.

7. Seleccione el método que desea usar para agregar usuarios:

   - **Seleccionar un usuario/grupo de Active Directory**. Puede otorgarle a Kaspersky Embedded Systems Security acceso a usuarios o grupos en particular dentro del dominio de Active Directory. Por ejemplo, un usuario específico puede contar con el permiso **Salir de la aplicación** aun cuando los miembros del grupo Everyone tengan prohibido cerrar el programa.

   - **Agregar un usuario/grupo de usuarios manualmente**. Puede crear una cuenta de usuario que no esté presente en Active Directory y asignar permisos individuales a esa cuenta de usuario. Es decir, puede crear una *cuenta de usuario de servicio* y usarla en lugar de KLAdmin. De esta manera, no necesita compartir su contraseña de KLAdmin con otros usuarios ni crear nuevas cuentas de usuario de Active Directory. Puede especificar cualquier nombre de usuario y contraseña. Por ejemplo, puede otorgar el permiso **Leer registros** a la cuenta de usuario del servicio. Como resultado, si la visualización de informes está prohibida en el grupo "Todos", puede abrir los informes usando la cuenta de usuario de servicio o la cuenta de usuario de KLAdmin.

     Para agregar un usuario o un grupo de usuarios manualmente, debe habilitar Protección con contraseña.

8. Seleccione al usuario o grupo de usuarios al que desea conceder acceso para administrar la aplicación.

9. En la lista **Permisos**, configure los permisos de acceso de los usuarios a la funcionalidad de la aplicación.

10. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados.

Cómo configurar los permisos de usuario para administrar Kaspersky Embedded Systems Security en la Consola de la aplicación

1. En el árbol de la Consola de la aplicación, seleccione el nodo **Kaspersky Embedded Systems Security** y seleccione **Permisos de acceso de usuario para administrar la aplicación** del menú contextual del nodo.

2. Esto abre una ventana; en esa ventana, seleccione la casilla de verificación **Permitir la confirmación de acciones con la aplicación usando credenciales de usuarios creados manualmente** y establezca una contraseña para la cuenta de usuario KLAdmin. La cuenta de usuario se agrega automáticamente a la lista de cuentas de usuarios.

3. Si es necesario, agregue las cuentas de usuario a las que desea otorgar acceso a la administración de la aplicación. Para hacerlo, haga clic en **Agregar** en la tabla de cuentas de usuarios.

   Se abre el formulario para configurar los permisos de acceso de los usuarios.

4. Seleccione el método que desea usar para agregar usuarios:

   - **Seleccionar un usuario/grupo de Active Directory**. Puede otorgarle a Kaspersky Embedded Systems Security acceso a usuarios o grupos en particular dentro del dominio de Active Directory. Por ejemplo, un usuario específico puede contar con el permiso **Salir de la aplicación** aun cuando los miembros del grupo Everyone tengan prohibido cerrar el programa.

   - **Agregar un usuario/grupo de usuarios manualmente**. Puede crear una cuenta de usuario que no esté presente en Active Directory y asignar permisos individuales a esa cuenta de usuario. Es decir, puede crear una *cuenta de usuario de servicio* y usarla en lugar de KLAdmin. De esta manera, no necesita compartir su contraseña de KLAdmin con otros usuarios ni crear nuevas cuentas de usuario de Active Directory. Puede especificar cualquier nombre de usuario y contraseña. Por ejemplo, puede otorgar el permiso **Leer registros** a la cuenta de usuario del servicio. Como resultado, si la visualización de informes está prohibida en el grupo "Todos", puede abrir los informes usando la cuenta de usuario de servicio o la cuenta de usuario de KLAdmin.

     Para agregar un usuario o un grupo de usuarios manualmente, debe habilitar Protección con contraseña.

5. Seleccione al usuario o grupo de usuarios al que desea conceder acceso para administrar la aplicación.

6. En la lista **Permisos**, configure los permisos de acceso de los usuarios a la funcionalidad de la aplicación.

7. Guarde los cambios.

Cómo configurar los derechos de acceso del usuario para administrar Kaspersky Embedded Systems Security en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.

2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la ficha **Configuración de la aplicación**.

4. Vaya a **Adicional** → **Permisos de acceso de usuario para administrar la aplicación** y haga clic en el botón **Configurar**.

5. Esto abre una ventana; en esa ventana, seleccione la casilla de verificación **Permitir la confirmación de acciones con la aplicación usando credenciales de usuarios creados manualmente** y establezca una contraseña para la cuenta de usuario KLAdmin. La cuenta de usuario se agrega automáticamente a la lista de cuentas de usuarios.

6. Si es necesario, agregue las cuentas de usuario a las que desea otorgar acceso a la administración de la aplicación. Para hacerlo, haga clic en **Agregar** en la tabla de cuentas de usuarios.

   Se abre el formulario para configurar los permisos de acceso de los usuarios.

7. Seleccione el método que desea usar para agregar usuarios:

   - **Seleccionar un usuario/grupo de Active Directory**. Puede otorgarle a Kaspersky Embedded Systems Security acceso a usuarios o grupos en particular dentro del dominio de Active Directory. Por ejemplo, un usuario específico puede contar con el permiso **Salir de la aplicación** aun cuando los miembros del grupo Everyone tengan prohibido cerrar el programa.

   - **Agregar un usuario/grupo de usuarios manualmente**. Puede crear una cuenta de usuario que no esté presente en Active Directory y asignar permisos individuales a esa cuenta de usuario. Es decir, puede crear una *cuenta de usuario de servicio* y usarla en lugar de KLAdmin. De esta manera, no necesita compartir su contraseña de KLAdmin con otros usuarios ni crear nuevas cuentas de usuario de Active Directory. Puede especificar cualquier nombre de usuario y contraseña. Por ejemplo, puede otorgar el permiso **Leer registros** a la cuenta de usuario del servicio. Como resultado, si la visualización de informes está prohibida en el grupo "Todos", puede abrir los informes usando la cuenta de usuario de servicio o la cuenta de usuario de KLAdmin.

     Para agregar un usuario o un grupo de usuarios manualmente, debe habilitar Protección con contraseña.

8. Seleccione al usuario o grupo de usuarios al que desea conceder acceso para administrar la aplicación.

9. En la lista **Permisos**, configure los permisos de acceso de los usuarios a la funcionalidad de la aplicación.

10. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados.

Configuración de permisos de acceso de usuarios para administrar el servicio de Kaspersky Security.

Durante la instalación, Kaspersky Embedded Systems Security registra el servicio de la aplicación, *Kaspersky Security Service*, en Windows. Por lo tanto, la aplicación incluye componentes funcionales que se inician durante el inicio del sistema operativo. Para reducir el riesgo de que un tercero acceda a la funcionalidad de la aplicación y a la configuración de seguridad del dispositivo protegido mediante el servicio de la aplicación, puede restringir los permisos para administrar el servicio de Kaspersky Security.

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 dispositivo protegido. Los permisos de lectura se conceden a los grupos SERVICE e INTERACTIVE, y los permisos de lectura y ejecución se conceden al grupo SYSTEM.

No se puede eliminar la cuenta de usuario SYSTEM o modificar permisos de 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 del nivel "Modificar permisos" pueden otorgar permisos de acceso para administrar el servicio de Kaspersky Security a otros usuarios registrados en el dispositivo protegido o incluidos en el dominio.

Los usuarios o grupos de usuarios de Kaspersky Embedded Systems Security pueden contar con uno de los siguientes niveles de permisos de acceso predeterminados 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.
- **Leer**: capacidad de ver las configuraciones generales y los permisos de usuario del servicio de Kaspersky Security.
- **Modificar**: capacidad de ver y modificar la configuración general y los permisos del usuario del servicio de Kaspersky Security.
- **Ejecutar**: 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).

Permisos de acceso para las funciones del servicio de Kaspersky Security.

Característica	Descripción
Leer configuración 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 al administrador de control de servicios de Microsoft Windows.
Solicitar estado del 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 con los servicios de los que depende el servicio de Kaspersky Security y aquellos que dependen del servicio de Kaspersky Security.
Modificar configuración del servicio	Capacidad de ver y modificar la configuración general y los permisos del usuario del servicio de Kaspersky Security.
Iniciar servicio	Capacidad para iniciar el servicio de Kaspersky Security.
Detener el servicio	Capacidad para detener el servicio de Kaspersky Security.
Pausar o 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.
Modificar 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.

Puede editar la lista de usuarios y grupos de usuarios autorizados para administrar el servicio de Kaspersky Security y también editar los permisos de acceso de esos usuarios y grupos de usuarios.

Cómo configurar los permisos de usuario para administrar Kaspersky Security Service en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de propiedades de la directiva, seleccione **Adicional**.

4. En la sección **Permisos de acceso de usuario para la administración del servicio de Kaspersky Security**, haga clic en **Configuración**.

   Se abre el formulario para configurar los permisos de acceso de los usuarios.

5. Agregue un usuario o grupo de Active Directory para el cual desea configurar los permisos de usuario de Kaspersky Security Service.

6. Seleccione al usuario o grupo de usuarios al que desea conceder acceso para administrar la aplicación.

7. En la lista de permisos, configure los permisos de usuario para administrar Kaspersky Security Service.

8. Si es necesario, configure permisos especiales para los usuarios:

   a. Haga clic en **Adicional**.

   b. En la ventana que se abre, seleccione una cuenta de usuario.

   c. Haga doble clic para abrir las propiedades de la cuenta de usuario.

   d. En la ventana que se abre, haga clic en el vínculo **Mostrar permisos adicionales**.

   e. En la ventana que se abre, configure permisos especiales para el usuario.

9. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados .

Cómo configurar los permisos de usuario para administrar Kaspersky Security Service en la Consola de la aplicación

1. En el árbol de la Consola de la aplicación, seleccione el nodo **Kaspersky Embedded Systems Security** y seleccione **Permisos de acceso de usuario para la administración del servicio de Kaspersky Security** del menú contextual del nodo.

2. En la ventana que se abre, en el bloque **Permisos**, haga clic en el botón **Agregar**.

   Se abre el formulario para configurar los permisos de acceso de los usuarios.

3. Agregue un usuario o grupo de Active Directory para el cual desea configurar los permisos de usuario de Kaspersky Security Service.

4. Seleccione al usuario o grupo de usuarios al que desea conceder acceso para administrar la aplicación.

5. En la lista de permisos, configure los permisos de usuario para administrar Kaspersky Security Service.

6. Si es necesario, configure permisos especiales para los usuarios:

   a. Haga clic en **Adicional**.

   b. En la ventana que se abre, seleccione una cuenta de usuario.

   c. Haga doble clic para abrir las propiedades de la cuenta de usuario.

d. En la ventana que se abre, haga clic en el vínculo **Mostrar permisos adicionales**.

e. En la ventana que se abre, configure permisos especiales para el usuario.

7. Guarde los cambios.

Cómo configurar los permisos de usuario para administrar Kaspersky Security Service en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Adicional** → **Permisos de acceso de usuario para la administración del servicio de Kaspersky Security** y haga clic en el botón **Configurar**.

   Se abre la ventana **Permisos de acceso de usuario para la administración del servicio de Kaspersky Security**.
5. Agregue un usuario o grupo de Active Directory para el cual desea configurar los permisos de usuario de Kaspersky Security Service.
6. Seleccione al usuario o grupo de usuarios al que desea conceder acceso para administrar la aplicación.

   No puede configurar permisos especiales para administrar el servicio de la aplicación en Web Console.
7. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados.

Acceso protegido por contraseña a funciones de Kaspersky Embedded Systems Security

La configuración de derechos de usuario le permite restringir el acceso a la administración de aplicaciones y servicios registrados configurando los permisos del usuario. También se puede establecer la protección con contraseña en Kaspersky Embedded Systems Security para obtener una protección adicional de las operaciones críticas.

Cuando un usuario intenta realizar una acción protegida con contraseña, Kaspersky Embedded Systems Security le solicita su nombre de usuario y contraseña o una contraseña temporal. La protección con contraseña admite las siguientes cuentas:

- **KLAdmin**. Cuenta de administración con acceso ilimitado a Kaspersky Embedded Systems Security. La cuenta KLAdmin puede realizar cualquier acción que esté protegida con contraseña. Los permisos de KLAdmin no pueden revocarse. Cuando habilite la protección con contraseña, Kaspersky Embedded Systems Security le pedirá que defina la contraseña de esta cuenta.

- **Cuenta agregada manualmente**. Una cuenta fuera del dominio de Active Directory. Puede usar esta cuenta del servicio en lugar de KLAdmin si no desea compartir la contraseña del administrador. Puede establecer cualquier nombre de usuario y contraseña, y configurar los permisos individuales.

- **El grupo Everyone**. Grupo propio de Windows en el que están incluidos todos los usuarios de la red corporativa. Los usuarios del grupo Everyone tendrán acceso a la aplicación conforme a los permisos que se les asigne.

- **Usuarios o grupos individuales**. Cuentas de usuario a las que pueden asignarse permisos individuales. Es posible, por ejemplo, autorizar a un usuario o grupo en particular a realizar una acción que se encuentra bloqueada para el grupo Everyone.

La interfaz de Kaspersky Embedded Systems Security oculta la contraseña especificada en la pantalla. Kaspersky Embedded Systems Security almacena la contraseña como una suma de control calculada cuando se ingresa la contraseña.

Kaspersky Embedded Systems Security no verifica la seguridad de la contraseña y no bloquea la entrada de la contraseña después de varios intentos fallidos.

Al crear una contraseña, se recomienda cumplir con las siguientes condiciones:

- La contraseña no contiene el nombre de la cuenta ni el nombre del equipo.
- La contraseña tiene al menos 8 caracteres de longitud.
- La contraseña contiene caracteres que coinciden con al menos tres de las siguientes categorías:
  - Letras mayúsculas latinas (A-Z)
  - Letras minúsculas latinas (a-z)
  - Numerales (0-9)
  - Signo de exclamación (!), signo de dólar ($), signo de numeral (#) y signo de porcentaje (%)

Cómo proteger con contraseña el acceso a la funcionalidad de Kaspersky Embedded Systems Security en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de propiedades de la directiva, seleccione **Adicional**.

4. En la sección **Permisos de acceso de usuario para administrar la aplicación**, haga clic en **Configuración**.

5. En la ventana que se abre, seleccione la casilla **Permitir la confirmación de acciones con la aplicación usando credenciales de usuarios creados manualmente**.

6. Si es necesario, anule la selección de la casilla **Solicitar contraseña para confirmar acciones críticas**.

   Si esta funcionalidad está habilitada, la aplicación solicita un nombre de usuario y una contraseña al eliminar, modificar o recuperar la aplicación, y al realizar **acciones en la línea de comandos que pueden reducir el nivel de protección del dispositivo.**

   La aplicación solicita credenciales cuando ejecuta los siguientes comandos:

   - `KAVSHELL APPCONTROL`
   - `KAVSHELL APPCONTROL /CONFIG`
   - `KAVSHELL APPCONTROL /GENERATE /import`
   - `KAVSHELL DEVCONTROL`
   - `KAVSHELL EXITPOLICY`
   - `KAVSHELL IMPORT`
   - `KAVSHELL ISOLATION /DISABLE`
   - `KAVSHELL LICENSE /DEL`
   - `KAVSHELL PASSWORD`
   - `KAVSHELL PREVENTION /DISABLE`
   - `KAVSHELL QUARANTINE /ADD`
   - `KAVSHELL QUARANTINE /DELETE`
   - `KAVSHELL REMOTEACCESS`
   - `KAVSHELL RESETMDRMACHINEID`
   - `KAVSHELL SERVERBINDINGDISABLE`
   - `KAVSHELL SIGMA /DISABLE`
   - `KAVSHELL SIGMA /ADD`
   - `KAVSHELL SIGMA /REMOVE>`
   - `KAVSHELL STOP`
   - `KAVSHELL TASK /STOP`
   - `KAVSHELL TELEMETRYFILTERS /IMPORT`

Si esta funcionalidad está deshabilitada y el usuario actual tiene los derechos necesarios, Kaspersky Embedded Systems Security no solicita credenciales. De manera predeterminada, esta opción está habilitada.

Si se establece una contraseña de Windows vacía para el usuario actual, debe ingresar las credenciales de un usuario que tenga los derechos necesarios y tenga una contraseña que no esté vacía.

7. Especifique la contraseña de la cuenta de usuario de KLAdmin.
8. Si es necesario, agregue las cuentas de usuario a las que desea otorgar acceso a la administración de la aplicación:
   a. Haga clic en **Agregar**.
      Se abre el formulario para configurar los permisos de acceso de los usuarios.
   b. En la ventana que se abre, seleccione el método para agregar usuarios: **Agregar un usuario/grupo de usuarios manualmente**.
   c. Especifique un nombre de usuario y una contraseña.
   d. En la lista **Permisos**, configure los permisos de acceso de los usuarios a la funcionalidad de la aplicación.
9. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados.

Cómo proteger con contraseña el acceso a la funcionalidad de Kaspersky Embedded Systems Security en la Consola de la aplicación

1. En el árbol de la Consola de la aplicación, seleccione el nodo **Kaspersky Embedded Systems Security** y seleccione **Permisos de acceso de usuario para administrar la aplicación** del menú contextual del nodo.
2. En la ventana que se abre, seleccione la casilla **Permitir la confirmación de acciones con la aplicación usando credenciales de usuarios creados manualmente**.
3. Si es necesario, anule la selección de la casilla **Solicitar contraseña para confirmar acciones críticas**.
   Si esta funcionalidad está habilitada, la aplicación solicita un nombre de usuario y una contraseña al eliminar, modificar o recuperar la aplicación, y al realizar **acciones en la línea de comandos que pueden reducir el nivel de protección del dispositivo.**

   La aplicación solicita credenciales cuando ejecuta los siguientes comandos:

   - `KAVSHELL APPCONTROL`
   - `KAVSHELL APPCONTROL /CONFIG`
   - `KAVSHELL APPCONTROL /GENERATE /import`
   - `KAVSHELL DEVCONTROL`
   - `KAVSHELL EXITPOLICY`

- KAVSHELL IMPORT
- KAVSHELL ISOLATION /DISABLE
- KAVSHELL LICENSE /DEL
- KAVSHELL PASSWORD
- KAVSHELL PREVENTION /DISABLE
- KAVSHELL QUARANTINE /ADD
- KAVSHELL QUARANTINE /DELETE
- KAVSHELL REMOTEACCESS
- KAVSHELL RESETMDRMACHINEID
- KAVSHELL SERVERBINDINGDISABLE
- KAVSHELL SIGMA /DISABLE
- KAVSHELL SIGMA /ADD
- KAVSHELL SIGMA /REMOVE>
- KAVSHELL STOP
- KAVSHELL TASK /STOP
- KAVSHELL TELEMETRYFILTERS /IMPORT

Si esta funcionalidad está deshabilitada y el usuario actual tiene los derechos necesarios, Kaspersky Embedded Systems Security no solicita credenciales. De manera predeterminada, esta opción está habilitada.

Si se establece una contraseña de Windows vacía para el usuario actual, debe ingresar las credenciales de un usuario que tenga los derechos necesarios y tenga una contraseña que no esté vacía.

4. Especifique la contraseña de la cuenta de usuario de KLAdmin.
5. Si es necesario, agregue las cuentas de usuario a las que desea otorgar acceso a la administración de la aplicación:

   a. Haga clic en **Agregar**.

   Se abre el formulario para configurar los permisos de acceso de los usuarios.

   b. En la ventana que se abre, seleccione el método para agregar usuarios: **Agregar un usuario/grupo de usuarios manualmente**.

c. Especifique un nombre de usuario y una contraseña.

d. En la lista **Permisos**, configure los permisos de acceso de los usuarios a la funcionalidad de la aplicación.

6. Guarde los cambios.

Cómo proteger con contraseña el acceso a la funcionalidad de Kaspersky Embedded Systems Security en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Adicional** → **Permisos de acceso de usuario para administrar la aplicación** y haga clic en el botón **Configurar**.
5. En la ventana que se abre, seleccione la casilla **Permitir la confirmación de acciones con la aplicación usando credenciales de usuarios creados manualmente**.
6. Si es necesario, anule la selección de la casilla **Solicitar contraseña para confirmar acciones críticas**.

   Si esta funcionalidad está habilitada, la aplicación solicita un nombre de usuario y una contraseña al eliminar, modificar o recuperar la aplicación, y al realizar **acciones en la línea de comandos que pueden reducir el nivel de protección del dispositivo.**

   La aplicación solicita credenciales cuando ejecuta los siguientes comandos:

   - `KAVSHELL APPCONTROL`
   - `KAVSHELL APPCONTROL /CONFIG`
   - `KAVSHELL APPCONTROL /GENERATE /import`
   - `KAVSHELL DEVCONTROL`
   - `KAVSHELL EXITPOLICY`
   - `KAVSHELL IMPORT`
   - `KAVSHELL ISOLATION /DISABLE`
   - `KAVSHELL LICENSE /DEL`
   - `KAVSHELL PASSWORD`
   - `KAVSHELL PREVENTION /DISABLE`
   - `KAVSHELL QUARANTINE /ADD`
   - `KAVSHELL QUARANTINE /DELETE`

- KAVSHELL REMOTEACCESS
- KAVSHELL RESETMDRMACHINEID
- KAVSHELL SERVERBINDINGDISABLE
- KAVSHELL SIGMA /DISABLE
- KAVSHELL SIGMA /ADD
- KAVSHELL SIGMA /REMOVE>
- KAVSHELL STOP
- KAVSHELL TASK /STOP
- KAVSHELL TELEMETRYFILTERS /IMPORT

Si esta funcionalidad está deshabilitada y el usuario actual tiene los derechos necesarios, Kaspersky Embedded Systems Security no solicita credenciales. De manera predeterminada, esta opción está habilitada.

Si se establece una contraseña de Windows vacía para el usuario actual, debe ingresar las credenciales de un usuario que tenga los derechos necesarios y tenga una contraseña que no esté vacía.

7. Especifique la contraseña de la cuenta de usuario de KLAdmin.
8. Si es necesario, agregue las cuentas de usuario a las que desea otorgar acceso a la administración de la aplicación:
   a. Haga clic en **Agregar**.
      Se abre el formulario para configurar los permisos de acceso de los usuarios.
   b. En la ventana que se abre, seleccione el método para agregar usuarios: **Agregar un usuario/grupo de usuarios manualmente**.
   c. Especifique un nombre de usuario y una contraseña.
   d. En la lista **Permisos**, configure los permisos de acceso de los usuarios a la funcionalidad de la aplicación.
9. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados.

Esta contraseña no se puede recuperar. Si pierde su contraseña, pierde completamente el control de la aplicación. Además, no podrá eliminar la aplicación del dispositivo protegido.

Puede reiniciar la contraseña en cualquier momento. Para hacerlo, anule la selección de la casilla **Permitir la confirmación de acciones con la aplicación usando credenciales de usuarios creados manualmente** y guarde los cambios. Se deshabilitará la protección con contraseña y se eliminará la suma de control de la contraseña anterior. Repita el proceso de creación de contraseña con una contraseña nueva.

Notificaciones de Secure Desktop

Kaspersky Embedded Systems Security es compatible con la funcionalidad (Secure Desktop). El propósito de esta funcionalidad es confirmar las acciones que potencialmente pueden reducir el nivel de seguridad del equipo. Esta funcionalidad permite que una aplicación muestre un cuadro de diálogo de confirmación aislado de otros procesos. Esta funcionalidad utiliza derechos de alto nivel para proteger la solicitud. De esta forma, solo el usuario puede confirmar la acción y no el malware.

Kaspersky Embedded Systems Security muestra las notificaciones de Secure Desktop para confirmar las siguientes acciones:

- Habilitación o deshabilitación del seguimiento
- Exportación o importación de la configuración de la aplicación
- Protección suspendida
- Aplicación cerrada
- Clave activa eliminada
- Desinstalación de Kaspersky Embedded Systems Security
- Deshabilitación de Control de dispositivos
- Deshabilitación de Protección de archivos en tiempo real
- Deshabilitación de la directiva de Kaspersky Security Center
- Informes visualizados
- Restauración de archivos desde Copia de seguridad
- Modificación de la configuración de Kaspersky Embedded Systems Security
- Administración de tareas de la aplicación de otra forma que no sea al inicio

Cómo habilitar o deshabilitar las notificaciones de Secure Desktop en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de las propiedades de la directiva, vaya a la sección **Configuración de la aplicación**.
4. En el bloque **Seguridad y confiabilidad**, haga clic en el botón **Configuración**.
5. En la ventana que se abre, seleccione la pestaña **Seguridad**.

6. En el bloque **Autoprotección**, seleccione o anule la selección de la casilla **Habilitar las notificaciones de Secure Desktop** para habilitar o deshabilitar las notificaciones de Secure Desktop.

   Si los mecanismos de Autodefensa están deshabilitados, la casilla **Habilitar las notificaciones de Secure Desktop** no estará disponible.

7. Cierre el candado para aplicar la directiva en los equipos.

8. Haga clic en **Aceptar** para guardar los cambios.

Cómo habilitar o deshabilitar las notificaciones de Secure Desktop en la Consola de la aplicación

1. En el árbol de la Consola de aplicaciones, seleccione el nodo **Kaspersky Embedded Systems Security** y, en el panel de resultados, haga clic en el vínculo **Propiedades de la aplicación**.

2. En la ventana que se abre, seleccione la pestaña **Configuración de seguridad**.

3. En el bloque **Autoprotección**, seleccione o anule la selección de la casilla **Habilitar las notificaciones de Secure Desktop** para habilitar o deshabilitar las notificaciones de Secure Desktop.

   Si los mecanismos de Autodefensa están deshabilitados, la casilla **Habilitar las notificaciones de Secure Desktop** no estará disponible.

4. Haga clic en **Aceptar** para guardar los cambios.

Cómo habilitar o deshabilitar las notificaciones de Secure Desktop en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.

2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la ficha **Configuración de la aplicación**.

4. Seleccione la sección **Configuración de la aplicación**.

5. En el bloque **Seguridad y confiabilidad**, haga clic en el botón **Configurar**.

   Se abre la ventana **Seguridad y confiabilidad**.

6. En el bloque **Autoprotección**, seleccione o anule la selección de la casilla **Habilitar las notificaciones de Secure Desktop** para habilitar o deshabilitar las notificaciones de Secure Desktop.

   Si los mecanismos de Autodefensa están deshabilitados, la casilla **Habilitar las notificaciones de Secure Desktop** no estará disponible.

7. Cierre el candado para aplicar la directiva en los equipos.

8. Haga clic en **Aceptar** para guardar los cambios.

Zona de confianza

Una *zona de confianza* es una lista de objetos y aplicaciones configurados por el administrador del sistema que Kaspersky Embedded Systems Security no supervisa cuando está activo.

El administrador crea la zona de confianza independientemente, teniendo en cuenta las características de los objetos manejados y las aplicaciones instaladas en el equipo. Puede ser necesario incluir objetos y aplicaciones en la zona de confianza cuando Kaspersky Embedded Systems Security bloquea el acceso a un objeto o una aplicación determinados, si está seguro de que dicho objeto o aplicación no suponen peligro alguno. Un administrador también puede permitir que un usuario cree su propia zona de confianza local para un equipo específico. De esta forma, los usuarios pueden crear sus propias listas locales de exclusiones y aplicaciones de confianza además de la zona de confianza general en una directiva.

También puede agregar telemetría EDR a la zona de confianza. Esto permite optimizar los datos que la aplicación envía al servidor de telemetría para la solución Kaspersky Anti Targeted Attack Platform (EDR).

Las exclusiones de análisis y aplicaciones de confianza predefinidas se agregaron a la zona de confianza. Las exclusiones de análisis y las aplicaciones de confianza predefinidas ayudan a configurar rápidamente Kaspersky Embedded Systems Security sin crear manualmente una zona de confianza.

Cómo crear una exclusión de análisis

Una *exclusión de análisis* es un conjunto de condiciones que deben cumplirse para que Kaspersky Embedded Systems Security no analice un objeto en particular en busca de virus y otras amenazas.

Los siguientes componentes y tareas de la aplicación pueden utilizar las exclusiones de análisis:

- **Protección de archivos en tiempo real**
- **Análisis a pedido**
- **Detección de comportamiento**
- **Protección vía AMSI**
- **Protección contra amenazas de red**

Kaspersky Embedded Systems Security no analiza un objeto si la unidad o la carpeta que lo contiene está incluida en el alcance del análisis al inicio de una de las tareas de análisis. Sin embargo, la exclusión de análisis no se aplica cuando se inicia una tarea de análisis personalizado para este objeto en particular.

Kaspersky Embedded Systems Security no admite listas de exclusión que contengan más de 5000 objetos.

Cómo crear una exclusión de análisis en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Adicional** → **Zona de confianza** y haga clic en **Configuración**.
4. Seleccione la ficha **Exclusiones de análisis**.
5. Seleccione la casilla **Combinar valores al heredar** si desea crear una lista de exclusiones unificada para todos los equipos de la empresa. La lista de exclusiones de la directiva principal se combinará con las listas de las directivas secundarias. Para que esto ocurra, debe haber habilitado la opción para que los valores se hereden y se combinen. Las exclusiones de la directiva principal aparecerán en las directivas secundarias, pero solo podrá verlas. No podrá modificarlas ni eliminarlas.
6. Seleccione la casilla **Permitir el uso de exclusiones locales** si desea permitir que el usuario cree una lista local de exclusiones. De esta manera, un usuario puede crear su propia lista local de exclusiones además de la lista general de exclusiones generada en la directiva. Un administrador puede usar Kaspersky Security Center para ver, agregar, editar o eliminar elementos de la lista en las propiedades del equipo.

   Si la casilla no está seleccionada, el usuario puede acceder solo a la lista general de exclusiones generada en la directiva. Además, si esta casilla está desactivada, Kaspersky Embedded Systems Security oculta la lista consolidada de exclusiones de análisis en la Consola de la aplicación.
7. Haga clic en **Agregar** y seleccione una acción:

   - **Categoría**. Puede agrupar las exclusiones del análisis en categorías separadas. Para crear una nueva categoría, escriba el nombre de la categoría y agregue al menos una exclusión de análisis a la categoría.
   - **Nueva exclusión**. Kaspersky Embedded Systems Security agrega una nueva exclusión de análisis a la raíz de la lista.
   - **Nueva exclusión en la categoría seleccionada**. Para agregar una nueva exclusión de análisis a una categoría específica, seleccione una categoría.
   - **Seleccionar exclusión de la lista**. Para configurar rápidamente Kaspersky Embedded Systems Security, puede agregar exclusiones de la lista de exclusiones de análisis predefinidas.
8. Para excluir un archivo o una carpeta del análisis, seleccione la casilla **Archivo o carpeta**. Haga clic en el vínculo **seleccionar archivo o carpeta** para abrir una ventana y, en esa ventana, seleccione un archivo o una carpeta haciendo clic en **Examinar**.

También puede escribir la ruta manualmente. Kaspersky Embedded Systems Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara:

- El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco C:, pero no en las subcarpetas.

- Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT ubicados en carpetas dentro de la `Folder`, excepto la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.

- El carácter `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las carpetas. Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.

  Puede usar máscaras al principio, en el medio o al final de la ruta del archivo. Por ejemplo, si desea agregar una carpeta a las exclusiones para todos los usuarios, escriba la máscara `?:\Users\*\Folder\`.

9. Para excluir un área predefinida del análisis, seleccione la casilla **Alcance predefinido**. Haga clic en el vínculo **Seleccionar alcance predefinido** para abrir una ventana y, en esa ventana, seleccione uno de los alcances estándar en el dispositivo protegido.

10. Para excluir objetos específicos del análisis, seleccione la casilla **Tipo del objeto detectado**. Haga clic en el vínculo **Ingresar nombres de objetos**, haga clic en el botón **Agregar** y, en la ventana que se muestra, escriba el nombre del tipo de objeto según la clasificación de la Enciclopedia de Kaspersky (por ejemplo, `Email-Worm`, `Rootkit` o `RemoteAdmin`).

    Puede usar máscaras con el carácter `?` (reemplaza cualquier carácter individual) y el carácter `*` (reemplaza cualquier número de caracteres). Por ejemplo, si se especifica la máscara `Client*`, Kaspersky Embedded Systems Security excluye los objetos `Client-IRC`, `Client-P2P` y `Client-SMTP` de los análisis.

11. Para excluir un archivo individual del análisis, seleccione la casilla **Hash del objeto**. Haga clic en el vínculo **Ingresar hash del objeto** para abrir una ventana y, en esa ventana, ingrese un hash del objeto.

    Si se modifica el archivo, también se modificará el hash del archivo. Si esto sucede, el archivo modificado no se agregará a las exclusiones.

12. En el bloque **Alcance de aplicación de la regla**, seleccione los componentes a los que desea que se aplique la exclusión de análisis.

13. Si es necesario, en el campo **Comentario**, ingrese una breve descripción de la exclusión de análisis que esté creando.

14. Guarde los cambios para agregar la exclusión a la lista. Puede deshabilitar la exclusión en cualquier momento utilizando la casilla de verificación que se encuentra junto al objeto.

Cómo crear una exclusión de análisis en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Adicional** → **Zona de confianza** y haga clic en el botón **Configurar**.
5. Seleccione la ficha **Exclusiones de análisis**.
6. Seleccione la casilla **Combinar valores al heredar** si desea crear una lista de exclusiones unificada para todos los equipos de la empresa. La lista de exclusiones de la directiva principal se combinará con las listas de las directivas secundarias. Para que esto ocurra, debe haber habilitado la opción para que los valores se hereden y se combinen. Las exclusiones de la directiva principal aparecerán en las directivas secundarias, pero solo podrá verlas. No podrá modificarlas ni eliminarlas.
7. Seleccione la casilla **Permitir el uso de exclusiones locales** si desea permitir que el usuario cree una lista local de exclusiones. De esta manera, un usuario puede crear su propia lista local de exclusiones además de la lista general de exclusiones generada en la directiva. Un administrador puede usar Kaspersky Security Center para ver, agregar, editar o eliminar elementos de la lista en las propiedades del equipo.

   Si la casilla no está seleccionada, el usuario puede acceder solo a la lista general de exclusiones generada en la directiva. Además, si esta casilla está desactivada, Kaspersky Embedded Systems Security oculta la lista consolidada de exclusiones de análisis en la Consola de la aplicación.
8. Haga clic en **Agregar** y seleccione una acción:

   - **Categoría**. Puede agrupar las exclusiones del análisis en categorías separadas. Para crear una nueva categoría, escriba el nombre de la categoría y agregue al menos una exclusión de análisis a la categoría.
   - **Nueva exclusión**. Kaspersky Embedded Systems Security agrega una nueva exclusión de análisis a la raíz de la lista.
   - **Seleccionar exclusión de la lista**. Para configurar rápidamente Kaspersky Embedded Systems Security, puede agregar exclusiones de la lista de exclusiones de análisis predefinidas.
9. Si desea excluir un archivo o una carpeta del análisis, seleccione **Archivo o carpeta** y seleccione la casilla en el campo que tiene el mismo nombre. Especifique la ruta al archivo o a la carpeta.

Kaspersky Embedded Systems Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara:

- El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco C:, pero no en las subcarpetas.

- Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT ubicados en carpetas dentro de la `Folder`, excepto la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.

- El carácter `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las carpetas. Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.

  Puede usar máscaras al principio, en el medio o al final de la ruta del archivo. Por ejemplo, si desea agregar una carpeta a las exclusiones para todos los usuarios, escriba la máscara `?:\Users\*\Folder\`.

10. Para excluir un alcance predefinido del análisis, seleccione **Predefined scope**. En la lista desplegable, seleccione uno de los alcances estándar en el dispositivo protegido.

11. Si desea excluir determinados objetos del análisis, seleccione la casilla **Tipo del objeto detectado** y escriba el nombre del tipo de objeto según la clasificación de la Enciclopedia de Kaspersky (por ejemplo, `Email-Worm`, `Rootkit`, o `RemoteAdmin`).

    Puede usar máscaras con el carácter `?` (reemplaza cualquier carácter individual) y el carácter `*` (reemplaza cualquier número de caracteres). Por ejemplo, si se especifica la máscara `Client*`, Kaspersky Embedded Systems Security excluye los objetos *Client-IRC*, *Client-P2P* y *Client-SMTP* de los análisis.

12. Para excluir un archivo individual del análisis, seleccione la casilla **Hash del objeto** y agregue un hash de un archivo o una lista de eventos.

    Si se modifica el archivo, también se modificará el hash del archivo. Si esto sucede, el archivo modificado no se agregará a las exclusiones.

13. Si es necesario, en el campo **Comentario**, ingrese una breve descripción de la exclusión de análisis que esté creando.

14. En el bloque **Componentes de protección**, seleccione los componentes a los que desea que se aplique la exclusión de análisis.

15. La nueva exclusión se agregará a la lista. Puede deshabilitar la exclusión en cualquier momento utilizando la casilla de verificación de la columna **Estado**.

16. Guarde los cambios.

Cómo crear una exclusión de análisis en la Consola de la aplicación

1. En el árbol de la Consola de la aplicación, seleccione el nodo **Kaspersky Embedded Systems Security** y seleccione **Zona de confianza** del menú contextual del nodo.

   Se abre la ventana **Configurar Zona de confianza**.

2. En la sección **Exclusiones**, haga clic en el botón **Configuración** junto al bloque **Exclusiones de análisis**.

3. Haga clic en **Agregar** y seleccione una acción:

   - **Categoría**. Puede agrupar las exclusiones del análisis en categorías separadas. Para crear una nueva categoría, escriba el nombre de la categoría y agregue al menos una exclusión de análisis a la categoría.
   - **Nueva exclusión**. Kaspersky Embedded Systems Security agrega una nueva exclusión de análisis a la raíz de la lista.
   - **Nueva exclusión en la categoría seleccionada**. Para agregar una nueva exclusión de análisis a una categoría específica, seleccione una categoría.
   - **Seleccionar exclusión de la lista**. Para configurar rápidamente Kaspersky Embedded Systems Security, puede agregar exclusiones de la lista de exclusiones de análisis predefinidas.

4. Para excluir un archivo o una carpeta del análisis, seleccione la casilla **Archivo o carpeta**. Haga clic en el vínculo **Seleccione el archivo o la carpeta** para abrir una ventana y, en esa ventana, seleccione un archivo o una carpeta haciendo clic en **Examinar**.

   También puede escribir la ruta manualmente. Kaspersky Embedded Systems Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara:

   - El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco C:, pero no en las subcarpetas.
   - Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT ubicados en carpetas dentro de la `Folder`, excepto la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.
   - El carácter `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las carpetas. Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.

     Puede usar máscaras al principio, en el medio o al final de la ruta del archivo. Por ejemplo, si desea agregar una carpeta a las exclusiones para todos los usuarios, escriba la máscara `?:\Users\*\Folder\`.

5. Para excluir un área predefinida del análisis, seleccione la casilla **Alcance predefinido**. Haga clic en el vínculo **Seleccionar alcance predefinido** para abrir una ventana y, en esa ventana, seleccione uno de los alcances estándar en el dispositivo protegido.

6. Para excluir objetos específicos del análisis, seleccione la casilla **Tipo del objeto detectado**. Haga clic en el vínculo **Ingresar nombres de objetos**, haga clic en el botón **Agregar** y, en la ventana que se muestra, escriba el nombre del tipo de objeto según la clasificación de la Enciclopedia de Kaspersky (por ejemplo, `Email-Worm`, `Rootkit` o `RemoteAdmin`).

   Puede usar máscaras con el carácter `?` (reemplaza cualquier carácter individual) y el carácter `*` (reemplaza cualquier número de caracteres). Por ejemplo, si se especifica la máscara `Client*`, Kaspersky Embedded Systems Security excluye los objetos `Client-IRC`, `Client-P2P` y `Client-SMTP` de los análisis.

7. Para excluir un archivo individual del análisis, seleccione la casilla **Hash del objeto**. Haga clic en el vínculo **Ingresar hash del objeto** para abrir una ventana y, en esa ventana, ingrese un hash del objeto.

   Si se modifica el archivo, también se modificará el hash del archivo. Si esto sucede, el archivo modificado no se agregará a las exclusiones.

8. En el bloque **Alcance de aplicación de la regla**, seleccione los componentes a los que desea que se aplique la exclusión de análisis.

9. Si es necesario, en el campo **Comentario**, ingrese una breve descripción de la exclusión de análisis que esté creando.

10. Guarde los cambios para agregar la exclusión a la lista. Puede deshabilitar la exclusión en cualquier momento utilizando la casilla de verificación que se encuentra junto al objeto.

Ejemplos de máscara de ruta:
Rutas a los archivos de cualquier carpeta:

- Si utiliza la máscara `*.exe`, se excluirán del análisis las rutas a todos los archivos de extensión EXE.
- La máscara `example*` comprende las rutas a todos los archivos de nombre EXAMPLE.

Rutas a los archivos de una carpeta específica:

- La máscara `C:\dir\*.*` comprende las rutas a los archivos almacenados en la carpeta C:\dir\, pero no a los almacenados en las subcarpetas de C:\dir\.
- La máscara `C:\dir\*` comprende las rutas a todos los archivos de la carpeta C:\dir\, incluidas las subcarpetas.
- La máscara `C:\dir\` comprende las rutas a todos los archivos de la carpeta C:\dir\, incluidas las subcarpetas.
- La máscara `C:\dir\*.exe` comprende las rutas a todos los archivos de extensión EXE almacenados en C:\dir\, pero no a los de las subcarpetas de C:\dir\.
- La máscara `C:\dir\test` comprende las rutas a todos los archivos de nombre "prueba" almacenados en C:\dir\, pero no a los almacenados en las subcarpetas de C:\dir\.
- La máscara `C:\dir\*\test` comprende las rutas a todos los archivos de nombre "prueba" almacenados en C:\dir\ y en las subcarpetas de C:\dir\.
- La máscara `C:\dir1\*\dir3\` incluirá todas las rutas a los archivos en las subcarpetas dir3, un nivel menos en la carpeta C:\dir1\.
- La máscara `C:\dir1\**\dirN\` incluirá todas las rutas a los archivos en las subcarpetas dirN, en cualquier nivel en la carpeta C:\dir1\.

Rutas a los archivos de cualquier carpeta que tenga un nombre específico:

- La máscara `dir\*.*` comprende las rutas a todos los archivos almacenados en carpetas de nombre "dir", pero no a los que se encuentran en subcarpetas de esas carpetas.
- La máscara `dir\*` comprende las rutas a todos los archivos almacenados en carpetas de nombre "dir", pero no a los que se encuentran en subcarpetas de esas carpetas.
- La máscara `dir\` comprende las rutas a todos los archivos almacenados en carpetas de nombre "dir", pero no a los que se encuentran en subcarpetas de esas carpetas.
- La máscara `dir\*.exe` comprende las rutas a todos los archivos de extensión EXE almacenados en carpetas de nombre "dir", pero no a los que se encuentran en subcarpetas de esas carpetas.
- La máscara `dir\test` comprende las rutas a todos los archivos de nombre "prueba" almacenados en carpetas de nombre "dir", pero no a los almacenados en subcarpetas de esas carpetas.

Selección de tipos de objetos detectables

Para seleccionar los tipos de objetos detectables:

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 **Configurar Zona de confianza** en el panel de resultados del nodo.
   - Seleccione **Zona de confianza** en el menú contextual del nodo.

   Se abre la ventana **Configurar Zona de confianza**.
2. En la sección **Tipos de objetos detectados**, haga clic en **Configuración**.

3. En la ventana que se abre, seleccione las casillas ubicadas junto a los tipos de objetos que desea que Kaspersky Embedded Systems Security detecte:

   - **Virus y gusanos**.

     Subcategoría: virus y gusanos (Viruses_and_Worms)

     Nivel de peligrosidad: alto

     Los virus y gusanos tradicionales realizan acciones no autorizadas por el usuario. Pueden crear copias de sí mismos capaces de replicarse.

     Virus habitual

     Cuando un virus tradicional ingresa a un equipo, lo que hace es infectar un archivo, activarse, realizar acciones malintencionadas y agregar copias de sí mismo a otros archivos.

     Los virus tradicionales solo se multiplican en los recursos locales del equipo; no pueden penetrar otros equipos por sí mismos. Solo pueden pasar a otro equipo si agregan una copia de sí mismos a un archivo almacenado en una carpeta compartida o en un CD dentro del equipo, o si el usuario reenvía un mensaje de correo con un archivo adjunto infectado.

     El código de los virus tradicionales puede penetrar diversas áreas de los equipos, los sistemas operativos y las aplicaciones. Según el entorno, los virus se dividen en *virus de archivos*, *virus de arranque*, *virus de scripts* y *virus de macros*.

     Los virus pueden infectar archivos mediante una variedad de técnicas. *Los virus de sobreescritura* escriben su código sobre el código del archivo infectado y borran el contenido de este. El archivo infectado deja de funcionar y no se puede restaurar. *Los virus parasitarios* modifican archivos y los dejan total o parcialmente funcionales. *Los virus de acompañamiento* no modifican archivos, sino que crean duplicados de ellos. Cuando se abre un archivo infectado, se inicia un duplicado de este (que, en realidad, es un virus). También se encuentran los siguientes tipos de virus: *virus de enlace*, *Virus OBJ*, *Virus LIB*, virus en el *código fuente* y muchos otros.

     Gusano

     Como ocurre con los virus tradicionales, el código de los gusanos está diseñado para infiltrarse en un equipo, activarse y realizar acciones maliciosas. Los gusanos reciben este nombre debido a su capacidad para "arrastrarse" de un equipo a otro y propagar copias de sí mismos sin el permiso del usuario mediante numerosos canales de datos.

     La principal función que permite diferenciar los distintos tipos de gusanos es la forma de propagarse. La siguiente tabla proporciona un resumen de distintos tipos de gusanos, clasificados según la forma en que se propagan.

Formas de propagación

Tipo	Name	Descripción
Email-Worm	Email-Worm	Se propagan mediante el correo electrónico. Un mensaje de correo infectado contiene un documento adjunto con una copia de un gusano o un vínculo a un archivo cargado en un sitio web que puede haber sufrido un ataque o haber sido creado exclusivamente con ese fin. Cuando se abre el documento adjunto, se activa el gusano. Cuando se hace clic en el vínculo, se descarga y se abre el archivo, y el gusano empieza a realizar acciones malintencionadas. Después de esto, empieza a distribuir copias de sí mismo. Para ello, busca otras direcciones de correo y les envía mensajes infectados.
IM-Worm	Gusanos de cliente de MI	Se propagan a través de clientes de MI. Por lo general, estos gusanos envían mensajes que incluyen un vínculo a un archivo con una copia del gusano ubicado en un sitio web y utilizan las listas de contactos del usuario. Cuando el usuario descarga el archivo y lo abre, se activa el gusano.
IRC-Worm	Gusanos de chat de Internet	Se propagan mediante Internet Relay Chats, sistemas de servicio que permiten comunicarse con otras personas a través de Internet en tiempo real. Estos gusanos publican un archivo con una copia de sí mismos o un vínculo al archivo en un chat de Internet. Cuando el usuario descarga el archivo y lo abre, se activa el gusano.
Net-Worm	Gusanos de red	Estos gusanos se propagan a través de redes de equipos. A diferencia de otros tipos de gusanos, un gusano de red típico se propaga sin la participación del usuario. Analiza la red local en busca de equipos que contengan programas con vulnerabilidades. Para ello, envía un paquete de red (punto vulnerable) especialmente formado que contiene el código del gusano o una parte de él. Si en la red hay algún equipo "vulnerable", recibe este paquete de red. El gusano se activa una vez que penetra completamente en el equipo.
P2P-Worm	Gusanos de redes de uso compartido de archivos	Se propagan mediante redes punto a punto de uso compartido de archivos. Para infiltrar una red P2P, el gusano se copia en una carpeta de uso compartido de archivos que, por lo general, está situada en el equipo del usuario. La red P2P muestra información sobre este archivo, de modo que el usuario pueda "encontrar" el archivo infectado en la red como a cualquier otro archivo, descargarlo y abrirlo. Gusanos más sofisticados emulan el protocolo de red de una red P2P específica: devuelven respuestas positivas a solicitudes de búsqueda y ofrecen copias de sí mismo para su descarga.
Gusano	Otros tipos de gusanos	Otros tipos de gusanos incluyen los siguientes: • Gusanos que distribuyen copias de sí mismos por los recursos de red. Al utilizar las funciones del sistema operativo, buscan carpetas disponibles de red, se conectan a equipos conectados a Internet e intentan obtener acceso total a sus unidades de disco. A diferencia de los tipos de gusanos descritos anteriormente, otras clases de gusanos no se activan por sí mismos, sino cuando el usuario abre un archivo que contiene una copia del gusano. • Gusanos que no utilizan ninguno de los métodos anteriores para propagarse (aquí se incluyen, por ejemplo, los que se propagan de un teléfono celular a otro).

- **Troyanos**.

Subcategoría: troyanos

Nivel de peligrosidad: alto

A diferencia de los gusanos y los virus, los troyanos no se autorreplican. Por ejemplo, penetran un equipo a través del correo o un navegador cuando el usuario visita una página web infectada. Los troyanos requieren la participación del usuario para iniciarse. Comienzan a realizar acciones malintencionadas inmediatamente después de iniciarse.

Los distintos troyanos se comportan de manera diferente en los equipos infectados. Las principales funciones de los troyanos consisten en bloquear, modificar o destruir información y en deshabilitar equipos o redes. Los troyanos también reciben o envían archivos, los ejecutan, muestran mensajes en pantalla, solicitan páginas web, descargan e instalan programas y reinician equipos.

Con frecuencia, los piratas usan "conjuntos" de varios troyanos.

Los tipos de comportamiento de los caballos de troya se describen en la siguiente tabla.

Tipos de comportamiento de caballos de troya en equipos infectados

Tipo	Name	Descripción
Trojan-ArcBomb	Troyanos: "bombas en archivos de almacenamiento"	Cuando se descomprimen, estos archivos de almacenamiento aumentan de tamaño en una medida tal que afecta el funcionamiento del equipo. Cuando el usuario intenta descomprimir un archivo de almacenamiento de esta clase, es posible que el equipo se ralentice o se bloquee, y el disco duro puede llenarse de datos "vacíos". Las "bombas en archivo de almacenamiento" son especialmente peligrosas para los servidores de correo y de archivos. Si el servidor utiliza un sistema automático para procesar la información entrante, una "bomba en archivo de almacenamiento" puede detener el servidor.
Backdoor	Troyanos de administración remota	Se considera que son los troyanos más peligrosos. Funcionan de manera bastante similar a las aplicaciones de administración remota instaladas en los equipos. Estos programas se instalan en el equipo sin que el usuario los detecte, lo que permite al intruso administrarlo de forma remota.
Troyano	Troyanos	En esta categoría se incluyen las siguientes aplicaciones maliciosas: • **Troyanos tradicionales**. Estos programas solo realizan las funciones principales de los troyanos: bloquear, modificar o destruir información y deshabilitar equipos o redes. A diferencia de los otros tipos de troyano descritos en la tabla, estos no tienen funciones avanzadas. • **Troyanos versátiles**. Estos programas tienen funciones avanzadas típicas de diversos tipos de troyanos.
Trojan-Ransom	Ransom troyanos	Toman la información del usuario como "rehén", modificándola o bloqueándola, o afectan el funcionamiento del equipo, de modo que el usuario pierde la capacidad de utilizar la información. El intruso le exige al usuario un rescate a cambio de una aplicación que permita restaurar la información y la operatividad del equipo.
Trojan-Clicker	Trojan-Clicker	Acceden a páginas web desde el equipo del usuario, ya sea mediante el envío de comandos a un navegador por su cuenta o por medio de la modificación de las direcciones web especificadas en los archivos del sistema operativo. Al utilizar estos programas, los intrusos realizan ataques de red e incrementan las visitas a sitios web, lo que aumenta la cantidad de anuncios publicitarios que se muestran.
Trojan-Downloader	Descargadores troyanos	Acceden a la página web del intruso para descargar de allí otra aplicación malintencionada e instalarla en el equipo del usuario. El nombre del archivo que se debe descargar puede venir establecido de antemano dentro del troyano o puede determinarse al acceder a la página del atacante.
Trojan-Dropper	Caballos de troya instaladores de software malintencionado	Contienen otros troyanos que descargan en el disco duro y luego instalan. Los intrusos pueden utilizar programas de este tipo para cumplir los siguientes objetivos: • Instalar una aplicación maliciosa sin que el usuario lo note: los troyanos de esta clase no muestran ningún mensaje o, si lo hacen, dan información falsa (por ejemplo, pueden advertir sobre la existencia de un archivo dañado o sobre incompatibilidades en el sistema operativo). • Impedir la detección de una aplicación malintencionada conocida. No todos los antivirus son capaces de detectar aplicaciones malintencionadas cuando vienen ocultas en troyanos de este tipo.
Trojan-Notifier	Caballos de troya notificadores	Le informan al atacante que puede introducirse en el sistema infectado y le envían información sobre el equipo: dirección IP, cantidad de puertos abiertos o dirección de correo electrónico. Se conectan con el intruso por medio del correo electrónico, FTP, ingreso a la página web del intruso o de otra manera. Los troyanos notificadores suelen utilizarse en conjuntos conformados por varios troyanos. Informan al intruso que se han instalado correctamente otros troyanos en el equipo del usuario.
Trojan-Proxy	Caballos de troya proxy	Permiten al intruso acceder de forma anónima a páginas web mediante el equipo del usuario. Con frecuencia, se utilizan para enviar correo no deseado.
Trojan-PSW	Programas que roban contraseñas	Los programas que roban contraseñas son una clase de caballo de troya que roba cuentas de usuarios, tales como datos de registro de software. Estos troyanos encuentran datos confidenciales en archivos del sistema y en el registro y se los envían al "atacante" mediante correo electrónico, FTP, acceso a la página web del intruso o de otro modo. Algunos de estos troyanos se categorizan en los distintos tipos descritos en esta tabla. Entre ellos se incluyen los que roban cuentas bancarias (Trojan-Banker), datos de usuarios de mensajería instantánea (Trojan-IM) e información de quienes juegan por Internet (Trojan-GameThief).

Tipo	Name	Descripción
Trojan-Spy	Caballos de troya espías	Espían al usuario y reúnen información acerca de las acciones que este realiza cuando trabaja en el equipo. Pueden interceptar los datos introducidos por el usuario mediante el teclado, realizar capturas de pantalla o compilar listas de aplicaciones activas. Después de recibir la información, se la transfieren al intruso mediante correo, FTP, acceso a la página web del intruso o de otro modo.
Trojan-DDoS	Caballos de troya atacantes de red	Envían numerosas solicitudes desde el equipo del usuario hasta un servidor remoto. El servidor carece de recursos para procesar todas las solicitudes, por lo que deja de funcionar (denegación de servicio, o simplemente DoS). Los piratas suelen infectar muchos equipos con estos programas de manera de utilizar los equipos para atacar a un único servidor simultáneamente. Los programas DoS llevan a cabo un ataque desde un único equipo con el conocimiento del usuario. Los programas DDoS (DoS distribuida) llevan a cabo ataques distribuidos desde distintos equipos sin que lo advierta el usuario del equipo infectado.
Trojan-IM	Troyanos que roban información de usuarios de clientes de mensajería instantánea	Roban los números de cuenta y contraseñas de quienes usan clientes de mensajería instantánea. Transfieren los datos al intruso mediante correo, FTP, acceso a la página web del intruso o de otro modo.
Rootkit	RootKits	Enmascaran la existencia y las acciones de otras aplicaciones malintencionadas para ayudarlas a perdurar en el sistema operativo. También pueden ocultar archivos, claves del registro que se utilicen para ejecutar aplicaciones malintencionadas o procesos que se encuentren cargados en la memoria del equipo infectado. Los rootkits pueden enmascarar el intercambio de datos entre aplicaciones en el equipo del usuario y en otros equipos de la red.
Trojan-SMS	Troyanos en la forma de mensajes SMS	Infectan teléfonos móviles y envían mensajes SMS a números de teléfono con tarifas elevadas.
Trojan-GameThief	Troyanos que roban información de usuarios de juegos en línea	Roban credenciales de las cuentas de usuarios de juegos en línea, tras lo cual envían los datos al intruso mediante correo, FTP, acceso a la página web del intruso o de otro modo.
Trojan-Banker	Troyanos que roban cuentas bancarias	Roban datos de cuentas bancarias o de sistemas de dinero electrónico y luego envían la información al hacker por correo electrónico, por FTP, a través de una página creada por el atacante o usando otros medios.
Trojan-Mailfinder	Troyanos que reúnen direcciones de correo	Recopilan direcciones de correo almacenadas en un equipo y se las envían al intruso mediante correo, FTP, acceso a la página web del intruso o de otro modo. Los intrusos pueden enviar correo no deseado a las direcciones que han recopilado.

- **Herramientas maliciosas**.

Subcategoría: herramientas maliciosas

Nivel de peligrosidad: medio

A diferencia de otros tipos de software malware, las herramientas maliciosas no realizan acciones inmediatamente después de iniciarse. Pueden almacenarse de manera segura e iniciarse en el equipo del usuario. A menudo, los intrusos utilizan las funciones de estos programas para crear virus, gusanos y troyanos, perpetrar ataques de red en servidores remotos, atacar equipos o llevar a cabo otras acciones malintencionadas.

Varias funciones de las herramientas maliciosas se agrupan en los tipos descritos en la siguiente tabla.

Funciones de herramientas maliciosas

Tipo	Name	Descripción
Constructor	Constructores	Permiten crear nuevos virus, gusanos y troyanos. Algunos constructores ofrecen una interfaz estándar, con ventanas para elegir el tipo de aplicación malintencionada que se va a crear, los métodos que se usarán para contrarrestar los depuradores y otras características.
DoS	Ataque de red	Envían numerosas solicitudes desde el equipo del usuario hasta un servidor remoto. El servidor carece de recursos para procesar todas las solicitudes, por lo que deja de funcionar (denegación de servicio, o simplemente DoS).
Exploit	Exploits	Los *puntos vulnerables* son conjuntos de datos o códigos de programas que se sirven de las vulnerabilidades de la aplicación en la que se procesa para realizar una acción maliciosa en un equipo. Por ejemplo, un punto vulnerable puede escribir o leer archivos o solicitar páginas web "infectadas". Distintos puntos vulnerables se sirven de las vulnerabilidades de diversos servicios de red o aplicaciones. Disfrazados como paquete de red, los puntos vulnerables se transfieren a través de la red a numerosos equipos y buscan equipos con servicios de red vulnerables. Un punto vulnerable en un archivo DOC se sirve de las vulnerabilidades de un editor de texto. Puede comenzar a realizar las acciones preprogramadas por el pirata cuando el usuario abre el archivo infectado. Un punto vulnerable incrustado en un mensaje de correo busca vulnerabilidades en cualquier cliente de correo. Puede empezar a realizar una acción malintencionada apenas el usuario abre el mensaje infectado en dicho cliente. Los gusanos de red se propagan por las redes mediante los puntos vulnerables. Los puntos vulnerables Nuker son paquetes de red que deshabilitan equipos.
FileCryptor	Cifradores	Se utilizan para cifrar otras aplicaciones malintencionadas y evitar, con ello, que las aplicaciones antivirus las detecten.
Flooder	Programas para "contaminar" redes	Envían numerosos mensajes a través de canales de red. Este tipo de herramienta incluye, por ejemplo, programas que contaminan Internet Relay Chats. Las herramientas de tipo "flooder" no incluyen programas que "contaminan" los canales usados por el correo, los clientes de mensajería instantánea y los sistemas de comunicaciones móviles. Estos programas se describen de manera individual en la tabla (flooder de correo, IM-Flooder y flooder de SMS).
HackTool	Herramientas de piratería	Permiten los ataques a los equipos en los que están instalados o atacan otro equipo (por ejemplo, mediante la adición de nuevas cuentas de sistema sin el permiso del usuario o la eliminación de registros del sistema para ocultar rastros de su presencia en el sistema operativo). Este tipo de herramienta incluye algunos analizadores de protocolos que ofrecen funciones malintencionadas, como la interceptación de contraseñas. Los analizadores de protocolos son programas que permiten ver el tráfico de red.
Hoax	Hoax	Alarman al usuario con mensajes similares a los de los virus: pueden "detectar un virus" en un archivo no infectado o notificar al usuario de que se dio formato a un disco, cuando esto no sucedió en realidad.
Spoofer	Herramientas de falsificación	Envían mensajes y solicitudes de red con una dirección falsa del remitente. Los intrusos utilizan herramientas de falsificación para hacerse pasar por los verdaderos remitentes de los mensajes, por ejemplo.
VirTool	Herramientas que pueden ingresar modificaciones en las aplicaciones malintencionadas	Permiten la modificación de otros programas de software malware y los ocultan de las aplicaciones antivirus.
Email-Flooder	Programas que "contaminan" las direcciones de correo	Envían numerosos mensajes a varias direcciones de correo electrónico y, de este modo, las contaminan. Un gran volumen de mensajes entrantes impide que los usuarios vean mensajes deseados en sus buzones.
IM-Flooder	Programas que "contaminan" el tráfico de los clientes de MI	"Inundan" a los usuarios de clientes de MI con mensajes. Un gran volumen de mensajes impide a los usuarios visualizar mensajes entrantes deseados.
SMS-Flooder	Programas que "contaminan" el tráfico con mensajes SMS	Envían numerosos mensajes de SMS a teléfonos móviles.

- **Adware**.

  Subcategoría: software de publicidad (Adware);

Nivel de peligrosidad: medio

El adware muestra información publicitaria al usuario. Los programas de adware muestran anuncios publicitarios en las interfaces de otros programas y redireccionan las solicitudes de búsqueda a páginas web publicitarias. Algunos reúnen información de marketing acerca del usuario y la envían a su desarrollador. Esta información puede incluir los nombres de los sitios web visitados por el usuario o el contenido de sus solicitudes de búsqueda. A diferencia de los caballos de troya espías, el adware envía esta información al desarrollador con el permiso del usuario.

- **Marcadores automáticos**.

  Subcategoría: marcadores automáticos (marcador).

  Nivel de peligrosidad: medio

  Los marcadores automáticos pueden establecer conexiones telefónicas de forma encubierta mediante un módem.

- **Software legítimo que los intrusos pueden usar para dañar su equipo o sus datos personales**.

  Subcategoría: software legal que los delincuentes pueden usar para dañar el equipo o sus datos personales

  Nivel de peligrosidad: medio

  La mayor parte de estas aplicaciones son útiles, por lo que muchos usuarios las ejecutan. Estas aplicaciones incluyen clientes IRC, marcadores automáticos, programas de descarga de archivos, supervisores de actividad del sistema del equipo, utilidades de contraseña y servidores de Internet para FTP, HTTP y Telnet.

  Sin embargo, si los intrusos obtienen acceso a estos programas, o si los plantan en el equipo del usuario, es posible que algunas de las funciones de la aplicación se utilicen para violar la seguridad.

  Estas aplicaciones tienen distintas funciones. En la tabla siguiente, se describen los distintos tipos.

Tipo	Name	Descripción
Client-IRC	Clientes de chat de Internet	Los usuarios instalan estos programas para hablar con gente en Internet Relay Chat. Los intrusos los utilizan para distribuir software malware.
Downloader	Programas para realizar descargas	Pueden descargar archivos de páginas web en modo oculto.
Monitor	Programas para supervisar	Permiten supervisar la actividad en el equipo en el que están instalados (ver qué aplicaciones están activas y cómo intercambian datos con aplicaciones instaladas en otros equipos).
PSWTool	Restauradores de contraseñas	Permiten visualizar y restaurar contraseñas olvidadas. Los intrusos los implantan en secreto en los equipos de los usuarios con el mismo propósito.
RemoteAdmin	Programas de administración remota	Su uso está muy extendido entre los administradores de sistemas. Estos programas permiten obtener acceso a la interfaz de un equipo remoto para supervisarlo y administrarlo. Los intrusos los implantan en secreto en los equipos de los usuarios con el mismo propósito: supervisar y administrar equipos remotos. Los programas legales de administración remota difieren de los troyanos de tipo Puerta trasera de administración remota. Los troyanos tienen la capacidad de penetrar en el sistema operativo por su cuenta e instalarse, mientras que los programas legales no pueden hacerlo.

Tipo	Name	Descripción
Server-FTP	Servidores FTP	Funcionan como servidores FTP. Los intrusos los implantan en el equipo del usuario para abrir un acceso remoto a él a través de FTP.
Server-Proxy	Servidores proxy	Funcionan como servidores proxy. Los intrusos los implantan en el equipo del usuario para enviar correo no deseado en nombre del usuario.
Server-Telnet	Servidores Telnet	Funcionan como servidores Telnet. Los intrusos los implantan en el equipo del usuario para abrir un acceso remoto a él a través de Telnet.
Server-Web	Servidores web	Funcionan como servidores web. Los intrusos los implantan en el equipo del usuario para abrir un acceso remoto a él a través de HTTP.
RiskTool	Herramientas para trabajar en un equipo local	Proporcionan al usuario opciones adicionales cuando trabajan en su propio equipo. Las herramientas permiten al usuario ocultar archivos o ventanas de aplicaciones activas y terminar procesos activos.
NetTool	Herramientas de red	Proporcionan al usuario opciones adicionales cuando trabajan con otros equipos de la red. Estas herramientas permiten reiniciarlos, detectar puertos abiertos y ejecutar aplicaciones instaladas en los equipos.
Client-P2P	Clientes de red P2P	Permiten trabajar en redes punto a punto. Pueden utilizarlos intrusos para distribuir software malware.
Client-SMTP	Clientes SMTP	Envían mensajes de correo electrónico sin el conocimiento del usuario. Los intrusos los implantan en el equipo del usuario para enviar correo no deseado en nombre del usuario.
WebToolbar	Barras de herramientas web	Agregan barras de herramientas a las interfaces de otras aplicaciones para usar motores de búsqueda.
FraudTool	Pseudoprogramas	Se hacen pasar por otros programas. Por ejemplo, existen pseudoprogramas antivirus que muestran mensajes acerca de la detección de software malware Sin embargo, en realidad no encuentran ni desinfectan nada.

- **Objetos comprimidos cuya compresión pueda usarse para proteger un código malicioso**.

  Subcategoría: archivos comprimidos que pueden causar daños.

  Nivel de peligrosidad: medio.

  El archivo se comprime con un compresor especial que se utiliza para comprimir malware: virus, gusanos, troyanos. Kaspersky Embedded Systems Security analiza el módulo descompresor dentro de los archivos de almacenamiento SFX (de autoextracción).

  Para ocultar el malware de la detección de un antivirus, los piratas informáticos lo comprimen con compresores especiales. Los expertos de Kaspersky identificaron los compresores más utilizados por los piratas informáticos.

- **Objetos comprimidos con más de un empaquetador**.

  Subcategoría: archivos de empaquetado múltiple.

  Nivel de peligrosidad: medio.

  El archivo se comprime con uno o más compresores tres o más veces.

  Para ocultar el malware de la detección de un antivirus, los piratas informáticos pueden comprimir un archivo varias veces. Kaspersky Embedded Systems Security analiza los archivos comprimidos.

4. Guarde los cambios.

Modificación de la lista de aplicaciones de confianza

La *lista de aplicaciones de confianza* es una lista de aplicaciones cuya actividad de archivos y de red (incluida la actividad maliciosa) y el acceso al registro del sistema no son supervisados por Kaspersky Embedded Systems Security. De manera predeterminada, Kaspersky Embedded Systems Security supervisa las acciones y el tráfico de red de todas las aplicaciones y analiza los objetos que abren, ejecutan o guardan los procesos asociados a las mismas. Una vez que se agrega una aplicación a la lista de aplicaciones de confianza, Kaspersky Embedded Systems Security deja de supervisar la actividad de la aplicación.

La diferencia entre las exclusiones de análisis y las aplicaciones de confianza es que, para las exclusiones, Kaspersky Embedded Systems Security no analiza los archivos, mientras que para las aplicaciones de confianza no controla los procesos iniciados. Si una aplicación de confianza crea un archivo malicioso en una carpeta que no está incluida en las exclusiones de análisis, Kaspersky Embedded Systems Security detectará el archivo y eliminará la amenaza. Si la carpeta se agrega a las exclusiones, Kaspersky Embedded Systems Security omitirá este archivo.

Por ejemplo, si considera que los objetos utilizados por la aplicación estándar Bloc de notas de Microsoft Windows son seguros, es decir, que confía en esta aplicación, puede agregar el Bloc de notas de Microsoft Windows a la lista de aplicaciones de confianza para no supervisar los objetos utilizados por esta aplicación. Esto aumentará el rendimiento del equipo, lo cual es especialmente importante cuando se usan aplicaciones de servidor.

Además, ciertas acciones clasificadas por Kaspersky Embedded Systems Security como sospechosas pueden ser seguras dentro del contexto de la funcionalidad de una cantidad de aplicaciones. Por ejemplo, la intercepción del texto escrito con el teclado es un proceso de rutina para los conmutadores de disposición del teclado automática (como Punto Switcher). Para tener en cuenta las características de estas aplicaciones y no supervisarlas, se recomienda agregarlas a la lista de aplicaciones de confianza.

Las aplicaciones de confianza ayudan a evitar problemas de compatibilidad entre Kaspersky Embedded Systems Security y otras aplicaciones (por ejemplo, el problema del análisis doble del tráfico de red de un equipo de terceros por parte de Kaspersky Embedded Systems Security y otra aplicación antivirus).

Al mismo tiempo, el archivo ejecutable y los procesos de la aplicación de confianza seguirán siendo analizados en busca de virus y otras clases de malware. Una aplicación se puede excluir completamente del análisis de Kaspersky Embedded Systems Security mediante Exclusiones de análisis.

Kaspersky Embedded Systems Security no admite listas de aplicaciones de confianza que contengan más de 5000 objetos.

Cómo agregar una aplicación a la lista de confianza en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Adicional**.
4. En el bloque **Zona de confianza**, haga clic en el botón **Configuración**.

5. En la ventana que se abre, seleccione la pestaña **Aplicaciones de confianza**.

   Esto abre una ventana que contiene una lista de las aplicaciones de confianza.

6. Seleccione la casilla de verificación **No analizar las operaciones de copia de seguridad de archivos** si desea omitir el análisis de operaciones de lectura de archivos si dichas operaciones son realizadas por las herramientas de copia de seguridad instaladas en el dispositivo protegido.

7. Active la casilla **Combinar valores al heredar** si desea crear una lista de aplicaciones de confianza unificada para todos los equipos de la empresa. La lista de aplicaciones de confianza de la directiva principal se combinará con las listas de las directivas secundarias. Para que esto ocurra, debe haber habilitado la opción para que los valores se hereden y se combinen. Las aplicaciones de confianza de la directiva principal aparecerán en las directivas secundarias, pero solo podrá verlas. No podrá modificarlas ni eliminarlas

8. Seleccione la casilla **Permitir la modificación de aplicaciones de confianza locales** si desea permitir que el usuario cree una lista local de aplicaciones de confianza. De esta manera, un usuario puede crear su propia lista local de aplicaciones de confianza además de la lista general de aplicaciones de confianza generada en la directiva. Un administrador puede usar Kaspersky Security Center para ver, agregar, editar o eliminar elementos de la lista en las propiedades del equipo.

   Si la casilla no está seleccionada, el usuario puede acceder solo a la lista general de aplicaciones de confianza generada en la directiva. Además, si esta casilla está desactivada, Kaspersky Embedded Systems Security oculta la lista consolidada de aplicaciones de confianza en la Consola de la aplicación.

9. Seleccione la casilla de verificación **No analizar la actividad de archivos de los procesos especificados** para omitir el análisis de operaciones sobre archivos para los procesos de confianza.

10. Haga clic en **Agregar** y seleccione una acción:

    - **Categoría**. Puede agrupar las aplicaciones de confianza en categorías separadas. Para crear una nueva categoría, ingrese el nombre de la categoría y agregue al menos una aplicación de confianza.
    - **Nueva exclusión**. Kaspersky Embedded Systems Security agrega la nueva aplicación de confianza a la raíz de la lista.
    - **Nueva exclusión en la categoría seleccionada**. Para agregar una nueva aplicación de confianza a una categoría específica, seleccione una categoría.
    - **Seleccionar exclusión de la lista**. Para configurar rápidamente Kaspersky Embedded Systems Security, puede agregar aplicaciones de la lista de aplicaciones de confianza predefinidas.

11. En la ventana que se abre, seleccione la casilla **Usar la ruta de acceso completa del proceso en el disco para determinar si el proceso es de confianza** e ingrese la ruta de acceso al archivo para determinar si el proceso es de confianza.

    Kaspersky Embedded Systems Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara:

    > Kaspersky Embedded Systems Security no admite la variable de entorno `%userprofile%` al generar una lista de aplicaciones de confianza en la consola de Kaspersky Security Center. Para aplicar la entrada a todas las cuentas de usuario, puede utilizar el carácter * (por ejemplo, `C:\Users\*\Documents\File.exe`). Siempre que se agregue una variable de entorno nueva, se deberá reiniciar la aplicación.

12. Defina la configuración avanzada para la aplicación de confianza (consulte la tabla a continuación).

13. Haga clic en **Aceptar**.

    La nueva aplicación de confianza se agregará a la lista. Puede excluir una aplicación de la zona de confianza en cualquier momento utilizando la casilla de verificación que se encuentra junto al objeto.

14. Guarde los cambios.

Cómo agregar una aplicación a la lista de confianza en Kaspersky Security Center Web Console

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.
4. Seleccione la ficha **Configuración de la aplicación**.
5. Vaya a **Adicional** → **Zona de confianza** y haga clic en el botón **Configurar**.
6. En la ventana que se abre, seleccione la pestaña **Aplicaciones de confianza**.
7. Seleccione la casilla de verificación **No analizar las operaciones de copia de seguridad de archivos** si desea omitir el análisis de operaciones de lectura de archivos si dichas operaciones son realizadas por las herramientas de copia de seguridad instaladas en el dispositivo protegido.
8. Active la casilla **Combinar valores al heredar** si desea crear una lista de aplicaciones de confianza unificada para todos los equipos de la empresa. La lista de aplicaciones de confianza de la directiva principal se combinará con las listas de las directivas secundarias. Para que esto ocurra, debe haber habilitado la opción para que los valores se hereden y se combinen. Las aplicaciones de confianza de la directiva principal aparecerán en las directivas secundarias, pero solo podrá verlas. No podrá modificarlas ni eliminarlas
9. Seleccione la casilla **Permitir la modificación de aplicaciones de confianza locales** si desea permitir que el usuario cree una lista local de aplicaciones de confianza. De esta manera, un usuario puede crear su propia lista local de aplicaciones de confianza además de la lista general de aplicaciones de confianza generada en la directiva. Un administrador puede usar Kaspersky Security Center para ver, agregar, editar o eliminar elementos de la lista en las propiedades del equipo.

   Si la casilla no está seleccionada, el usuario puede acceder solo a la lista general de aplicaciones de confianza generada en la directiva. Además, si esta casilla está desactivada, Kaspersky Embedded Systems Security oculta la lista consolidada de aplicaciones de confianza en la Consola de la aplicación.
10. Seleccione la casilla de verificación **No analizar la actividad de archivos de los procesos especificados** para omitir el análisis de operaciones sobre archivos para los procesos de confianza.
11. Haga clic en **Agregar** y seleccione una acción:

    - **Categoría**. Puede agrupar las aplicaciones de confianza en categorías separadas. Para crear una nueva categoría, ingrese el nombre de la categoría y agregue al menos una aplicación de confianza.
    - **Nueva exclusión**. Kaspersky Embedded Systems Security agrega la nueva aplicación de confianza a la raíz de la lista.

- **Nueva exclusión en la categoría seleccionada**. Para agregar una nueva aplicación de confianza a una categoría específica, seleccione una categoría.
- **Seleccionar exclusión de la lista**. Para configurar rápidamente Kaspersky Embedded Systems Security, puede agregar aplicaciones de la lista de aplicaciones de confianza predefinidas.

12. En la ventana que se abre, seleccione la casilla **Usar la ruta de acceso completa del proceso en el disco para determinar si el proceso es de confianza** e ingrese la ruta de acceso al archivo para determinar si el proceso es de confianza.

    Kaspersky Embedded Systems Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara:

    Kaspersky Embedded Systems Security no admite la variable de entorno `%userprofile%` al generar una lista de aplicaciones de confianza en la consola de Kaspersky Security Center. Para aplicar la entrada a todas las cuentas de usuario, puede utilizar el carácter * (por ejemplo, `C:\Users\*\Documents\File.exe`). Siempre que se agregue una variable de entorno nueva, se deberá reiniciar la aplicación.

13. Defina la configuración avanzada para la aplicación de confianza (consulte la tabla a continuación).
14. Haga clic en **OK**.

    La nueva aplicación de confianza se agregará a la lista. Puede excluir una aplicación de la zona de confianza en cualquier momento utilizando la casilla de verificación de la columna **Acción**.

15. Guarde los cambios.

Cómo agregar una aplicación a la lista de confianza en la Consola de la aplicación

1. En el árbol de la Consola de la aplicación, seleccione el nodo **Kaspersky Embedded Systems Security** y seleccione **Zona de confianza** del menú contextual del nodo.

   Se abre la ventana **Configurar Zona de confianza**.

2. En la sección **Exclusiones**, haga clic en el botón **Configuración** junto al bloque **Aplicaciones de confianza**.
3. Haga clic en **Agregar** y seleccione una acción:
   - **Categoría**. Puede agrupar las aplicaciones de confianza en categorías separadas. Para crear una nueva categoría, ingrese el nombre de la categoría y agregue al menos una aplicación de confianza.
   - **Nueva exclusión**. Kaspersky Embedded Systems Security agrega la nueva aplicación de confianza a la raíz de la lista.
   - **Nueva exclusión en la categoría seleccionada**. Para agregar una nueva aplicación de confianza a una categoría específica, seleccione una categoría.
   - **Seleccionar exclusión de la lista**. Para configurar rápidamente Kaspersky Embedded Systems Security, puede agregar aplicaciones de la lista de aplicaciones de confianza predefinidas.
4. Seleccione un archivo de la lista o ingrese la ruta al archivo ejecutable de la aplicación de confianza.

   Kaspersky Embedded Systems Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara:

Kaspersky Embedded Systems Security admite variables de entorno. Al mismo tiempo, Kaspersky Endpoint Security convierte la ruta en la interfaz local de la aplicación. Es decir, si ingresa la ruta de archivo `%userprofile%\Documents\File.exe`, se agregará un registro `C:\Users\Fred123\Documents\File.exe` en la interfaz local de la aplicación para el usuario Fernando123. De forma similar, Kaspersky Embedded Systems Security omite el programa de confianza `File.exe` para otros usuarios. Para aplicar la entrada a todas las cuentas de usuario, puede utilizar el carácter `*` (por ejemplo, `C:\Users\*\Documents\File.exe`).

Siempre que se agregue una variable de entorno nueva, se deberá reiniciar la aplicación.

5. Defina la configuración avanzada para la aplicación de confianza (consulte la tabla a continuación).
6. Haga clic en **Aceptar**.

   La nueva aplicación de confianza se agregará a la lista. Puede excluir una aplicación de la zona de confianza en cualquier momento utilizando la casilla de verificación que se encuentra junto al nombre del objeto.
7. Guarde los cambios.

Configuración de la aplicación de confianza

Parámetro	Descripción
Usar la ruta de acceso completa del proceso en el disco para determinar si el proceso es de confianza	Kaspersky Embedded Systems Security usa la ruta de acceso completa al archivo para determinar si el proceso es de confianza.
Usar hash de archivo de proceso para que se considere de confianza	Kaspersky Embedded Systems Security usa 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.
Permitir interacción con la interfaz de la aplicación	Kaspersky Embedded Systems Security bloquea todos los intentos de administrar servicios de aplicaciones desde un equipo remoto. Si se selecciona esta casilla, se permite que la aplicación de acceso remoto administre la configuración de Kaspersky Embedded Systems Security a través de la interfaz de Kaspersky Embedded Systems Security.
No supervisar la actividad de las aplicaciones secundarias	Kaspersky Embedded Systems Security no supervisará las actividades de red ni las operaciones de archivo que realicen las aplicaciones iniciadas por la aplicación. Puede aplicar la exclusión de manera recurrente. De esta manera, la aplicación no supervisa la actividad de toda la cadena de aplicaciones secundarias.
No heredar restricciones del proceso principal (aplicación)	Kaspersky Embedded Systems Security no aplicará las restricciones configuradas para el proceso principal a un proceso secundario. El proceso principal lo inicia una aplicación para la que se configuran los derechos de aplicaciones y las reglas de red de aplicaciones.
No analizar memoria del proceso	Kaspersky Embedded Systems Security no analiza la memoria del proceso.

Crear una zona de confianza local

El usuario ahora puede crear su propia zona de confianza local para un equipo específico. De esta forma, el usuario puede crear sus propias listas locales de exclusiones de análisis y aplicaciones de confianza además de la zona de confianza general en una directiva. Un administrador puede permitir o bloquear el uso de exclusiones locales o aplicaciones de confianza locales en la configuración de la directiva. Para ello, utilice las casillas de verificación **Permitir el uso de exclusiones locales** y **Permitir la modificación de aplicaciones de confianza locales** en las pestañas **Exclusiones de análisis** y **Aplicaciones de confianza** de la sección **Zona de confianza** de la directiva.

Si un administrador permite la creación de una zona de confianza local, el usuario puede agregar sus propias exclusiones de análisis y aplicaciones de confianza en la Consola de la aplicación. Al mismo tiempo, el usuario no tiene permisos para modificar o eliminar objetos de la zona de confianza configurada en la directiva. El administrador también puede ver, agregar, modificar o eliminar elementos de la lista en la consola de Kaspersky Security Center si es necesario agregar exclusiones para un equipo individual.

Kaspersky Embedded Systems Security oculta las listas de exclusiones de análisis y aplicaciones de confianza en la Consola de la aplicación si el administrador bloquea la configuración de la zona de confianza en la consola (símbolo de "candado cerrado") y las exclusiones de análisis y las aplicaciones de confianza locales están prohibidas.

Cómo agregar un objeto a la zona de confianza local en la Consola de administración de Kaspersky Security Center

1. En la carpeta **Dispositivos administrados** del árbol de la Consola de administración, abra la carpeta con el nombre del grupo de administración al cual pertenecen los equipos cliente en cuestión.
2. En el espacio de trabajo, seleccione la ficha **Dispositivos**.
3. Haga doble clic en un equipo para abrir su ventana de propiedades.
4. En la ventana de propiedades del equipo, elija la sección **Aplicaciones**.
5. En la lista de aplicaciones de Kaspersky instaladas en el equipo, seleccione **Kaspersky Embedded Systems Security** y haga doble clic para abrir las propiedades de la aplicación.
6. En la ventana de configuración de la aplicación, seleccione **Adicional** → **Zona de confianza** y haga clic en **Configuración**.
7. En la pestaña **Exclusiones de análisis**, haga una lista de exclusiones de análisis locales.

   Las reglas para crear exclusiones de análisis locales son las mismas que para las exclusiones generales. Kaspersky Embedded Systems Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara:
8. En la pestaña **Aplicaciones de confianza**, haga una lista de las aplicaciones de confianza locales. Esto abre una ventana que contiene una lista de las aplicaciones de confianza locales.

   Las reglas para agregar aplicaciones a la lista de aplicaciones de confianza locales son las mismas que las reglas para agregarlas a la lista general. Kaspersky Embedded Systems Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara:
9. Guarde los cambios.

Cómo agregar un objeto a la zona de confianza local en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Dispositivos administrados**.
2. Haga clic en el nombre del equipo donde quiere permitir que un usuario realice una acción bloqueada.
3. Seleccione la ficha **Aplicaciones**.

4. Haga clic en **Kaspersky Embedded Systems Security**.

   Se abre la configuración local de la aplicación.

5. Seleccione la ficha **Configuración de la aplicación**.

6. En la ventana de configuración de la aplicación, seleccione **Adicional** → **Zona de confianza** y haga clic en **Configurar**.

   Se abre la ventana **Exclusiones y tipos de objetos detectados**.

7. En la pestaña **Exclusiones de análisis**, haga una lista de exclusiones de análisis locales.

   Las reglas para crear exclusiones locales son las mismas que las reglas para crear exclusiones generales. Kaspersky Embedded Systems Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara:

8. En la pestaña **Aplicaciones de confianza**, haga una lista de las aplicaciones de confianza locales.

   Las reglas para agregar aplicaciones a la lista de aplicaciones de confianza locales son las mismas que las reglas para agregarlas a la lista general. Kaspersky Embedded Systems Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara:

9. Guarde los cambios.

Cómo crear una exclusión de análisis local en la Consola de la aplicación

1. En el árbol de la Consola de la aplicación, seleccione el nodo **Kaspersky Embedded Systems Security** y seleccione **Zona de confianza** del menú contextual del nodo.

   Se abre la ventana **Configurar Zona de confianza**.

2. En la sección **Exclusiones de análisis y aplicaciones de confianza**, haga clic en el botón **Configuración** junto al bloque **Exclusiones de análisis locales**.

   Kaspersky Embedded Systems Security oculta la lista de exclusiones de análisis en la Consola de la aplicación si el administrador bloquea la configuración de las exclusiones de análisis en la Consola de administración de Kaspersky Security Center (símbolo de "candado cerrado") y las exclusiones de análisis locales están prohibidas (la casilla **Permitir el uso de exclusiones locales** está desactivada).

3. Haga clic en **Agregar** y seleccione una acción:

   - **Categoría**. Puede agrupar las exclusiones del análisis en categorías separadas. Para crear una nueva categoría, escriba el nombre de la categoría y agregue al menos una exclusión de análisis a la categoría.
   - **Nueva exclusión**. Kaspersky Embedded Systems Security agrega una nueva exclusión de análisis a la raíz de la lista.
   - **Nueva exclusión en la categoría seleccionada**. Para agregar una nueva exclusión de análisis a una categoría específica, seleccione una categoría.
   - **Seleccionar exclusión de la lista**. Para configurar rápidamente Kaspersky Embedded Systems Security, puede agregar exclusiones de la lista de exclusiones de análisis predefinidas.

4. Si selecciona **Nueva exclusión**, se abre la ventana **Exclusión de análisis**.

5. Para excluir un archivo o una carpeta del análisis, seleccione la casilla **Archivo o carpeta**. Haga clic en el vínculo **Seleccione el archivo o la carpeta** para abrir una ventana y, en esa ventana, seleccione un archivo o una carpeta haciendo clic en **Examinar**.

   También puede escribir la ruta manualmente. Kaspersky Embedded Systems Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara:

   - El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco C:, pero no en las subcarpetas.

   - Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT ubicados en carpetas dentro de la `Folder`, excepto la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.

   - El carácter `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las carpetas. Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.

     Puede usar máscaras al principio, en el medio o al final de la ruta del archivo. Por ejemplo, si desea agregar una carpeta a las exclusiones para todos los usuarios, escriba la máscara `?:\Users\*\Folder\`.

6. Para excluir un área predefinida del análisis, seleccione la casilla **Alcance predefinido**. Haga clic en el vínculo **Seleccionar alcance predefinido** para abrir una ventana y, en esa ventana, seleccione uno de los alcances estándar en el dispositivo protegido.

7. Para excluir objetos específicos del análisis, seleccione la casilla **Tipo del objeto detectado**. Haga clic en el vínculo **Ingresar nombres de objetos**, haga clic en el botón **Agregar** y, en la ventana que se muestra, escriba el nombre del tipo de objeto según la clasificación de la Enciclopedia de Kaspersky (por ejemplo, `Email-Worm`, `Rootkit` o `RemoteAdmin`).

   Puede usar máscaras con el carácter `?` (reemplaza cualquier carácter individual) y el carácter `*` (reemplaza cualquier número de caracteres). Por ejemplo, si se especifica la máscara `Client*`, Kaspersky Embedded Systems Security excluye los objetos `Client-IRC`, `Client-P2P` y `Client-SMTP` de los análisis.

8. Para excluir un archivo individual del análisis, seleccione la casilla **Hash del objeto**. Haga clic en el vínculo **Ingresar hash del objeto** para abrir una ventana y, en esa ventana, ingrese un hash del objeto.

   Si se modifica el archivo, también se modificará el hash del archivo. Si esto sucede, el archivo modificado no se agregará a las exclusiones.

9. En el bloque **Alcance de aplicación de la regla**, seleccione los componentes a los que desea que se aplique la exclusión de análisis.

10. Si es necesario, en el campo **Comentario**, ingrese una breve descripción de la exclusión de análisis que esté creando.

11. Guarde los cambios para agregar la exclusión a la lista. Puede deshabilitar la exclusión en cualquier momento utilizando la casilla de verificación que se encuentra junto al objeto.

Cómo agregar una aplicación a la lista de aplicaciones de confianza locales en la interfaz de la Consola de la aplicación

1. En el árbol de la Consola de la aplicación, seleccione el nodo **Kaspersky Embedded Systems Security** y seleccione **Zona de confianza** del menú contextual del nodo.

   Se abre la ventana **Configurar Zona de confianza**.

2. En la sección **Exclusiones**, haga clic en el botón **Configuración** junto al bloque **Aplicaciones de confianza locales**.

   Kaspersky Embedded Systems Security oculta la lista consolidada de aplicaciones de confianza en la Consola de la aplicación si el administrador bloquea la configuración de las aplicaciones de confianza en la Consola de administración de Kaspersky Security Center (símbolo de "candado cerrado") y las aplicaciones de confianza locales están prohibidas (la casilla **Permitir la modificación de aplicaciones de confianza locales** está desactivada).

3. Haga clic en **Agregar** y seleccione una acción:

   - **Categoría**. Puede agrupar las aplicaciones de confianza en categorías separadas. Para crear una nueva categoría, ingrese el nombre de la categoría y agregue al menos una aplicación de confianza.
   - **Nueva exclusión**. Kaspersky Embedded Systems Security agrega la nueva aplicación de confianza a la raíz de la lista.
   - **Nueva exclusión en la categoría seleccionada**. Para agregar una nueva aplicación de confianza a una categoría específica, seleccione una categoría.
   - **Seleccionar exclusión de la lista**. Para configurar rápidamente Kaspersky Embedded Systems Security, puede agregar aplicaciones de la lista de aplicaciones de confianza predefinidas.

4. Si selecciona **Nueva exclusión**, se abre la ventana **Exclusión de análisis**.

5. Seleccione la casilla **Usar la ruta de acceso completa del proceso en el disco para determinar si el proceso es de confianza** e ingrese la ruta al archivo ejecutable de la aplicación de confianza.

   Kaspersky Embedded Systems Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara:

   Kaspersky Embedded Systems Security admite variables de entorno. Al mismo tiempo, Kaspersky Endpoint Security convierte la ruta en la interfaz local de la aplicación. Es decir, si ingresa la ruta de archivo `%userprofile%\Documents\File.exe`, se agregará un registro `C:\Users\Fred123\Documents\File.exe` en la interfaz local de la aplicación para el usuario Fernando123. De forma similar, Kaspersky Embedded Systems Security omite el programa de confianza `File.exe` para otros usuarios. Para aplicar la entrada a todas las cuentas de usuario, puede utilizar el carácter `*` (por ejemplo, `C:\Users\*\Documents\File.exe`).

   Siempre que se agregue una variable de entorno nueva, se deberá reiniciar la aplicación.

6. En la ventana de propiedades de la aplicación de confianza, defina la configuración avanzada.

7. Guarde los cambios para agregar la exclusión a la lista.

Exportar e importar la zona de confianza

Una *zona de confianza* es una lista de objetos y aplicaciones configurados por el administrador del sistema que Kaspersky Embedded Systems Security no supervisa cuando está activo. La zona de confianza consta de las siguientes listas: *exclusiones de análisis* y *aplicaciones de confianza*. A continuación, puede modificar el archivo para, por ejemplo, agregar una gran cantidad de exclusiones del mismo tipo. También puede usar la función de exportación/importación para realizar una copia de seguridad de la lista de exclusiones y de la lista de aplicaciones de confianza, o para migrar la lista a un servidor diferente.

La aplicación utiliza el formato XML para exportar e importar la *lista de exclusiones* y aplicaciones de confianza:

Kaspersky Embedded Systems Security no admite listas de exclusión ni listas de aplicaciones de confianza que contengan más de 5000 objetos.

Cómo exportar e importar la zona de confianza en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.

2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de la directiva, seleccione **Adicional** → **Zona de confianza** y haga clic en **Configuración**.

4. Para exportar la lista de reglas:

   a. Seleccione la ficha **Exclusiones de análisis**.

   b. Seleccione las exclusiones que desea exportar.

      Si no seleccionó ninguna exclusión, Kaspersky Embedded Systems Security exportará todas las exclusiones.

   c. Haga clic en el ícono de la carpeta y seleccione **Exportar** en la lista desplegable.

      En la ventana que se abre, escriba el nombre del archivo XML en el que se exportará la lista de exclusiones. Seleccione también la carpeta en la que se guardará este archivo.

   d. Guarde el archivo.

5. Para exportar la lista de aplicaciones de confianza:

   a. Seleccione la ficha **Aplicaciones de confianza**.

      Esto abre una ventana que contiene una lista de las aplicaciones de confianza.

b. Seleccione las aplicaciones de confianza que desea exportar.

Si no selecciona ninguna aplicación de confianza, Kaspersky Embedded Systems Security exporta todas las aplicaciones de confianza.

c. Haga clic en el ícono de la carpeta y seleccione **Exportar** en la lista desplegable.

d. En la ventana que se abre, ingrese el nombre del archivo XML en el que se exportará la lista de aplicaciones de confianza. Seleccione la carpeta en la que se guardará este archivo.

e. Guarde el archivo.

Kaspersky Embedded Systems Security exportará la lista al archivo XML.

6. Para importar la lista de exclusiones:

a. Seleccione la ficha **Exclusiones de análisis**.

Esto abre una ventana que contiene una lista de exclusiones.

b. Haga clic en el ícono de la carpeta y seleccione **Importar** en la lista desplegable.

c. En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de exclusiones.

d. Abra el archivo.

Cuando ya exista una lista de exclusiones en el equipo, Kaspersky Embedded Systems Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.

7. Para importar una lista de aplicaciones de confianza:

a. Seleccione la ficha **Aplicaciones de confianza**.

Esto abre una ventana que contiene una lista de las aplicaciones de confianza.

b. Haga clic en **Importar**.

c. En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de aplicaciones de confianza.

d. Abra el archivo.

Cuando ya exista una lista de aplicaciones de confianza en el equipo, Kaspersky Embedded Systems Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas nuevas del archivo XML.

8. Guarde los cambios.

Cómo exportar e importar la zona de confianza en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

Se abre la ventana de propiedades de la directiva.

3. Seleccione la ficha **Configuración de la aplicación**.

4. Vaya a **Adicional** → **Zona de confianza** y haga clic en el botón **Configurar**.

5. Para exportar la lista de reglas:

   a. En la pestaña **Exclusiones de análisis y aplicaciones de confianza**, seleccione las exclusiones que desea exportar.

   b. Haga clic en los tres puntos y seleccione **Exportar**.

   c. Confirme que desea exportar solo las exclusiones seleccionadas, o bien exporte la lista completa de exclusiones.

   Kaspersky Embedded Systems Security exportará la lista al archivo XML.

6. Para exportar la lista de aplicaciones de confianza:

   a. En la pestaña **Exclusiones de análisis y aplicaciones de confianza**, seleccione las aplicaciones que desea exportar.

   b. Haga clic en los tres puntos y seleccione **Exportar**.

   c. Confirme que desea exportar solo las aplicaciones seleccionadas, o bien exporte la lista completa.

   Kaspersky Embedded Systems Security exportará la lista al archivo XML.

7. Para importar la lista de exclusiones:

   a. En la pestaña **Exclusiones de análisis y aplicaciones de confianza**, haga clic en **Importar desde la versión anterior** si desea importar la lista de exclusiones desde un archivo XML creado en la versión 3.4 o una versión anterior de la aplicación.

   Si importará reglas desde un archivo XML creado en la versión 4.0 o una versión posterior, haga clic en **Importar**.

   b. Cuando ya exista una lista de exclusiones en el equipo, Kaspersky Embedded Systems Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.

   c. En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de exclusiones.

   d. Haga clic en **Importar**.

8. Para importar una lista de aplicaciones de confianza:

   a. En la pestaña **Exclusiones de análisis y aplicaciones de confianza**, haga clic en **Importar desde la versión anterior** si desea importar la lista de aplicaciones de confianza desde un archivo XML creado en la versión 3.4 o una versión anterior de la aplicación.

   Si importara aplicaciones de confianza desde un archivo XML creado en la versión 4.0 o una versión posterior, haga clic en **Importar**.

   b. Cuando ya exista una lista de aplicaciones de confianza en el equipo, Kaspersky Embedded Systems Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas nuevas del archivo XML.

c. En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de aplicaciones de confianza.

d. Haga clic en **Importar**.

9. Guarde los cambios.

Cómo exportar o importar la zona de confianza en la Consola de la aplicación

1. En el árbol de la Consola de la aplicación, seleccione el nodo **Kaspersky Embedded Systems Security** y seleccione **Zona de confianza** del menú contextual del nodo.

   Se abre la ventana **Configurar Zona de confianza**.

2. Para exportar la lista de exclusiones o aplicaciones de confianza:

   a. En la sección **Exclusiones**, haga clic en el botón **Configuración** junto al bloque **Exclusiones de análisis** o **Aplicaciones de confianza**.

   b. Seleccione las exclusiones o aplicaciones de confianza que desea exportar.

   c. Haga clic en el ícono de la carpeta y seleccione **Exportar**.

   d. En la ventana que se abre, ingrese el nombre del archivo XML en el que se exportará la lista de exclusiones o aplicaciones de confianza. Seleccione la carpeta en la que se guardará este archivo.

   e. Guarde el archivo.

   Kaspersky Embedded Systems Security exportará la lista al archivo XML.

3. Para importar una lista de exclusiones o aplicaciones de confianza:

   a. En la sección **Exclusiones**, haga clic en el botón **Configuración** junto al bloque **Exclusiones de análisis** o **Aplicaciones de confianza**.

   b. Seleccione las exclusiones o aplicaciones de confianza que desea importar.

   c. Haga clic en el ícono de la carpeta y seleccione **Exportar**.

   d. En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de exclusiones o aplicaciones de confianza.

   e. Abra el archivo.

   Cuando ya exista una lista de exclusiones en el equipo, Kaspersky Embedded Systems Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.

4. Guarde los cambios.

Uso de almacenamiento de certificados de sistema de confianza

Utilizar el almacenamiento de certificados de sistema le permite excluir aplicaciones firmadas con una firma digital de confianza del análisis antivirus. Kaspersky Embedded Systems Security asigna automáticamente dichas aplicaciones al grupo *De confianza*.

Para comenzar a utilizar el almacenamiento de certificados de sistema de confianza:

Cómo configurar el uso de un almacén de certificados del sistema de confianza en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Adicional** → **Zona de confianza** y haga clic en **Configuración**.
4. Seleccione la ficha **Almacén de confianza de certificados del sistema**.
5. Seleccione la casilla **Usar un almacén de confianza de certificados del sistema** y, en la lista desplegable, seccione el almacén del sistema que desea que Kaspersky Embedded Systems Security considere de confianza.
6. Guarde los cambios.

Cómo configurar el uso de un almacén de certificados del sistema de confianza en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Adicional** → **Zona de confianza** y haga clic en el botón **Configurar**.
5. Seleccione la ficha **Almacén de confianza de certificados del sistema**.
6. Seleccione la casilla **Usar un almacén de confianza de certificados del sistema** y, en la lista desplegable, seccione el almacén del sistema que desea que Kaspersky Embedded Systems Security considere de confianza.
7. Guarde los cambios.

Cómo configurar el uso de un almacén de certificados del sistema de confianza en la Consola de la aplicación

1. En el árbol de la Consola de la aplicación, seleccione el nodo **Kaspersky Embedded Systems Security** y seleccione **Zona de confianza** del menú contextual del nodo.

   Se abre la ventana **Configurar Zona de confianza**.

2. En **Almacén de confianza de certificados del sistema**, seccione la casilla **Usar un almacén de confianza de certificados del sistema** y, en la lista desplegable, el almacén del sistema que desea que Kaspersky Embedded Systems Security considere de confianza.

3. Guarde los cambios.

Protección de archivos en tiempo real

El componente Protección de archivos en tiempo real de Kaspersky Embedded Systems Security analiza los siguientes objetos del dispositivo protegido cuando se accede a ellos:

- Archivos
- Flujos NTFS de datos alternativos.
- Sectores de inicio y registros de inicio maestro en discos duros locales y dispositivos externos.
- Archivos de contenedor de Windows Server 2016 y Windows Server 2019.

Cuando una aplicación escribe o lee un archivo en el dispositivo protegido, Kaspersky Embedded Systems Security intercepta el archivo, lo analiza en busca de amenazas y, si detecta una amenaza, realiza una acción predeterminada o la acción que usted haya especificado (intenta desinfectar el archivo, lo pasa a Cuarentena o lo elimina). 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 intercepta las operaciones sobre archivos ejecutadas en contenedores de Windows Server 2016 y Windows Server 2019.

Un *contenedor* es un entorno aislado que permite a las aplicaciones ejecutarse sin interactuar directamente con el sistema operativo. Si el contenedor está ubicado en el alcance de la protección del componente Kaspersky Embedded Systems Security analiza los archivos del contenedor, a los que el usuario accede, en busca de amenazas. Cuando se detecta una amenaza, la aplicación intenta desinfectar el contenedor. Si la desinfección se realiza correctamente, el contenedor sigue funcionando. Si la desinfección falla, el contenedor se desactiva.

Kaspersky Embedded Systems Security también detecta malware para procesos que se ejecutan bajo el Subsistema de Windows para Linux®. Para tales procesos, el componente Protección de archivos en tiempo real aplica la acción definida por la configuración vigente.

Acerca del área de protección de la tarea y la configuración de seguridad

De forma predeterminada, el componente Protección de archivos en tiempo real protege a todos los objetos del sistema de archivos del dispositivo. 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 área de protección.

En la Consola de la aplicación, el área de la protección se muestra como lista de recursos de archivos del dispositivo que Kaspersky Embedded Systems Security puede supervisar.

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 área de la protección, o como configuraciones diferentes para cada nodo o elemento en la lista del recurso del archivo del dispositivo.

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 de protección seleccionada se puede realizar mediante uno de los métodos siguientes:

- Seleccionar uno de tres niveles de seguridad predefinidos.
- Configuración manual de las opciones de seguridad para los nodos o elementos seleccionados en la lista de recursos del archivo (el nivel de seguridad cambia a **Personalizada**).

Áreas de protección predefinidas

La lista de recursos de archivos muestra los nodos a los cuales tiene acceso de lectura según las opciones de seguridad configuradas 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 dispositivo.
- **Unidades extraíbles**. Kaspersky Embedded Systems Security protege archivos en dispositivos externos, por ejemplo, unidades extraíbles o CD. Todas las unidades extraíbles, discos, carpetas o archivos individuales pueden incluirse o excluirse del área de 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 dispositivo. Kaspersky Embedded Systems Security no protege archivos cuando aplicaciones de otros dispositivos protegidos acceden a ellos.

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 área de protección.

Las unidades de red conectadas tampoco se mostrarán en la lista de recursos de archivos del dispositivo protegido. Para incluir objetos de unidades de red en el área de la protección, especifique la ruta a la carpeta que corresponde a esta unidad de red en formato UNC (Universal Naming Convention).

Acerca de los 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 dispositivo protegido o la lista de recursos de archivo: **Máximo rendimiento**, **Recomendado**, **Máxima protección** e **Informar**. 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 su red tiene medidas de seguridad adicionales para los dispositivos protegidos, por ejemplo, firewalls y directivas de seguridad existentes, además de usar Kaspersky Embedded Systems Security en estaciones de trabajo y dispositivos protegidos.

Recomendado

El nivel de seguridad **Recomendado** garantiza la mejor combinación de protección e impacto en el rendimiento de los dispositivos protegidos. Los expertos de Kaspersky recomiendan este nivel porque es adecuado para proteger los dispositivos en la mayoría de las redes corporativas. 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 dispositivo.

Informar

Se recomienda el nivel de seguridad **Informar** si potencialmente hay varios equipos infectados en la red corporativa y bloquearlos podría interrumpir considerablemente el funcionamiento de la organización.

Niveles de seguridad predefinidos y valores de configuración correspondientes

Opciones	Nivel de seguridad			
Máximo rendimiento	**Recomendado**	**Máxima protección**	**Informar**	
Protección de objetos	Objetos analizados según la lista de extensiones de la base de datos antivirus	Objetos analizados según su formato	Objetos analizados según su formato	Objetos analizados según su formato
Analizar solo archivos nuevos y modificados	Habilitado	Habilitado	Deshabilitado	Habilitado
Análisis de archivos compuestos	Deshabilitado	Analizar archivos de Microsoft Office	Analizar archivos de Microsoft Office	Analizar archivos de Microsoft Office
Acción que se realizará con los objetos infectados y otros objetos	Bloquear acceso y desinfectar. Si falla la desinfección, eliminar	Bloquear el acceso y realizar la acción recomendada por los expertos de Kaspersky	Bloquear acceso y desinfectar. Si falla la desinfección, eliminar	Informar
Aplicar la acción a los tipos de objetos seleccionados	Deshabilitado	Deshabilitado	Deshabilitado	Deshabilitado
Si se detecta un objeto integrado, eliminar todo el archivo compuesto que la aplicación no pueda modificar	Deshabilitado	Deshabilitado	Habilitado	Deshabilitado
La denominación "objeto crítico del sistema" hace referencia a aquellos archivos que el sistema operativo y Kaspersky Embedded Systems Security requieren para funcionar. Estos archivos no se pueden eliminar. Los procesos asociados con dichos objetos no se pueden finalizar.				
Descomprimir en segundo plano archivos compuestos más grandes que (MB)				

Opciones	Nivel de seguridad			
Detener el análisis si demora más de (s)	60 segundos.	60 segundos.	60 segundos.	60 segundos.
Omitir objetos compuestos de más de (MB)	8 MB	8 MB	No definida	8 MB
Usar la tecnología iSwift	Habilitado	Habilitado	Habilitado	Habilitado
Usar la tecnología iChecker	Habilitado	Habilitado	Habilitado	Habilitado

Extensiones de archivo analizadas de manera predeterminada en el componente 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?.*

Configurar el componente Protección de archivos en tiempo real

De manera predeterminada, el componente Protección de archivos en tiempo real utiliza la configuración descrita en la siguiente tabla. Puede cambiar los valores de esta configuración.

Configuración predeterminada del componente Protección de archivos en tiempo real

Parámetro	Valor predeterminado	Descripción
Área de protección	El dispositivo protegido completo, excluidas las unidades virtuales.	Utilice esta opción para cambiar el área de protección.
Configuración de seguridad	La configuración común para toda el área de protección corresponde al nivel de seguridad **Recomendado**.	Para los nodos seleccionados en la lista o el árbol de recursos de archivos del dispositivo protegido, puede realizar lo siguiente: • Seleccionar un nivel de seguridad predefinido diferente • Cambiar manualmente la configuración de seguridad Puede guardar un grupo de opciones de seguridad para un nodo seleccionado como una plantilla y usarla más tarde en un nodo diferente.

Parámetro	Valor predeterminado	Descripción
Modo de protección de objetos	**Modo inteligente**.	Utilice esta opción para seleccionar el modo de protección, es decir, definir el tipo de intentos de acceso para los que Kaspersky Embedded Systems Security analiza 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.
Bloquear acceso a recursos compartidos en la red para las sesiones que muestran actividad maliciosa	No aplicado.	Utilice esta opción para bloquear la sesión actual y agregar la IP del host o el LUID del host hacia el cual se detectó actividad maliciosa en la sección Depósito de hosts bloqueados.
Iniciar análisis de áreas críticas al detectar infección activa	Aplicado.	Cuando se detecta una infección activa, Kaspersky Embedded Systems Security crea e inicia una tarea de Análisis de áreas críticas.
Detener el contenedor si la desinfección falla	Aplicado.	Es posible que la aplicación no tenga permisos de lectura y escritura para el objeto detectado. En este caso, no se puede desinfectar ni eliminar el objeto detectado. Si se selecciona esta casilla, la aplicación bloquea el objeto detectado y detiene el contenedor. Si no se selecciona esta casilla, la aplicación solo bloquea el objeto detectado.
No analizar las operaciones ejecutadas en contenedores de Windows	Aplicado.	Si se selecciona esta casilla, la aplicación analiza el contenedor solo cuando se inicia. Si no se selecciona la casilla, la aplicación analiza el contenedor continuamente en tiempo real.

Cómo habilitar el análisis antivirus de los archivos en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de propiedades de la directiva, seleccione **Protección del equipo en tiempo real**.
4. En la sección **Configuración de Protección de archivos en tiempo real**, haga clic en **Configuración**.
5. Seleccione la casilla de verificación **Protección de archivos en tiempo real**.
6. En el bloque **Modo de protección de objetos**, en la pestaña **General**, seleccione el modo de operación Protección de archivos en tiempo real:
   - **Modo inteligente**. Kaspersky Embedded Systems Security selecciona objetos para analizar por su cuenta. Un objeto se analiza cuando se abre y, luego, nuevamente después de guardarlo si se modificó. Si se accede al objeto varias veces y el proceso lo modifica, Kaspersky Embedded Systems Security vuelve a analizar el objeto sólo después de que el proceso lo guarde por última vez.
   - **Al acceder y realizar modificaciones**. Kaspersky Embedded Systems Security analiza un objeto cuando se abre y, si el objeto se modifica, vuelve a analizarlo después de que se guarda. De forma predeterminada, esta opción está seleccionada.
   - **Ante operaciones de acceso**. Kaspersky Embedded Systems Security analiza todos los objetos cuando se abren para su lectura, ejecución o modificación.
   - **Durante ejecución**. Kaspersky Embedded Systems Security analiza un archivo solo cuando se accede para su ejecución.
7. Desactive o seleccione la casilla de verificación **Utilizar análisis heurístico**.

8. Seleccione o desactive la casilla **Bloquear acceso a recursos compartidos en la red para las sesiones que muestran actividad maliciosa**.
9. Desactive o seleccione la casilla de verificación **Iniciar análisis de áreas críticas al detectar infección activa**.

   Si la casilla está seleccionada, al detectar una infección activa, Kaspersky Embedded Systems Security ejecuta la tarea *Análisis de áreas críticas*. De forma predeterminada, la casilla está activada.
10. Especifique la configuración para analizar las operaciones sobre archivos ejecutadas en los contenedores de Windows.
11. Guarde los cambios.

Cómo habilitar el análisis antivirus de los archivos Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Protección del equipo en tiempo real** → **Protección de archivos en tiempo real** y haga clic en el botón **Configurar**.
5. Seleccione la casilla de verificación **Habilitar Protección de archivos en tiempo real**.
6. En el bloque **Modo de protección de objetos**, en la pestaña **General**, seleccione el modo de operación Protección de archivos en tiempo real:

   - **Modo inteligente**. Kaspersky Embedded Systems Security selecciona objetos para analizar por su cuenta. Un objeto se analiza cuando se abre y, luego, nuevamente después de guardarlo si se modificó. Si se accede al objeto varias veces y el proceso lo modifica, Kaspersky Embedded Systems Security vuelve a analizar el objeto sólo después de que el proceso lo guarde por última vez.
   - **Al acceder y realizar modificaciones**. Kaspersky Embedded Systems Security analiza un objeto cuando se abre y, si el objeto se modifica, vuelve a analizarlo después de que se guarda. De forma predeterminada, esta opción está seleccionada.
   - **Ante operaciones de acceso**. Kaspersky Embedded Systems Security analiza todos los objetos cuando se abren para su lectura, ejecución o modificación.
   - **Durante ejecución**. Kaspersky Embedded Systems Security analiza un archivo solo cuando se accede para su ejecución.
7. Desactive o seleccione la casilla de verificación **Utilizar análisis heurístico**.
8. Seleccione o desactive la casilla **Bloquear acceso a recursos compartidos en la red para las sesiones de red que muestran actividad maliciosa**.

9. Desactive o seleccione la casilla de verificación **Iniciar análisis de áreas críticas al detectar infección activa**.

   Si la casilla está seleccionada, al detectar una infección activa, Kaspersky Embedded Systems Security ejecuta la tarea *Análisis de áreas críticas*. De forma predeterminada, la casilla está activada.

10. Especifique la configuración para analizar las operaciones sobre archivos ejecutadas en los contenedores de Windows.

11. Guarde los cambios.

Cómo habilitar el análisis antivirus de los archivos en la Consola de la aplicación

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Protección del equipo en tiempo real → Protección de archivos en tiempo real**.

2. En el panel de resultados del nodo **Protección de archivos en tiempo real**, haga clic en **Propiedades**.

   Se abre la ventana **Propiedades: Protección de archivos en tiempo real**.

3. Seleccione la casilla de verificación **Protección de archivos en tiempo real**.

4. En el bloque **Modo de protección de objetos**, en la pestaña **General**, seleccione el modo de operación Protección de archivos en tiempo real:

   - **Modo inteligente**. Kaspersky Embedded Systems Security selecciona objetos para analizar por su cuenta. Un objeto se analiza cuando se abre y, luego, nuevamente después de guardarlo si se modificó. Si se accede al objeto varias veces y el proceso lo modifica, Kaspersky Embedded Systems Security vuelve a analizar el objeto sólo después de que el proceso lo guarde por última vez.

   - **Al acceder y realizar modificaciones**. Kaspersky Embedded Systems Security analiza un objeto cuando se abre y, si el objeto se modifica, vuelve a analizarlo después de que se guarda. De forma predeterminada, esta opción está seleccionada.

   - **Ante operaciones de acceso**. Kaspersky Embedded Systems Security analiza todos los objetos cuando se abren para su lectura, ejecución o modificación.

   - **Durante ejecución**. Kaspersky Embedded Systems Security analiza un archivo solo cuando se accede para su ejecución.

5. Desactive o seleccione la casilla de verificación **Utilizar análisis heurístico**.

6. Seleccione o desactive la casilla **Bloquear acceso a recursos compartidos en la red para las sesiones que muestran actividad maliciosa**.

7. Desactive o seleccione la casilla de verificación **Iniciar análisis de áreas críticas al detectar infección activa**.

   Si la casilla está seleccionada, al detectar una infección activa, Kaspersky Embedded Systems Security ejecuta la tarea *Análisis de áreas críticas*. De forma predeterminada, la casilla está activada.

8. Especifique la configuración para analizar las operaciones sobre archivos ejecutadas en los contenedores de Windows.

9. Guarde los cambios.

Configurar el alcance de la protección para el componente de Protección de archivos en tiempo real

De manera predeterminada, el componente Protección de archivos en tiempo real utiliza la configuración de seguridad común para toda el área de protección. Estos ajustes corresponden al nivel de seguridad predefinido **Recomendado**.

Los valores predeterminados de la configuración de seguridad se pueden modificar configurándolos como valores comunes para toda el área de la protección o como valores diferentes para los elementos individuales de la lista de recursos de archivos del dispositivo.

Si el mismo objeto figura en varias entradas del alcance de protección y estas entradas tienen diferentes niveles de seguridad, la última regla de la lista tendrá prioridad. Por ejemplo, considere un alcance de protección que incluye dos entradas: **Todos los discos duros** (nivel de seguridad **Informar**) y `*\Users\*\Downloads\*` (nivel de seguridad **Personalizada**). La aplicación analiza los discos duros según el nivel Informar, excepto la carpeta `Downloads`. La aplicación analiza la carpeta `Downloads` según la configuración que se especificó manualmente porque esta entrada es la última en la lista del alcance de la protección.

Para configurar las opciones de seguridad del nodo seleccionado en forma manual:

Cómo configurar el alcance de la protección para Protección de archivos en tiempo real en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de propiedades de la directiva, seleccione **Protección del equipo en tiempo real**.
4. En la sección **Protección de archivos en tiempo real**, haga clic en **Configuración**.
5. Seleccione la ficha **Alcance de la protección**.
6. En la lista de recursos del archivo protegido, seleccione los elementos para los que desea establecer un nivel de seguridad predefinido.
7. Si el recurso compartido de archivos no está en la lista, agréguelo manualmente:
    a. Haga clic en **Agregar**.
    b. Use el árbol de carpetas para especificar la ruta al objeto necesario o ingrese la ruta en el campo **Objeto**.

Si es necesario, use caracteres especiales para ingresar la máscara de la ruta del objeto:

- El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco C:, pero no en las subcarpetas.

- Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT ubicados en carpetas dentro de la `Folder`, excepto la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.

- El carácter `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las carpetas. Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.

El objeto **Este equipo** en la lista de recursos del equipo incluye los siguientes objetos: **Todos los discos duros**, **Todas las unidades de red** y **Todas las unidades extraíbles**.

c. Haga clic en **Aceptar**.

8. Asegúrese de que el recurso del archivo seleccionado se incluya en el área de la protección.

9. Especifique un nivel de seguridad predefinido para el alcance de la protección; para ello, haga clic en **Configurar**. De manera predeterminada, se aplica la misma configuración de seguridad en todo el alcance de la protección. Estos ajustes corresponden al nivel de seguridad predefinido **Recomendado**. También puede editar la configuración de seguridad predeterminada.

10. Guarde los cambios.

Cómo configurar el alcance de la protección para Protección de archivos en tiempo real en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.

2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la ficha **Configuración de la aplicación**.

4. Vaya a **Protección del equipo en tiempo real** → **Protección de archivos en tiempo real** y haga clic en el botón **Configurar**.

5. Seleccione la ficha **Alcance de la protección**.

6. En la lista de recursos del archivo protegido, seleccione los elementos para los que desea establecer un nivel de seguridad predefinido.

7. Si el recurso compartido de archivos no está en la lista, agréguelo manualmente:

   a. Haga clic en **Agregar**.

   b. En la lista **Tipo de objeto**, seleccione una opción:

      Para la opción **Máscara**, use caracteres especiales para ingresar la máscara de ruta del objeto:

      - El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco C:, pero no en las subcarpetas.

      - Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT ubicados en carpetas dentro de la `Folder`, excepto la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.

      - El carácter `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las carpetas. Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.

      El objeto **Este equipo** en la lista de recursos del equipo incluye los siguientes objetos: **Todos los discos duros**, **Todas las unidades de red** y **Todas las unidades extraíbles**.

   c. Haga clic en **Aceptar**.

8. Asegúrese de que el recurso del archivo seleccionado se incluya en el área de la protección; para ello, use el interruptor que se encuentra junto al elemento de la lista.

9. Especifique un nivel de seguridad predefinido para el alcance de la protección; para ello, haga clic en **Modificar**. De manera predeterminada, se aplica la misma configuración de seguridad en todo el alcance de la protección. Estos ajustes corresponden al nivel de seguridad predefinido **Recomendado**. También puede editar la configuración de seguridad predeterminada.

10. Guarde los cambios.

Cómo configurar el alcance de la protección para Protección de archivos en tiempo real en la Consola de la aplicación

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Protección del equipo en tiempo real → Protección de archivos en tiempo real**.

2. En el panel de resultados del nodo **Protección de archivos en tiempo real**, haga clic en **Configurar el área de protección**.

   Se abre la ventana **Propiedades: Protección de archivos en tiempo real**.

3. En la lista de recursos del archivo protegido, seleccione los elementos para los que desea establecer un nivel de seguridad predefinido.

4. Si el recurso compartido de archivos no está en la lista, agréguelo manualmente:

   a. Haga clic en **Agregar**.

   b. Use el árbol de carpetas para especificar la ruta al objeto necesario o ingrese la ruta en el campo **Objeto**.

   Si es necesario, use caracteres especiales para ingresar la máscara de la ruta del objeto:

   - El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco C:, pero no en las subcarpetas.

   - Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT ubicados en carpetas dentro de la `Folder`, excepto la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.

   - El carácter `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las carpetas. Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.

   El objeto **Este equipo** en la lista de recursos del equipo incluye los siguientes objetos: **Todos los discos duros**, **Todas las unidades de red** y **Todas las unidades extraíbles**.

   c. Haga clic en **Aceptar**.

5. Asegúrese de que el recurso del archivo seleccionado se incluya en el área de la protección.

6. Especifique un nivel de seguridad predefinido para el alcance de la protección; para ello, haga clic en **Configurar**. De manera predeterminada, se aplica la misma configuración de seguridad en todo el alcance de la protección. Estos ajustes corresponden al nivel de seguridad predefinido **Recomendado**. También puede editar la configuración de seguridad predeterminada.

7. Guarde los cambios.

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 toda el área de protección. Estos ajustes corresponden al nivel de seguridad predefinido **Recomendado**.

Los valores predeterminados de la configuración de seguridad se pueden modificar configurándolos como valores comunes para toda el área de la protección o como valores diferentes para los elementos individuales de la lista de recursos de archivos del dispositivo o nodos del árbol.

Al trabajar con el árbol de recursos de archivos del dispositivo protegido, 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.

Cómo ajustar la configuración de seguridad manualmente en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de propiedades de la directiva, seleccione **Protección del equipo en tiempo real**.
4. En la sección **Protección de archivos en tiempo real**, haga clic en **Configuración**.
5. En la ventana **Protección de archivos en tiempo real**, vaya a la pestaña **Alcance de la protección**.
6. Seleccione el recurso cuya configuración de seguridad desea ajustar.
7. Haga clic en **Configurar**.
8. En la ventana que se abre, seleccione el nivel de seguridad requerido y haga clic en **Configuración**.
9. En la pestaña **General**, especifique la siguiente configuración:
   - Objetos que deberían incluirse en el alcance de la protección:
     - Todos los objetos
     - Objetos analizados según su formato
     - Objetos analizados según la lista de extensiones de la base de datos antivirus
   - En el bloque **Optimización**, seleccione o desactive la casilla de verificación Analizar solo archivos nuevos y modificados.
   - En la sección **Análisis de archivos compuestos**, especifique los objetos compuestos que desea incluir en el área de análisis:
     - Analizar archivos de almacenamiento
     - Analizar paquetes de distribución
     - Analizar archivos de Microsoft Office
     - Analizar archivos de formato de correo electrónico
10. En la pestaña **Acciones**, especifique la siguiente configuración:
    - Seleccione la acción que se debe realizar en los objetos infectados y otros objetos detectados:
      - Informar

- Bloquear
- **Realizar acción adicional**

  Seleccione la acción en la lista desplegable:

  - **Desinfectar**
  - **Desinfectar; eliminar si falla la desinfección**
  - Eliminar
  - Recomendada

- Configure las acciones que se deben realizar en los objetos según el tipo de objeto detectado:

  a. Desactive o seleccione la casilla de verificación Aplicar la acción a los tipos de objetos seleccionados.

  b. Haga clic en **Configuración** y seleccione los tipos de objetos que se deben detectar.

- Configure las acciones en los archivos compuestos que no están disponibles para su modificación: desactive o seleccione la casilla Si se detecta un objeto integrado, eliminar todo el archivo compuesto que la aplicación no pueda modificar.

11. En la pestaña **Rendimiento**, especifique la siguiente configuración:

    - Descomprimir en segundo plano archivos compuestos más grandes que (MB)
    - Detener el análisis si demora más de (s)
    - No analizar objetos compuestos de más de (MB)
    - Usar la tecnología iSwift
    - Usar la tecnología iChecker

12. Guarde la nueva configuración de seguridad.

Cómo ajustar la configuración de seguridad manualmente en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Protección del equipo en tiempo real** → **Protección de archivos en tiempo real** y haga clic en el botón **Configurar**.
5. Seleccione la ficha **Alcance de la protección**.

6. Realice una de las siguientes acciones:

   - Haga clic en el botón **Agregar** para agregar una nueva regla y especifique su configuración de seguridad.
   - Seleccione una regla existente y haga clic en el botón **Editar**.

   Se abre la ventana **Modificar alcance**.

7. Configure el interruptor en **Habilitada**.
8. Seleccione un nivel de seguridad y especifique la configuración de seguridad según sea necesario.
9. En la sección **Modo de protección de objetos**, seleccione el tipo de objeto que desea incluir en el alcance de la protección:

   - **Todos los objetos**
   - **Objetos analizados según su formato**
   - **Objetos analizados según la lista de extensiones de la base de datos antivirus**

10. En la sección **Optimización**, seleccione o desactive la casilla de verificación **Proteger solo los archivos nuevos y modificados**.
11. En la sección **Protección de objetos compuestos**, especifique los objetos compuestos que desea incluir en el área de análisis:

    - **Analizar archivos de almacenamiento**
    - **Analizar paquetes de distribución**
    - **Analizar archivos de Microsoft Office**
    - **Analizar archivos de formato de correo electrónico**

12. Seleccione la acción que se debe realizar en los objetos infectados y otros objetos detectados:

    - **Informar**
    - **Bloquear**
    - **Realizar acción adicional**

      Seleccione la acción en la lista desplegable:

      - **Desinfectar**
      - **Desinfectar; eliminar si falla la desinfección**
      - **Eliminar**
      - **Recomendada**

13. Configure las acciones que se deben realizar en los objetos según el tipo de objeto detectado:

    a. Desactive o seleccione la casilla de verificación **Aplicar la acción a los tipos de objetos seleccionados**.

    b. Si la casilla de verificación está seleccionada, haga clic en **Configuración** y seleccione los tipos de objetos que se deben detectar.

14. Configure las acciones en los archivos compuestos que no están disponibles para su modificación: desactive o seleccione la casilla **Si se detecta un objeto integrado, eliminar todo el archivo compuesto que la aplicación no pueda modificar**.

15. En la sección **Optimización**, configure las siguientes opciones:

    - **Descomprimir archivos compuestos en segundo plano**
    - **Detener el análisis si demora más de (s)**
    - **No analizar objetos compuestos de más de (MB)**
    - **Usar la tecnología iSwift**
    - **Usar la tecnología iChecker**

16. Guarde la nueva configuración de seguridad.

Cómo establecer la configuración de seguridad manualmente en la Consola de la aplicación

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Protección del equipo en tiempo real** → **Protección de archivos en tiempo real**.

2. En el panel de resultados del nodo **Protección de archivos en tiempo real**, haga clic en **Configurar el área de protección**.

   Se abre la ventana **Propiedades: Protección de archivos en tiempo real**.

3. Seleccione el recurso cuya configuración de seguridad desea ajustar.

4. Haga clic en **Configurar**.

5. En la ventana que se abre, seleccione el nivel de seguridad requerido y haga clic en **Configuración**.

6. En la pestaña **General**, especifique la siguiente configuración:

- Objetos que deberían incluirse 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 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 compila la lista de extensiones. Se incluye en las bases de datos de Kaspersky Embedded Systems Security.
- En el bloque **Optimización**, seleccione o desactive la casilla de verificación **Proteger solo los archivos nuevos y modificados**.
- En la sección **Análisis de archivos compuestos**, especifique los objetos compuestos que desea incluir en el área de análisis:
  - **Analizar archivos de almacenamiento**. Analizar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros archivos de almacenamiento. La aplicación analiza los archivos no solo por su extensión, sino también por su formato. Al verificar archivos de almacenamiento, la aplicación realiza un descomprimido recursivo. Esto permite detectar amenazas dentro de archivos de almacenamiento multinivel (un archivo de almacenamiento dentro de un archivo de almacenamiento).
  - **Analizar paquetes de distribución**. Use esta casilla para habilitar/deshabilitar el análisis de paquetes de distribución de terceros.
  - **Analizar archivos de Microsoft Office**. Analiza archivos de Microsoft Office (DOC, DOCX, XLS, PPT y otras extensiones de Microsoft). Los objetos OLE también se consideran archivos de Office. Kaspersky Embedded Systems Security analiza los archivos en formato Office con un tamaño inferior a 1 MB independientemente de si la casilla está seleccionada o no.
  - **Analizar archivos de formato de correo electrónico**.

7. En la pestaña **Acciones**, especifique la siguiente configuración:

- Seleccione la acción que se debe realizar en los objetos infectados y otros objetos detectados:
  - **Informar**.
  - **Bloquear**.
  - **Realizar acción adicional**.

    Seleccione la acción en la lista desplegable:
    - **Desinfectar**
    - **Desinfectar; eliminar si falla la desinfección**
    - **Eliminar**.
    - **Recomendada**.

- Configure las acciones que se deben realizar en los objetos según el tipo de objeto detectado:

  a. Desactive o seleccione la casilla de verificación **Aplicar la acción a los tipos de objetos seleccionados**.

  b. Haga clic en **Configuración** y seleccione los tipos de objetos que se deben detectar.

- Configure las acciones en los archivos compuestos que no están disponibles para su modificación: desactive o seleccione la casilla **Si se detecta un objeto integrado, eliminar todo el archivo compuesto que la aplicación no pueda modificar**.

8. En la pestaña **Rendimiento**, especifique la siguiente configuración:

- **Descomprimir en segundo plano archivos compuestos más grandes que (MB)**.
- **Detener el análisis si demora más de (s)**.
- **No analizar objetos compuestos de más de (MB)**.
- **Usar la tecnología iSwift**.
- **Usar la tecnología iChecker**.

9. Guarde la nueva configuración de seguridad.

Análisis de contenedores

Un *contenedor* es un entorno aislado en el que una aplicación puede ejecutarse sin interactuar directamente con el sistema operativo. El uso de contenedores conlleva los siguientes riesgos:

- Los piratas informáticos pueden aprovechar las vulnerabilidades de la contenedorización para poner en peligro las aplicaciones dentro del contenedor.
- Los piratas informáticos pueden explotar una configuración poco segura del entorno del contenedor para obtener acceso no autorizado a los datos del equipo o para comprometer la integridad del sistema.
- Un ataque exitoso a un contenedor puede permitir a un pirata informático obtener acceso a los datos del equipo.
- Los piratas informáticos pueden aprovechar las vulnerabilidades de la red para interceptar el tráfico de la red.

Kaspersky Embedded Systems Security es una herramienta externa para detectar actividad maliciosa dentro de contenedores. Esto permite mantener el rendimiento de los contenedores y evita conflictos con otras aplicaciones dentro del contenedor. La instalación de Kaspersky Embedded Systems Security dentro del contenedor no es compatible.

Además de proporcionar seguridad para los contenedores, Kaspersky Embedded Systems Security permite administrar aplicaciones dentro de contenedores mediante el Control de inicio de aplicaciones. El Control de inicio de aplicaciones está configurado para contenedores de la misma manera que para las aplicaciones instaladas en el equipo. Control de integridad del sistema también admite contenedores.

Requisitos del contenedor

- El contenedor debe ser un contenedor Docker. No se admiten otras herramientas de contenedorización.
- El contenedor debe ejecutarse en el modo de aislamiento de procesos. El modo de aislamiento de Hyper-V no es compatible.
- El contenedor debe colocarse en un servidor Windows Server 2016, 2019 o 2022 (Docker Host).
- El contenedor debe incluir una imagen de Windows (Docker Image). Windows 10 y 11 no son compatibles. Las imágenes de Linux no son compatibles.
- El análisis de contenedores que se ejecutan en el modo WSL2 – Windows Subsystem for Linux v2 (Docker Wine) no es compatible.

Acción al detectar amenaza

Si se detecta una amenaza dentro de un contenedor, la aplicación aplica la acción seleccionada para el componente Protección de archivos en tiempo real. El análisis de contenedores tiene configuraciones adicionales (consulte las instrucciones a continuación). Si se detecta una amenaza, la aplicación bloquea la actividad maliciosa y realiza la acción seleccionada (por ejemplo, intenta desinfectar el objeto). Kaspersky Embedded Systems Security puede detener el contenedor si falla para desinfectar el objeto detectado. De manera predeterminada, se permite detener el contenedor.

Cómo ajustar el análisis de contenedores en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de propiedades de la directiva, seleccione **Protección del equipo en tiempo real**.
4. En la sección **Protección de archivos en tiempo real**, haga clic en **Configuración**.
5. En el bloque **Análisis de las operaciones ejecutadas en contenedores de Windows**, ajuste la configuración del análisis de contenedor:
   - **Detener el contenedor si la desinfección falla**. Es posible que la aplicación no tenga permisos de lectura y escritura para el objeto detectado. En este caso, no se puede desinfectar ni eliminar el objeto detectado. Si se selecciona esta casilla, la aplicación bloquea el objeto detectado y detiene el contenedor. Si no se selecciona esta casilla, la aplicación solo bloquea el objeto detectado.
   - **No analizar las operaciones ejecutadas en contenedores de Windows**. Si se selecciona esta casilla, la aplicación analiza el contenedor solo cuando se inicia. Si no se selecciona la casilla, la aplicación analiza el contenedor continuamente en tiempo real.
6. Guarde la nueva configuración de seguridad.

Cómo configurar el análisis de contenedores en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Protección del equipo en tiempo real** → **Protección de archivos en tiempo real** y haga clic en el botón **Configurar**.
5. En el bloque **Análisis de las operaciones ejecutadas en contenedores de Windows**, ajuste la configuración del análisis de contenedor:

   - **Detener el contenedor si la desinfección falla**. Es posible que la aplicación no tenga permisos de lectura y escritura para el objeto detectado. En este caso, no se puede desinfectar ni eliminar el objeto detectado. Si se selecciona esta casilla, la aplicación bloquea el objeto detectado y detiene el contenedor. Si no se selecciona esta casilla, la aplicación solo bloquea el objeto detectado.
   - **No analizar las operaciones ejecutadas en contenedores de Windows**. Si se selecciona esta casilla, la aplicación analiza el contenedor solo cuando se inicia. Si no se selecciona la casilla, la aplicación analiza el contenedor continuamente en tiempo real.
6. Guarde la nueva configuración de seguridad.

Cómo configurar el análisis de contenedores en la Consola de la aplicación

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Protección del equipo en tiempo real** → **Protección de archivos en tiempo real**.
2. En el panel de resultados del nodo **Protección de archivos en tiempo real**, haga clic en **Propiedades**.

   Se abre la ventana **Propiedades: Protección de archivos en tiempo real**.
3. En el bloque **Análisis de las operaciones ejecutadas en contenedores de Windows**, ajuste la configuración del análisis de contenedor:

   - **Detener el contenedor si la desinfección falla**. Es posible que la aplicación no tenga permisos de lectura y escritura para el objeto detectado. En este caso, no se puede desinfectar ni eliminar el objeto detectado. Si se selecciona esta casilla, la aplicación bloquea el objeto detectado y detiene el contenedor. Si no se selecciona esta casilla, la aplicación solo bloquea el objeto detectado.
   - **No analizar las operaciones ejecutadas en contenedores de Windows**. Si se selecciona esta casilla, la aplicación analiza el contenedor solo cuando se inicia. Si no se selecciona la casilla, la aplicación analiza el contenedor continuamente en tiempo real.
4. Guarde los cambios.

Uso de KSN

A fin de proteger el equipo con mayor eficacia, Kaspersky Embedded Systems Security utiliza datos que recibimos de usuarios de todo el mundo. Kaspersky Security Network está diseñado para obtener estos datos.

La función de KSN puede dejar de estar disponible en el software en el territorio de EE. UU.

Kaspersky Security Network (KSN) es una infraestructura de servicios en la nube que brinda acceso a la Base de conocimientos de Kaspersky, un recurso en línea que permite conocer la reputación de los archivos, los recursos web y el software. El uso de los datos de Kaspersky Security Network garantiza respuestas más rápidas de Kaspersky Embedded Systems Security ante las amenazas nuevas, mejora el rendimiento de algunos componentes de protección y reduce la probabilidad de falsos positivos. Si participa en Kaspersky Security Network, Kaspersky Embedded Systems Security podrá utilizar los servicios de KSN para conocer la categoría y la reputación de los archivos analizados u obtener información sobre la reputación de las direcciones web que se analicen.

El uso de Kaspersky Security Network es voluntario. La aplicación invita al usuario a participar en KSN durante la configuración inicial de la aplicación. Los usuarios pueden iniciar o discontinuar su participación en KSN en cualquier momento.

La Declaración de Kaspersky Security Network y el sitio web de Kaspersky contienen más detalles sobre la información que se genera cuando el usuario participa en KSN, sobre la transmisión de dicha información a Kaspersky y sobre el almacenamiento y la destrucción de dicha información. Encontrará el texto de la Declaración de Kaspersky Security Network en el archivo ksn_<identificador del idioma>.txt, que forma parte del kit de distribución de la aplicación.

La infraestructura de las bases de datos de reputación de Kaspersky

Kaspersky Embedded Systems Security da soporte a las siguientes soluciones de infraestructura para trabajar con las bases de datos de reputación de Kaspersky:

- *Kaspersky Security Network (KSN).* Esta es la solución que utilizan la mayoría de las aplicaciones de Kaspersky. Quienes participan en KSN reciben información de Kaspersky y, a su vez, envían a Kaspersky información sobre los objetos detectados en sus equipos. Los analistas de Kaspersky examinan la información recibida e incluyen los datos estadísticos y de reputación pertinentes en las bases de datos.

- *Kaspersky Private Security Network (KPSN).* A través de esta solución, quienes utilizan Kaspersky Embedded Systems Security u otras aplicaciones de Kaspersky en sus equipos pueden acceder a las bases de datos de reputación de Kaspersky, así como a otras clases de información estadística, sin enviar información de sus equipos a Kaspersky. KPSN se ha diseñado para clientes corporativos que no pueden participar en Kaspersky Security Network por alguno de los siguientes motivos:

  - porque las estaciones de trabajo locales no tienen acceso a Internet;

  - Por motivos legales o debido a las directivas de seguridad de la empresa, no es posible transmitir datos de ningún tipo fuera del país o fuera de la LAN corporativa.

Habilitar el uso de Kaspersky Security Network

Cómo habilitar el uso de Kaspersky Security Network en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Network, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente de Kaspersky Embedded Systems Security y haga doble clic para abrir las propiedades de la directiva.
3. Se abre una ventana. En esa ventana, en la lista de secciones, seleccione **Protección del equipo en tiempo real** → **Uso de KSN**.
4. Haga clic en **Configuración**.
5. Seleccione la casilla **Kaspersky Security Network** para habilitar el componente.

   Si habilitó el uso de KSN, Kaspersky Embedded Systems Security mostrará la Declaración de Kaspersky Security Network. Lea y acepte los términos de uso de la Declaración de Kaspersky Security Network (KSN) si está de acuerdo con ellos.

   De manera predeterminada, Kaspersky Embedded Systems Security usa el modo Extendido de Kaspersky Security Network. El modo Extendido de Kaspersky Security Network es un modo por el cual Kaspersky Embedded Systems Security remite información adicional a Kaspersky.
6. Si es necesario, anule la selección de la casilla **Habilitar el modo KSN extendido**.
7. Guarde los cambios.

Si el uso de Kaspersky Security Network está habilitado, Kaspersky Embedded Systems Security usa información sobre la reputación de los archivos, los recursos web y las aplicaciones recibida de Kaspersky Security Network.

Cómo habilitar el uso de Kaspersky Security Network en la Consola de Kaspersky Embedded Systems Security

1. En el árbol de la Consola de la aplicación, expanda el nodo **Protección del equipo en tiempo real**.
2. Seleccione el nodo secundario **Kaspersky Security Network**.
3. En la ventana principal de la aplicación, haga clic en **Propiedades**.
4. Seleccione la casilla **Kaspersky Security Network** para habilitar el componente.

   Si habilitó el uso de KSN, Kaspersky Embedded Systems Security mostrará la Declaración de Kaspersky Security Network. Lea y acepte los términos de uso de la Declaración de Kaspersky Security Network (KSN) si está de acuerdo con ellos.

   De manera predeterminada, Kaspersky Embedded Systems Security usa el modo Extendido de Kaspersky Security Network. El modo Extendido de Kaspersky Security Network es un modo por el cual Kaspersky Embedded Systems Security remite información adicional a Kaspersky.

5. Si es necesario, anule la selección de la casilla **Habilitar el modo KSN extendido**.

6. Guarde los cambios.

Si el uso de Kaspersky Security Network está habilitado, Kaspersky Embedded Systems Security usa información sobre la reputación de los archivos, los recursos web y las aplicaciones recibida de Kaspersky Security Network.

Cómo habilitar el uso de Kaspersky Security Network en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.

2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la ficha **Configuración de la aplicación**.

4. Vaya a la sección **Protección del equipo en tiempo real** → **Uso de KSN** y haga clic en el botón **Configurar**.

5. En la ventana mostrada, seleccione la casilla **Habilitar Kaspersky Security Network** para habilitar el componente.

   Si habilitó el uso de KSN, Kaspersky Embedded Systems Security mostrará la Declaración de Kaspersky Security Network. Si está de acuerdo, acepte los términos de uso de Kaspersky Security Network.

   De manera predeterminada, Kaspersky Embedded Systems Security usa el modo Extendido de Kaspersky Security Network. El modo Extendido de Kaspersky Security Network es un modo por el cual Kaspersky Embedded Systems Security remite información adicional a Kaspersky.

6. Si es necesario, anule la selección de la casilla **Habilitar el modo KSN extendido**.

7. Guarde los cambios.

Como resultado, si el uso de KSN está habilitado, Kaspersky Embedded Systems Security usa información sobre la reputación de los archivos, los recursos web y las aplicaciones recibida de Kaspersky Security Network.

Estadísticas de uso de Kaspersky Security Network

Mientras se ejecuta la tarea *Uso de KSN*, puede ver información en tiempo real sobre la cantidad de objetos que procesó Kaspersky Embedded Systems Security desde el momento en que se inició la tarea hasta ahora.

Para ver las estadísticas del uso de KSN:

1. En el árbol de la Consola de la aplicación, seleccione la sección **Protección del equipo en tiempo real**.

2. Seleccione el nodo secundario **Kaspersky Security Network**.

   En el panel de resultados, en la sección **Estadísticas**, se muestran las estadísticas de la tarea (consulte la tabla a continuación).

Estadísticas de KSN

Campo	Descripción
Solicitudes de archivos enviadas	Número de consultas sobre la reputación de objetos enviadas por Kaspersky Embedded Systems Security a KSN.
Archivos no confiables en KSN	Número de objetos con una reputación de "no confianza" asignada por KSN.
Errores de envío de solicitudes	Número de solicitudes de KSN procesadas con un error.
Estadísticas creadas	Número de paquetes estadísticos generados enviados a KSN.
Objetos eliminados	Cantidad de objetos eliminados correctamente por Kaspersky Embedded Systems Security.
Objetos no eliminados	Cantidad de objetos que Kaspersky Embedded Systems Security intentó eliminar sin éxito debido a que, por ejemplo, el acceso al objeto estaba bloqueado por otra aplicación.
Pasados a Copia de seguridad	Número de objetos copiados correctamente a Copia de seguridad por Kaspersky Embedded Systems Security.
Objetos no pasados a Copia de seguridad	Número de objetos que Kaspersky Embedded Systems Security intentó copiar a Copia de seguridad sin éxito, 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.
Modo limitado	El estado significa si la aplicación envía solicitudes de reputación de archivos en un modo limitado. En un modo limitado, Kaspersky Embedded Systems Security envía solo una parte de las solicitudes de reputación de archivos según la recomendación de los expertos de Kaspersky.

Los valores de los campos **Objetos eliminados**, **Objetos no eliminados**, **Pasados a Copia de seguridad** y **Objetos no pasados a Copia de seguridad** se generan a partir de las estadísticas del componente Protección de archivos en tiempo real.

Limitaciones de Kaspersky Private Security Network

Kaspersky Private Security Network (KPSN). A través de esta solución, quienes utilizan Kaspersky Embedded Systems Security u otras aplicaciones de Kaspersky en sus equipos pueden acceder a las bases de datos de reputación de Kaspersky, así como a otras clases de información estadística, sin enviar información de sus equipos a Kaspersky. Kaspersky Private Security Network le permite utilizar su propia base de datos de reputación local para comprobar la reputación de los objetos (archivos o direcciones web). La reputación de un objeto agregado a la base de datos de reputación local tiene mayor prioridad que uno agregado a KSN/KPSN. Por ejemplo, imagine que Kaspersky Embedded Systems Security está analizando un equipo y solicita la reputación de un archivo en KSN/KPSN. Si el archivo tiene una reputación *No confiables* en la base de datos de reputación local, pero tiene una reputación *De confianza* en KSN/KPSN, Kaspersky Embedded Systems Security detectará el archivo como *No confiables* y realizará la acción definida para las amenazas detectadas.

Sin embargo, en algunos casos, es posible que Kaspersky Embedded Systems Security no solicite la reputación de un objeto en KSN/KPSN. Si este es el caso, Kaspersky Embedded Systems Security no recibirá datos de la base de datos de reputación local de KPSN. Es posible que Kaspersky Embedded Systems Security no solicite la reputación de un objeto en KSN/KPSN por las siguientes razones:

- Las aplicaciones de Kaspersky utilizan bases de datos de reputación sin conexión. Las bases de datos de reputación sin conexión están diseñadas para optimizar los recursos durante el funcionamiento de las aplicaciones de Kaspersky y para proteger los objetos de importancia crítica en el equipo. Expertos de Kaspersky se encargan de crear las bases de datos de reputación sin conexión basándose en datos de Kaspersky Security Network. Las aplicaciones de Kaspersky actualizan las bases de datos de reputación sin conexión con bases de datos antivirus de la aplicación específica. Si las bases de datos de reputación sin conexión contienen información sobre un objeto que se está analizando, la aplicación no solicita la reputación de este objeto a KSN/KPSN.

- Las exclusiones de análisis (zona de confianza) se configuran en la configuración de la aplicación. Si este es el caso, la aplicación no tiene en cuenta la reputación del objeto en la base de datos de reputación local.

- La aplicación usa tecnologías de optimización de análisis, como iSwift o iChecker, o almacena en caché solicitudes de reputación en KSN/KPSN. Si este es el caso, es posible que la aplicación no solicite la reputación de los objetos analizados anteriormente.

- Para optimizar su carga de trabajo, la aplicación analiza archivos de cierto formato y tamaño. Los expertos de Kaspersky determinan la lista de formatos relevantes y límites de tamaño. Esta lista se actualiza con las bases de datos antivirus de la aplicación.

Configuración del proxy de KSN

Los equipos de usuarios administrados por el Servidor de administración de Kaspersky Security Center pueden interactuar con KSN a través del servicio Proxy de KSN.

El servicio Proxy de KSN ofrece las siguientes capacidades:

- El equipo del usuario puede consultar KSN y enviarle información, incluso sin acceso directo a Internet.

- El servicio Proxy de KSN almacena los datos procesados en una caché; con ello, el equipo recibe más rápido la información que solicita y se reduce la congestión en el canal externo de comunicaciones por red.

De forma predeterminada, después de habilitar KSN y aceptar la declaración de KSN, la aplicación utiliza un servidor proxy para conectarse a Kaspersky Security Network. El servidor proxy que utiliza la aplicación es el Servidor de administración de Kaspersky Security Center a través del puerto TCP 13111. Por lo tanto, si Proxy de KSN no está disponible, debe verificar el funcionamiento del dispositivo como servidor proxy de KSN. Debe verificar lo siguiente:

- Que el servicio *ksnproxy* se esté ejecutando en el Servidor de administración.

- Que el firewall en el equipo no esté bloqueando el puerto 13111.

Puede configurar el uso del proxy de KSN de la siguiente manera: habilite o deshabilite el proxy de KSN y configure el puerto para la conexión. Para hacerlo, debe abrir las propiedades del Servidor de administración. Para obtener más información sobre la configuración del proxy de KSN, consulte la Ayuda de Kaspersky Security Center. También puede habilitar o deshabilitar el proxy de KSN para equipos individuales en la directiva de Kaspersky Embedded Systems Security.

Cómo habilitar Proxy de KSN en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente de Kaspersky Embedded Systems Security y haga doble clic para abrir las propiedades de la directiva.
3. Se abre una ventana. En esa ventana, en la lista de secciones, seleccione **Protección del equipo en tiempo real** → Uso de KSN.
4. Haga clic en **Configuración**.
5. En el bloque **Configuración del proxy de KSN**, use la casilla **Usar el Servidor de administración como servidor proxy de KSN** para habilitar o deshabilitar el proxy de KSN.
6. Si es necesario, seleccione la casilla **Usar los servidores de Kaspersky Security Network cuando el servidor proxy de KSN no esté disponible**.

   Cuando esta casilla está activada y el servicio proxy de KSN no está disponible, Kaspersky Embedded Systems Security usa los servidores de KSN. Los servidores de KSN pueden estar alojados tanto en la infraestructura de Kaspersky como en la de terceros (cuando se utiliza Kaspersky Private Security Network).
7. Guarde los cambios.

Cómo habilitar Proxy de KSN en la Consola de Kaspersky Embedded Systems Security

1. En el árbol de la Consola de la aplicación, expanda el nodo **Protección del equipo en tiempo real**.
2. Seleccione el nodo secundario **Kaspersky Security Network**.
3. En la ventana principal de la aplicación, haga clic en **Propiedades**.
4. En el bloque **Configuración del proxy de KSN**, use la casilla **Usar el Servidor de administración como servidor proxy de KSN** para habilitar o deshabilitar el proxy de KSN.
5. Si es necesario, seleccione la casilla **Usar los servidores de Kaspersky Security Network cuando el servidor proxy de KSN no esté disponible**.

   Cuando esta casilla está activada y el servicio proxy de KSN no está disponible, Kaspersky Embedded Systems Security usa los servidores de KSN. Los servidores de KSN pueden estar alojados tanto en la infraestructura de Kaspersky como en la de terceros (cuando se utiliza Kaspersky Private Security Network).
6. Guarde los cambios.

Cómo habilitar Proxy de KSN en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Protección del equipo en tiempo real** → **Uso de KSN** y haga clic en el botón **Configurar**.
5. Seleccione o desactive la casilla **Usar el Servidor de administración como servidor proxy de KSN** para habilitar o deshabilitar el Proxy de KSN.
6. Si es necesario, seleccione la casilla **Usar los servidores de Kaspersky Security Network cuando el servidor proxy de KSN no esté disponible**.

   Cuando esta casilla está activada y el servicio proxy de KSN no está disponible, Kaspersky Embedded Systems Security usa los servidores de KSN. Los servidores de KSN pueden estar alojados tanto en la infraestructura de Kaspersky como en la de terceros (cuando se utiliza Kaspersky Private Security Network).
7. Guarde los cambios.

La dirección del proxy de KSN coincide con la dirección del Servidor de administración. Cuando se cambia el nombre de dominio del Servidor de administración, debe actualizar de forma manual la dirección del proxy de KSN.

Prevención de exploits

Kaspersky Embedded Systems Security proporciona la capacidad de proteger la memoria del proceso de exploits. A esta funcionalidad la implementa el componente de Prevención de exploits, y puede usarla para cambiar el estado de actividad del componente y configurar la protección de los procesos frente a exploits.

El componente Prevención de exploits detecta código de software diseñado para aprovechar vulnerabilidades en el equipo y, a través de estas, realizar acciones maliciosas o abusar de los privilegios de administración. Un exploit puede, por ejemplo, llevar a cabo un ataque de desbordamiento de búfer. Para ello, el exploit envía una gran cantidad de datos a una aplicación vulnerable. Al procesar estos datos, la aplicación vulnerable ejecuta código malintencionado. El ataque permite al exploit instalar malware sin autorización. Cuando se detecta que una aplicación vulnerable ha intentado iniciar un archivo ejecutable y se determina que la orden no provino del usuario, Kaspersky Embedded Systems Security bloquea la ejecución del archivo o le muestra una notificación al usuario. El componente protege la memoria de un proceso contra los exploits a través de un Agente de protección externo ("Agente de protección") insertado 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 dispositivo protegido (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.

Modo de Prevención de exploits

Puede seleccionar uno de los modos siguientes para configurar acciones tomadas para reducir los riesgos de que las vulnerabilidades sufran ataques de exploits en procesos protegidos:

- **Bloquear**. 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.

  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.

- **Informar** (cuando trabaja en Kaspersky Security Center Web Console – **Informar**). Aplique este modo para recibir la información sobre casos de exploits en procesos protegidos mediante eventos en el registro de seguridad. El proceso abusado continúa ejecutándose.

  Si selecciona este modo, Kaspersky Embedded Systems Security crea eventos para registrar todos los intentos de realizar un ataque de exploit en vulnerabilidades. Seleccionado por defecto.

Habilitación y deshabilitación de la Prevención de exploits

Kaspersky Embedded Systems Security permite supervisar los archivos ejecutables que ejecutan las aplicaciones vulnerables. Si Kaspersky Embedded Systems Security detecta que no fue el usuario quien ejecutó un archivo de una aplicación vulnerable, Kaspersky Embedded Systems Security realizará la acción seleccionada (por ejemplo, bloqueará la operación).

Cómo habilitar o deshabilitar Prevención de exploits en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente de Kaspersky Embedded Systems Security y haga doble clic para abrir las propiedades de la directiva.
3. Se abre una ventana. En esa ventana, en la lista de secciones, seleccione **Protección del equipo en tiempo real** → **Prevención de exploits**.
4. Haga clic en **Configuración**.
5. Seleccione la casilla **Prevención de exploits** para habilitar el componente.
6. En la pestaña **General**, seleccione un modo de prevención de exploits: **Bloquear** o **Informar**.
7. Si es necesario, desactive la casilla **Prevención de exploits** para deshabilitar el componente.
8. Guarde los cambios.

Cómo habilitar o deshabilitar Prevención de exploits en la Consola de Kaspersky Embedded Systems Security

1. En el árbol de la Consola de la aplicación, expanda el nodo **Protección del equipo en tiempo real**.
2. Seleccione el nodo secundario **Prevención de exploits**.
3. En la ventana principal de la aplicación, haga clic en **Propiedades**.
4. Seleccione la casilla **Prevención de exploits** para habilitar el componente.
5. En la pestaña **General**, seleccione un modo de prevención de exploits: **Bloquear** o **Informar**.
6. Si es necesario, desactive la casilla **Prevención de exploits** para deshabilitar el componente.
7. Guarde los cambios.

Cómo habilitar o deshabilitar Prevención de exploits en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Protección del equipo en tiempo real** → **Prevención de exploits** y haga clic en el botón **Configurar**.
5. En la ventana que se abre, en **Modo de prevención de exploits**, seleccione la casilla **Impedir exploit de procesos vulnerables** para habilitar el componente.
6. Seleccione un modo de prevención de exploits: **Bloquear** o **Informar**.
7. Si es necesario, desactive la casilla **Impedir exploit de procesos vulnerables** para deshabilitar el componente.
8. Guarde los cambios.

Habilitar y deshabilitar la protección de memoria

Kaspersky Embedded Systems Security bloquea los procesos externos que intentan acceder a los procesos del sistema. De manera predeterminada, la protección de la memoria de procesos del sistema está habilitada.

Cómo habilitar o deshabilitar la protección de la memoria en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente de Kaspersky Embedded Systems Security y haga doble clic para abrir las propiedades de la directiva.
3. Se abre una ventana. En esa ventana, en la lista de secciones, seleccione **Protección del equipo en tiempo real** → **Prevención de exploits**.
4. Haga clic en **Configuración**.
5. En la pestaña **General**, seleccione la casilla **Habilitar la protección de la memoria de procesos del sistema**.
6. Si es necesario, anule la selección de la casilla **Habilitar la protección de la memoria de procesos del sistema**.
7. Guarde los cambios.

Cómo habilitar o deshabilitar la protección de la memoria en la Consola de Kaspersky Embedded Systems Security

1. En el árbol de la Consola de la aplicación, expanda el nodo **Protección del equipo en tiempo real**.
2. Seleccione el nodo secundario **Prevención de exploits**.
3. En la ventana principal de la aplicación, haga clic en **Propiedades**.
4. En la pestaña **General**, seleccione la casilla **Habilitar la protección de la memoria de procesos del sistema**.
5. Si es necesario, anule la selección de la casilla **Habilitar la protección de la memoria de procesos del sistema**.
6. Guarde los cambios.

Cómo habilitar o deshabilitar la protección de la memoria en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.

4. Vaya a **Protección del equipo en tiempo real** → **Prevención de exploits** y haga clic en el botón **Configurar**.

5. En la ventana que se abre, en el bloque **Protección de la memoria de procesos del sistema**, seleccione la casilla **Protección de la memoria de procesos del sistema**.

6. Si es necesario, desactive la casilla **Protección de la memoria de procesos del sistema** para deshabilitar la protección de la memoria de procesos del sistema.

7. Guarde los cambios.

Crear la lista de procesos protegidos

De manera predeterminada, el componente de Prevención de exploits protege diferentes procesos. La aplicación puede generar la lista de procesos protegidos automáticamente. También puede agregar o eliminar procesos de forma manual.

Cómo administrar la lista de procesos protegidos en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.

2. Seleccione la directiva correspondiente de Kaspersky Embedded Systems Security y haga doble clic para abrir las propiedades de la directiva.

3. Se abre una ventana. En esa ventana, en la lista de secciones, seleccione **Protección del equipo en tiempo real** → **Prevención de exploits**.

4. Haga clic en **Configuración**.

5. En la pestaña **Procesos protegidos**, seleccione una de las siguientes opciones para proteger a los procesos de la infiltración de códigos maliciosos:

   - **Detectar procesos protegidos automáticamente**. Si selecciona esta opción, la aplicación crea automáticamente una lista de los procesos protegidos.

   - **Proteger solo los procesos de la lista siguiente**. Si selecciona esta opción, puede seleccionar los procesos que desea proteger.

6. Si selecciona **Proteger solo los procesos de la lista siguiente**, puede editar la lista de procesos protegidos a través de uno de los siguientes pasos:

   - Si es necesario, haga clic en **Agregar** y seleccione un proceso que desee agregar a la lista de procesos protegidos.
   - Si desea eliminar un proceso de la lista creada de procesos protegidos, seleccione el proceso en la lista y haga clic en **Eliminar**.

     El botón **Eliminar** aparece si selecciona uno o más procesos de la lista.

7. Guarde los cambios.

Cómo administrar la lista de procesos protegidos con la Consola de Kaspersky Embedded Systems Security

1. En el árbol de la Consola de la aplicación, expanda el nodo **Protección del equipo en tiempo real**.
2. Seleccione el nodo secundario **Prevención de exploits**.
3. En la ventana principal de la aplicación, haga clic en **Propiedades**.
4. En la pestaña **Procesos protegidos**, seleccione una de las siguientes opciones para proteger a los procesos de la infiltración de códigos maliciosos:

   - **Detectar procesos protegidos automáticamente**. Si selecciona esta opción, la aplicación crea automáticamente una lista de los procesos protegidos.
   - **Proteger solo los procesos de la lista siguiente**. Si selecciona esta opción, puede seleccionar los procesos que desea proteger.

5. Si selecciona **Proteger solo los procesos de la lista siguiente**, puede editar la lista de procesos protegidos a través de uno de los siguientes pasos:

   - Si es necesario, haga clic en **Agregar** y seleccione un proceso que desee agregar a la lista de procesos protegidos.
   - Si desea eliminar un proceso de la lista creada de procesos protegidos, seleccione el proceso en la lista y haga clic en **Eliminar**.

     El botón **Eliminar** aparece si selecciona uno o más procesos de la lista.

6. Guarde los cambios.

Cómo administrar la lista de procesos protegidos en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la ficha **Configuración de la aplicación**.

4. Vaya a la sección **Protección del equipo en tiempo real** → **Prevención de exploits** y haga clic en el botón **Configurar**.

5. En **Lista de procesos protegidos**, seleccione una de las siguientes opciones para proteger a los procesos de la infiltración de códigos maliciosos:

   - **Detectar procesos protegidos automáticamente**. Si selecciona esta opción, la aplicación crea automáticamente una lista de los procesos protegidos.

   - **Proteger solo los procesos de la lista siguiente**. Si selecciona esta opción, puede agregar, editar y eliminar los procesos que desea proteger.

6. Si seleccionó **Proteger solo los procesos de la lista siguiente**, realice una de las siguientes acciones:

   - Haga clic en **Agregar** para abrir la ventana **Proceso protegido** y, en esa ventana:

     a. Seleccione la casilla de verificación **Proceso protegido**.

     b. En el campo **Nombre del proceso**, escriba el nombre del proceso.

     c. Guarde los cambios.

   - Si es necesario, edite la configuración el proceso en la lista de procesos protegidos. Para ello, realice las siguientes acciones:

     a. Seleccione un proceso en la lista de procesos protegidos.

     b. Haga clic en **Modificar**. El botón **Modificar** aparece si selecciona uno o más procesos de la lista.

     c. En la ventana **Proceso protegido**, seleccione o desactive la casilla de verificación **Proceso protegido**.

     d. Si es necesario, edite el nombre del proceso en el campo **Nombre del proceso**.

     e. Guarde los cambios.

   - Si es necesario, puede eliminar un proceso de la lista de procesos protegidos. Para ello, realice las siguientes acciones:

     a. Seleccione uno o más procesos en la lista de procesos protegidos.

     b. Haga clic en **Eliminar**. El botón **Eliminar** aparece si selecciona uno o más procesos de la lista.

7. Guarde los cambios.

Motor de reparación

El Motor de reparación permite a Kaspersky Embedded Systems Security deshacer acciones que han sido realizadas por el malware en el sistema operativo.

Al revertir la actividad del malware en el sistema operativo, Kaspersky Embedded Systems Security realiza las siguientes acciones:

- **Actividad de archivos**
  - Elimina los archivos ejecutables que el malware ha creado en cualquier tipo de soporte, excepto unidades de red.
  - Elimina los archivos ejecutables creados por programas en los que el malware se ha infiltrado.
  - Restaura los archivos que el malware ha modificado o eliminado.

  La capacidad de recuperar archivos está sujeta a **algunas limitaciones**.

  - La aplicación solo puede restaurar archivos en dispositivos que utilizan los sistemas de archivos NTFS o FAT32.
  - La aplicación puede restaurar archivos de las siguientes extensiones: odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls, xlsx, xlsm, xlsb, xlk, ppt, pptx, pptm, mdb, accdb, pst, dwg, dxf, dxg, wpd, rtf, wb2, pdf, mdf, dbf, psd, pdd, eps, ai, indd, cdr, jpg, jpe, dng, 3fr, arw, srf, sr2, bay, crw, cr2, dcr, kdc, erf, mef, mrw, nef, nrw, orf, raf, raw, rwl, rw2, r3d, ptx, pef, srw, x3f, der, cer, crt, pem, pfx, p12, p7b, p7c, 1cd.
  - Los archivos almacenados en unidades de red o en discos CD o DVD regrabables no pueden restaurarse.
  - Los archivos cifrados con el sistema de cifrado de archivos EFS no pueden restaurarse. Para más información sobre el funcionamiento de EFS, visite el sitio web de Microsoft.
  - La aplicación no controla los cambios que se realizan en los archivos a través de procesos que funcionan en el nivel del núcleo del sistema operativo.
  - La aplicación no controla los cambios que se realizan en los archivos a través de las interfaces de red (esta situación puede ocurrir, por ejemplo, si un archivo está almacenado en una carpeta compartida y un proceso se inicia a distancia desde otro equipo).

- **Actividad de registro**
  - Elimina las claves del Registro que el malware ha creado.

  Kaspersky Embedded Systems Security no restaura las claves del Registro que el malware eliminó o modificó.

- **Actividad del sistema**
  - Finaliza los procesos iniciados por el malware.
  - Finaliza los procesos en los cuales ha penetrado una aplicación malintencionada.

  Kaspersky Embedded Systems Security no reanuda procesos que el malware suspendió.

- **Actividad de la red**
  - Bloquea la actividad de red del malware.
  - Bloquea la actividad de red de los procesos en los que el malware se ha infiltrado.

Se puede iniciar una reversión de las acciones de la aplicación maliciosa a través del componente Protección de archivos en tiempo real o durante un Análisis a pedido.

La reversión de las operaciones del malware afecta a un conjunto de datos estrictamente definido. La reversión no tiene efectos negativos en el sistema operativo ni en la integridad de los datos de su equipo.

Cómo habilitar o deshabilitar el componente Motor de reparación en la Consola de administración de Kaspersky Security Center

1. Abra la configuración del componente Motor de reparación en la directiva que desea configurar.

   a. En el árbol de la Consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados**.

   b. Seleccione el grupo de administración para el cual desea configurar la tarea.

   c. Seleccione la ficha **Directivas**.

   d. Haga doble clic en el nombre de la directiva para abrir la ventana de propiedades.

   e. En la ventana de las propiedades de la directiva, vaya a la sección **Protección del equipo en tiempo real**.

   f. En el bloque **Motor de reparación**, haga clic en el botón **Configuración**.

   Se abre la ventana **Motor de reparación** en la pestaña **General**.

2. Realice una de las siguientes acciones:
   - Seleccione la casilla **Motor de reparación** si desea habilitar el componente Motor de reparación.
   - Desactive la casilla **Motor de reparación** si desea deshabilitar el componente Motor de reparación.

3. Haga clic en el botón **Aceptar** de la ventana **Motor de reparación**.
4. Haga clic en el botón **Aceptar** de la ventana **Propiedades: <Nombre de directiva>**.

Cómo habilitar o deshabilitar el componente Motor de reparación en la Consola de Kaspersky Embedded Systems Security

1. En el árbol de la Consola de la aplicación, seleccione la sección **Protección del equipo en tiempo real** → **Motor de reparación**.
2. Haga clic en el vínculo **Propiedades** del panel de resultados.
   Se abre la ventana **Motor de reparación** en la pestaña **General**.
3. Realice una de las siguientes acciones:
   - Seleccione la casilla **Motor de reparación** si desea habilitar el componente Motor de reparación.
   - Desactive la casilla **Motor de reparación** si desea deshabilitar el componente Motor de reparación.
4. Haga clic en el botón **Aceptar** de la ventana **Motor de reparación**.

Cómo habilitar o deshabilitar el componente Motor de reparación en Kaspersky Security Center Web Console

1. Abra la configuración del componente Motor de reparación en la directiva que desea configurar.
   a. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
   b. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.
      Se abre la ventana de propiedades de la directiva.
   c. Seleccione la ficha **Configuración de la aplicación**.
   d. Seleccione la sección **Protección del equipo en tiempo real**.
   e. En el bloque **Motor de reparación**, haga clic en el botón **Configurar**.
      Se abre la ventana **Motor de reparación**.
2. Realice una de las siguientes acciones:
   - Seleccione la casilla **Motor de reparación** si desea habilitar el componente Motor de reparación.
   - Desactive la casilla **Motor de reparación** si desea deshabilitar el componente Motor de reparación.
3. Haga clic en el botón **Aceptar** de la ventana **Motor de reparación**.
4. En la ventana **<Nombre de directiva>**, haga clic en **Guardar**.

Detección de comportamiento

El componente Detección de comportamiento recibe datos sobre las acciones de las aplicaciones del equipo y transmite esta información a los demás componentes de protección para mejorar su rendimiento. El componente Detección de comportamiento utiliza firmas de patrones de comportamiento para aplicaciones. Si la actividad de la aplicación coincide con un patrón de actividad peligrosa, Kaspersky Embedded Systems Security realiza la acción de respuesta especificada. Las funcionalidades de Kaspersky Embedded Systems Security basadas en firmas de patrones de comportamiento proporcionan una defensa proactiva para el equipo.

Habilitar y deshabilitar la protección de cifrado para las carpetas locales

Cómo habilitar o deshabilitar el componente Detección de comportamiento en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de propiedades de la directiva, seleccione **Protección del equipo en tiempo real**.
4. En la sección **Detección de comportamiento**, haga clic en **Configuración**.
5. Seleccione o desactive la casilla **Behavior Detection** para habilitar o deshabilitar el componente.
6. Vaya a la pestaña **General**.
7. Utilice la casilla **Habilitar protección de carpetas locales contra el cifrado externo** para habilitar o deshabilitar la opción. Si se selecciona esta casilla de verificación, Kaspersky Embedded Systems Security responde a la actividad maliciosa con la acción que se especifica a continuación.
8. Seleccione la acción correspondiente en el bloque **Acción al detectar actividad de malware**:
   - **Eliminar**. Si este elemento está seleccionado, al detectar actividad malintencionada, Kaspersky Embedded Systems Security elimina el archivo ejecutable de la aplicación malintencionada y crea una copia de seguridad del archivo en Copia de seguridad.
   - **Bloquear**. Si este elemento se encuentra seleccionado, Kaspersky Embedded Systems Security cierra la aplicación al detectar alguna actividad de software malintencionado.
   - **Informar**. Si este elemento está seleccionado y se detecta actividad de malware de una aplicación, Kaspersky Embedded Systems Security agrega información sobre la actividad de malware a la lista de amenazas activas.
9. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados .

Cómo habilitar o deshabilitar el componente Detección de comportamiento en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Protección del equipo en tiempo real** → **Detección de comportamiento** y haga clic en el botón **Configurar**.

   Se abre la ventana **Detección de comportamiento**.
5. Utilice la casilla **Habilitar Detección de comportamiento** para habilitar o deshabilitar el componente.
6. Vaya a la pestaña **General**.
7. Utilice la casilla **Habilitar protección de carpetas locales contra el cifrado externo** para habilitar o deshabilitar la opción. Si se selecciona esta casilla de verificación, Kaspersky Embedded Systems Security responde a la actividad maliciosa con la acción que se especifica a continuación.
8. Seleccione la acción correspondiente en el bloque **Al detectar intentos de cifrado externo en las carpetas compartidas**:

   - **Eliminar**. Si este elemento está seleccionado, al detectar actividad malintencionada, Kaspersky Embedded Systems Security elimina el archivo ejecutable de la aplicación malintencionada y crea una copia de seguridad del archivo en Copia de seguridad.
   - **Bloquear**. Si este elemento se encuentra seleccionado, Kaspersky Embedded Systems Security cierra la aplicación al detectar alguna actividad de software malintencionado.
   - **Informar**. Si este elemento está seleccionado y se detecta actividad de malware de una aplicación, Kaspersky Embedded Systems Security agrega información sobre la actividad de malware a la lista de amenazas activas.
9. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados.

Cómo habilitar o deshabilitar el componente Detección de comportamiento en la Consola de la aplicación

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Protección del equipo en tiempo real** → **Detección de comportamiento**.
2. En el panel de resultados del nodo **Detección de comportamiento**, haga clic en **Propiedades**.

   Se abre la ventana **Propiedades: Detección de comportamiento**.
3. Seleccione la casilla de verificación **Detección de comportamiento**.
4. Vaya a la pestaña **General**.

5. Utilice la casilla **Habilitar protección de carpetas locales contra el cifrado externo** para habilitar o deshabilitar la opción. Si se selecciona esta casilla de verificación, Kaspersky Embedded Systems Security responde a la actividad maliciosa con la acción que se especifica a continuación.

6. Seleccione la acción correspondiente en el bloque **Al detectar intentos de cifrado externo en las carpetas compartidas**:

   - **Eliminar**. Si este elemento está seleccionado, al detectar actividad malintencionada, Kaspersky Embedded Systems Security elimina el archivo ejecutable de la aplicación malintencionada y crea una copia de seguridad del archivo en Copia de seguridad.

   - **Bloquear**. Si este elemento se encuentra seleccionado, Kaspersky Embedded Systems Security cierra la aplicación al detectar alguna actividad de software malintencionado.

   - **Informar**. Si este elemento está seleccionado y se detecta actividad de malware de una aplicación, Kaspersky Embedded Systems Security agrega información sobre la actividad de malware a la lista de amenazas activas.

7. Guarde los cambios.

Protección de carpetas compartidas contra cifrado externo

Este componente supervisa solamente las operaciones realizadas con los archivos almacenados en dispositivos de almacenamiento masivo con el sistema de archivos NTFS y que no están cifrados con EFS.

La protección de las carpetas compartidas contra el cifrado externo permite el análisis de la actividad en carpetas compartidas. Cuando la actividad coincide con una firma de patrones de comportamiento que suele verse en actos de cifrado externo, Kaspersky Embedded Systems Security realiza la acción seleccionada.

Si Kaspersky Embedded Systems Security detecta un intento de modificar los archivos de las carpetas compartidas, realiza las siguientes acciones:

- Bloquea el acceso a la modificación del archivo para la sesión que originó la actividad maliciosa (el archivo será de solo lectura).

- Crea copias de seguridad de los archivos que se están modificando.

- Agrega una entrada a informes de la interfaz de la aplicación local y envía información sobre la actividad maliciosa detectada a Kaspersky Security Center.

- Además, si el componente Motor de reparación está habilitado, los archivos modificados se restaurarán de sus copias de seguridad.

Habilitación y deshabilitación de la protección de carpetas compartidas contra el cifrado externo

De manera predeterminada, la protección de carpetas compartidas contra el cifrado externo está habilitada y funciona en el modo recomendado por los especialistas de Kaspersky. Para configurar esta funcionalidad, puede crear un alcance de la protección y configurar exclusiones, si es necesario. De manera predeterminada, la aplicación identifica automáticamente las carpetas compartidas y supervisa la actividad de los archivos en todas las carpetas. Si se detecta un intento de cifrado externo de archivos en carpetas compartidas, Kaspersky Embedded Systems Security bloquea la sesión del usuario remoto durante una hora (de manera predeterminada).

Después de instalar Kaspersky Embedded Systems Security, la protección de carpetas compartidas contra cifrado externo será limitada hasta que se reinicie el equipo.

Cómo habilitar o deshabilitar la protección de carpetas compartidas contra el cifrado externo en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de propiedades de la directiva, seleccione **Protección del equipo en tiempo real**.
4. En la sección **Detección de comportamiento**, haga clic en **Configuración**.
5. Seleccione o desactive la casilla **Behavior Detection** para habilitar o deshabilitar el componente.
6. Vaya a la pestaña **Protección de carpetas compartidas**.
7. Utilice la casilla **Proteger carpetas compartidas** para habilitar o deshabilitar la opción.
8. Seleccione la acción correspondiente en el bloque **Protección de carpetas compartidas contra el cifrado externo**:

   - **Bloquear la conexión durante N min**. Si se elige esta opción, cuando Kaspersky Embedded Systems Security detecta un intento de modificar los archivos de una carpeta compartida, bloquea el acceso a la modificación de archivos (solo lectura) para la sesión que inició la actividad maliciosa y crea copias de seguridad de los archivos modificados.

     Si el componente Motor de reparación se habilita y la opción **Bloquear la conexión durante N minutos** se selecciona, los archivos modificados se restauran desde copias de seguridad.

   - **Informar**. Si se selecciona esta opción, si se detecta un intento de modificar archivos en carpetas compartidas, Kaspersky Embedded Systems Security agrega información acerca de este intento de modificación de archivos en carpetas compartidas a la lista de amenazas activas, agrega un registro a los informes de la interfaz local de la aplicación y envía información acerca de la detección de actividades maliciosas a Kaspersky Security Center.

9. Si es necesario, cree un alcance de la protección y configure exclusiones.
10. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados.

Cómo habilitar o deshabilitar la protección de carpetas compartidas contra el cifrado externo en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Protección del equipo en tiempo real** → **Detección de comportamiento** y haga clic en el botón **Configurar**.

   Se abre la ventana **Detección de comportamiento**.
5. Utilice la casilla **Habilitar Detección de comportamiento** para habilitar o deshabilitar el componente.
6. Vaya a la pestaña **Protección de carpetas compartidas**.
7. Utilice la casilla **Habilitar protección de carpetas compartidas contra el cifrado externo** para habilitar o deshabilitar la opción.
8. Seleccione la acción correspondiente en el bloque **Detección de cifrado externo**:
   - **Bloquear conexión**. Si se elige esta opción, cuando Kaspersky Embedded Systems Security detecta un intento de modificar los archivos de una carpeta compartida, bloquea el acceso a la modificación de archivos (solo lectura) para la sesión que inició la actividad maliciosa y crea copias de seguridad de los archivos modificados.

     Si el componente Motor de reparación se habilita y se selecciona la opción **Bloquear conexión**, los archivos modificados se restauran desde copias de seguridad.
   - **Informar**. Si se selecciona esta opción, si se detecta un intento de modificar archivos en carpetas compartidas, Kaspersky Embedded Systems Security agrega información acerca de este intento de modificación de archivos en carpetas compartidas a la lista de amenazas activas, agrega un registro a los informes de la interfaz local de la aplicación y envía información acerca de la detección de actividades maliciosas a Kaspersky Security Center.
9. Si es necesario, cree un alcance de la protección y configure exclusiones.
10. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados.

Cómo habilitar o deshabilitar la protección de carpetas compartidas contra el cifrado externo en la Consola de la aplicación

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Protección del equipo en tiempo real → Detección de comportamiento**.
2. En el panel de resultados del nodo **Detección de comportamiento**, haga clic en **Propiedades**.

   Se abre la ventana **Propiedades: Detección de comportamiento**.
3. Seleccione la casilla de verificación **Detección de comportamiento**.
4. Vaya a la pestaña **Protección de carpetas compartidas**.
5. Utilice la casilla **Proteger carpetas compartidas** para habilitar o deshabilitar la opción.
6. Seleccione la acción correspondiente en el bloque **Protección de carpetas compartidas contra el cifrado externo**:
   - **Bloquear conexión por N min**. Si se elige esta opción, cuando Kaspersky Embedded Systems Security detecta un intento de modificar los archivos de una carpeta compartida, bloquea el acceso a la modificación de archivos (solo lectura) para la sesión que inició la actividad maliciosa y crea copias de seguridad de los archivos modificados.

     Si el componente Motor de reparación se habilita y la opción **Bloquear conexión por N minutos** se selecciona, los archivos modificados se restauran desde copias de seguridad.
   - **Informar**. Si se selecciona esta opción, si se detecta un intento de modificar archivos en carpetas compartidas, Kaspersky Embedded Systems Security agrega información acerca de este intento de modificación de archivos en carpetas compartidas a la lista de amenazas activas, agrega un registro a los informes de la interfaz local de la aplicación y envía información acerca de la detección de actividades maliciosas a Kaspersky Security Center.
7. Si es necesario, cree un alcance de la protección y configure exclusiones.
8. Guarde los cambios.

Creación del área de protección

El *alcance de la protección* es una lista de rutas a carpetas compartidas en las que Kaspersky Embedded Systems Security supervisa la actividad de los archivos. Kaspersky Embedded Systems Security admite variables de entorno y los caracteres `*` y `?` cuando se ingresa una máscara: de manera predeterminada, la aplicación identifica automáticamente las carpetas compartidas y rastrea la actividad de los archivos en todas las carpetas.

Excluir una carpeta del alcance de la protección puede reducir la cantidad de falsos positivos si su organización utiliza el cifrado de datos cuando se intercambian archivos utilizando carpetas compartidas. Por ejemplo, el componente Detección de comportamiento puede generar falsos positivos cuando el usuario trabaja con archivos con la extensión ENC en una carpeta compartida. Dicha actividad coincide con un patrón de comportamiento típico del cifrado externo. Si tiene archivos cifrados en una carpeta compartida para proteger datos, agregue esa carpeta a las exclusiones.

También puede excluir los equipos si desea que se ignoren los intentos de cifrado externo que provienen de ellos.

Cómo configurar el alcance de la protección en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de propiedades de la directiva, seleccione **Protección del equipo en tiempo real**.
4. En la sección **Detección de comportamiento**, haga clic en **Configuración**.
5. Seleccione o desactive la casilla **Behavior Detection** para habilitar o deshabilitar el componente.
6. Vaya a la pestaña **Protección de carpetas compartidas**.
7. En el bloque **Alcance de la protección**, haga clic en el botón **Configurar**.
8. En la ventana que se abre, seleccione el modo **Solo las carpetas compartidas especificadas**.
9. Haga clic en **Agregar**.
10. Esto abre una ventana. En esa ventana, ingrese la ruta a la carpeta compartida que desee incluir en el alcance de la protección (por ejemplo, `C:\Share`).

    Para agregar una carpeta compartida al alcance de la protección, use una ruta de acceso local.

11. Haga clic en **Aceptar**.
12. Si es necesario, configure exclusiones del alcance de la protección:
    a. En el bloque **Exclusiones**, haga clic en el botón **Configurar**.
    b. Haga clic en el botón **Agregar** en la ventana que se abre.
    c. En la ventana que se muestra, escriba la ruta del archivo o la carpeta.

Usar máscaras:

- El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco C:, pero no en las subcarpetas.

- Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT ubicados en carpetas dentro de la `Folder`, excepto la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.

- El carácter `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las carpetas. Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.

Puede excluir un objeto del análisis sin eliminarlo de la lista de objetos en el alcance de la protección. Para hacerlo, desactive la casilla ubicada junto al objeto.

13. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados.

Cómo configurar el alcance de la protección en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Protección del equipo en tiempo real** → **Detección de comportamiento** y haga clic en el botón **Configurar**.

   Se abre la ventana **Detección de comportamiento**.
5. Utilice la casilla **Habilitar Detección de comportamiento** para habilitar o deshabilitar el componente.
6. Vaya a la pestaña **Protección de carpetas compartidas**.
7. En **Alcance de la protección**, seleccione el modo **Solo las carpetas compartidas especificadas**.
8. Haga clic en **Agregar**.
9. Esto abre una ventana. En esa ventana, ingrese la ruta a la carpeta compartida que desee incluir en el alcance de la protección (por ejemplo, `C:\Share`).

   Para agregar una carpeta compartida al alcance de la protección, use una ruta de acceso local.

10. Haga clic en **Aceptar**.

11. Si es necesario, configure exclusiones del alcance de la protección:

    a. En el bloque **Objeto que excluir**, haga clic en el botón **Agregar**.

    b. En la ventana que se muestra, escriba la ruta del archivo o la carpeta.

    Usar máscaras:

    - El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco C:, pero no en las subcarpetas.

    - Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT ubicados en carpetas dentro de la `Folder`, excepto la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.

    - El carácter `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las carpetas. Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.

    Puede excluir un objeto del análisis sin eliminarlo de la lista de objetos en el alcance de la protección. Para hacerlo, desactive la casilla ubicada junto al objeto.

12. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados.

Cómo configurar el alcance de la protección en la Consola de la aplicación

1. En la ventana de propiedades de la directiva, seleccione **Protección del equipo en tiempo real**.

2. En la sección **Detección de comportamiento**, haga clic en **Configuración**.

3. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Protección del equipo en tiempo real** → **Detección de comportamiento**.

4. En el panel de resultados del nodo **Detección de comportamiento**, haga clic en **Propiedades**.

   Se abre la ventana **Propiedades: Detección de comportamiento**.

5. Seleccione o desactive la casilla **Behavior Detection** para habilitar o deshabilitar el componente.

6. Vaya a la pestaña **Protección de carpetas compartidas**.

7. En el bloque **Área de protección**, haga clic en el botón **Configurar**.

8. En la ventana que se abre, seleccione el modo **Solo las carpetas compartidas especificadas**.

9. En el bloque **Área de protección**, haga clic en el botón **Agregar**.

10. Esto abre una ventana. En esa ventana, ingrese la ruta a la carpeta compartida que desee incluir en el alcance de la protección (por ejemplo, `C:\Share`).

    Para agregar una carpeta compartida al alcance de la protección, use una ruta de acceso local.

11. Haga clic en **Aceptar**.

12. Si es necesario, configure exclusiones del alcance de la protección:

    a. En el bloque **Exclusiones**, haga clic en el botón **Configuración**.

    b. En la ventana **Exclusiones por máscara** que se muestra, haga clic en el botón **Agregar**.

    c. En la ventana que se muestra, escriba la ruta del archivo o la carpeta.

    Usar máscaras:

    - El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco C:, pero no en las subcarpetas.

    - Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT ubicados en carpetas dentro de la `Folder`, excepto la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida.

    - El carácter `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las carpetas. Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.

    Puede excluir un objeto del análisis sin eliminarlo de la lista de objetos en el alcance de la protección. Para hacerlo, desactive la casilla ubicada junto al objeto.

13. Guarde los cambios.

Agregar equipos de confianza para el cifrado de datos externo

Si su organización utiliza cifrado de datos externo para el intercambio de archivos, debe crear una lista de equipos de confianza. Kaspersky Embedded Systems Security no supervisa el cifrado de datos realizado por equipos de confianza.

El servicio Audit Logon debe estar habilitado para permitir realizar exclusiones de direcciones desde Protección de carpetas compartidas contra el cifrado externo. De manera predeterminada, el servicio Inicio de sesión de auditoría está deshabilitado (para obtener información detallada sobre la habilitación del servicio Inicio de sesión de auditoría, visite el sitio web de Microsoft).

La funcionalidad para la exclusión de direcciones desde Protección de carpetas compartidas no funcionará en un equipo remoto si dicho equipo estaba encendido antes de iniciar Kaspersky Embedded Systems Security. Puede reiniciar el equipo remoto después de haber iniciado Kaspersky Embedded Systems Security para asegurarse de que la funcionalidad de excluir direcciones desde la protección de carpetas compartidas funcione en este equipo remoto.

Cómo agregar un equipo de confianza para el cifrado de datos en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de propiedades de la directiva, seleccione **Protección del equipo en tiempo real**.
4. En la sección **Detección de comportamiento**, haga clic en **Configuración**.
5. Vaya a la pestaña **Protección de carpetas compartidas**.
6. En el bloque **Exclusiones de direcciones IP**, haga clic en el botón **Configurar**.
7. Haga clic en el botón **Agregar** en la ventana que se abre.
8. Escriba la Dirección IP o el nombre del equipo desde el cual no se deben gestionar los intentos de cifrado.
9. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados .

Cómo agregar un equipo de confianza para el cifrado de datos en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.
   Se abre la ventana de propiedades de la directiva.

3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Protección del equipo en tiempo real** → **Detección de comportamiento** y haga clic en el botón **Configurar**.

   Se abre la ventana **Detección de comportamiento**.
5. Vaya a la pestaña **Protección de carpetas compartidas**.
6. En el bloque **Exclusiones**, haga clic en el botón **Agregar**.
7. Escriba la Dirección IP o el nombre del equipo desde el cual no se deben gestionar los intentos de cifrado.
8. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados.

Cómo agregar un equipo de confianza para el cifrado de datos en la Consola de la aplicación

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Protección del equipo en tiempo real** → **Detección de comportamiento**.
2. En el panel de resultados del nodo **Detección de comportamiento**, haga clic en **Propiedades**.

   Se abre la ventana **Propiedades: Detección de comportamiento**.
3. Vaya a la pestaña **Protección de carpetas compartidas**.
4. En el bloque **Exclusiones de direcciones IP**, haga clic en el botón **Configurar**.
5. Haga clic en el botón **Agregar** en la ventana que se abre.
6. Escriba la Dirección IP o el nombre del equipo desde el cual no se deben gestionar los intentos de cifrado.
7. Guarde los cambios.

Configurar el periodo de bloqueo de un equipo no confiable

Un *equipo no confiable* es un equipo remoto que forma parte de actividades maliciosas o cifrado de datos. De manera predeterminada, Kaspersky Embedded Systems Security bloquea la sesión de un usuario remoto durante una hora. Cuando el período de bloqueo caduca, Kaspersky Embedded Systems Security elimina el equipo de la lista de bloqueo y restaura el acceso a la carpeta compartida.

Cómo configurar el periodo de bloqueo de un equipo no confiable en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de propiedades de la directiva, seleccione **Protección del equipo en tiempo real**.

4. En la sección **Detección de comportamiento**, haga clic en **Configuración**.
5. Seleccione o desactive la casilla **Behavior Detection** para habilitar o deshabilitar el componente.
6. Vaya a la pestaña **Protección de carpetas compartidas**.
7. En **Al detectar intentos de cifrado externo en las carpetas compartidas**, configure el período de bloqueo de un equipo no confiable que forme parte de actividades maliciosas o cifrado de datos.
8. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados .

Cómo configurar el periodo de bloqueo de un equipo no confiable en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Protección del equipo en tiempo real** → **Detección de comportamiento** y haga clic en el botón **Configurar**.

   Se abre la ventana **Detección de comportamiento**.
5. Utilice la casilla **Habilitar Detección de comportamiento** para habilitar o deshabilitar el componente.
6. Vaya a la pestaña **Protección de carpetas compartidas**.
7. En **Detección de cifrado externo**, configure el período de bloqueo de un equipo no confiable que forme parte de actividades maliciosas o cifrado de datos.
8. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados .

Cómo configurar el período de bloqueo de un equipo no confiable en la Consola de la aplicación

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Protección del equipo en tiempo real** → **Detección de comportamiento**.
2. En el panel de resultados del nodo **Detección de comportamiento**, haga clic en **Propiedades**.

   Se abre la ventana **Propiedades: Detección de comportamiento**.
3. Seleccione la casilla de verificación **Detección de comportamiento**.
4. Vaya a la pestaña **Protección de carpetas compartidas**.
5. En **Protección de carpetas compartidas contra el cifrado externo**, configure el período de bloqueo de un equipo no confiable que forme parte de actividades maliciosas o cifrado de datos.
6. Guarde los cambios.

Exportar e importar una lista de exclusiones de la protección de carpetas compartidas contra el cifrado externo

Puede exportar la lista de exclusiones a un archivo XML. A continuación, puede modificar el archivo para, por ejemplo, agregar una gran cantidad de direcciones del mismo tipo. También puede utilizar la función de exportación/importación para realizar una copia de seguridad de la lista de exclusiones o para migrar la lista a un servidor diferente.

Cómo exportar e importar una lista de exclusiones en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de propiedades de la directiva, seleccione **Protección del equipo en tiempo real**.
4. En la sección **Detección de comportamiento**, haga clic en **Configuración**.
5. Vaya a la pestaña **Protección de carpetas compartidas**.
6. En el bloque **Exclusiones de direcciones IP**, haga clic en el botón **Configurar**.
7. Para exportar la lista de reglas:
   a. Si es necesario, seleccione las exclusiones que desea exportar.
   b. Haga clic en el botón y seleccione el modo de exportación: exportar la lista completa de exclusiones o solo las exclusiones seleccionadas.
   c. En la ventana que se abre, escriba el nombre del archivo XML en el que se exportará la lista de exclusiones. Seleccione también la carpeta en la que se guardará este archivo.
   d. Guarde el archivo.

      Kaspersky Embedded Systems Security exportará la lista de exclusiones al archivo XML.
8. Para importar la lista de exclusiones:
   a. Haga clic en el botón → **Importar**.

      En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de exclusiones.
   b. Abra el archivo.

      Kaspersky Embedded Systems Security importa las exclusiones.
9. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados.

Cómo exportar e importar una lista de exclusiones en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Protección del equipo en tiempo real** → **Detección de comportamiento** y haga clic en el botón **Configurar**.

   Se abre la ventana **Detección de comportamiento**.
5. Utilice la casilla **Habilitar Detección de comportamiento** para habilitar o deshabilitar el componente.
6. Vaya a la pestaña **Protección de carpetas compartidas**.
7. Para exportar la lista de exclusiones al bloque **Exclusiones**:
   a. Si es necesario, seleccione las exclusiones que desea exportar.
   b. Haga clic en el botón **Exportar** y seleccione el modo de exportación: exportar la lista completa de exclusiones o solo las exclusiones seleccionadas.
   c. Guarde el archivo.

      Kaspersky Embedded Systems Security exportará la lista de exclusiones al archivo XML.
8. Para importar la lista de exclusiones al bloque **Exclusiones**, haga lo siguiente:
   a. Haga clic en el botón **Importar** y seleccione un modo de importación: agregar o reemplazar.
   b. En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de exclusiones.
   c. Abra el archivo.

      Kaspersky Embedded Systems Security importa las exclusiones según el modo seleccionado.
9. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados.

Protección contra amenazas de red

El componente Protección contra amenazas de red analiza el tráfico de red entrante en busca de actividad típica de los ataques de red. Al detectar un intento de ataque de red que apunta a su equipo, Kaspersky Embedded Systems Security bloquea la actividad de red del equipo atacante. Las distintas clases de ataques de red sobre las que se tiene registro, así como las maneras de combatirlos, se describen en las bases de datos de la aplicación. La lista de ataques de red que detecta el componente Protección contra amenazas de red se actualiza durante las actualizaciones de las bases de datos y los módulos de la aplicación.

De forma predeterminada, la tarea *Protección contra amenazas de red* se ejecuta en el modo **Bloquear**. En este modo, Kaspersky Embedded Systems Security bloquea la conexión a los equipos que muestran actividad típica de ataques de red y, en algunos casos, agrega las direcciones IP de los equipos a la lista de sesiones de red bloqueadas.

Puede ver la lista de hosts bloqueados en el depósito de Hosts bloqueados.

La lista de equipos bloqueados se vacía cada vez que Kaspersky Embedded Systems Security se reinicia o cuando se modifica la configuración de Protección contra amenazas de red.

Puede restaurar el acceso a los hosts bloqueados y especificar la cantidad de días, horas y minutos tras la cual los hosts recuperarán el acceso a los recursos de archivos en red después de ser bloqueados a través de la configuración de almacenamiento para hosts bloqueados.

Las direcciones IP de los hosts que muestran la actividad típica de los ataques de red se eliminan de la lista de hosts bloqueados en los siguientes casos:

- Se desinstala Kaspersky Embedded Systems Security.
- La dirección IP se eliminó manualmente de la lista de hosts bloqueados.
- El plazo de bloqueo del host ha caducado.
- Se desactivó el modo **Bloquear**.

Cómo habilitar y configurar la Protección contra amenazas de red en la Consola de administración de Kaspersky Security Center

1. En el árbol de la consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados**.
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 de las propiedades de la directiva, vaya a la sección **Control de actividad de red**.
6. En el bloque **Protección contra amenazas de red**, haga clic en el botón **Configuración**.

   Se abre la ventana **Protección contra amenazas de red** en la pestaña **General**.

7. Seleccione la casilla **Protección contra amenazas de red** para habilitar el componente Protección contra amenazas de red.

8. En la sección **Modo de funcionamiento**, seleccione un modo para la tarea:

   - **Bloquear**. Si selecciona este modo, Kaspersky Embedded Systems Security analiza el tráfico de red entrante en busca de actividad típica de ataques de red, bloquea la conexión a los equipos que muestren esta actividad y, en algunos casos, agrega las direcciones IP de los equipos a la lista de sesiones de red bloqueadas. La aplicación también registra eventos sobre la actividad detectada típica de ataques de red en el registro de componentes.

   - **Informar**. Si selecciona este modo, Kaspersky Embedded Systems Security analiza el tráfico de red entrante en busca de actividad típica de ataques de red, pero no bloquea la conexión a los equipos que muestren esta actividad ni agrega las direcciones IP de los equipos a la lista de sesiones de red bloqueadas. La aplicación registra eventos sobre la actividad detectada típica de ataques de red en el registro de componentes.

9. Use la casilla **Tratar los análisis de puertos e inundaciones de red como ataques** para habilitar o deshabilitar la detección de ataques correspondientes.

10. Si es necesario, seleccione la casilla **Bloquear dispositivos atacantes durante N minutos**.

11. En el bloque **Protección contra suplantación de MAC**, seleccione o desactive la casilla de verificación **Habilitar la protección contra suplantación de MAC**.

12. Si es necesario, puede **agregar exclusiones del bloqueo**.

    Kaspersky Embedded Systems Security puede reconocer un ataque a la red y bloquear una conexión de red no segura que transmita una gran cantidad de paquetes (por ejemplo, desde cámaras de vigilancia). Para trabajar con dispositivos de confianza, puede agregar las direcciones IP de estos dispositivos a la lista de exclusiones. También puede seleccionar el protocolo y el puerto que se utilizan para la comunicación y permitir actividades de red específicas.

    > La capacidad de seleccionar protocolos y puertos para exclusiones se agregó en Kaspersky Embedded Systems Security 4.0. Asegúrese de que la aplicación y el complemento de administración estén actualizados a la versión 4.0 o posterior. Si está utilizando una versión anterior de la aplicación o el complemento de administración, Kaspersky Embedded Systems Security puede permitir actividades de red solo por dirección IP.

    a. Seleccione la ficha **Exclusiones**.

    b. Seleccione la casilla **No controlar las direcciones excluidas** para prevenir que Kaspersky Embedded Systems Security analice el tráfico entrante de la red para las direcciones IP excluidas.

    c. Haga clic en **Agregar**.

    d. En la ventana **Exclusiones**, ingrese la dirección IP del equipo desde el cual no se deben bloquear ataques de red.

    e. Si es necesario, seleccione el protocolo y los puertos a través de los cuales se transmiten los datos.

f. Haga clic en **Aceptar**.

g. Realice los pasos c al f para cada exclusión agregada.

13. Guarde los cambios.

Cómo habilitar y configurar la Protección contra amenazas de red en la Consola de la aplicación

1. En el árbol de la Consola de la aplicación, seleccione el nodo **Protección del equipo en tiempo real** → **Protección contra amenazas de red**.
2. Haga clic en el vínculo **Propiedades** del panel de resultados.

   Se abre la ventana **Propiedades: Protección contra amenazas de red**.
3. Seleccione la casilla **Protección contra amenazas de red** para habilitar el componente Protección contra amenazas de red.
4. En la sección **Modo de operación**, seleccione un modo para la tarea:
   - **Bloquear**. Si selecciona este modo, Kaspersky Embedded Systems Security analiza el tráfico de red entrante en busca de actividad típica de ataques de red, bloquea la conexión a los equipos que muestren esta actividad y, en algunos casos, agrega las direcciones IP de los equipos a la lista de sesiones de red bloqueadas. La aplicación también registra eventos sobre la actividad detectada típica de ataques de red en el registro de componentes.
   - **Informar**. Si selecciona este modo, Kaspersky Embedded Systems Security analiza el tráfico de red entrante en busca de actividad típica de ataques de red, pero no bloquea la conexión a los equipos que muestren esta actividad ni agrega las direcciones IP de los equipos a la lista de sesiones de red bloqueadas. La aplicación registra eventos sobre la actividad detectada típica de ataques de red en el registro de componentes.
5. Use la casilla **Tratar los análisis de puertos e inundaciones de red como ataques** para habilitar o deshabilitar la detección de ataques correspondientes.
6. Si es necesario, seleccione la casilla **Bloquear dispositivos atacantes durante N minutos**.
7. En el bloque **Protección contra suplantación de MAC**, seleccione o desactive la casilla de verificación **Habilitar la protección contra suplantación de MAC**.
8. Si es necesario, puede **agregar exclusiones del bloqueo**.

   Kaspersky Embedded Systems Security puede reconocer un ataque a la red y bloquear una conexión de red no segura que transmita una gran cantidad de paquetes (por ejemplo, desde cámaras de vigilancia). Para trabajar con dispositivos de confianza, puede agregar las direcciones IP de estos dispositivos a la lista de exclusiones. También puede seleccionar el protocolo y el puerto que se utilizan para la comunicación y permitir actividades de red específicas.

La capacidad de seleccionar protocolos y puertos para exclusiones se agregó en Kaspersky Embedded Systems Security 4.0. Asegúrese de que la aplicación y el complemento de administración estén actualizados a la versión 4.0 o posterior. Si está utilizando una versión anterior de la aplicación o el complemento de administración, Kaspersky Embedded Systems Security puede permitir actividades de red solo por dirección IP.

a. Seleccione la ficha **Exclusiones**.

b. Seleccione la casilla **No controlar las direcciones excluidas** para prevenir que Kaspersky Embedded Systems Security analice el tráfico entrante de la red para las direcciones IP excluidas.

c. Haga clic en **Agregar**.

d. En la ventana **Exclusiones**, ingrese la dirección IP del equipo desde el cual no se deben bloquear ataques de red.

e. Si es necesario, seleccione el protocolo y los puertos a través de los cuales se transmiten los datos.

f. Haga clic en **Aceptar**.

g. Realice los pasos c al f para cada exclusión agregada.

9. Guarde los cambios.

Cómo habilitar y configurar la Protección contra amenazas de red en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Seleccione **Control de actividad de red** → **Protección contra amenazas de red**.
5. Seleccione la casilla **Habilitar protección contra amenazas de red** en la pestaña **General** para habilitar el componente Protección contra amenazas de red.

6. Seleccionar el modo de operación de tareas:

   - **Bloquear**. Si selecciona este modo, Kaspersky Embedded Systems Security analiza el tráfico de red entrante en busca de actividad típica de ataques de red, bloquea la conexión a los equipos que muestren esta actividad y, en algunos casos, agrega las direcciones IP de los equipos a la lista de sesiones de red bloqueadas. La aplicación también registra eventos sobre la actividad detectada típica de ataques de red en el registro de componentes.

   - **Informar**. Si selecciona este modo, Kaspersky Embedded Systems Security analiza el tráfico de red entrante en busca de actividad típica de ataques de red, pero no bloquea la conexión a los equipos que muestren esta actividad ni agrega las direcciones IP de los equipos a la lista de sesiones de red bloqueadas. La aplicación registra eventos sobre la actividad detectada típica de ataques de red en el registro de componentes.

7. Use la casilla **Tratar los análisis de puertos e inundaciones de red como ataques** para habilitar o deshabilitar la detección de ataques correspondientes.

8. Si es necesario, seleccione la casilla **Bloquear dispositivos atacantes durante N minutos**.

9. Seleccione o desactive la casilla **Habilitar la protección contra suplantación de MAC**.

10. Si es necesario, puede **agregar exclusiones del bloqueo**.

    Kaspersky Embedded Systems Security puede reconocer un ataque a la red y bloquear una conexión de red no segura que transmita una gran cantidad de paquetes (por ejemplo, desde cámaras de vigilancia). Para trabajar con dispositivos de confianza, puede agregar las direcciones IP de estos dispositivos a la lista de exclusiones. También puede seleccionar el protocolo y el puerto que se utilizan para la comunicación y permitir actividades de red específicas.

    La capacidad de seleccionar protocolos y puertos para exclusiones se agregó en Kaspersky Embedded Systems Security 4.0. Asegúrese de que la aplicación y el complemento de administración estén actualizados a la versión 4.0 o posterior. Si está utilizando una versión anterior de la aplicación o el complemento de administración, Kaspersky Embedded Systems Security puede permitir actividades de red solo por dirección IP.

    a. Seleccione la ficha **Exclusiones**.

    b. Seleccione la casilla **No controlar las direcciones excluidas** para prevenir que Kaspersky Embedded Systems Security analice el tráfico entrante de la red para las direcciones IP excluidas.

    c. Haga clic en **Agregar**.

    d. En la ventana **Exclusiones**, ingrese la dirección IP del equipo desde el cual no se deben bloquear ataques de red.

    e. Si es necesario, seleccione el protocolo y los puertos a través de los cuales se transmiten los datos.

    f. Haga clic en **Aceptar**.

    g. Realice los pasos c al f para cada exclusión agregada.

11. Guarde los cambios.

Escáner AMSI

Cuando se ejecuta la tarea del Escáner AMSI, Kaspersky Embedded Systems Security controla la ejecución de los scripts creados con tecnologías de scripting de Microsoft Windows (Active Scripting) como VBScript o JScript. La aplicación también puede procesar los scripts de PowerShell y los scripts que se ejecutan en las aplicaciones de Microsoft Office en sistemas operativos con Antimalware Scan Interface (AMSI).

AMSI permite que las aplicaciones y los servicios se integren con cualquier aplicación antimalware instalada en un dispositivo para que el antimalware intercepte y analice todos los scripts ejecutados. Puede encontrar más información sobre la funcionalidad AMSI en el sitio web de Microsoft.

En la configuración del componente, puede permitir o denegar la ejecución de scripts peligrosos. Si Kaspersky Embedded Systems Security identifica un script como peligroso, bloquea o permite la ejecución del script de acuerdo con la acción seleccionada. Si selecciona la acción **Bloquear**, la aplicación bloquea los scripts peligrosos y permite otros scripts.

Kaspersky Embedded Systems Security admite la tecnología AMSI en Microsoft Windows 10 y Microsoft Windows Server 2016 y versiones posteriores.

Habilitar y deshabilitar el Escáner AMSI

Cómo habilitar o deshabilitar el Escáner AMSI en la Consola de administración de Kaspersky Security Center

1. Abra la configuración del Escáner AMSI en la directiva que desee configurar.

   a. En el árbol de la consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados**.

   b. Seleccione el grupo de administración para el cual desea configurar la tarea.

   c. Seleccione la pestaña **Directivas**.

   d. Haga doble clic en el nombre de la directiva para abrir la ventana de propiedades.

   e. En la ventana de las propiedades de la directiva, vaya a la sección **Protección del equipo en tiempo real**.

   f. En el bloque **Escáner AMSI**, haga clic en el botón **Configuración**.

   Se abre la ventana **Escáner AMSI** en la pestaña **General**.

2. Realice una de las siguientes acciones:

   - Seleccione la casilla de verificación **Escáner AMSI** si desea habilitar el Escáner AMSI.
   - Desactive la casilla **Escáner AMSI** si desea deshabilitar el Escáner AMSI.

3. En la ventana **Escáner AMSI**, haga clic en el botón **Aceptar**.
4. Haga clic en el botón **Aceptar** de la ventana **Propiedades: <Nombre de la directiva>**.

Cómo habilitar el Escáner AMSI en la Consola de Kaspersky Embedded Systems Security

1. En el árbol de la Consola de la aplicación, seleccione la sección **Protección del equipo en tiempo real → Escáner AMSI**.
2. Haga clic en el vínculo **Propiedades** del panel de resultados.
   Se abre la ventana **Escáner AMSI** en la pestaña **General**.
3. Realice una de las siguientes acciones:
   - Seleccione la casilla de verificación **Escáner AMSI** si desea habilitar el Escáner AMSI.
   - Desactive la casilla **Escáner AMSI** si desea deshabilitar el Escáner AMSI.
4. En la ventana **Escáner AMSI**, haga clic en el botón **Aceptar**.

Cómo habilitar Escáner AMSI en Kaspersky Security Center Web Console

1. Abra la configuración del Escáner AMSI en la directiva que desee configurar.
   a. En la ventana principal de Web Console, seleccione **Activos (dispositivos) → Directivas y perfiles**.
   b. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.
      Se abre la ventana de propiedades de la directiva.
   c. Seleccione la ficha **Configuración de la aplicación**.
   d. Seleccione la sección **Protección del equipo en tiempo real**.
   e. En el bloque **Escáner AMSI**, haga clic en el botón **Configurar**.
      Se abre la ventana **Escáner AMSI**.
2. Realice una de las siguientes acciones:
   - Seleccione la casilla de verificación **Escáner AMSI** si desea habilitar el Escáner AMSI.
   - Desactive la casilla **Escáner AMSI** si desea deshabilitar el Escáner AMSI.
3. Haga clic en el botón **Aceptar** de la ventana **Escáner AMSI**.
4. En la ventana **<Nombre de directiva>**, haga clic en **Guardar**.

Configuración del Escáner AMSI

Cómo configurar Escáner AMSI en la Consola de administración de Kaspersky Security Center

1. Abra la configuración del Escáner AMSI en la directiva que desee configurar.

   a. En el árbol de la consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados**.

   b. Seleccione el grupo de administración para el cual desea configurar la tarea.

   c. Seleccione la pestaña **Directivas**.

   d. Haga doble clic en el nombre de la directiva para abrir la ventana de propiedades.

   e. En la ventana de las propiedades de la directiva, vaya a la sección **Protección del equipo en tiempo real**.

   f. En el bloque **Escáner AMSI**, haga clic en el botón **Configuración**.

   Se abre la ventana **Escáner AMSI** en la pestaña **General**.

2. Seleccione la acción que desea que Kaspersky Embedded Systems Security realice cuando se ejecuta un script peligroso:

   - **Informar**. La aplicación permite la ejecución de scripts probablemente peligrosos. Se registra el evento correspondiente en registros de tareas.
   - **Bloquear**. La aplicación bloquea los scripts probablemente peligrosos.

3. En el bloque **Análisis de archivos compuestos**, especifique los tipos de archivos compuestos que desea analizar: archivos de almacenamiento, paquetes de distribución o archivos en formatos de Office.

4. En el bloque **Límite de tamaño**, realice una de las siguientes acciones:

   - Para que el componente Escáner AMSI no descomprima archivos compuestos de gran tamaño, seleccione la casilla **No desempaquetar archivos compuestos grandes** e ingrese el valor que considere apropiado en el campo **Tamaño máximo de archivo (MB)**. El componente Escáner AMSI ya no descomprimirá archivos compuestos que superen el tamaño especificado.
   - Para permitir que el componente Escáner AMSI descomprima archivos compuestos de gran tamaño, borre la selección de la casilla **No desempaquetar archivos compuestos grandes**.

   El componente Escáner AMSI analizará los archivos de gran tamaño que se extraigan de archivos de almacenamiento independientemente de si la casilla **No desempaquetar archivos compuestos grandes** está seleccionada.

5. En la ventana **Escáner AMSI**, haga clic en el botón **Aceptar**.

6. Haga clic en el botón **Aceptar** de la ventana **Propiedades: <Nombre de la directiva>**.

Cómo configurar Escáner AMSI en la Consola de Kaspersky Embedded Systems Security

1. En el árbol de la Consola de la aplicación, seleccione la sección **Protección del equipo en tiempo real** → **Escáner AMSI**.

2. Haga clic en el vínculo **Propiedades** del panel de resultados.

   Se abre la ventana **Escáner AMSI** en la pestaña **General**.

3. Seleccione la acción que desea que Kaspersky Embedded Systems Security realice cuando se ejecuta un script peligroso:

   - **Informar**. La aplicación permite la ejecución de scripts probablemente peligrosos. Se registra el evento correspondiente en registros de tareas.

   - **Bloquear**. La aplicación bloquea los scripts probablemente peligrosos.

4. En el bloque **Análisis de archivos compuestos**, especifique los tipos de archivos compuestos que desea analizar: archivos de almacenamiento, paquetes de distribución o archivos en formatos de Office.

5. En el bloque **Límite de tamaño**, realice una de las siguientes acciones:

   - Para que el componente Escáner AMSI no descomprima archivos compuestos de gran tamaño, seleccione la casilla **No desempaquetar archivos compuestos grandes** e ingrese el valor que considere apropiado en el campo **Tamaño máximo de archivo (MB)**. El componente Escáner AMSI ya no descomprimirá archivos compuestos que superen el tamaño especificado.

   - Para permitir que el componente Escáner AMSI descomprima archivos compuestos de gran tamaño, borre la selección de la casilla **No desempaquetar archivos compuestos grandes**.

   El componente Escáner AMSI analizará los archivos de gran tamaño que se extraigan de archivos de almacenamiento independientemente de si la casilla **No desempaquetar archivos compuestos grandes** está seleccionada.

6. En la ventana **Escáner AMSI**, haga clic en el botón **Aceptar**.

Cómo configurar Escáner AMSI en Kaspersky Security Center Web Console

1. Abra la configuración del Escáner AMSI en la directiva que desee configurar.

   a. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.

   b. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

      Se abre la ventana de propiedades de la directiva.

c. Seleccione la ficha **Configuración de la aplicación**.

d. Seleccione la sección **Protección del equipo en tiempo real**.

e. En el bloque **Escáner AMSI**, haga clic en el botón **Configurar**.

Se abre la ventana **Escáner AMSI**.

2. Seleccione la acción que desea que Kaspersky Embedded Systems Security realice cuando se ejecuta un script peligroso:

   - **Informar**. La aplicación permite la ejecución de scripts probablemente peligrosos. Se registra el evento correspondiente en registros de tareas.
   - **Bloquear**. La aplicación bloquea los scripts probablemente peligrosos.

3. En el bloque **Análisis de archivos compuestos**, especifique los tipos de archivos compuestos que desea analizar: archivos de almacenamiento, paquetes de distribución o archivos en formatos de Office.

4. En el bloque **Límite de tamaño**, realice una de las siguientes acciones:

   - Para que el componente Escáner AMSI no descomprima archivos compuestos de gran tamaño, seleccione la casilla **No desempaquetar archivos compuestos grandes** e ingrese el valor que considere apropiado en el campo **Tamaño máximo de archivo (MB)**. El componente Escáner AMSI ya no descomprimirá archivos compuestos que superen el tamaño especificado.
   - Para permitir que el componente Escáner AMSI descomprima archivos compuestos de gran tamaño, borre la selección de la casilla **No desempaquetar archivos compuestos grandes**.

   El componente Escáner AMSI analizará los archivos de gran tamaño que se extraigan de archivos de almacenamiento independientemente de si la casilla **No desempaquetar archivos compuestos grandes** está seleccionada.

5. Haga clic en el botón **Aceptar** de la ventana **Escáner AMSI**.

6. En la ventana **<Nombre de directiva>**, haga clic en **Guardar**.

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 permitir la ejecución de aplicaciones mediante la creación de reglas de autorización de Control de inicio de aplicaciones.

Todos los intentos de iniciar aplicaciones se registran en el registro de tareas.

La tarea Control de inicio de aplicaciones puede funcionar en uno de los dos modos siguientes:

- **Bloquear**. Kaspersky Embedded Systems Security controla la ejecución de aplicaciones mediante reglas de Control de inicio de aplicaciones. El alcance de las reglas de Control de inicio de aplicaciones se especifica en la configuración general de la tarea de Control de inicio de aplicaciones. Si una aplicación satisface las reglas de Control de inicio de aplicaciones, pero ninguna de las reglas coincide con el alcance de las reglas de Control de inicio de aplicaciones, se impide la ejecución de dichas aplicaciones.

  Se prohíbe la ejecución de aplicaciones que no están cubiertas por las reglas de Control de inicio de aplicaciones.

  La tarea **Control de inicio de aplicaciones** no puede iniciarse en el modo Activo si no se creó ninguna regla de Control de inicio de aplicaciones o si hay más de 65 535 reglas de Control de inicio de aplicaciones para un dispositivo protegido.

- **Informar**. Kaspersky Embedded Systems Security permite el inicio de todas las aplicaciones. Solo se registra información acerca de las ejecuciones de todas las aplicaciones, las reglas que cubren las aplicaciones ejecutadas y las acciones que se realizarían si la tarea se ejecutara en el modo **Bloquear**. Este modo está configurado de forma predeterminada.

Cuando crea reglas de Control de inicio de aplicaciones, le recomendamos que se asegure de que no bloqueen la ejecución de las aplicaciones de su sistema operativo.

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 de Control de inicio de aplicaciones detecta los inicios de aplicaciones y genera las reglas correspondientes para las aplicaciones que se ejecutan en Windows Subsystem for 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 aplicaciones. En consecuencia, se las llama reglas de *autorización* o *denegación*.

- Área de aplicación de regla.

  Las reglas de Control de inicio de aplicaciones pueden aplicarse a *archivos ejecutables*, *scripts* y *paquetes MSI*.

- Condiciones de activación de regla.

  Las reglas de Control de inicio de aplicaciones regulan la ejecución de archivos que satisfacen al menos una condición de activación especificada en la configuración de la regla. Por ejemplo, los archivos ejecutables se firman con el *certificado digital* especificado, tienen el *hash SHA256* especificado, están ubicados en la *ruta* especificada, coinciden con los argumentos de la *línea de comandos* especificados. Debe agregar al menos una condición de activación de regla. De lo contrario, no se agrega la regla Control de inicio de aplicaciones.

- Exclusiones de la regla.

  Puede configurar exclusiones para la regla de Control de inicio de aplicaciones, que pueden basarse en el mismo criterio que las condiciones de activación de regla. 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.

- Usuario o grupo de usuarios.

  Las reglas de Control de inicio de aplicaciones pueden controlar el inicio de aplicaciones especificadas por usuarios o grupos de usuarios.

Cuando crea reglas de Control de inicio de aplicaciones, le recomendamos que se asegure de que las nuevas reglas no bloqueen la ejecución de las aplicaciones de su sistema operativo.

Administración de Reglas de Control de inicio de aplicaciones

Puede realizar las siguientes acciones con las Reglas de Control de inicio de aplicaciones:

- Agregar manualmente.
- Generar y agregar reglas automáticamente
- Eliminar.
- Importar y exportar.
- Filtrar la lista de reglas.

Acerca del control de distribución de software

La generación del Control de inicio de aplicaciones puede volverse más complicada si desea controlar la distribución del software. Por ejemplo, es posible que quiera hacerlo en dispositivos protegidos donde el software instalado se actualiza automáticamente de forma regular. 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 Control de distribución de software.

Un *paquete de instalación* (en adelante, denominado "paquete") representa una o varias aplicaciones que se instalan en un dispositivo protegido. Un paquete de instalación también puede contener actualizaciones y comandos individuales.

El subsistema de Control de distribución de software se implementa como lista de exclusiones adicional. Cuando se agrega un paquete de instalación a la lista, el mismo se convierte en paquete de confianza. El desempaquetado de paquetes de confianza está permitido, y se permite también que las aplicaciones instaladas o actualizadas desde paquetes de confianza se inicien 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 el ciclo completo de la distribución de la aplicación y 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.

Para usar el Control de distribución de software, debe habilitar la funcionalidad **Aplicar reglas a archivos ejecutables** en la configuración general de Control de inicio de aplicaciones.

Caché de distribución del software

Kaspersky Embedded Systems Security utiliza una 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. De manera predeterminada, se permite el inicio de todos los archivos que tienen información guardada en la caché de distribución.

No puede revisar, eliminar ni modificar manualmente la caché de distribución mediante la interfaz de usuario. Kaspersky Embedded Systems Security completa y controla el caché.

Puede exportar la caché de distribución a un archivo de configuración (en formato XML) y eliminar la caché de distribución en la línea de comandos.

Para exportar el caché de distribución a un archivo de configuración, ejecute el siguiente comando:

```
kavshell appcontrol /config /savetofile:<full path> /sdc
```

Para eliminar la 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

Los archivos extraídos y los paquetes creados por un paquete de distribución de confianza principal (en el primer nivel de anidación) heredan el atributo de confianza cuando sus sumas de control se agregan a la caché de distribución al abrirse por primera vez el paquete de distribución de software de la lista de exclusiones. Por lo tanto, el propio paquete de distribución y todos los archivos extraídos de este paquete también serán de confianza.

Por ejemplo, si test.msi, un paquete que contiene varios paquetes y aplicaciones, se agrega a la lista de exclusiones y se selecciona la funcionalidad **Permitir la ejecución de todos los archivos secundarios como paquetes de distribución de confianza**, todos los paquetes y aplicaciones contenidos en el paquete test.msi se podrán descomprimir y ejecutar, incluso si contienen otros archivos anidados. Esta situación funciona para archivos extraídos en todos los niveles anidados.

Si el paquete test.msi se agrega a la lista de exclusiones y la funcionalidad **Permitir la ejecución de todos los archivos secundarios como paquetes de distribución de confianza** está deshabilitada, la aplicación asigna el atributo de confianza solo a aquellos paquetes y los archivos ejecutables que se extrajeron directamente del paquete de confianza (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.

Los archivos extraídos conservarán el atributo de confianza después de reiniciar el sistema operativo.

Para eliminar el atributo de herencia de todos los archivos extraídos, debe eliminar la caché de distribución y deshabilitar la funcionalidad **Permitir la ejecución de todos los archivos secundarios como paquetes de distribución de confianza** antes de volver a ejecutar el paquete de instalación de confianza.

Trabajar con la lista de reglas de Control de inicio de aplicaciones

La lista de paquetes de confianza del 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.

Acerca del Generador 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 dispositivos protegidos y los grupos de dispositivos protegidos en la red corporativa. Se recomiendan los siguientes escenarios si la red corporativa no tiene una máquina de referencia y no puede crear una lista de reglas de autorización basadas en las aplicaciones instaladas en la máquina modelo.

Puede ejecutar localmente la tarea Generador de reglas de Control de inicio de aplicaciones a través de la Consola de la aplicación para crear una lista de reglas basadas en las aplicaciones que se ejecutan en un solo dispositivo protegido.

Puede crear listas de reglas de Control de inicio de aplicaciones del lado de Kaspersky Security Center en uno de dos modos:

- Con la tarea de grupo Generador de reglas de 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 dispositivo protegido en la red y guarda esas listas a un archivo XML en la carpeta compartida especificada. El archivo XML generado con la tarea Generador de reglas de Control de inicio de aplicaciones contiene las reglas de autorización especificadas en la configuración de la tarea Control de inicio de aplicaciones antes de que se inicie la tarea. No se crearán reglas para aplicaciones cuya ejecución no se haya permitido en la configuración de la tarea. El inicio de tales aplicaciones se rechaza de forma predeterminada. Luego, puede importar manualmente la lista creada de reglas en la configuración de la tarea de Control de inicio de aplicaciones en la directiva de Kaspersky Security Center.

  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. Recomendamos configurar el inicio programado de la tarea Generador de reglas de Control de inicio de aplicaciones solo si el área de aplicación de las reglas de autorización incluye carpetas y archivos que usted sabe que son seguros.

  Antes de usar la tarea de Control de inicio de aplicaciones en la red, asegúrese de que todos los dispositivos protegidos puedan acceder a una carpeta compartida. Si la directiva de la organización no permite utilizar una carpeta compartida en la red, recomendamos que inicie la tarea Generador de reglas de Control de inicio de aplicaciones en un dispositivo protegido del grupo de dispositivos protegidos de prueba o en una máquina de referencia.

- Según el informe de eventos generado en Kaspersky Security Center para la tarea de Control de inicio de aplicaciones, se ejecuta en el modo *Informar*.

  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 *Informar*, informa todos los inicios de aplicaciones autorizados y denegados en todos los dispositivos protegidos de red en la pestaña **Eventos** del espacio de trabajo del nodo Servidor de administración de Kaspersky Security Center. Kaspersky Security Center utiliza los registros 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 se realicen durante el periodo especificado todos los escenarios posibles de dispositivos protegidos y grupos de dispositivos protegidos y, al menos, un reinicio del dispositivo protegido. Luego de que finalice el periodo de ejecución de la tarea, 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 dispositivos protegidos 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 dispositivo protegido se debe ejecutar bajo una directiva de Kaspersky Security Center activa. En este caso, todos los eventos en el dispositivo protegido se envían al Servidor de administración.

Le recomendamos actualizar la lista de reglas cuando el conjunto de aplicaciones instaladas en dispositivos protegidos 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 Generador de reglas de Control de inicio de aplicaciones o la tarea Control de inicio de aplicaciones en el modo *Informar* en dispositivos protegidos del grupo de administración de prueba. El grupo de administración de prueba incluye los dispositivos protegidos requeridos para evaluar el inicio de aplicaciones nuevas antes de que se instalen en dispositivos protegidos de red.

Los archivos XML que contienen listas de reglas de autorización se crean según un análisis de las tareas iniciadas en el dispositivo protegido. Para agrupar todas las aplicaciones utilizadas en la red al generar listas de reglas, le aconsejamos iniciar la tarea Generador de reglas de Control de inicio de aplicaciones y la tarea Control de inicio de aplicaciones en el modo *Informar* en una máquina modelo.

Antes de generar las reglas de autorización sobre la base de aplicaciones iniciadas en una máquina de referencia, asegúrese de que la máquina modelo 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.

Habilitar y configurar el Control de inicio de aplicaciones

Cómo habilitar y ajustar la configuración general para el Control de inicio de aplicaciones en la Consola de administración de Kaspersky Security Center

1. Abra la configuración de Control de inicio de aplicaciones en la directiva que desee configurar.

   a. En el árbol de la Consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados**.

   b. Seleccione el grupo de administración para el cual desea configurar la tarea.

c. Seleccione la ficha **Directivas**.

d. Haga doble clic en el nombre de la directiva que desea configurar.

e. En la ventana de las propiedades de la directiva, vaya a la sección **Control de actividad local**.

f. En el bloque **Control de inicio de aplicaciones**, haga clic en el botón **Configuración**.
Se abre la ventana **Control de inicio de aplicaciones** en la pestaña **General**.

2. Habilite **Control de inicio de aplicaciones** mediante la casilla de verificación con el mismo nombre.

3. En la sección **Modo de funcionamiento de las reglas de bloqueo**, configure las siguientes opciones:

- Modo de funcionamiento: de la tarea:
  - **Bloquear**. Kaspersky Embedded Systems Security aplica todas las reglas de Control de inicio de aplicaciones creadas.
  - **Informar**. Kaspersky Embedded Systems Security no utiliza las reglas de Control de inicio de aplicaciones. Solo guarda información sobre el inicio de las aplicaciones en el registro de la tarea. 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.
- Repetir la acción realizada durante el inicio del primer archivo en todos los inicios subsiguientes de este archivo.
- Denegar el inicio de los intérpretes de comando si no tienen ningún comando que ejecutar.

4. En la sección **Alcance de aplicación de la regla**, configure las siguientes opciones:

- Aplicar reglas a archivos ejecutables.
- Supervisar la carga de módulos DLL.

  El control de la carga de módulos DLL puede afectar el rendimiento del sistema operativo.

- Aplicar reglas a scripts y paquetes MSI.

5. En **Control de certificados**, habilite o deshabilite la funcionalidad Ignorar una marca de hora que no tiene firma al validar certificados.

6. En la ventana **Control de inicio de aplicaciones**, haga clic en **Aceptar** para guardar sus cambios.

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.

Cómo habilitar y ajustar la configuración general para el Control de inicio de aplicaciones en la Consola de Kaspersky Embedded Systems Security

1. En el árbol de la Consola de la aplicación, seleccione la sección **Control del equipo** → **Control de inicio de aplicaciones**.
2. Haga clic en el vínculo **Propiedades** del panel de resultados.

   Se abre la ventana **Control de inicio de aplicaciones** en la pestaña **General**.
3. Habilite **Control de inicio de aplicaciones** mediante la casilla de verificación con el mismo nombre.
4. En la sección **Modo de funcionamiento de las reglas de bloqueo**, configure las siguientes opciones:
   - Modo de funcionamiento: de la tarea:
     - **Bloquear**. Kaspersky Embedded Systems Security aplica todas las reglas de Control de inicio de aplicaciones creadas.
     - **Informar**. Kaspersky Embedded Systems Security no utiliza las reglas de Control de inicio de aplicaciones. Solo guarda información sobre el inicio de las aplicaciones en el registro de la tarea. 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.
   - Repetir la acción realizada durante el inicio del primer archivo en todos los inicios subsiguientes de este archivo.
   - Denegar el inicio de los intérpretes de comando si no tienen ningún comando que ejecutar.
5. En la sección **Alcance de aplicación de la regla**, configure las siguientes opciones:
   - Aplicar reglas a archivos ejecutables.
   - Supervisar la carga de módulos DLL.

     El control de la carga de módulos DLL puede afectar el rendimiento del sistema operativo.
   - Aplicar reglas a scripts y paquetes MSI.
6. En **Control de certificados**, habilite o deshabilite la funcionalidad Ignorar una marca de hora que no tiene firma al validar certificados.
7. En la ventana **Control de inicio de aplicaciones**, haga clic en **Aceptar** para guardar sus cambios.

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.

Cómo habilitar y ajustar la configuración general para el Control de inicio de aplicaciones en Kaspersky Security Center Web Console

1. Abra la configuración de Control de inicio de aplicaciones en la directiva que desee configurar.

   a. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.

   b. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.
   Se abre la ventana de propiedades de la directiva.

   c. Seleccione la ficha **Configuración de la aplicación**.

   d. Seleccione la sección **Control de actividad local**.

   e. En el bloque **Control de inicio de aplicaciones**, haga clic en el botón **Configurar**.
   Se abre la ventana **Control de inicio de aplicaciones** en la pestaña **General**.

2. Habilite **Control de inicio de aplicaciones** mediante la casilla de verificación con el mismo nombre.

3. En la sección **Modo de funcionamiento de las reglas de bloqueo**, configure las siguientes opciones:

   - Modo de funcionamiento: de la tarea:
     - **Bloquear**. Kaspersky Embedded Systems Security aplica todas las reglas de Control de inicio de aplicaciones creadas.
     - **Informar**. Kaspersky Embedded Systems Security no utiliza las reglas de Control de inicio de aplicaciones. Solo guarda información sobre el inicio de las aplicaciones en el registro de la tarea. 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.
   - Repetir la acción realizada durante el inicio del primer archivo en todos los inicios subsiguientes de este archivo.
   - Denegar el inicio de los intérpretes de comando si no tienen ningún comando que ejecutar.

4. En la sección **Alcance de aplicación de la regla**, configure las siguientes opciones:

   - Aplicar reglas a archivos ejecutables.
   - Supervisar la carga de módulos DLL.

     El control de la carga de módulos DLL puede afectar el rendimiento del sistema operativo.

   - Aplicar reglas a scripts y paquetes MSI.

5. En **Control de certificados**, habilite o deshabilite la funcionalidad Ignorar una marca de hora que no tiene firma al validar certificados.

6. En la ventana **Control de inicio de aplicaciones**, haga clic en **Aceptar** para guardar sus cambios.

7. Guarde la directiva modificada.

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

Cómo configurar el Control de distribución de software en la Consola de administración de Kaspersky Security Center

1. Abra la configuración de Control de inicio de aplicaciones en la directiva que desee configurar.

   a. En el árbol de la Consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados**.

   b. Seleccione el grupo de administración para el cual desea configurar la tarea.

   c. Seleccione la ficha **Directivas**.

   d. Haga doble clic en el nombre de la directiva que desea configurar.

   e. En la ventana de las propiedades de la directiva, vaya a la sección **Control de actividad local**.

   f. En el bloque **Control de inicio de aplicaciones**, haga clic en el botón **Configuración**.

   Se abre la ventana **Control de inicio de aplicaciones** en la pestaña **General**.

2. Seleccione la ficha **Control de distribución de software**.

3. Habilite la funcionalidad **Permitir la distribución automática de software mediante las aplicaciones y los paquetes de la lista**.

   Puede habilitar la funcionalidad **Permitir la distribución automática de software mediante las aplicaciones y los paquetes de la lista** si, en la pestaña **General**, la funcionalidad **Aplicar reglas a archivos ejecutables** está habilitada.

4. Si es necesario, deshabilite la funcionalidad **Permitir siempre la distribución de software a través de Windows Installer**.

   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.

5. Si es necesario, habilite la funcionalidad **Permitir siempre la distribución de software a través de SCCM mediante el Servicio de transferencia inteligente en segundo plano**.

   La aplicación controla el ciclo de distribución del software en el dispositivo protegido; 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 Kaspersky Embedded Systems Security en el dispositivo protegido.

6. Agregue archivos ejecutables y paquetes de instalación que desea permitir que se ejecuten:

   - **Agregar uno manualmente**

     a. En el menú contextual del botón **Agregar**, seleccione **Agregar un paquete de distribución**.

     b. Haga clic en el botón **Examinar** en la ventana que se abre.

     c. Seleccione el archivo ejecutable o el paquete de distribución.

     Los campos de **Criterios de confianza** se completan automáticamente con información del archivo seleccionado.

     d. Si es necesario, habilite la funcionalidad **Permitir la ejecución de todos los archivos secundarios como paquetes de distribución de confianza**.

     e. Seleccione el criterio que decidirá que el archivo ejecutable o el paquete de instalación es de confianza: **Detalles del certificado** o **Hash SHA256**.

     f. Haga clic en **Aceptar**.

     Se agrega el archivo ejecutable o paquete de instalación a la lista.

   - **Agregar varios por hash**

     a. En el menú contextual del botón **Agregar**, seleccione **Agregar varios paquetes por hash**.

     b. En la ventana que se abre, seleccione cualquier cantidad de archivos o paquetes de instalación.

     c. Haga clic en **Abrir**.

     Se agregan los archivos ejecutables o paquetes de instalación a la lista. Se especifica el hash SHA256 en sus propiedades.

   - **Importar de archivo**

     a. Haga clic en **Importar**.

     b. En la ventana que se abre, seleccione un archivo .TXT con información acerca de los archivos ejecutables y paquetes de instalación.

     c. Haga clic en **Abrir**.

Se agregan los archivos ejecutables o paquetes de instalación a la lista. Se especifica el hash SHA256 en sus propiedades.

Si crea un paquete de distribución de confianza basado en un archivo ejecutable luego de agregar, en la configuración de la Zona de confianza, un proceso basado en ese mismo archivo ejecutable que luego designó como de confianza para la tarea Control de inicio de aplicaciones, la configuración de la Zona de confianza tendrá mayor prioridad. Kaspersky Embedded Systems Security no permitirá iniciar el archivo ejecutable, pero considerará que el proceso de dicho archivo es de confianza.

7. Si es necesario, edite la lista de archivos ejecutables y paquetes de instalación adicionales haciendo clic en el botón **Modificar**.
8. Si es necesario, retire los archivos ejecutables y paquetes de instalación adicionales haciendo clic en el botón **Eliminar**. En este caso, se permite la ejecución de archivos ejecutables que no están dentro de paquetes.

   Para prevenir la ejecución de archivos ejecutables que no están dentro de paquetes, debe eliminar Kaspersky Embedded Systems Security del dispositivo protegido o crear reglas de denegación de Control de inicio de aplicaciones para los archivos que no están dentro de paquetes.

9. Haga clic en **Aceptar**.

Cómo configurar el Control de distribución de software en la Consola de Kaspersky Embedded Systems Security

1. En el árbol de la Consola de la aplicación, seleccione la sección **Control del equipo → Control de inicio de aplicaciones**.
2. Haga clic en el vínculo **Propiedades** del panel de resultados.

   Se abre la ventana **Control de inicio de aplicaciones** en la pestaña **General**.
3. Seleccione la ficha **Control de distribución de software**.
4. Habilite la funcionalidad **Permitir la distribución automática de software mediante las aplicaciones y los paquetes de la lista**.

   Puede habilitar la funcionalidad **Permitir la distribución automática de software mediante las aplicaciones y los paquetes de la lista** si, en la pestaña **General**, la funcionalidad **Aplicar reglas a archivos ejecutables** está habilitada.

5. Si es necesario, deshabilite la funcionalidad **Permitir siempre la distribución de software a través de Windows Installer**.

   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.

6. Si es necesario, habilite la funcionalidad **Permitir siempre la distribución de software a través de SCCM mediante el Servicio de transferencia inteligente en segundo plano**.

   La aplicación controla el ciclo de distribución del software en el dispositivo protegido; 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 Kaspersky Embedded Systems Security en el dispositivo protegido.

7. Agregue archivos ejecutables y paquetes de instalación que desea permitir que se ejecuten:

   - **Agregar uno manualmente**

     a. En el menú contextual del botón **Agregar**, seleccione **Agregar un paquete de distribución**.

     b. Haga clic en el botón **Examinar** en la ventana que se abre.

     c. Seleccione el archivo ejecutable o el paquete de distribución.

     Los campos de **Criterios de confianza** se completan automáticamente con información del archivo seleccionado.

     d. Si es necesario, habilite la funcionalidad **Permitir la ejecución de todos los archivos secundarios como paquetes de distribución de confianza**.

     e. Seleccione el criterio que decidirá que el archivo ejecutable o el paquete de instalación es de confianza: **Detalles del certificado** o **Hash SHA256**.

     f. Haga clic en **Aceptar**.

     Se agrega el archivo ejecutable o paquete de instalación a la lista.

   - **Agregar varios por hash**

     a. En el menú contextual del botón **Agregar**, seleccione **Agregar varios paquetes por hash**.

     b. En la ventana que se abre, seleccione cualquier cantidad de archivos o paquetes de instalación.

     c. Haga clic en **Abrir**.

     Se agregan los archivos ejecutables o paquetes de instalación a la lista. Se especifica el hash SHA256 en sus propiedades.

   - **Importar de archivo**

     a. Haga clic en **Importar**.

     b. En la ventana que se abre, seleccione un archivo .TXT con información acerca de los archivos ejecutables y paquetes de instalación.

     c. Haga clic en **Abrir**.

Se agregan los archivos ejecutables o paquetes de instalación a la lista. Se especifica el hash SHA256 en sus propiedades.

Si crea un paquete de distribución de confianza basado en un archivo ejecutable luego de agregar, en la configuración de la Zona de confianza, un proceso basado en ese mismo archivo ejecutable que luego designó como de confianza para la tarea Control de inicio de aplicaciones, la configuración de la Zona de confianza tendrá mayor prioridad. Kaspersky Embedded Systems Security no permitirá iniciar el archivo ejecutable, pero considerará que el proceso de dicho archivo es de confianza.

8. Si es necesario, edite la lista de archivos ejecutables y paquetes de instalación adicionales haciendo clic en el botón **Modificar**.
9. Si es necesario, retire los archivos ejecutables y paquetes de instalación adicionales haciendo clic en el botón **Eliminar**. En este caso, se permite la ejecución de archivos ejecutables que no están dentro de paquetes.

   Para prevenir la ejecución de archivos ejecutables que no están dentro de paquetes, debe eliminar Kaspersky Embedded Systems Security del dispositivo protegido o crear reglas de denegación de Control de inicio de aplicaciones para los archivos que no están dentro de paquetes.

10. Haga clic en **Aceptar**.

Cómo configurar el Control de distribución de software en Kaspersky Security Center Web Console

1. Abra la configuración de Control de inicio de aplicaciones en la directiva que desee configurar.

   a. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.

   b. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.

   c. Seleccione la ficha **Configuración de la aplicación**.

   d. Seleccione la sección **Control de actividad local**.

   e. En el bloque **Control de inicio de aplicaciones**, haga clic en el botón **Configurar**.

   Se abre la ventana **Control de inicio de aplicaciones** en la pestaña **General**.

2. Seleccione la ficha **Control de distribución de software**.
3. Habilite la funcionalidad **Permitir la distribución automática de software mediante las aplicaciones y los paquetes de la lista**.

   Puede habilitar la funcionalidad **Permitir la distribución automática de software mediante las aplicaciones y los paquetes de la lista** si, en la pestaña **General**, la funcionalidad **Aplicar reglas a archivos ejecutables** está habilitada.

4. Si es necesario, deshabilite la funcionalidad **Permitir siempre la distribución de software a través de Windows Installer**.

   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.

5. Si es necesario, habilite la funcionalidad **Permitir siempre la distribución de software a través de SCCM mediante el Servicio de transferencia inteligente en segundo plano**.

   La aplicación controla el ciclo de distribución del software en el dispositivo protegido; 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 Kaspersky Embedded Systems Security en el dispositivo protegido.

6. Agregue archivos ejecutables y paquetes de instalación que desea permitir que se ejecuten:

   - **De forma manual**

     a. Haga clic en el botón **Agregar**.

     b. En **Criterios de confianza**, seleccione el criterio que decidirá que el archivo ejecutable o el paquete de instalación es de confianza: **Usar certificado digital** o **Usar hash SHA256**.

     c. Si seleccionó **Usar certificado digital**, ingrese el encabezado y la huella digital del certificado con el que está firmado el archivo ejecutable o el paquete de instalación, además del nombre del archivo ejecutable o paquete de instalación.

     d. Si seleccionó **Usar hash SHA256**, haga clic en **Examinar** para seleccionar el archivo ejecutable o paquete de instalación.

     e. Si es necesario, habilite la funcionalidad **Permitir la ejecución de todos los archivos secundarios como paquetes de distribución de confianza**.

     f. Haga clic en **Aceptar**.

     Se agrega el archivo ejecutable o paquete de instalación a la lista.

   - **Importar de archivo**

     a. Haga clic en **Importar**.

     b. En la ventana que se abre, seleccione un archivo .TXT con información acerca de los archivos ejecutables y paquetes de instalación.

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

     Se agregan los archivos ejecutables o paquetes de instalación a la lista. Se especifica el hash SHA256 en sus propiedades.

Si crea un paquete de distribución de confianza basado en un archivo ejecutable luego de agregar, en la configuración de la Zona de confianza, un proceso basado en ese mismo archivo ejecutable que luego designó como de confianza para la tarea Control de inicio de aplicaciones, la configuración de la Zona de confianza tendrá mayor prioridad. Kaspersky Embedded Systems Security no permitirá iniciar el archivo ejecutable, pero considerará que el proceso de dicho archivo es de confianza.

7. Si es necesario, edite la lista de archivos ejecutables y paquetes de instalación adicionales haciendo clic en el botón **Modificar**.
8. Si es necesario, retire los archivos ejecutables y paquetes de instalación adicionales haciendo clic en el botón **Eliminar**. En este caso, se permite la ejecución de archivos ejecutables que no están dentro de paquetes.

   Para prevenir la ejecución de archivos ejecutables que no están dentro de paquetes, debe eliminar Kaspersky Embedded Systems Security del dispositivo protegido o crear reglas de denegación de Control de inicio de aplicaciones para los archivos que no están dentro de paquetes.

9. Haga clic en **Aceptar**.
10. Haga clic en el botón **Aceptar** de la ventana **Control de inicio de aplicaciones**.

Trabajar con las reglas de Control de inicio de aplicaciones

En esta sección se proporcionan instrucciones para crear una lista de reglas para el Control de inicio de aplicaciones.

Agregar reglas de Control de inicio de aplicaciones

Cómo agregar reglas de Control de inicio de aplicaciones en la Consola de administración de Kaspersky Security Center

1. Abra la configuración de Control de inicio de aplicaciones en la directiva que desee configurar.

   a. En el árbol de la Consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados**.

   b. Seleccione el grupo de administración para el cual desea configurar la tarea.

   c. Seleccione la ficha **Directivas**.

   d. Haga doble clic en el nombre de la directiva que desea configurar.

e. En la ventana de las propiedades de la directiva, vaya a la sección **Control de actividad local**.

f. En el bloque **Control de inicio de aplicaciones**, haga clic en el botón **Configuración**.

Se abre la ventana **Control de inicio de aplicaciones** en la pestaña **General**.

2. Seleccione la ficha **Reglas**.

3. En la lista desplegable **Aplicación de reglas**, seleccione el modo de aplicación de las reglas:

- **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.
- **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 de un grupo de dispositivos protegidos. Las listas de reglas locales no se pueden crear, modificar ni aplicar.

4. Si es necesario, habilite la funcionalidad **Denegar a los usuarios la modificación de reglas locales**.

Si se habilita esta funcionalidad, la aplicación no permite la edición local de las reglas de Control de inicio de aplicaciones en la Consola de la aplicación. De manera predeterminada, esta opción está deshabilitada.

5. Agregue reglas de Control de inicio de aplicaciones de una de las siguientes maneras:

- **Manualmente**.

a. Haga clic en **Agregar**.

Se abre la ventana **Control de inicio de aplicaciones**.

b. En el campo **Nombre**, escriba el nombre de la regla.

c. Si es necesario, en el campo **Descripción**, escriba la descripción de la regla.

d. En la lista desplegable **Tipo**, seleccione el tipo de regla:

- **De autorización** si desea que la regla permita la ejecución de las aplicaciones descritas por la regla.
- **De denegación** si desea que la regla bloquee la ejecución de las aplicaciones descritas por la regla.

e. 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. Se admiten archivos con las siguientes extensiones: .js, .vbs, .cmd, .bat, .py, .ps1, .pl, .msi, .msp, .mst, .com, .vbe, .jse, .psd1, .psm1, .pyd, .pyc, .pm, .hta, .chm, .wsf, .wsc, .wsh, .sct.

f. Seleccione la casilla **Actualizadores de confianza** si desea que Kaspersky Embedded Systems Security considere las aplicaciones que cumplen las condiciones de activación de la regla como actualizadores de confianza. Los Actualizadores de confianza son aplicaciones que pueden crear otros archivos ejecutables que podrán ejecutarse posteriormente.

Si una aplicación activa varias reglas, Kaspersky Embedded Systems Security establece el marcador de *Actualizadores de confianza* si se cumplen las siguientes condiciones:

- Todas las reglas permiten que la aplicación se ejecute.
- Al menos una regla tiene la casilla **Actualizadores de confianza** seleccionada.

g. Agregue condiciones de activación para la regla de Control de inicio de aplicaciones.

h. Agregue exclusiones de las condiciones de activación para la regla de Control de inicio de aplicaciones.

i. **Agregue usuarios o grupos de usuarios que tengan permitido o prohibido ejecutar aplicaciones que satisfacen la regla**.

a. Seleccione la ficha **Usuario o grupo**.

b. En el menú contextual del botón **Agregar**, seleccione el método para agregar usuarios o grupos.

c. En la ventana que se abre, ingrese o seleccione el nombre de un usuario o un grupo de usuarios.

d. Haga clic en **Aceptar**.

e. Complete los pasos b al d para cada usuario o grupo de usuarios.

j. Haga clic en **Aceptar**.

- **Mediante la importación de un archivo XML que contenga reglas de Control de inicio de aplicaciones**

a. En el menú contextual del botón , seleccione el elemento **Importar → Del archivo XML**.

b. Elija cómo se agregarán las reglas de Control de dispositivos del archivo XML a las que estén disponibles en la directiva:

- **Reemplazar reglas existentes**, si desea reemplazar las reglas existentes con las reglas importadas.
- **Agregar a reglas existentes**, si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con configuración idéntica se duplican.
- **Combinar con reglas existentes**, si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con configuración idéntica no se duplican. Si una regla tiene al menos un valor de configuración único, esa regla se agrega.

c. En la ventana que se abre, especifique la ruta al archivo XML que se haya creado al finalizar la tarea local o de grupo Generador de reglas de Control de inicio de aplicaciones.

d. Haga clic en **Abrir**.

- Según los eventos de Kaspersky Security Center mediante una solicitud.

  a. En el menú contextual del botón , seleccione el elemento **Importar → Crear reglas de autorización basadas en los eventos de Kaspersky Security Center (solicitud)**.

  b. 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**.

  c. Seleccione los tipos de eventos que la aplicación usará para crear las reglas de Control de inicio de aplicaciones:

  - **Inicio de la aplicación denegado**.
  - **Modo Solo estadísticas: inicio de aplicación denegado**.

  d. Seleccione un periodo de la lista desplegable **Solicitar eventos generados dentro del periodo**.

  e. Desactive o seleccione la casilla de verificación **Priorizar el uso del hash al generar reglas**.

  Si la casilla está seleccionada, Kaspersky Embedded Systems Security usa la suma de control del archivo para generar la regla cuando tanto la suma de control como el certificado del archivo están disponibles.

  Si la casilla está desactivada, Kaspersky Embedded Systems Security usa el certificado digital del archivo para generar la regla cuando tanto la suma de control como el certificado del archivo están disponibles.

  f. Haga clic en **Generar reglas**.

  g. Haga clic en **Aceptar**.

- Mediante la importación de un archivo TXT con una selección de eventos bloqueados de la aplicación de Kaspersky Security Center.

  1. En el árbol de la Consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados**.

  2. Seleccione el grupo de administración para el cual desea configurar la tarea.

  3. Seleccione la ficha **Directivas**.

4. Haga doble clic en el nombre de la directiva que desea configurar.
5. En la ventana de las propiedades de la directiva, vaya a la sección **Registros y notificaciones**.
6. En el bloque **Registros de tareas**, haga clic en el botón **Configuración**.

   Se abre la ventana **Notificaciones**.
7. Expanda el nodo **Control de actividad local**.
8. Seleccione la sección **Control de inicio de aplicaciones**.
9. En la lista de eventos del Control de inicio de aplicaciones, en la columna **Enviar eventos a Kaspersky Security Center**, seleccione las casillas junto a *Inicio de aplicación prohibido* y *Inicio de aplicación prohibido en el modo de prueba*.
10. Guarde los cambios.
11. En la sección **Configuración de eventos** de la directiva, asegúrese de que la duración del almacenamiento de eventos especificada en el campo **Guardar en la base de datos del Servidor de administración por (días)** sea mayor al periodo para el que tiene pensado recopilar información acerca de las ejecuciones de la aplicación que se impidieron (el valor predeterminado es 30 días).

    Una vez que se cumpla el periodo de retención de registros de tareas de Control de inicio de aplicaciones, los eventos registrados se eliminarán y no aparecerán en el informe.
12. Active la directiva configurada para recopilar datos acerca de las ejecuciones denegadas de la aplicación.
13. De ser necesario, modifique el modo de Control de inicio de aplicaciones.
14. Cuando se cumpla el periodo de recopilación de información acerca de las ejecuciones impedidas de la aplicación, realice una selección de eventos *Inicio de aplicación prohibido* y *Inicio de aplicación prohibido en el modo de prueba* y expórtela a un archivo TXT. Para obtener más información, consulte la sección "Selecciones de eventos" en la *Ayuda de Kaspersky Security Center*.
15. Abra el archivo TXT exportado.
16. Si es necesario, edite la lista de eventos.

Antes de importar los datos de las aplicaciones bloqueadas, asegúrese de que la lista que está importando contenga solo aplicaciones que desea permitir, y nada más.

a. En el menú contextual del botón , seleccione el elemento **Importar → Crear reglas de autorización basadas en el archivo TXT con eventos seleccionados de Kaspersky Security Center**.

b. Elija cómo se agregarán las reglas de Control de inicio de aplicaciones del informe a la lista de reglas que están disponibles en la directiva:

- **Combinar con reglas existentes**, si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con configuración idéntica no se duplican. Si una regla tiene al menos un valor de configuración único, esa regla se agrega.
- **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.

c. En la ventana del sistema de Windows que se abre, indique la ruta al archivo TXT al que se hayan exportado los eventos del informe sobre dispositivos bloqueados de Kaspersky Security Center.

d. Haga clic en **Abrir**.

Las reglas de Control de inicio de aplicaciones agregadas se muestran en la lista.

6. Si es necesario realice el paso 5 para agregar más reglas de Control de inicio de aplicaciones.
7. Si es necesario, edite las reglas de Control de inicio de aplicaciones agregadas; para ello, haga clic en el botón **Modificar**.
8. Si es necesario, elimine las reglas de Control de inicio de aplicaciones agregadas; para ello, haga clic en el botón **Eliminar**.
9. Haga clic en **Aceptar**.

Cómo agregar reglas de Control de inicio de aplicaciones en la Consola de Kaspersky Embedded Systems Security

1. En el árbol de la Consola de la aplicación, seleccione la sección **Control del equipo → Control de inicio de aplicaciones**.
2. Haga clic en el vínculo **Propiedades** del panel de resultados.

   Se abre la ventana **Control de inicio de aplicaciones** en la pestaña **General**.
3. Seleccione la ficha **Reglas**.

4. Agregue reglas de Control de inicio de aplicaciones de una de las siguientes maneras:

- **De forma manual**

  a. Haga clic en **Agregar**.

  Se abre la ventana **Control de inicio de aplicaciones**.

  b. En el campo **Nombre**, escriba el nombre de la regla.

  c. Si es necesario, en el campo **Descripción**, escriba la descripción de la regla.

  d. En la lista desplegable **Tipo**, seleccione el tipo de regla:

  - **De autorización** si desea que la regla permita la ejecución de las aplicaciones descritas por la regla.
  - **De denegación** si desea que la regla bloquee la ejecución de las aplicaciones descritas por la regla.

  e. 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. Se admiten archivos con las siguientes extensiones: .js, .vbs, .cmd, .bat, .py, .ps1, .pl, .msi, .msp, .mst, .com, .vbe, .jse, .psd1, .psm1, .pyd, .pyc, .pm, .hta, .chm, .wsf, .wsc, .wsh, .sct.

  f. Seleccione la casilla **Actualizadores de confianza** si desea que Kaspersky Embedded Systems Security considere las aplicaciones que cumplen las condiciones de activación de la regla como actualizadores de confianza. Los Actualizadores de confianza son aplicaciones que pueden crear otros archivos ejecutables que podrán ejecutarse posteriormente.

  Si una aplicación activa varias reglas, Kaspersky Embedded Systems Security establece el marcador de *Actualizadores de confianza* si se cumplen las siguientes condiciones:

  - Todas las reglas permiten que la aplicación se ejecute.
  - Al menos una regla tiene la casilla **Actualizadores de confianza** seleccionada.

  g. Agregue condiciones de activación para la regla de Control de inicio de aplicaciones.

  h. Agregue exclusiones de las condiciones de activación para la regla de Control de inicio de aplicaciones.

  i. **Agregue usuarios o grupos de usuarios que tengan permitido o prohibido ejecutar aplicaciones que satisfacen la regla**.

  a. Seleccione la ficha **Usuario o grupo**.

  b. En el menú contextual del botón **Agregar**, seleccione el método para agregar usuarios o grupos.

c. En la ventana que se abre, ingrese o seleccione el nombre de un usuario o un grupo de usuarios.

d. Haga clic en **Aceptar**.

e. Complete los pasos b al d para cada usuario o grupo de usuarios.

j. Haga clic en **Aceptar**.

- Mediante la importación de un archivo XML que contenga reglas de Control de inicio de aplicaciones.

a. En el menú contextual del botón , seleccione el elemento **Importar** → **Del archivo XML**.

b. Elija cómo se agregarán las reglas de Control de dispositivos del archivo XML a las que estén disponibles en la directiva:

- **Reemplazar reglas existentes**, si desea reemplazar las reglas existentes con las reglas importadas.
- **Agregar a reglas existentes**, si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con configuración idéntica se duplican.
- **Combinar con reglas existentes**, si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con configuración idéntica no se duplican. Si una regla tiene al menos un valor de configuración único, esa regla se agrega.

c. En la ventana que se abre, especifique la ruta al archivo XML que se haya creado al finalizar la tarea local o de grupo Generador de reglas de Control de inicio de aplicaciones.

d. Haga clic en **Abrir**.

Las reglas de Control de inicio de aplicaciones agregadas se muestran en la lista.

5. Si es necesario realice el paso 5 para agregar más reglas de Control de inicio de aplicaciones.
6. Si es necesario, edite las reglas de Control de inicio de aplicaciones agregadas; para ello, haga clic en el botón **Modificar**.
7. Si es necesario, elimine las reglas de Control de inicio de aplicaciones agregadas; para ello, haga clic en el botón **Eliminar**.
8. Haga clic en **Aceptar**.

Cómo agregar reglas de Control de inicio de aplicaciones en Kaspersky Security Center Web Console

1. Abra la configuración de Control de inicio de aplicaciones en la directiva que desee configurar.

   a. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.

   b. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.

   c. Seleccione la ficha **Configuración de la aplicación**.

   d. Seleccione la sección **Control de actividad local**.

   e. En el bloque **Control de inicio de aplicaciones**, haga clic en el botón **Configurar**.

   Se abre la ventana **Control de inicio de aplicaciones** en la pestaña **General**.

2. Seleccione la ficha **Reglas**.

3. En la lista desplegable **Aplicación de reglas**, seleccione el modo de aplicación de las reglas:

   - **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.
   - **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 de un grupo de dispositivos protegidos. Las listas de reglas locales no se pueden crear, modificar ni aplicar.

4. Si es necesario, habilite la funcionalidad **Denegar a los usuarios la modificación de reglas locales**.

5. Agregue reglas de Control de inicio de aplicaciones de una de las siguientes maneras:

   - De forma manual

     a. Haga clic en **Agregar**.

     Se abre la ventana **Configuración de la regla**.

     b. En el campo **Nombre**, escriba el nombre de la regla.

     c. En la lista desplegable **Tipo**, seleccione el tipo de regla:

     - **De autorización** si desea que la regla permita la ejecución de las aplicaciones descritas por la regla.
     - **De denegación** si desea que la regla bloquee la ejecución de las aplicaciones descritas por la regla.

d. 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.

e. Seleccione la casilla **Denegar a los demás usuarios** si desea que la aplicación bloquee la ejecución de las aplicaciones descritas por la regla para todos los usuarios que no aparecen en la pestaña **Usuario o grupo**.

f. Seleccione la casilla **Actualizadores de confianza** si desea que Kaspersky Embedded Systems Security considere las aplicaciones que cumplen las condiciones de activación de la regla como actualizadores de confianza. Los Actualizadores de confianza son aplicaciones que pueden crear otros archivos ejecutables que podrán ejecutarse posteriormente.

Si una aplicación activa varias reglas, Kaspersky Embedded Systems Security establece el marcador de *Actualizadores de confianza* si se cumplen las siguientes condiciones:

- Todas las reglas permiten que la aplicación se ejecute.
- Al menos una regla tiene la casilla **Actualizadores de confianza** seleccionada.

g. Agregue condiciones de activación para la regla de Control de inicio de aplicaciones.

h. Agregue exclusiones de las condiciones de activación para la regla de Control de inicio de aplicaciones.

i. **Agregue usuarios o grupos de usuarios que tengan permitido o prohibido ejecutar aplicaciones que satisfacen la regla**.

a. Seleccione la ficha **Usuario o grupo**.

b. Haga clic en **Agregar**.

c. En la ventana que se abre, ingrese o seleccione el nombre de un usuario o un grupo de usuarios.

d. Haga clic en **Seleccionar**.

e. Complete los pasos b al d para cada usuario o grupo de usuarios.

j. Haga clic en **Aceptar**.

Las reglas de Control de inicio de aplicaciones agregadas se muestran en la lista.

- **Mediante la importación de un archivo XML que contenga reglas de Control de inicio de aplicaciones.**

a. Haga clic en **Importar**.

b. En la ventana **Importar de archivo** que se muestra, haga clic en el botón **Seleccionar**.

c. Especifique la ruta al archivo XML que se haya creado al finalizar la tarea local o de grupo para Generador de reglas de Control de inicio de aplicaciones.

d. Haga clic en **Abrir**.

e. Haga clic en **Importar**.

Las reglas de Control de inicio de aplicaciones importadas se agregan a la lista de reglas existentes. Las reglas con configuración idéntica no se duplican. Si una regla tiene al menos un valor de configuración único, esa regla se agrega.

- Mediante la importación de un archivo XML que contenga reglas de Control de inicio de aplicaciones de Kaspersky Embedded Systems Security 4.0.

  a. Haga clic en **Importar desde la versión anterior**.

  b. En la ventana **Importar de archivo** que se muestra, haga clic en el botón **Seleccionar**.

  c. Especifique la ruta al archivo XML con las reglas de Control de inicio de aplicaciones que se exportaron de Kaspersky Embedded Systems Security 4.0.

  d. Haga clic en **Abrir**.

  e. Haga clic en **Importar**.

  Las reglas de Control de inicio de aplicaciones importadas se agregan a la lista de reglas existentes. Las reglas con configuración idéntica no se duplican. Si una regla tiene al menos un valor de configuración único, esa regla se agrega.

- Importando reglas desde el archivo de informe de Kaspersky Security Center.

  a. Haga clic en **Importar desde el informe de KSC**.

  b. En la ventana que se abre, seleccione el archivo TXT al que se exportaron los eventos del informe.

  c. Haga clic en **Abrir**.

  Las reglas basadas en el informe de Kaspersky Security Center se agregan a la lista de reglas de la directiva.

- Según los eventos de Kaspersky Security Center mediante una solicitud

  a. Haga clic en **Regla de autorización de eventos de KSC**.

  Se abre la ventana **Generador de reglas de Control de inicio de aplicaciones**.

b. Seleccione los tipos de eventos que la aplicación usará para crear las reglas de Control de inicio de aplicaciones:

- **Todos los eventos**.
- **Inicio de la aplicación denegado**.
- **Modo Solo estadísticas: inicio de aplicación denegado**.

c. Seleccione un periodo de la lista desplegable **Usar eventos generados dentro del periodo**.

d. Desactive o seleccione la casilla de verificación **Priorizar el uso del hash al generar reglas**.

Si la casilla está seleccionada, Kaspersky Embedded Systems Security usa la suma de control del archivo para generar la regla cuando tanto la suma de control como el certificado del archivo están disponibles.

Si la casilla está desactivada, Kaspersky Embedded Systems Security usa el certificado digital del archivo para generar la regla cuando tanto la suma de control como el certificado del archivo están disponibles.

e. Si es necesario, especifique el nombre del grupo de dispositivos administrados en el campo **Usar eventos generados para un grupo de dispositivos administrados**.

f. Haga clic en **Generar reglas**.

g. De la lista desplegable, **Regla para agregar a la lista principal**, 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.

h. Seleccione las reglas que desea exportar a las reglas de Control de inicio de aplicaciones de la directiva y haga clic en el botón **Exportar**.

i. Guarde los cambios.

6. Si es necesario realice el paso 5 para agregar más reglas de Control de inicio de aplicaciones.
7. Si es necesario, edite las reglas de Control de inicio de aplicaciones agregadas; para ello, haga clic en el botón **Modificar**.
8. Si es necesario, elimine las reglas de Control de inicio de aplicaciones agregadas; para ello, haga clic en el botón **Eliminar**.
9. Haga clic en **Aceptar**.

Agregar condiciones de activación para la regla de Control de inicio de aplicaciones

Cómo agregar condiciones de activación para la regla de Control de inicio de aplicaciones en la Consola de administración de Kaspersky Security Center

1. Abra la configuración de Control de inicio de aplicaciones en la directiva que desee configurar.

   a. En el árbol de la Consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados**.

   b. Seleccione el grupo de administración para el cual desea configurar la tarea.

   c. Seleccione la ficha **Directivas**.

   d. Haga doble clic en el nombre de la directiva que desea configurar.

   e. En la ventana de las propiedades de la directiva, vaya a la sección **Control de actividad local**.

   f. En el bloque **Control de inicio de aplicaciones**, haga clic en el botón **Configuración**.

   Se abre la ventana **Control de inicio de aplicaciones** en la pestaña **General**.

2. Seleccione la ficha **Reglas**.

3. Realice una de las siguientes acciones:

   a. Haga clic en el botón **Agregar** si agregará una nueva regla de Control de inicio de aplicaciones.

   b. En la lista de reglas de Control de inicio de aplicaciones, seleccione la regla para la que desea agregar condiciones de activación y haga clic en el botón **Modificar**.

   Se abre la ventana **Control de inicio de aplicaciones**.

4. En la pestaña **Condiciones**, en el menú contextual del botón **Agregar**, seleccione una condición de activación para la regla de Control de inicio de aplicaciones:

   - **Información del archivo**. Se utiliza Información del archivo seleccionado como condición de activación.

     a. Haga clic en el botón **Examinar** de la ventana **Información del archivo**.

     Se abre la ventana estándar **Abrir archivo** de Microsoft Windows.

     b. Seleccione el archivo.

     c. Haga clic en **Abrir**.

     Se muestra información acerca del archivo seleccionado en la ventana **Información del archivo**.

d. Seleccione al menos una opción:

- **Detalles del certificado**. Si se selecciona esta casilla, la regla no controla el inicio de las aplicaciones firmadas con un certificado digital que incluye los datos especificados.
- **Metadatos**. Si se selecciona esta casilla, la regla no controla el inicio de las aplicaciones que tienen los metadatos especificados.
- **Hash del archivo**. Si se selecciona esta casilla, la regla no controla el inicio de las aplicaciones que tienen el hash SHA256 especificado.
- **Ruta de archivo**. Si se selecciona esta casilla de verificación, la regla no controla la ejecución de las aplicaciones en la ruta especificada.

e. Si es necesario, en el campo **Línea de comandos**, ingrese el comando para iniciar la aplicación en la línea de comandos. La regla controla la ejecución de esta aplicación. Puede usar los caracteres ? Y * para ingresar una máscara.

> Kaspersky Embedded Systems Security no reconoce rutas de acceso que contengan barras invertidas ("/"). Use la barra invertida ("\") en las rutas.

f. Haga clic en **Aceptar**.

- **Tipo de unidad**. La regla controla la ejecución de aplicaciones desde todas las unidades extraíbles conectadas al equipo protegido.
- **Categoría KL**. La regla controla la ejecución de aplicaciones que pertenecen a las categorías KL seleccionadas.
- **Confiable según KSN**. La regla controla la ejecución de aplicaciones que son de confianza en KSN.
- **No confiable según KSN**. La regla controla la ejecución de aplicaciones que no son confiables en KSN.
- **Confiable según SO**. La regla controla el inicio de aplicaciones de confianza en el sistema operativo.

La condición agregada aparecerá en la lista.

5. Si es necesario, lleve a cabo el paso anterior de las instrucciones para cada una de las condiciones de activación de regla posteriores.
6. Si es necesario, edite las condiciones de activación de regla haciendo clic en el botón **Modificar**.
7. Guarde los cambios.

Cómo agregar condiciones de activación para la regla de Control de inicio de aplicaciones en la Consola de Kaspersky Embedded Systems Security

1. En el árbol de la Consola de la aplicación, seleccione la sección **Control del equipo → Control de inicio de aplicaciones**.
2. Haga clic en el vínculo **Propiedades** del panel de resultados.

   Se abre la ventana **Control de inicio de aplicaciones** en la pestaña **General**.
3. Seleccione la ficha **Reglas**.
4. Realice una de las siguientes acciones:

   a. Haga clic en el botón **Agregar** si agregará una nueva regla de Control de inicio de aplicaciones.

   b. En la lista de reglas de Control de inicio de aplicaciones, seleccione la regla para la que desea agregar condiciones de activación y haga clic en el botón **Modificar**.

   Se abre la ventana **Control de inicio de aplicaciones**.
5. En la pestaña **Condiciones**, en el menú contextual del botón **Agregar**, seleccione una condición de activación para la regla de Control de inicio de aplicaciones:

   - **Información del archivo**. Se utiliza Información del archivo seleccionado como condición de activación.

     a. Haga clic en el botón **Examinar** de la ventana **Información del archivo**.

     Se abre la ventana estándar **Abrir archivo** de Microsoft Windows.

     b. Seleccione el archivo.

     c. Haga clic en **Abrir**.

     Se muestra información acerca del archivo seleccionado en la ventana **Información del archivo**.

     d. Seleccione al menos una opción:

     - **Detalles del certificado**. Si se selecciona esta casilla, la regla no controla el inicio de las aplicaciones firmadas con un certificado digital que incluye los datos especificados.
     - **Metadatos**. Si se selecciona esta casilla, la regla no controla el inicio de las aplicaciones que tienen los metadatos especificados.
     - **Hash del archivo**. Si se selecciona esta casilla, la regla no controla el inicio de las aplicaciones que tienen el hash SHA256 especificado.
     - **Ruta de archivo**. Si se selecciona esta casilla de verificación, la regla no controla la ejecución de las aplicaciones en la ruta especificada.

e. Si es necesario, en el campo **Línea de comandos**, ingrese el comando para iniciar la aplicación en la línea de comandos. La regla controla la ejecución de esta aplicación. Puede usar los caracteres ? Y * para ingresar una máscara.

> Kaspersky Embedded Systems Security no reconoce rutas de acceso que contengan barras invertidas ("/"). Use la barra invertida ("\") en las rutas.

f. Haga clic en **Aceptar**.

- **Tipo de unidad**. La regla controla la ejecución de aplicaciones desde todas las unidades extraíbles conectadas al equipo protegido.
- **Categoría KL**. La regla controla la ejecución de aplicaciones que pertenecen a las categorías KL seleccionadas.
- **Confiable según KSN**. La regla controla la ejecución de aplicaciones que son de confianza en KSN.
- **No confiable según KSN**. La regla controla la ejecución de aplicaciones que no son confiables en KSN.
- **Confiable según SO**. La regla controla el inicio de aplicaciones de confianza en el sistema operativo.

La condición agregada aparecerá en la lista.

6. Si es necesario, lleve a cabo el paso anterior de las instrucciones para cada una de las condiciones de activación de regla posteriores.
7. Si es necesario, edite las condiciones de activación de regla haciendo clic en el botón **Modificar**.
8. Guarde los cambios.

Cómo agregar condiciones de activación para la regla de Control de inicio de aplicaciones en Kaspersky Security Center Web Console

1. Abra la configuración de Control de inicio de aplicaciones en la directiva que desee configurar.

   a. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.

   b. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.
   Se abre la ventana de propiedades de la directiva.

   c. Seleccione la ficha **Configuración de la aplicación**.

   d. Seleccione la sección **Control de actividad local**.

   e. En el bloque **Control de inicio de aplicaciones**, haga clic en el botón **Configurar**.
   Se abre la ventana **Control de inicio de aplicaciones** en la pestaña **General**.

2. Seleccione la ficha **Reglas**.

3. Haga clic en **Agregar**.

   Se abre la ventana **Configuración de la regla**.

4. En la ficha **Condiciones**, haga clic en el botón **Agregar**.

   Se abre la ventana **Configuración de la regla**.

5. Seleccione una condición de activación para la regla de Control de inicio de aplicaciones:

   - **Información del archivo**. Se utiliza Información del archivo como condición de activación.

     a. En **Criterios de activación de la regla**, especifique un valor para al menos un criterio:

     - **Certificado digital**. Si se selecciona esta casilla, la regla no controla el inicio de las aplicaciones firmadas con un certificado digital que incluye los datos especificados.
     - **Metadatos**. Si se selecciona esta casilla, la regla no controla el inicio de las aplicaciones que tienen los metadatos especificados.
     - **Hash SHA256**. Si se selecciona esta casilla, la regla no controla el inicio de las aplicaciones que tienen el hash SHA256 especificado.
     - **Ruta del archivo**. Si se selecciona esta casilla de verificación, la regla no controla la ejecución de las aplicaciones en la ruta especificada.

     b. Haga clic en **Aceptar**.

   - **De la categoría KL**. La regla controla la ejecución de aplicaciones que pertenecen a las categorías KL seleccionadas.
   - **Unidad extraíble**. La regla controla la ejecución de aplicaciones desde todas las unidades extraíbles conectadas al equipo protegido.
   - **Confiable según SO**. La regla controla el inicio de aplicaciones de confianza en el sistema operativo.

   La condición agregada aparecerá en la lista.

6. Si es necesario, lleve a cabo los pasos 4 y 5 de las instrucciones para cada una de las condiciones de activación de regla posteriores.

7. Si es necesario, edite las condiciones de activación de regla haciendo clic en el botón **Modificar**.

8. Guarde los cambios.

Agregar exclusiones del alcance de una regla de Control de inicio de aplicaciones

Cómo agregar exclusiones del alcance de la regla de Control de inicio de aplicaciones en la Consola de administración de Kaspersky Security Center

1. Abra la configuración de Control de inicio de aplicaciones en la directiva que desee configurar.

   a. En el árbol de la Consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados**.

   b. Seleccione el grupo de administración para el cual desea configurar la tarea.

   c. Seleccione la ficha **Directivas**.

   d. Haga doble clic en el nombre de la directiva que desea configurar.

   e. En la ventana de las propiedades de la directiva, vaya a la sección **Control de actividad local**.

   f. En el bloque **Control de inicio de aplicaciones**, haga clic en el botón **Configuración**.
   Se abre la ventana **Control de inicio de aplicaciones** en la pestaña **General**.

2. Seleccione la ficha **Reglas**.

3. Realice una de las siguientes acciones:

   a. Haga clic en el botón **Agregar** si agregará una nueva regla de Control de inicio de aplicaciones.

   b. En la lista de reglas de Control de inicio de aplicaciones, seleccione la regla para la que desea agregar exclusiones y haga clic en el botón **Modificar**.

   Se abre la ventana **Control de inicio de aplicaciones**.

4. En la pestaña **Exclusiones**, en el menú contextual del botón **Agregar**, seleccione un criterio para crear una exclusión del alcance en la regla de Control de inicio de aplicaciones:

   - **Información del archivo**. Se utiliza Información del archivo seleccionado como criterio.

     a. Haga clic en el botón **Examinar** de la ventana **Información del archivo**.
     Se abre la ventana estándar **Abrir archivo** de Microsoft Windows.

     b. Seleccione el archivo.

     c. Haga clic en **Abrir**.
     Se muestra información acerca del archivo seleccionado en la ventana **Información del archivo**.

d. Seleccione al menos una opción:

- **Detalles del certificado**. Si se selecciona esta casilla, la regla no controla el inicio de las aplicaciones firmadas con un certificado digital que incluye los datos especificados.
- **Metadatos**. Si se selecciona esta casilla, la regla no controla el inicio de las aplicaciones que tienen los metadatos especificados.
- **Hash del archivo**. Si se selecciona esta casilla, la regla no controla el inicio de las aplicaciones que tienen el hash SHA256 especificado.
- **Ruta de archivo**. Si se selecciona esta casilla de verificación, la regla no controla la ejecución de las aplicaciones en la ruta especificada.

e. Si es necesario, en el campo **Línea de comandos**, ingrese el comando para iniciar la aplicación en la línea de comandos. La regla no controla la ejecución de esta aplicación. Puede usar los caracteres ? Y * para ingresar una máscara.

> Kaspersky Embedded Systems Security no reconoce rutas de acceso que contengan barras invertidas ("/"). Use la barra invertida ("\") en las rutas.

f. Haga clic en **Aceptar**.

- **Tipo de unidad**. La regla no controla la ejecución de aplicaciones desde todas las unidades extraíbles conectadas al equipo protegido.
- **Categoría KL**. La regla no controla la ejecución de aplicaciones que pertenecen a las categorías KL seleccionadas.
- **Confiable según KSN**. La regla no controla la ejecución de aplicaciones que son de confianza en KSN.
- **No confiable según KSN**. La regla no controla la ejecución de aplicaciones que no son confiables en KSN.
- **Confiable según SO**. La regla no controla el inicio de aplicaciones de confianza en el sistema operativo.

La exclusión agregada aparecerá en la lista.

5. Si es necesario, realice el paso anterior de las instrucciones para agregar cada exclusión posterior del alcance de la regla de Control de inicio de aplicaciones.
6. Si es necesario, edite las exclusiones haciendo clic en el botón **Modificar**.
7. Guarde los cambios.

Cómo agregar exclusiones del alcance de la regla de Control de inicio de aplicaciones en la Consola de Kaspersky Embedded Systems Security

1. En el árbol de la Consola de la aplicación, seleccione la sección **Control del equipo** → **Control de inicio de aplicaciones**.
2. Haga clic en el vínculo **Propiedades** del panel de resultados.

   Se abre la ventana **Control de inicio de aplicaciones** en la pestaña **General**.
3. Seleccione la ficha **Reglas**.
4. Realice una de las siguientes acciones:

   a. Haga clic en el botón **Agregar** si agregará una nueva regla de Control de inicio de aplicaciones.

   b. En la lista de reglas de Control de inicio de aplicaciones, seleccione la regla para la que desea agregar exclusiones y haga clic en el botón **Modificar**.

   Se abre la ventana **Control de inicio de aplicaciones**.
5. En la pestaña **Exclusiones**, en el menú contextual del botón **Agregar**, seleccione un criterio para crear una exclusión del alcance en la regla de Control de inicio de aplicaciones:

   - **Información del archivo**. Se utiliza Información del archivo seleccionado como criterio.

     a. Haga clic en el botón **Examinar** de la ventana **Información del archivo**.

     Se abre la ventana estándar **Abrir archivo** de Microsoft Windows.

     b. Seleccione el archivo.

     c. Haga clic en **Abrir**.

     Se muestra información acerca del archivo seleccionado en la ventana **Información del archivo**.

     d. Seleccione al menos una opción:

     - **Detalles del certificado**. Si se selecciona esta casilla, la regla no controla el inicio de las aplicaciones firmadas con un certificado digital que incluye los datos especificados.
     - **Metadatos**. Si se selecciona esta casilla, la regla no controla el inicio de las aplicaciones que tienen los metadatos especificados.
     - **Hash del archivo**. Si se selecciona esta casilla, la regla no controla el inicio de las aplicaciones que tienen el hash SHA256 especificado.
     - **Ruta de archivo**. Si se selecciona esta casilla de verificación, la regla no controla la ejecución de las aplicaciones en la ruta especificada.

e. Si es necesario, en el campo **Línea de comandos**, ingrese el comando para iniciar la aplicación en la línea de comandos. La regla no controla la ejecución de esta aplicación. Puede usar los caracteres ? Y * para ingresar una máscara.

> Kaspersky Embedded Systems Security no reconoce rutas de acceso que contengan barras invertidas ("/"). Use la barra invertida ("\") en las rutas.

f. Haga clic en **Aceptar**.

- **Tipo de unidad**. La regla no controla la ejecución de aplicaciones desde todas las unidades extraíbles conectadas al equipo protegido.
- **Categoría KL**. La regla no controla la ejecución de aplicaciones que pertenecen a las categorías KL seleccionadas.
- **Confiable según KSN**. La regla no controla la ejecución de aplicaciones que son de confianza en KSN.
- **No confiable según KSN**. La regla no controla la ejecución de aplicaciones que no son confiables en KSN.
- **Confiable según SO**. La regla no controla el inicio de aplicaciones de confianza en el sistema operativo.

La exclusión agregada aparecerá en la lista.

6. Si es necesario, realice el paso anterior de las instrucciones para agregar cada exclusión posterior del alcance de la regla de Control de inicio de aplicaciones.
7. Si es necesario, edite las exclusiones haciendo clic en el botón **Modificar**.
8. Guarde los cambios.

Cómo agregar exclusiones del alcance de la regla de Control de inicio de aplicaciones en Kaspersky Security Center Web Console

1. Abra la configuración de Control de inicio de aplicaciones en la directiva que desee configurar.

   a. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.

   b. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.
   Se abre la ventana de propiedades de la directiva.

   c. Seleccione la ficha **Configuración de la aplicación**.

   d. Seleccione la sección **Control de actividad local**.

   e. En el bloque **Control de inicio de aplicaciones**, haga clic en el botón **Configurar**.
   Se abre la ventana **Control de inicio de aplicaciones** en la pestaña **General**.

2. Seleccione la ficha **Reglas**.

3. Haga clic en **Agregar**.

   Se abre la ventana **Configuración de la regla**.

4. En la ficha **Exclusiones**, haga clic en el botón **Agregar**.

   Se abre la ventana **Configuración de la regla**.

5. Seleccione un criterio para crear una exclusión del alcance de la regla de Control de inicio de aplicaciones:

   - **Información del archivo**. La regla no controla el inicio de aplicaciones cuyos datos coinciden con los datos en el archivo.

     a. En **Criterios de activación de la regla**, especifique un valor para al menos un criterio:

     - **Certificado digital**. Si se selecciona esta casilla, la regla no controla el inicio de las aplicaciones firmadas con un certificado digital que incluye los datos especificados.
     - **Metadatos**. Si se selecciona esta casilla, la regla no controla el inicio de las aplicaciones que tienen los metadatos especificados.
     - **Hash SHA256**. Si se selecciona esta casilla, la regla no controla el inicio de las aplicaciones que tienen el hash SHA256 especificado.
     - **Ruta del archivo**. Si se selecciona esta casilla de verificación, la regla no controla la ejecución de las aplicaciones en la ruta especificada.

     b. Haga clic en **Aceptar**.

   - **Categoría KL**. La regla no controla la ejecución de aplicaciones que pertenecen a las categorías KL seleccionadas.
   - **Tipo de unidad**. La regla no controla la ejecución de aplicaciones desde todas las unidades extraíbles conectadas al equipo protegido.
   - **Confiable según SO**. La regla no controla el inicio de aplicaciones de confianza en el sistema operativo.

   La condición agregada aparecerá en la lista.

6. Si es necesario, realice los pasos 4 a 5 de las instrucciones para agregar cada exclusión posterior del alcance de la regla de Control de inicio de aplicaciones.

7. Si es necesario, edite las exclusiones haciendo clic en el botón **Modificar**.

8. Guarde los cambios.

Habilitación del modo Habilitación predeterminada

Puede permitir la ejecución de todas las aplicaciones mediante reglas de autorización del Control de inicio de aplicaciones configuradas especialmente.

Para permitir la ejecución de todas las aplicaciones:

1. Agregue manualmente dos reglas de autorización del Control de inicio de aplicaciones con los siguientes parámetros:
   - Tipo de regla: *Permitir*, Alcance: *Archivos ejecutables*, Ruta del archivo: `?:\`.
   - Tipo de regla: *Permitir*, Alcance: *Scripts y paquetes MSI*, Ruta del archivo: `?:\`.
2. Si se agregaron reglas de denegación del Control de inicio de aplicaciones, elimínelas.
3. Para todas las reglas de autorización del Control de inicio de aplicaciones creadas previamente, elimine las exclusiones.
4. Guarde los cambios.

Generar un archivo TXT con una selección de eventos bloqueados de la aplicación de Kaspersky Security Center

Puede exportar una selección de eventos bloqueados de la aplicación de Kaspersky Security Center a un archivo TXT y, luego, importar estos datos para generar una lista de reglas de autorización del Control de inicio de aplicaciones en una directiva que está configurando.

Cómo generar un archivo TXT con una selección de eventos bloqueados de la aplicación de Kaspersky Security Center con la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados**.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Seleccione la ficha **Directivas**.
4. Haga doble clic en el nombre de la directiva que desea configurar.
5. En la ventana de las propiedades de la directiva, vaya a la sección **Registros y notificaciones**.
6. En el bloque **Registros de tareas**, haga clic en el botón **Configuración**.

   Se abre la ventana **Notificaciones**.
7. Expanda el nodo **Control de actividad local**.
8. Seleccione la sección **Control de inicio de aplicaciones**.
9. En la lista de eventos del Control de inicio de aplicaciones, en la columna **Enviar eventos a Kaspersky Security Center**, seleccione las casillas junto a *Inicio de aplicación prohibido* y *Inicio de aplicación prohibido en el modo de prueba*.
10. Guarde los cambios.

11. En la sección **Configuración de eventos** de la directiva, asegúrese de que la duración del almacenamiento de eventos especificada en el campo **Guardar en la base de datos del Servidor de administración por (días)** sea mayor al periodo para el que tiene pensado recopilar información acerca de las ejecuciones de la aplicación que se impidieron (el valor predeterminado es 30 días).

    Una vez que se cumpla el periodo de retención de registros de tareas de Control de inicio de aplicaciones, los eventos registrados se eliminarán y no aparecerán en el informe.

12. Active la directiva configurada para recopilar datos acerca de las ejecuciones denegadas de la aplicación.
13. De ser necesario, modifique el modo de Control de inicio de aplicaciones.
14. Cuando se cumpla el periodo de recopilación de información acerca de las ejecuciones impedidas de la aplicación, realice una selección de eventos *Inicio de aplicación prohibido* y *Inicio de aplicación prohibido en el modo de prueba* y expórtela a un archivo TXT. Para obtener más información, consulte la sección "Selecciones de eventos" en la *Ayuda de Kaspersky Security Center*.
15. Abra el archivo TXT exportado.
16. Si es necesario, edite la lista de eventos.

Cómo generar un archivo TXT con una selección de eventos bloqueados de la aplicación de Kaspersky Security Center con Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

    Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Seleccione la sección **Registros y notificaciones**.
5. En el bloque **Registros de tareas**, haga clic en el botón **Configurar**.

    Se abre la ventana **Registros de tareas**.
6. Seleccione la sección **Control de inicio de aplicaciones**.
7. En la lista de eventos del Control de inicio de aplicaciones, en la columna **Enviar eventos a Kaspersky Security Center**, seleccione las casillas junto a *Inicio de aplicación prohibido* y *Inicio de aplicación prohibido en el modo de prueba*.
8. Guarde los cambios.

9. En la pestaña **Configuración de eventos** de la directiva que está configurando, asegúrese de que la duración del almacenamiento de eventos especificada en el campo **Guardar en la base de datos del Servidor de administración por (días)** sea mayor al periodo para el que tiene pensado recopilar información acerca de las ejecuciones de la aplicación que se impidieron (el valor predeterminado es 30 días).

   Una vez que se cumpla el periodo de retención de registros de tareas de Control de inicio de aplicaciones, los eventos registrados se eliminarán y no aparecerán en el informe.

10. Active la directiva configurada para recopilar datos acerca de las ejecuciones denegadas de la aplicación.
11. De ser necesario, modifique el modo de Control de inicio de aplicaciones.
12. Cuando se cumpla el periodo de recopilación de información acerca de las ejecuciones impedidas de la aplicación, realice una selección de eventos *Inicio de aplicación prohibido* y *Inicio de aplicación prohibido en el modo de prueba* y expórtela a un archivo TXT. Para obtener más información, consulte la sección "Selecciones de eventos" en la *Ayuda de Kaspersky Security Center*.
13. Abra el archivo TXT exportado.
14. Si es necesario, edite la lista de eventos.

Configurar una tarea de grupo de Generador de reglas de Control de inicio de aplicaciones

Cómo configurar la tarea de grupo Generador de reglas de Control de inicio de aplicaciones en la Consola de administración de Kaspersky Security Center

1. Abra las propiedades de la tarea Generador de reglas de Control de inicio de aplicaciones.

   a. En el árbol de la Consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados**.

   b. Seleccione el grupo de administración para el cual desea configurar la tarea.

   c. Seleccione la ficha **Tareas**.

   d. En la lista de tareas de grupo, abra la tarea Generador de reglas de Control de inicio de aplicaciones con un doble clic en el nombre de la tarea.

   Se abre la ventana **Propiedades: Generador de reglas de Control de inicio de aplicaciones**.

2. Vaya a la sección **Opciones**.
3. Si es necesario, en la pestaña **Reglas**, ingrese un prefijo para nombres de reglas.

4. En **Área de aplicación de las reglas de autorización**, especifique el método que desea usar para crear reglas de autorización:

   - Crear reglas de autorización para las aplicaciones en ejecución.
   - Crear reglas de autorización para las aplicaciones de las carpetas.

5. En la pestaña **Configuración**, seleccione el criterio que la tarea aplicará durante la creación de 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.

6. Configure la opción **Agregar una ruta de archivo para las reglas generadas a partir de sumas de hash**.

   Si selecciona esta casilla, al exportar las reglas, Kaspersky Embedded Systems Security agrega rutas completas a los archivos ejecutables en el archivo XML. Con las rutas completas, es posible saber a qué software pertenece un archivo ejecutable.

   Si la casilla no está seleccionada, el archivo XML solo contiene nombres y hashes SHA256 de archivos ejecutables. De forma predeterminada, la casilla no está activada.

7. Agregue usuarios o grupos de usuarios que desea que puedan ejecutar aplicaciones que satisfacen las reglas creadas mediante la tarea.

   a. En el menú contextual del botón **Agregar**, seleccione el método para agregar usuarios o grupos.

   b. En la ventana que se abre, ingrese o seleccione el nombre de un usuario o un grupo de usuarios.

   c. Haga clic en **Aceptar**.

   d. Complete los pasos a al c para cada usuario o grupo de usuarios.

8. 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.
   - Principio de adición.
   - **Exportar reglas de autorización a archivo**. Puede hacer clic en el botón **Examinar** para especificar una ruta en la que Kaspersky Embedded Systems Security guardará un archivo XML con las reglas de autorización exportadas cuando finaliza la tarea Generador de reglas de Control de inicio de aplicaciones.
   - Agregar detalles del dispositivo protegido al nombre del archivo.

9. Si es necesario, en la pestaña **Exclusiones**, especifique los objetos que desea excluir del alcance de la tarea.

10. Haga clic en el botón **Aceptar** de la ventana **Propiedades: Generador de reglas de Control de inicio de aplicaciones**.

Cómo configurar la tarea de grupo Generador de reglas de Control de inicio de aplicaciones en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Tareas**.
2. En la lista de tareas de grupo, abra la tarea Generador de reglas de Control de inicio de aplicaciones.

   Se abre la ventana **Generador de reglas de Control de inicio de aplicaciones**.
3. Abra la pestaña **Configuración de la aplicación**.
4. Si es necesario, en la sección **Área de aplicación de las reglas de autorización**, ingrese un prefijo para nombres de reglas.
5. En **Área de aplicación de las reglas de autorización**, especifique el método que desea usar para crear reglas de autorización:
   - Crear reglas de autorización para las aplicaciones en ejecución
   - Crear reglas de autorización para las aplicaciones de las carpetas
6. En la pestaña **Parámetros**, seleccione el criterio que la tarea aplicará durante la creación de 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.
7. Configure la opción **Agregar una ruta de archivo para las reglas generadas a partir de sumas de hash**.

   Si selecciona esta casilla, al exportar las reglas, Kaspersky Embedded Systems Security agrega rutas completas a los archivos ejecutables en el archivo XML. Con las rutas completas, es posible saber a qué software pertenece un archivo ejecutable.

   Si la casilla no está seleccionada, el archivo XML solo contiene nombres y hashes SHA256 de archivos ejecutables. De forma predeterminada, la casilla no está activada.
8. Agregue usuarios o grupos de usuarios que desea que puedan ejecutar aplicaciones que satisfacen las reglas creadas mediante la tarea.

   a. Haga clic en **Seleccionar usuario o grupo**.

   b. En la ventana que se abre, ingrese o seleccione el nombre de un usuario o un grupo de usuarios.

   c. Haga clic en **Seleccionar**.

   d. Complete los pasos a al c para cada usuario o grupo de usuarios.

9. 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.
   - Principio de adición.
   - **Las reglas de autorización se exportarán a un archivo**. En el campo **Especificar la ruta completa al archivo con extensión .xml**, puede especificar una ruta en la que Kaspersky Embedded Systems Security guardará un archivo XML con las reglas de autorización exportadas cuando finaliza la tarea Generador de reglas de Control de inicio de aplicaciones.
   - Agregar detalles del dispositivo protegido al nombre del archivo.

10. Si es necesario, en la pestaña **Exclusiones**, especifique los objetos que desea excluir del alcance de la tarea.

11. Haga clic en el botón **Aceptar** de la ventana **Generador de reglas de Control de inicio de aplicaciones**.

Crear reglas con la tarea de grupo del Generador de reglas de Control de inicio de aplicaciones.

Para crear reglas con la tarea de grupo Generador de reglas de Control de inicio de aplicaciones:

1. Cree una tarea de grupo *Generador de reglas de Control de inicio de aplicaciones* o seleccione una tarea existente.

2. Configure la tarea Generador de reglas de Control de inicio de aplicaciones.

3. Ejecute la tarea Generador de reglas de Control de inicio de aplicaciones.

Después de que finaliza la tarea, según la configuración de la tarea:

- Si especificó la acción **Agregar reglas de autorización a la lista de reglas de Control de inicio de aplicaciones** al completar la tarea, se agregan las reglas de Control de inicio de aplicaciones generadas a la lista de la configuración de Control de inicio de aplicaciones en la Consola de la aplicación.
- Se especificó la acción **Las reglas de autorización se exportarán a un archivo** al completar la tarea, las reglas de Control de inicio de aplicaciones generadas se guardan en un archivo XML en la ruta especificada en la configuración de la tarea.

Las listas contienen reglas de ejecución de aplicaciones cuyo tipo coincide con la configuración de la tarea de grupo Generador de reglas de Control de inicio de aplicaciones.

Control de dispositivos

El Control de dispositivos administra el acceso de los usuarios a los dispositivos que se instalan o se conectan al equipo (por ejemplo, discos duros, cámaras o módulos Wi-Fi). Esto impide la infección del equipo cuando se conectan dichos dispositivos y evita las pérdidas o fugas de datos.

Control de dispositivos proporciona las siguientes características:

- Administrar los permisos de acceso de los usuarios a los dispositivos de almacenamiento (por ejemplo, unidades extraíbles, teléfonos móviles, unidades de CD/DVD, etc.).
- Controlar la conexión de dispositivos sin un sistema de archivos (por ejemplo, módems externos, adaptadores Bluetooth, teclados USB, etc.).
- Administrar las conexiones Wi-Fi.

De manera predeterminada, el componente Control de dispositivos está deshabilitado. De manera predeterminada, cuando habilita Control de dispositivos, Kaspersky Embedded Systems Security deniega el acceso a los siguientes tipos de dispositivos:

- Unidades extraíbles (incluidas las unidades flash USB)
- Disquetes
- Unidades de CD/DVD
- Dispositivos portátiles (MTP)
- Módems
- Lectores de tarjetas inteligentes
- Adaptadores de red externos
- Bluetooth (con excepción de los dispositivos de entrada)

Niveles de Control de dispositivos

Kaspersky Embedded Systems Security controla el acceso a los dispositivos en los siguientes niveles:

1. **Tipo de dispositivo**.

   Cuando conecta un dispositivo al equipo, el sistema operativo determina el tipo de dispositivo: impresora, unidad extraíble, unidad de CD/DVD, etc. En este nivel, puede permitir o denegar la conexión de dispositivos por tipo.

2. **Bus de conexión**.

   Un *bus de conexión* es una interfaz que se utiliza para conectar dispositivos al equipo. Algunos dispositivos tienen varias interfaces de conexión. Por ejemplo, puede conectar una impresora a un puerto USB o serie (COM).

   En este nivel, puede permitir o denegar el acceso a los dispositivos según el bus de conexión.

Por ejemplo, imagine que deniega el acceso a través de USB. Kaspersky Embedded Systems Security deniega el acceso a todos los tipos de dispositivos con el modo **Depende del bus de conexión** cuando se conectan por USB.

> Si selecciona el modo de acceso **Permitir** o **Bloquear** para el dispositivo, el control del acceso ignora el bus de conexión del dispositivo.

3. **Dispositivos de confianza**.

   Los *dispositivos de confianza* son dispositivos a los que los usuarios especificados en la configuración de dispositivos de confianza tienen acceso completo en todo momento.

Modos de funcionamiento de Control de dispositivos

Control de dispositivos puede funcionar en los siguientes modos:

- **Modo Activo**.

  Kaspersky Embedded Systems Security deniega o permite dispositivos según las reglas de acceso a dispositivos configuradas. La aplicación también permite el acceso a dispositivos de confianza. La aplicación registra eventos de conexión y desconexión de dispositivos.

- **Informar**.

  Kaspersky Embedded Systems Security permite todos los eventos correspondientes de dispositivos y registros. Se permiten todos los dispositivos. Este modo está configurado de forma predeterminada. Puede habilitar este modo para realizar una auditoría de los dispositivos de su organización y usar esta información para redactar una lista de dispositivos de confianza.

Reglas de acceso a dispositivos

Una *regla de acceso a dispositivos* es un grupo de configuraciones que determinan de qué forma los usuarios pueden acceder a los dispositivos que están instalados o conectados al equipo. Estas configuraciones incluyen el acceso a un dispositivo específico, una programación de acceso, permisos de lectura o escritura y otros. El grupo de configuraciones para una regla de acceso varía según el tipo de dispositivo.

Configuración de las reglas de acceso

Dispositivos	Asignación de usuarios y/o un grupo de usuarios	Programación de acceso a un dispositivo	Lea/escriba el permiso	Monitoreo del bus de conexión
Discos duros	✓	✓	✓	✓
Unidades extraíbles (incluidas las unidades flash USB)	✓	✓	✓	✓
Disquetes	✓	✓	✓	✓
Unidades de CD/DVD	✓	✓	✓	✓
Dispositivos portátiles (MTP)	✓	✓	✓	✓
Impresoras locales	✓	–	–	✓
Impresoras de red	✓	–	–	–
Módems	–	–	–	✓
Dispositivos de transmisión	–	–	–	✓
Dispositivos multifunción	–	–	–	✓

Dispositivos	Asignación de usuarios y/o un grupo de usuarios	Programación de acceso a un dispositivo	Lea/escriba el permiso	Monitoreo del bus de conexión
Lectores de tarjetas inteligentes	–	–	–	✓
Dispositivos USB ActiveSync de Windows CE	–	–	–	✓
Adaptadores de red externos	–	–	–	✓
Bluetooth	–	–	–	–
Cámaras y escáneres	–	–	–	✓
Wi-Fi	–	–	–	–
Teclados USB	–	–	–	✓
Ratones USB	–	–	–	✓

Control de acceso a dispositivos por tipo

Control de dispositivos permite controlar el acceso a los dispositivos por tipo de dispositivo. El sistema operativo determina el tipo de dispositivo durante su conexión. Puede descubrir el tipo de dispositivo con la herramienta administradora de dispositivos integrada en el sistema operativo. Para administrar el acceso a los dispositivos, necesita configurar reglas. Una *regla de acceso a dispositivos* es un grupo de configuraciones que determinan de qué forma los usuarios pueden acceder a los dispositivos que están instalados o conectados al equipo. Estas configuraciones incluyen el acceso a un dispositivo específico, una programación de acceso, permisos de lectura o escritura y otros. El grupo de configuraciones para una regla de acceso varía según el tipo de dispositivo.

Puede configurar el acceso a los dispositivos de la siguiente manera:

- **Permitir**.

  Kaspersky Embedded Systems Security les otorga a todos los usuarios acceso completo a los dispositivos.

- **Bloquear**.

  Kaspersky Embedded Systems Security bloquea la conexión de dispositivos. La aplicación permite conectar solo dispositivos de confianza.

- **Depende del bus de conexión**.

  Kaspersky Embedded Systems Security identifica el bus de conexión del dispositivo y controla los accesos según el modo de acceso del bus de conexión. La aplicación también permite conectar dispositivos de confianza.

- **Por reglas**.

  Para algunos tipos de dispositivos, puede seleccionar usuarios o un grupo de usuarios que tendrán permitido usar los dispositivos, configurar una programación de acceso al dispositivo y permisos de lectura y escritura. La aplicación también permite conectar dispositivos de confianza.

Tenga cuidado al configurar el acceso a los dispositivos del tipo **Discos duros**. Si prohíbe el acceso a la unidad del sistema, la aplicación puede provocar errores en el sistema operativo de arranque (BSOD).

Si un dispositivo queda fuera del esquema de clasificación de Control de dispositivos, no se puede restringir el acceso a dicho dispositivo.

Cómo controlar el acceso a los dispositivos por tipo en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de propiedades de la directiva, seleccione **Control de actividad local**.
4. En la sección **Control de dispositivos**, haga clic en **Configuración**.
5. Seleccione la casilla de verificación **Control de dispositivos**.
6. En el bloque **Modo de funcionamiento de las reglas de bloqueo**, seleccione **Bloquear** o **Informar**.
7. En **Configuración de Control de dispositivos**, seleccione la pestaña **Tipos de dispositivos**.

   En la pestaña **Tipos de dispositivos**, se muestran las reglas de acceso para todos los dispositivos incluidos en la clasificación de componentes de Control de dispositivos.
8. Configure reglas de acceso a dispositivos:

   a. Seleccione un modo de acceso: **Permitir**, **Bloquear**, **Depende del bus de conexión** o **Por reglas**.

   Para seleccionar el modo de acceso **Por reglas**, debe hacer doble clic para abrir las propiedades de la regla de acceso.

   b. Si selecciona el modo de acceso **Depende del bus de conexión**, debe configurar reglas de acceso para las interfaces de conexión en la pestaña **Buses de conexión**.

   c. En el caso de los dispositivos de almacenamiento (por ejemplo, unidades extraíbles), puede configurar derechos de acceso de usuarios individuales. También puede configurar una programación de acceso al dispositivo y configurar permisos de lectura y escritura.

   d. Si es necesario, configure reglas de impresión.

   e. Si es necesario, configure reglas de conexión Wi-Fi.
9. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados .

Cómo controlar el acceso a los dispositivos por tipo en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Control de actividad local** → **Control de dispositivos** y haga clic en el botón **Configurar**.

   Se abre la ventana **Control de dispositivos**.

5. Seleccione la casilla de verificación **Habilitar Control de dispositivos**.
6. En el bloque **Modo de funcionamiento de las reglas de bloqueo**, seleccione **Bloquear** o **Informar**.
7. En el bloque **Configuración de Control de dispositivos**, haga clic en **Reglas de acceso para dispositivos y redes Wi-Fi**.

   Se abre una ventana que muestra las reglas de acceso para todos los dispositivos incluidos en la clasificación de componentes de Control de dispositivos.
8. Configure reglas de acceso a dispositivos:
   a. Seleccione un modo de acceso: **Permitir**, **Bloquear**, **Depende del bus de conexión** o **Por reglas**.

      Si el modo de acceso no está disponible en el menú desplegable, abra las propiedades de la regla de acceso al hacer doble clic en el tipo de dispositivo.
   b. Si selecciona el modo de acceso **Depende del bus de conexión**, debe volver a la ventana que contiene la configuración de Control de dispositivos, hacer clic en **Buses de conexión** y configurar las reglas de acceso para las interfaces de conexión.
   c. En el caso de los dispositivos de almacenamiento (por ejemplo, unidades extraíbles), puede configurar derechos de acceso de usuarios individuales. También puede configurar una programación de acceso al dispositivo y configurar permisos de lectura y escritura.
   d. Si es necesario, configure reglas de impresión.
   e. Si es necesario, configure reglas de conexión Wi-Fi.
9. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados.

Cómo controlar el acceso a dispositivos por tipo en la Consola de la aplicación

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Control del equipo** → **Control de dispositivos**.
2. En el panel de resultados del nodo **Control de dispositivos**, haga clic en **Propiedades**.

   Se abre la ventana **Propiedades: Control de dispositivos**.
3. Seleccione la casilla de verificación **Control de dispositivos**.
4. En el bloque **Modo de funcionamiento de las reglas de bloqueo**, seleccione **Bloquear** o **Informar**.
5. En **Configuración de Control de dispositivos**, seleccione la pestaña **Tipos de dispositivos**.

   Se abre una ventana que muestra las reglas de acceso para todos los dispositivos incluidos en la clasificación de componentes de Control de dispositivos.
6. Configure reglas de acceso a dispositivos:
   a. Seleccione el modo de acceso: **Permitir**, **Bloquear**, **Depende del bus de conexión** o **Por reglas**.

      Para seleccionar el modo de acceso **Por reglas**, debe hacer doble clic para abrir las propiedades de la regla de acceso.

b. Si selecciona el modo de acceso **Depende del bus de conexión**, debe configurar reglas de acceso para las interfaces de conexión en la pestaña **Buses de conexión**.

c. En el caso de los dispositivos de almacenamiento (por ejemplo, unidades extraíbles), puede configurar derechos de acceso de usuarios individuales. También puede configurar una programación de acceso al dispositivo y configurar permisos de lectura y escritura.

d. Si es necesario, configure reglas de impresión.

e. Si es necesario, configure reglas de conexión Wi-Fi.

7. Guarde los cambios.

Como resultado, cuando el usuario intenta obtener acceso al dispositivo, la aplicación bloquea el acceso de acuerdo con las reglas. Kaspersky Embedded Systems Security también registra el evento correspondiente. Si desea conceder acceso a dispositivos individuales, puede agregar estos dispositivos a la lista de dispositivos de confianza.

Control de conexiones Wi-Fi

El Control de dispositivos permite administrar la conexión Wi-Fi del equipo (terminal). Las redes Wi-Fi públicas pueden ser inseguras y su uso puede provocar la pérdida de datos. El Control de dispositivos le permite bloquear a un usuario para que no se conecte a Wi-Fi o permitir que se conecte solo a redes de confianza. Por ejemplo, puede permitir conectarse solo a la red Wi-Fi corporativa que sea lo suficientemente segura. El Control de dispositivos bloqueará el acceso a todas las redes Wi-Fi salvo por las especificadas en la lista de confianza.

En los equipos que ejecutan Windows 11, debe habilitar los servicios de ubicación para controlar las conexiones Wi-Fi. Para hacerlo, debe habilitar el interruptor **Servicios de ubicación** en la configuración del sistema operativo (**Configuración** → **Privacidad y seguridad** → **Ubicación**). Si los servicios de ubicación están deshabilitados, Kaspersky Embedded Systems Security no controla las conexiones a redes Wi-Fi.

Cómo restringir conexiones Wi-Fi en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de propiedades de la directiva, seleccione **Control de actividad local**.
4. En la sección **Control de dispositivos**, haga clic en **Configuración**.
5. Seleccione la casilla de verificación **Control de dispositivos**.
6. En el bloque **Modo de funcionamiento de las reglas de bloqueo**, seleccione **Bloquear** o **Informar**.
7. En **Configuración de Control de dispositivos**, seleccione la pestaña **Tipos de dispositivos**.

   En la pestaña **Tipos de dispositivos**, se muestran las reglas de acceso para todos los dispositivos incluidos en la clasificación de componentes de Control de dispositivos.

8. Para los dispositivos **Wi-Fi**, configure una regla de acceso:

    a. Seleccione un modo de acceso: **Permitir**, **Bloquear** o **Bloquear con excepciones**.

    b. Si seleccionó el modo **Bloquear con excepciones**, debe crear una lista de redes Wi-Fi de confianza:

        1. Haga doble clic en el tipo de dispositivo **Wi-Fi** para abrir la lista de redes Wi-Fi de confianza.
        2. Haga clic en el botón **Agregar** en la ventana que se abre.
        3. Se abre una ventana en la que puede configurar la red Wi-Fi de confianza:

            - **Nombre de la red**. Nombre o SSID (Service Set Identifier) de la red Wi-Fi.
            - **Tipo de autenticación**. Tipo de autenticación utilizado cuando se conecta a la red Wi-Fi.
            - **Tipo de cifrado**. Tipo de cifrado utilizado para proteger el tráfico de Wi-Fi.
            - **Comentario**. Más información sobre la red Wi-Fi agregada.

        Puede ver la configuración de la red Wi-Fi de confianza en la configuración del router.

        > Una red Wi-Fi se considera de confianza si su configuración coincide con todos los parámetros especificados en la regla.

9. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados .

Cómo restringir conexiones Wi-Fi en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Control de actividad local** → **Control de dispositivos** y haga clic en el botón **Configurar**.
   Se abre la ventana **Control de dispositivos**.
5. Seleccione la casilla de verificación **Habilitar Control de dispositivos**.
6. En el bloque **Modo de funcionamiento de las reglas de bloqueo**, seleccione **Bloquear** o **Informar**.
7. En el bloque **Configuración de Control de dispositivos**, haga clic en **Reglas de acceso para dispositivos y redes Wi-Fi**.
   Se abre una ventana que muestra las reglas de acceso para todos los dispositivos incluidos en la clasificación de componentes de Control de dispositivos.
8. Haga doble clic en el tipo de dispositivo **Wi-Fi** para abrir las propiedades de la regla de acceso.
9. Seleccione un modo de acceso: **Permitir**, **Bloquear** o **Bloquear con excepciones**.

10. Si seleccionó el modo **Bloquear con excepciones**, debe crear una lista de redes Wi-Fi de confianza:

    1. En el bloque **Redes Wi-Fi de confianza**, haga clic en el botón **Agregar**.

    2. Se abre una ventana en la que puede configurar la red Wi-Fi de confianza:

        - **Nombre de la red**. Nombre o SSID (Service Set Identifier) de la red Wi-Fi.
        - **Tipo de autenticación**. Tipo de autenticación utilizado cuando se conecta a la red Wi-Fi.
        - **Tipo de cifrado**. Tipo de cifrado utilizado para proteger el tráfico de Wi-Fi.
        - **Comentario**. Más información sobre la red Wi-Fi agregada.

    Puede ver la configuración de la red Wi-Fi de confianza en la configuración del router.

    > Una red Wi-Fi se considera de confianza si su configuración coincide con todos los parámetros especificados en la regla.

11. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados.

Cómo restringir conexiones Wi-Fi en la Consola de la aplicación

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Control del equipo** → **Control de dispositivos**.

2. En el panel de resultados del nodo **Control de dispositivos**, haga clic en **Propiedades**.

   Se abre la ventana **Propiedades: Control de dispositivos**.

3. Seleccione la casilla de verificación **Control de dispositivos**.

4. En el bloque **Modo de funcionamiento de las reglas de bloqueo**, seleccione **Bloquear** o **Informar**.

5. En **Configuración de Control de dispositivos**, seleccione la pestaña **Tipos de dispositivos**.

   Se abre una ventana que muestra las reglas de acceso para todos los dispositivos incluidos en la clasificación de componentes de Control de dispositivos.

6. Para los dispositivos **Wi-Fi**, configure una regla de acceso:

    a. Seleccione un modo de acceso: **Permitir**, **Bloquear** o **Bloquear con excepciones**.

    b. Si seleccionó el modo **Bloquear con excepciones**, debe crear una lista de redes Wi-Fi de confianza:

        1. Haga doble clic en el tipo de dispositivo **Wi-Fi** para abrir la lista de redes Wi-Fi de confianza.

        2. Haga clic en el botón **Agregar** en la ventana que se abre.

3. Se abre una ventana en la que puede configurar la red Wi-Fi de confianza:

- **Nombre de la red**. Nombre o SSID (Service Set Identifier) de la red Wi-Fi.
- **Tipo de autenticación**. Tipo de autenticación utilizado cuando se conecta a la red Wi-Fi.
- **Tipo de cifrado**. Tipo de cifrado utilizado para proteger el tráfico de Wi-Fi.
- **Comentario**. Más información sobre la red Wi-Fi agregada.

Puede ver la configuración de la red Wi-Fi de confianza en la configuración del router.

> Una red Wi-Fi se considera de confianza si su configuración coincide con todos los parámetros especificados en la regla.

7. Guarde los cambios.

Como resultado, cuando un usuario intenta conectarse a una red Wi-Fi que no figura como confiable, la aplicación bloquea la conexión y muestra una notificación.

Control de impresión

Control de dispositivos permite la configuración del acceso de los usuarios a las impresoras locales y de red.

Control de impresoras locales

Kaspersky Embedded Systems Security controla la conexión de la impresora local a través de los siguientes buses: USB, puerto serie (COM) o puerto paralelo (LPT).

> Kaspersky Embedded Systems Security controla la conexión de las impresoras locales a los puertos COM y LPT solo en el nivel del bus. Es decir, para evitar la conexión de impresoras a los puertos COM y LPT, para el tipo de dispositivo **Impresoras locales**, seleccione el modo **Depende del bus de conexión** y prohíba la conexión de los dispositivos a los buses COM y LPT.

Para impresoras conectadas a USB, la aplicación ejerce control en dos niveles: tipo de dispositivo (impresoras locales) y bus de conexión (USB).

Puede seleccionar uno de los siguientes modos de acceso a las impresoras locales por USB:

- **Permitir**. Kaspersky Embedded Systems Security les otorga a todos los usuarios acceso completo a las impresoras locales. Los usuarios pueden conectar impresoras e imprimir documentos a través de los medios que el sistema operativo ofrece.
- **Bloquear**. Kaspersky Embedded Systems Security bloquea la conexión de impresoras locales. La aplicación permite conectar solo impresoras de confianza.

- **Depende del bus de conexión**. Kaspersky Embedded Systems Security permite conectar impresoras locales según el estado de conexión del bus USB (**Permitir** o **Bloquear**).

- **Por reglas**. Para controlar la impresión, debe agregar *reglas de impresión*. En estas reglas, puede seleccionar usuarios o un grupo de usuarios para los que desea permitir o bloquear el acceso a la impresión de documentos en impresoras locales.

Control de impresoras de red

Kaspersky Embedded Systems Security permite configurar el acceso a la impresión en impresoras de red. Puede seleccionar uno de los siguientes modos de acceso para las impresoras de red:

- **Permitir y no registrar**. Kaspersky Embedded Systems Security no controla la impresión en impresoras de red. La aplicación otorga acceso a la impresión a todos los usuarios y no guarda información sobre la impresión en el registro de eventos.

- **Permitir**. Kaspersky Embedded Systems Security otorga acceso a la impresión en impresoras de red a todos los usuarios.

- **Bloquear**. Kaspersky Embedded Systems Security restringe el acceso a las impresoras de red para todos los usuarios. La aplicación solo permite el acceso a las impresoras de confianza.

- **Por reglas**. Para controlar la impresión, debe agregar *reglas de impresión*. En estas reglas, puede seleccionar usuarios o un grupo de usuarios para los que desea permitir o bloquear el acceso a la impresión de documentos en impresoras de red.

Agregar reglas de impresión para impresoras

Para agregar reglas de impresión en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de propiedades de la directiva, seleccione **Control de actividad local**.
4. En la sección **Control de dispositivos**, haga clic en **Configuración**.
5. Seleccione la casilla de verificación **Control de dispositivos**.
6. En el bloque **Modo de funcionamiento de las reglas de bloqueo**, seleccione **Bloquear** o **Informar**.
7. En **Configuración de Control de dispositivos**, seleccione la pestaña **Tipos de dispositivos**.

   En la pestaña **Tipos de dispositivos**, se muestran las reglas de acceso para todos los dispositivos incluidos en la clasificación de componentes de Control de dispositivos.

8. Configure las reglas de acceso a la impresora:

    a. Para los tipos de dispositivos **Impresoras locales** y **Impresoras de red**, configure las reglas de acceso: **Permitir**, **Bloquear**, **Permitir y no registrar** (solo para impresoras de red), **Depende del bus de conexión** (solo para impresoras locales) y **Por reglas**.

    b. Si selecciona el modo de acceso **Depende del bus de conexión**, debe configurar reglas de acceso para las interfaces de conexión en la pestaña **Buses de conexión**.

    c. Si selecciona el modo de acceso **Por reglas**, debe configurar las reglas de impresión:

        1. Haga doble clic en el tipo de dispositivo **Impresoras locales** y **Impresoras de red** para abrir las propiedades de la regla de acceso.

        2. Seleccione los usuarios o los grupos de usuarios a los que desea aplicar la regla de acceso al dispositivo. Para ello, haga clic en el botón **Agregar**.

            Se abre una ventana para agregar una nueva regla de acceso al dispositivo.

        3. Asigne una prioridad a la *entrada de regla*. Una entrada de regla incluye los siguientes atributos: cuenta de usuario, acción (permitir/bloquear) y prioridad.

            Una regla tiene una prioridad específica. Si se ha agregado un usuario a varios grupos, Kaspersky Embedded Systems Security regula el acceso al dispositivo en función de la regla de mayor prioridad. Kaspersky Embedded Systems Security permite asignar prioridad con valores de 0 a 10 000. Cuanto mayor el valor, mayor la prioridad. En otras palabras, una entrada con el valor de 0 tiene la prioridad más baja.

            Por ejemplo, puede otorgar permisos de solo lectura al grupo Todos y otorgar permisos de lectura/escritura al grupo de administradores. Para hacerlo, asigne una prioridad de 1 para el grupo de administradores y asigne una prioridad de 0 para el grupo Todos.

            La prioridad de una regla de bloqueo es mayor que la prioridad de una regla de autorización. En otras palabras, si un usuario ha sido agregado a varios grupos y la prioridad de todas las reglas es la misma, Kaspersky Embedded Systems Security regula el acceso al dispositivo en función de cualquier regla de bloqueo existente.

        4. En **Acción**, configure el acceso del usuario a las impresoras.

        5. Haga clic en **Usuarios y grupos** y seleccione los usuarios o los grupos de usuarios que podrán acceder a las impresoras. Puede seleccionar usuarios en Active Directory, en la lista de cuentas en Kaspersky Security Center o ingresando un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio.

        6. Haga clic en **Aceptar**.

9. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados .

Para agregar reglas de impresión en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.

2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

    Se abre la ventana de propiedades de la directiva.

3. Seleccione la ficha **Configuración de la aplicación**.

4. Vaya a **Control de actividad local** → **Control de dispositivos** y haga clic en el botón **Configurar**.

   Se abre la ventana **Control de dispositivos**.

5. Seleccione la casilla de verificación **Habilitar Control de dispositivos**.

6. En el bloque **Modo de funcionamiento de las reglas de bloqueo**, seleccione **Bloquear** o **Informar**.

7. En el bloque **Configuración de Control de dispositivos**, haga clic en **Reglas de acceso para dispositivos y redes Wi-Fi**.

   Se abre una ventana que muestra las reglas de acceso para todos los dispositivos incluidos en la clasificación de componentes de Control de dispositivos.

8. Configure las reglas de acceso a la impresora:

   a. Para los tipos de dispositivos **Impresoras locales** y **Impresoras de red**, seleccione un modo de acceso: **Permitir**, **Bloquear**, **Permitir y no registrar** (solo para impresoras de red), **Depende del bus de conexión** (solo para impresoras locales) o **Por reglas**.

      Si el modo de acceso no está disponible en el menú desplegable, abra las propiedades de la regla de acceso al hacer doble clic en el tipo de dispositivo.

   b. Si selecciona el modo de acceso **Depende del bus de conexión**, debe volver a la ventana que contiene la configuración de Control de dispositivos, hacer clic en **Buses de conexión** y configurar las reglas de acceso para las interfaces de conexión.

   c. Si necesita configurar la impresión:

      1. Haga doble clic en el tipo de dispositivo **Impresoras locales** o **Impresoras de red** para abrir las propiedades de la regla de acceso.

      2. Seleccione el modo de acceso **Por reglas**.

      3. Seleccione los usuarios o los grupos de usuarios a los que desea aplicar la regla de acceso al dispositivo. Para ello, haga clic en el botón **Agregar**.

         Se abre una ventana para agregar una nueva regla de acceso al dispositivo.

      4. Asigne una prioridad a la *entrada de regla*. Una entrada de regla incluye los siguientes atributos: cuenta de usuario, acción (permitir/bloquear) y prioridad.

         Una regla tiene una prioridad específica. Si se ha agregado un usuario a varios grupos, Kaspersky Embedded Systems Security regula el acceso al dispositivo en función de la regla de mayor prioridad. Kaspersky Embedded Systems Security permite asignar prioridad con valores de 0 a 10 000. Cuanto mayor el valor, mayor la prioridad. En otras palabras, una entrada con el valor de 0 tiene la prioridad más baja.

         Por ejemplo, puede otorgar permisos de solo lectura al grupo Todos y otorgar permisos de lectura/escritura al grupo de administradores. Para hacerlo, asigne una prioridad de 1 para el grupo de administradores y asigne una prioridad de 0 para el grupo Todos.

         La prioridad de una regla de bloqueo es mayor que la prioridad de una regla de autorización. En otras palabras, si un usuario ha sido agregado a varios grupos y la prioridad de todas las reglas es la misma, Kaspersky Embedded Systems Security regula el acceso al dispositivo en función de cualquier regla de bloqueo existente.

      5. En **Acción**, configure el acceso del usuario a las impresoras.

6. En **Usuarios y grupos**, haga clic en **Agregar** y seleccione los usuarios o los grupos de usuarios que podrán acceder a las impresoras. Puede seleccionar usuarios en Active Directory, en la lista de cuentas en Kaspersky Security Center o ingresando un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio.

7. Haga clic en **Aceptar**.

9. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados.

Cómo agregar reglas de impresión en la Consola de la aplicación

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Control del equipo** → **Control de dispositivos**.

2. En el panel de resultados del nodo **Control de dispositivos**, haga clic en **Propiedades**.

   Se abre la ventana **Propiedades: Control de dispositivos**.

3. Seleccione la casilla de verificación **Control de dispositivos**.

4. En el bloque **Modo de funcionamiento de las reglas de bloqueo**, seleccione **Bloquear** o **Informar**.

5. En **Configuración de Control de dispositivos**, seleccione la pestaña **Tipos de dispositivos**.

   Se abre una ventana que muestra las reglas de acceso para todos los dispositivos incluidos en la clasificación de componentes de Control de dispositivos.

6. Configure las reglas de acceso a la impresora:

   a. Para los tipos de dispositivos **Impresoras locales** y **Impresoras de red**, configure las reglas de acceso: **Permitir**, **Bloquear**, **Permitir y no registrar** (solo para impresoras de red), **Depende del bus de conexión** (solo para impresoras locales) y **Por reglas**.

   b. Si selecciona el modo de acceso **Depende del bus de conexión**, debe configurar reglas de acceso para las interfaces de conexión en la pestaña **Buses de conexión**.

   c. Si selecciona el modo de acceso **Por reglas**, debe configurar las reglas de impresión:

      1. Haga doble clic en el tipo de dispositivo **Impresoras locales** y **Impresoras de red** para abrir las propiedades de la regla de acceso.

      2. Seleccione los usuarios o los grupos de usuarios a los que desea aplicar la regla de acceso al dispositivo. Para ello, haga clic en el botón **Agregar**.

         Se abre una ventana para agregar una nueva regla de acceso al dispositivo.

      3. Asigne una prioridad a la *entrada de regla*. Una entrada de regla incluye los siguientes atributos: cuenta de usuario, acción (permitir/bloquear) y prioridad.

         Una regla tiene una prioridad específica. Si se ha agregado un usuario a varios grupos, Kaspersky Embedded Systems Security regula el acceso al dispositivo en función de la regla de mayor prioridad. Kaspersky Embedded Systems Security permite asignar prioridad con valores de 0 a 10 000. Cuanto mayor el valor, mayor la prioridad. En otras palabras, una entrada con el valor de 0 tiene la prioridad más baja.

Por ejemplo, puede otorgar permisos de solo lectura al grupo Todos y otorgar permisos de lectura/escritura al grupo de administradores. Para hacerlo, asigne una prioridad de 1 para el grupo de administradores y asigne una prioridad de 0 para el grupo Todos.

La prioridad de una regla de bloqueo es mayor que la prioridad de una regla de autorización. En otras palabras, si un usuario ha sido agregado a varios grupos y la prioridad de todas las reglas es la misma, Kaspersky Embedded Systems Security regula el acceso al dispositivo en función de cualquier regla de bloqueo existente.

4. En **Acción**, configure el acceso del usuario a las impresoras.

5. Haga clic en **Usuarios y grupos** y seleccione los usuarios o los grupos de usuarios que podrán acceder a las impresoras. Puede seleccionar usuarios en Active Directory, en la lista de cuentas en Kaspersky Security Center o ingresando un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio.

6. Haga clic en **Aceptar**.

7. Guarde los cambios.

Control de dispositivos de entrada (HID)

Los dispositivos de entrada incluyen teclados, mouses, trackballs, touchpads y otros dispositivos. Puede conectar dispositivos de entrada utilizando las siguientes interfaces: USB, Bluetooth, puerto PS/2, puerto RS-232 (COM), puerto IR, etc.

Kaspersky Embedded Systems Security permite controlar teclados y mouses USB y Bluetooth. Control de dispositivos registra la conexión y desconexión de los dispositivos de entrada.

Cuando se conectan o desconectan los dispositivos Bluetooth, la aplicación puede crear múltiples eventos sobre el dispositivo. El motivo es que el sistema operativo puede detectar un dispositivo Bluetooth como varios dispositivos de diferentes tipos. Kaspersky Embedded Systems Security también administra el adaptador Bluetooth a través del cual se conecta el dispositivo como un dispositivo independiente. Es por eso que la aplicación crea un evento para cada uno de los dispositivos detectados.

Kaspersky Embedded Systems Security deja que permita o prohíba el uso de un dispositivo de entrada, así como la creación de una lista de dispositivos de confianza.

Cómo habilitar Control de dispositivos en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.

2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la ventana de propiedades de la directiva, seleccione **Control de actividad local**.

4. En la sección **Control de dispositivos**, haga clic en **Configuración**.

5. Seleccione la casilla de verificación **Control de dispositivos**.

6. En el bloque **Modo de funcionamiento de las reglas de bloqueo**, seleccione **Bloquear** o **Informar**.
7. En **Configuración de Control de dispositivos**, seleccione la pestaña **Tipos de dispositivos**.

   En la pestaña **Tipos de dispositivos**, se muestran las reglas de acceso para todos los dispositivos incluidos en la clasificación de componentes de Control de dispositivos.
8. Para el tipo de dispositivo **Bluetooth**, seleccione un modo de acceso: **Permitir**, **Bloquear** o **Permitir y no registrar**.

   Puede bloquear o permitir todos los dispositivos Bluetooth o puede permitir la conexión únicamente de dispositivos de entrada Bluetooth (clase de dispositivos de interfaz humana [HDI]).

   > Puede permitir la conexión de dispositivos de entrada solo en Kaspersky Security Center Web Console. No puede permitir la conexión de dispositivos de entrada en la Consola de administración (MMC) o en la Consola de Kaspersky Embedded Systems Security.
9. Para los tipos de dispositivos **Teclados USB** y **Mouses USB**, seleccione un modo de acceso: **Permitir**, **Bloquear** o **Depende del bus de conexión**.
10. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados .

Cómo habilitar Control de dispositivos en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Control de actividad local** → **Control de dispositivos** y haga clic en el botón **Configurar**.

   Se abre la ventana **Control de dispositivos**.
5. Seleccione la casilla de verificación **Habilitar Control de dispositivos**.
6. En el bloque **Modo de funcionamiento de las reglas de bloqueo**, seleccione **Bloquear** o **Informar**.
7. En el bloque **Configuración de Control de dispositivos**, haga clic en **Reglas de acceso para dispositivos y redes Wi-Fi**.

   Se abre una ventana que muestra las reglas de acceso para todos los dispositivos incluidos en la clasificación de componentes de Control de dispositivos.
8. Haga clic en el tipo de dispositivo **Bluetooth** para abrir las propiedades de la regla de acceso.
9. Seleccione un modo de acceso: **Permitir**, **Bloquear** o **Permitir y no registrar**.

   Puede bloquear o permitir todos los dispositivos Bluetooth o puede permitir la conexión únicamente de dispositivos de entrada Bluetooth (clase de dispositivos de interfaz humana [HDI]).

10. Para los tipos de dispositivos **Teclados USB** y **Mouses USB**, seleccione un modo de acceso: **Permitir**, **Bloquear** o **Depende del bus de conexión**.
11. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados.

Cómo configurar Control de dispositivos en la Consola de la aplicación

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Control del equipo** → **Control de dispositivos**.
2. En el panel de resultados del nodo **Control de dispositivos**, haga clic en **Propiedades**.

   Se abre la ventana **Propiedades: Control de dispositivos**.
3. Seleccione la casilla de verificación **Control de dispositivos**.
4. En el bloque **Modo de funcionamiento de las reglas de bloqueo**, seleccione **Bloquear** o **Informar**.
5. En **Configuración de Control de dispositivos**, seleccione la pestaña **Tipos de dispositivos**.

   Se abre una ventana que muestra las reglas de acceso para todos los dispositivos incluidos en la clasificación de componentes de Control de dispositivos.
6. Para el tipo de dispositivo **Bluetooth**, seleccione un modo de acceso: **Permitir**, **Bloquear** o **Permitir y no registrar**.

   Puede bloquear o permitir todos los dispositivos Bluetooth o puede permitir la conexión únicamente de dispositivos de entrada Bluetooth (clase de dispositivos de interfaz humana [HDI]).

   > Puede permitir la conexión de dispositivos de entrada solo en Kaspersky Security Center Web Console. No puede permitir la conexión de dispositivos de entrada en la Consola de administración (MMC) o en la Consola de Kaspersky Embedded Systems Security.
7. Para los tipos de dispositivos **Teclados USB** y **Mouses USB**, seleccione un modo de acceso: **Permitir**, **Bloquear** o **Depende del bus de conexión**.
8. Guarde los cambios.

Supervisar el uso de unidades extraíbles

Supervisar el uso de unidades extraíbles incluye:

- Supervisión de operaciones en archivos en unidades extraíbles.
- Supervisión de la conexión y desconexión de unidades extraíbles de confianza.

  Kaspersky Embedded Systems Security permite supervisar la conexión y desconexión de todos los dispositivos de confianza y no solo las unidades extraíbles. Puede activar el registro de eventos en configuración de notificaciones para el componente Control de dispositivos. Los eventos tienen el nivel de gravedad *Informativo*.

Cómo habilitar el monitoreo de operaciones sobre archivos en las unidades extraíbles en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de propiedades de la directiva, seleccione **Control de actividad local**.
4. En la sección **Control de dispositivos**, haga clic en **Configuración**.
5. Seleccione la casilla de verificación **Control de dispositivos**.
6. En el bloque **Modo de funcionamiento de las reglas de bloqueo**, seleccione **Bloquear** o **Informar**.
7. En **Configuración de Control de dispositivos**, seleccione la pestaña **Tipos de dispositivos**.

   En la pestaña **Tipos de dispositivos**, se muestran las reglas de acceso para todos los dispositivos incluidos en la clasificación de componentes de Control de dispositivos.
8. Seleccione el tipo de dispositivo **Unidades extraíbles** y haga clic en el botón **Registro**.

   Se abre la ventana de registro de eventos.
9. Seleccione la casilla de verificación **Habilitar registro**.
10. En el bloque **Operaciones sobre archivos**, seleccione las operaciones que desea supervisar: **Escritura**, **Eliminación**.
11. En el bloque **Filtro por formatos de archivo**, seleccione los formatos de archivos cuyas operaciones asociadas debe seguir Control de dispositivos.
12. Seleccione los usuarios o el grupo de usuarios cuyo uso de unidades extraíbles desea supervisar.
13. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados .

Cómo habilitar el monitoreo de operaciones sobre archivos en las unidades extraíbles en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Control de actividad local** → **Control de dispositivos** y haga clic en el botón **Configurar**.

   Se abre la ventana **Control de dispositivos**.
5. Seleccione la casilla de verificación **Habilitar Control de dispositivos**.

6. En el bloque **Modo de funcionamiento de las reglas de bloqueo**, seleccione **Bloquear** o **Informar**.
7. En el bloque **Configuración de Control de dispositivos**, haga clic en **Reglas de acceso para dispositivos y redes Wi-Fi**.

   Se abre una ventana que muestra las reglas de acceso para todos los dispositivos incluidos en la clasificación de componentes de Control de dispositivos.
8. Haga doble clic en el tipo de dispositivo **Unidades extraíbles** para abrir las propiedades de la regla de acceso.
9. En la ventana que se abre, seleccione la pestaña **Registro**.
10. Configure el interruptor en **Registro HABILITADO**.
11. En el bloque **Operaciones sobre archivos**, seleccione las operaciones que desea supervisar: **Escribir**, **Eliminar**.
12. En el bloque **Filtro por formatos de archivo**, seleccione los formatos de archivos cuyas operaciones asociadas debe seguir Control de dispositivos.
13. Seleccione los usuarios o el grupo de usuarios cuyo uso de unidades extraíbles desea supervisar.
14. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados.

Cómo habilitar el monitoreo de operaciones sobre archivos en las unidades extraíbles en la Consola de la aplicación

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Control del equipo** → **Control de dispositivos**.
2. En el panel de resultados del nodo **Control de dispositivos**, haga clic en **Propiedades**.

   Se abre la ventana **Propiedades: Control de dispositivos**.
3. Seleccione la casilla de verificación **Control de dispositivos**.
4. En el bloque **Modo de funcionamiento de las reglas de bloqueo**, seleccione **Bloquear** o **Informar**.
5. En **Configuración de Control de dispositivos**, seleccione la pestaña **Tipos de dispositivos**.

   Se abre una ventana que muestra las reglas de acceso para todos los dispositivos incluidos en la clasificación de componentes de Control de dispositivos.
6. Seleccione el tipo de dispositivo **Unidades extraíbles** y haga clic en el botón **Registro**.

   Se abre la ventana de registro de eventos.
7. Seleccione la casilla de verificación **Habilitar registro**.
8. En el bloque **Operaciones sobre archivos**, seleccione las operaciones que desea supervisar: **Escritura**, **Eliminación**.
9. En el bloque **Filtro por formatos de archivo**, seleccione los formatos de archivos cuyas operaciones asociadas debe seguir Control de dispositivos.

10. Seleccione los usuarios o el grupo de usuarios cuyo uso de unidades extraíbles desea supervisar.

11. Guarde los cambios.

De esta manera, cuando los usuarios escriban en archivos ubicados en unidades extraíbles o eliminen archivos de unidades extraíbles, Kaspersky Embedded Systems Security guardará la información sobre dichas operaciones en el registro de eventos y enviará un mensaje al Servidor de administración de Kaspersky Security Center. Puede ver eventos asociados con archivos en unidades extraíbles en la Consola de administración de Kaspersky Security Center en el espacio de trabajo del nodo del **Servidor de administración** en la pestaña **Eventos**. Para que se muestren los eventos en el registro de eventos local de Kaspersky Embedded Systems Security, debe seleccionar la casilla **Se realizó una operación en un archivo** en la notifications settings para el componente Control de dispositivos.

Administrar el acceso a los dispositivos Bluetooth

Kaspersky Embedded Systems Security permite administrar el acceso a dispositivos Bluetooth. Los dispositivos Bluetooth incluyen teclados, mouses, auriculares, impresoras, etc. inalámbricos. También puede utilizar Bluetooth para comunicarse, por ejemplo, con un dispositivo móvil.

Cuando se conectan o desconectan los dispositivos Bluetooth, la aplicación puede crear múltiples eventos sobre el dispositivo. El motivo es que el sistema operativo puede detectar un dispositivo Bluetooth como varios dispositivos de diferentes tipos. Kaspersky Embedded Systems Security también administra el adaptador Bluetooth a través del cual se conecta el dispositivo como un dispositivo independiente. Es por eso que la aplicación crea un evento para cada uno de los dispositivos detectados.

Puede seleccionar uno de los siguientes modos de acceso a dispositivos Bluetooth:

- **Permitir y no registrar** . Kaspersky Embedded Systems Security permite conectar cualquier dispositivo Bluetooth y no guarda información sobre la conexión en el registro de eventos. Puede conectar dispositivos de entrada Bluetooth (teclados, mouses, etc.), enviar datos a través de Bluetooth y administrar otros dispositivos Bluetooth (auriculares, audífonos, etc.).
- **Permitir** . Kaspersky Embedded Systems Security permite conectar cualquier dispositivo Bluetooth. Puede conectar dispositivos de entrada Bluetooth (teclados, mouses, etc.), enviar datos a través de Bluetooth y administrar otros dispositivos Bluetooth (auriculares, audífonos, etc.).
- **Bloquear** . Kaspersky Embedded Systems Security restringe el acceso a dispositivos Bluetooth. Puede permitir la conexión solo de dispositivos de entrada Bluetooth (la clase Dispositivos de interfaz humana). Estos dispositivos incluyen teclado, mouse, joystick, etc.

No es posible crear una lista de dispositivos Bluetooth de confianza. Si tiene acceso restringido a dispositivos Bluetooth, solo puede conectar dispositivos de entrada Bluetooth.

Puede permitir la conexión de dispositivos de entrada solo en la Consola de la aplicación o en Kaspersky Security Center Web Console. No puede permitir la conexión de dispositivos de entrada en la Consola de administración de Kaspersky Security Center.

Cómo configurar reglas de acceso a dispositivos Bluetooth en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Control de actividad local** → **Control de dispositivos** y haga clic en **Configuración**.
4. En **Configuración de Control de dispositivos**, seleccione la pestaña **Tipos de dispositivos**.

   En la tabla se enumeran las reglas de acceso para todos los dispositivos que están presentes en la clasificación del componente Control de dispositivos.
5. En el menú contextual para el tipo de dispositivo **Bluetooth**, configure el modo de acceso al dispositivo Bluetooth: **Permitir**, **Bloquear**, **Permitir y no registrar**.

   Si bloqueó el acceso a dispositivos Bluetooth, puede permitir la conexión de dispositivos de entrada (teclados, mouses, etc.) solo en la Consola de la aplicación o en Kaspersky Security Center Web Console. No puede permitir la conexión de dispositivos de entrada en la Consola de administración de Kaspersky Security Center.
6. Guarde los cambios.

Cómo configurar las reglas de acceso a dispositivos Bluetooth en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. En la ventana de la directiva, seleccione **Control de actividad local** → **Control de dispositivos** y haga clic en **Configuración**.
5. En el bloque **Configuración de Control de dispositivos**, haga clic en el vínculo **Reglas de acceso para dispositivos y redes Wi-Fi**.

   En la tabla se enumeran las reglas de acceso para todos los dispositivos que están presentes en la clasificación del componente Control de dispositivos.
6. Seleccione el tipo de dispositivo **Bluetooth**.

   Esto abre la configuración de acceso a dispositivos Bluetooth.
7. Configure el modo de acceso al dispositivo Bluetooth: **Permitir**, **Bloquear**, **Permitir y no registrar**.

8. Si selecciona el modo **Bloquear**, puede permitir la conexión solo de dispositivos de entrada Bluetooth (teclados, mouses, etc.). Para eso, en **Exclusiones**, seleccione la casilla de verificación **Dispositivos de entrada (ratones y teclados)**.

9. Guarde los cambios.

Cómo configurar reglas de acceso a dispositivos Bluetooth en la Consola de la aplicación

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Control del equipo** → **Control de dispositivos**.

2. En el panel de resultados del nodo **Control de dispositivos**, haga clic en **Propiedades**.

   Se abre la ventana **Propiedades: Control de dispositivos**.

3. En **Configuración de Control de dispositivos**, seleccione la pestaña **Tipos de dispositivos**.

   En la tabla se enumeran las reglas de acceso para todos los dispositivos que están presentes en la clasificación del componente Control de dispositivos.

4. En **Acceso**, configure el modo de acceso al dispositivo Bluetooth: **Permitir**, **Bloquear**, **Permitir y no registrar**.

5. Si selecciona el modo **Bloquear**, puede permitir la conexión solo de dispositivos de entrada Bluetooth (teclados, mouses, etc.). Para eso, en **Exclusiones**, seleccione la casilla de verificación **Dispositivos de entrada (ratones y teclados)**.

6. Guarde los cambios.

Diferenciación de los derechos de acceso del usuario a los dispositivos

Puede configurar derechos de acceso del usuario por tipo de dispositivo o acceso a dispositivos de confianza.

Diferenciación de los derechos de acceso del usuario por tipo de dispositivo

Control de dispositivos permite configurar derechos de acceso del usuario a los datos de los *dispositivos de almacenamiento*. Puede configurar permisos de lectura y escritura para estos dispositivos. Control de dispositivos admite los siguientes tipos de dispositivos de almacenamiento:

- Discos duros
- Unidades extraíbles
- Disquetes
- Unidades de CD/DVD
- Los dispositivos portátiles (MTP) incluyen, por ejemplo, dispositivos móviles, cámaras de fotos, reproductores multimedia, etc.

Esto significa que puede, por ejemplo, permitir el uso de unidades extraíbles solo para el grupo de administradores. Para otro tipo de dispositivos, puede denegar o permitir el acceso de todos los usuarios. También puede configurar derechos de acceso del usuario a las impresoras.

Cómo configurar derechos de acceso del usuario a los datos de las unidades extraíbles en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de propiedades de la directiva, seleccione **Control de actividad local**.
4. En la sección **Control de dispositivos**, haga clic en **Configuración**.
5. Seleccione la casilla de verificación **Control de dispositivos**.
6. En el bloque **Modo de funcionamiento de las reglas de bloqueo**, seleccione **Bloquear** o **Informar**.
7. En **Configuración de Control de dispositivos**, seleccione la pestaña **Tipos de dispositivos**.

   En la pestaña **Tipos de dispositivos**, se muestran las reglas de acceso para todos los dispositivos incluidos en la clasificación de componentes de Control de dispositivos.
8. Para configurar las reglas de acceso a dispositivos de almacenamiento, haga doble clic para abrir la lista de reglas.
9. Configure la regla de acceso a dispositivos de almacenamiento:

   a. En el bloque **Reglas de acceso**, haga clic en el botón **Agregar**.

   Esto abre una ventana para agregar una nueva regla de acceso a dispositivos de almacenamiento.

   b. En el campo **Prioridad**, establezca la prioridad de la *entrada de regla*. Una regla incluye los siguientes atributos: cuenta de usuario, programación, permisos (lectura/escritura) y prioridad.

   Una regla tiene una prioridad específica. Si se ha agregado un usuario a varios grupos, Kaspersky Embedded Systems Security regula el acceso al dispositivo en función de la regla de mayor prioridad. Kaspersky Embedded Systems Security permite asignar prioridad con valores de 0 a 10 000. Cuanto mayor el valor, mayor la prioridad. En otras palabras, una entrada con el valor de 0 tiene la prioridad más baja.

   Por ejemplo, puede otorgar permisos de solo lectura al grupo Todos y otorgar permisos de lectura/escritura al grupo de administradores. Para hacerlo, asigne una prioridad de 1 para el grupo de administradores y asigne una prioridad de 0 para el grupo Todos.

   La prioridad de una regla de bloqueo es mayor que la prioridad de una regla de autorización. En otras palabras, si un usuario ha sido agregado a varios grupos y la prioridad de todas las reglas es la misma, Kaspersky Embedded Systems Security regula el acceso al dispositivo en función de cualquier regla de bloqueo existente.

   c. En **Regla para usuarios y grupos**, seleccione usuarios o grupos de usuarios. Puede seleccionar usuarios en Active Directory, en la lista de cuentas en Kaspersky Security Center o ingresando un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio.

   d. Haga clic en **Aceptar**.

10. En **Programaciones para la regla de acceso seleccionada**, configure una programación de acceso del usuario para los dispositivos de almacenamiento.

    Por ejemplo, puede permitir el acceso el usuario a dispositivos de almacenamiento solo durante las horas de trabajo.

11. Configure los permisos de acceso de los usuarios a los dispositivos de almacenamiento en el administrador de archivos (**Leer**/**Escribir**).

12. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados .

Cómo configurar derechos de acceso del usuario a los dispositivos de almacenamiento en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.

2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la ficha **Configuración de la aplicación**.

4. Vaya a **Control de actividad local** → **Control de dispositivos** y haga clic en el botón **Configurar**.

   Se abre la ventana **Control de dispositivos**.

5. Seleccione la casilla de verificación **Habilitar Control de dispositivos**.

6. En el bloque **Modo de funcionamiento de las reglas de bloqueo**, seleccione **Bloquear** o **Informar**.

7. En el bloque **Configuración de Control de dispositivos**, haga clic en **Reglas de acceso para dispositivos y redes Wi-Fi**.

   Se abre una ventana que muestra las reglas de acceso para todos los dispositivos incluidos en la clasificación de componentes de Control de dispositivos.

8. En el bloque **Acceso a dispositivos de almacenamiento**, abra las propiedades de la regla de acceso al dispositivo de almacenamiento.

9. Configure la regla de acceso a dispositivos de almacenamiento:

   a. En el bloque **Usuarios**, haga clic en el botón **Agregar**.

      Esto abre una ventana para agregar una nueva regla de acceso a dispositivos de almacenamiento.

   b. En el campo **Prioridad**, establezca la prioridad de la *entrada de regla*. Una regla incluye los siguientes atributos: cuenta de usuario, programación, permisos (lectura/escritura) y prioridad.

      Una regla tiene una prioridad específica. Si se ha agregado un usuario a varios grupos, Kaspersky Embedded Systems Security regula el acceso al dispositivo en función de la regla de mayor prioridad. Kaspersky Embedded Systems Security permite asignar prioridad con valores de 0 a 10 000. Cuanto mayor el valor, mayor la prioridad. En otras palabras, una entrada con el valor de 0 tiene la prioridad más baja.

      Por ejemplo, puede otorgar permisos de solo lectura al grupo Todos y otorgar permisos de lectura/escritura al grupo de administradores. Para hacerlo, asigne una prioridad de 1 para el grupo de administradores y asigne una prioridad de 0 para el grupo Todos.

La prioridad de una regla de bloqueo es mayor que la prioridad de una regla de autorización. En otras palabras, si un usuario ha sido agregado a varios grupos y la prioridad de todas las reglas es la misma, Kaspersky Embedded Systems Security regula el acceso al dispositivo en función de cualquier regla de bloqueo existente.

c. En **Usuarios**, seleccione usuarios o grupos de usuarios. Puede seleccionar usuarios en Active Directory, en la lista de cuentas en Kaspersky Security Center o ingresando un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio.

d. En **Programación de acceso a dispositivos**, configure una programación de acceso del usuario para los dispositivos de almacenamiento.

Por ejemplo, puede permitir el acceso el usuario a dispositivos de almacenamiento solo durante las horas de trabajo.

e. Configure los permisos de acceso de los usuarios a los dispositivos de almacenamiento en el administrador de archivos (**Leer**/**Escribir**).

f. Haga clic en **Aceptar**.

10. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados.

Cómo configurar derechos de acceso del usuario a los dispositivos de almacenamiento en la Consola de Kaspersky Embedded Systems Security

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Control del equipo** → **Control de dispositivos**.
2. En el panel de resultados del nodo **Control de dispositivos**, haga clic en **Propiedades**.

   Se abre la ventana **Propiedades: Control de dispositivos**.
3. Seleccione la casilla de verificación **Control de dispositivos**.
4. En el bloque **Modo de funcionamiento de las reglas de bloqueo**, seleccione **Bloquear** o **Informar**.
5. En **Configuración de Control de dispositivos**, seleccione la pestaña **Tipos de dispositivos**.

   Se abre una ventana que muestra las reglas de acceso para todos los dispositivos incluidos en la clasificación de componentes de Control de dispositivos.
6. Para configurar las reglas de acceso a dispositivos de almacenamiento, haga doble clic para abrir la lista de reglas.
7. Configure la regla de acceso a dispositivos de almacenamiento:

   a. En el bloque **Reglas de acceso**, haga clic en el botón **Agregar**.

   Esto abre una ventana para agregar una nueva regla de acceso a dispositivos de almacenamiento.

   b. En el campo **Prioridad de la regla**, establezca la prioridad de la *entrada de regla*. Una regla incluye los siguientes atributos: cuenta de usuario, programación, permisos (lectura/escritura) y prioridad.

Una regla tiene una prioridad específica. Si se ha agregado un usuario a varios grupos, Kaspersky Embedded Systems Security regula el acceso al dispositivo en función de la regla de mayor prioridad. Kaspersky Embedded Systems Security permite asignar prioridad con valores de 0 a 10 000. Cuanto mayor el valor, mayor la prioridad. En otras palabras, una entrada con el valor de 0 tiene la prioridad más baja.

Por ejemplo, puede otorgar permisos de solo lectura al grupo Todos y otorgar permisos de lectura/escritura al grupo de administradores. Para hacerlo, asigne una prioridad de 1 para el grupo de administradores y asigne una prioridad de 0 para el grupo Todos.

La prioridad de una regla de bloqueo es mayor que la prioridad de una regla de autorización. En otras palabras, si un usuario ha sido agregado a varios grupos y la prioridad de todas las reglas es la misma, Kaspersky Embedded Systems Security regula el acceso al dispositivo en función de cualquier regla de bloqueo existente.

c. En **Regla para usuarios y grupos**, seleccione usuarios o grupos de usuarios. Puede seleccionar usuarios en Active Directory o ingresar un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio.

d. Haga clic en **Aceptar**.

8. En **Programaciones para la regla de acceso seleccionada**, configure una programación de acceso del usuario para los dispositivos de almacenamiento.

   Por ejemplo, puede permitir el acceso el usuario a dispositivos de almacenamiento solo durante las horas de trabajo.

9. Configure los permisos de acceso de los usuarios a los dispositivos de almacenamiento en el administrador de archivos (**Leer**/**Escribir**).

10. Guarde los cambios.

Diferenciación de los derechos de acceso del usuario a los dispositivos de confianza

Los *dispositivos de confianza* son dispositivos a los que los usuarios especificados en la configuración de dispositivos de confianza tienen acceso completo en todo momento. Puede conceder acceso a los dispositivos de confianza a un usuario específico, a un grupo de usuarios o a todos los usuarios de su organización. Puede configurar derechos de acceso del usuario en las propiedades del dispositivo de confianza.

Auditoría de dispositivos externos

Para crear una lista de dispositivos de confianza, debe realizar una auditoría de los dispositivos externos de su organización. Para agregar un dispositivo de confianza, debe seleccionar un dispositivo conectado y asignar el estado de confianza al dispositivo. Puede obtener una lista de dispositivos de las siguientes maneras:

- Habilite Control de dispositivos en el modo Informar.

Cómo habilitar Control de dispositivos en el modo Informar en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de propiedades de la directiva, seleccione **Control de actividad local**.
4. En la sección **Control de dispositivos**, haga clic en **Configuración**.
5. Seleccione la casilla de verificación **Control de dispositivos**.
6. En **Modo de funcionamiento de las reglas de bloqueo**, seleccione **Informar**.
7. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados .

Cómo habilitar Control de dispositivos en el modo Informar en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Control de actividad local** → **Control de dispositivos** y haga clic en el botón **Configurar**.
   Se abre la ventana **Control de dispositivos**.
5. Seleccione la casilla de verificación **Habilitar Control de dispositivos**.
6. En **Modo de funcionamiento de las reglas de bloqueo**, seleccione **Informar**.
7. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados .

Cómo habilitar Control de dispositivos en el modo Informar en la Consola de la aplicación

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Control del equipo** → **Control de dispositivos**.
2. En el panel de resultados del nodo **Control de dispositivos**, haga clic en **Propiedades**.
   Se abre la ventana **Propiedades: Control de dispositivos**.
3. Seleccione la casilla de verificación **Control de dispositivos**.
4. En **Modo de funcionamiento de las reglas de bloqueo**, seleccione **Informar**.
5. Guarde los cambios.

Como resultado, Kaspersky Embedded Systems Security registrará eventos de conexión y desconexión de dispositivos externos. Puede generar un informe del equipo y, después de analizar el informe, agregar dispositivos de confianza.

- Ejecute la tarea de *Generador de reglas para Control de dispositivos*.

  Cómo ejecutar la tarea Generador de reglas para Control de dispositivos en la Consola de administración de Kaspersky Security Center

  1. Abra la Consola de administración de Kaspersky Security Center.
  2. En el árbol de la consola, seleccione **Tareas**.
  3. Seleccione la tarea *Generador de reglas para Control de dispositivos* y haga doble clic para abrir las propiedades de la tarea.

     Si es necesario, cree una tarea nueva.
  4. En la sección **Modo**, seleccione el modo de la tarea:

     - **Tener en cuenta los datos del sistema sobre todos los dispositivos externos que se hayan conectado**.

       La aplicación obtiene información de la memoria del sistema operativo acerca de todos los dispositivos que se conectaron al equipo.

     - **Tener en cuenta solo los dispositivos externos conectados actualmente**.

       La aplicación obtiene información acerca de los dispositivos que están conectados cuando se inicia la tarea.
  5. Ingrese la ruta en la que desea guardar el archivo con los datos.
  6. Si ejecuta la tarea en varios equipos, recomendamos seleccionar la casilla de verificación **Agregar detalles del dispositivo protegido al nombre del archivo**.
  7. Guarde los cambios.
  8. Ejecute la tarea.

  Cómo ejecutar la tarea Generador de reglas para Control de dispositivos en Kaspersky Security Center Web Console

  1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Tareas**.

     Se abre la lista de tareas.
  2. Seleccione la tarea *Generador de reglas para Control de dispositivos* y haga doble clic para abrir las propiedades de la tarea.

     Si es necesario, cree una tarea nueva.

3. En la sección **Modo**, seleccione el modo de la tarea:

   - **Tener en cuenta los datos del sistema sobre todos los dispositivos externos que se hayan conectado**.

     La aplicación obtiene información de la memoria del sistema operativo acerca de todos los dispositivos que se conectaron al equipo.

   - **Tener en cuenta solo los dispositivos externos conectados actualmente**.

     La aplicación obtiene información acerca de los dispositivos que están conectados cuando se inicia la tarea.

4. Ingrese la ruta en la que desea guardar el archivo con los datos.

5. Si ejecuta la tarea en varios equipos, recomendamos seleccionar la casilla de verificación **Agregar detalles del dispositivo protegido al nombre del archivo**.

6. Guarde los cambios.

7. Ejecute la tarea.

Cómo iniciar la tarea Generador de reglas para Control de dispositivos en la Consola de la aplicación

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Generación automática de reglas → Generador de reglas para Control de dispositivos**.

2. En el panel de resultados del nodo **Generador de reglas para Control de dispositivos**, haga clic en **Propiedades**.

   Se abre la ventana **Propiedades: Generador de reglas para Control de dispositivos**.

3. En la sección **Modo**, seleccione el modo de la tarea:

   - **Tener en cuenta los datos del sistema sobre todos los dispositivos externos que se hayan conectado**.

     La aplicación obtiene información de la memoria del sistema operativo acerca de todos los dispositivos que se conectaron al equipo.

   - **Tener en cuenta solo los dispositivos externos conectados actualmente**.

     La aplicación obtiene información acerca de los dispositivos que están conectados cuando se inicia la tarea.

4. En la sección **Después de completada la tarea**, seleccione las acciones de la aplicación después de que se completa la tarea:

   - **Agregar reglas de autorización a la lista de reglas de Control de dispositivos**. La lista de reglas de Control de dispositivos está disponible en la configuración de Control de dispositivos.

     Si esta casilla de verificación está seleccionada, la aplicación agrega las reglas generadas por la tarea a la lista de reglas de Control de dispositivos, según el principio de adición seleccionado.

     Si esta casilla de verificación está desactivada, la aplicación no agrega las reglas de autorización recientemente generadas a la lista de reglas de Control de dispositivos. La aplicación solo exporta reglas a un archivo.

- **Principio de adición**. Un método utilizado para agregar las reglas de autorización recién generadas a la lista de reglas de Control de dispositivos:
  - **Agregar a reglas existentes**. La aplicación agrega una regla a la lista de reglas existentes. En este caso, la aplicación duplica reglas idénticas.
  - **Reemplazar reglas existentes**. La aplicación agrega reglas nuevas en lugar de reglas existentes.
  - **Combinar con reglas existentes**. La aplicación agrega una regla a la lista de reglas existentes. En este caso, la aplicación fusiona reglas idénticas.
- **Exportar reglas de autorización a archivo**. La aplicación exporta las reglas de autorización al archivo especificado en el campo a continuación. Luego, puede importar el archivo de configuración de la aplicación en otros equipos para distribuir las reglas de autorización. El archivo también se puede utilizar para crear una copia de seguridad de las reglas de autorización.
- **Agregar detalles del dispositivo protegido al nombre del archivo**. Además de la fecha y hora, la aplicación agrega el nombre del equipo al nombre del archivo exportado. Es conveniente recopilar reglas de autorización de varios equipos.

5. Guarde los cambios.

Como resultado, Kaspersky Embedded Systems Security realiza una auditoría de los dispositivos externos y guarda la información en el registro de Kaspersky Security Center. La lista de dispositivos externos está disponible cuando agrega dispositivos de confianza.

Incorporación de dispositivos de confianza

Los *dispositivos de confianza* son dispositivos a los que los usuarios especificados en la configuración de dispositivos de confianza tienen acceso completo en todo momento.

Puede conceder acceso a los dispositivos de confianza a un usuario específico, a un grupo de usuarios o a todos los usuarios de su organización.

Por ejemplo, si usar unidades extraíbles está prohibido en su organización, pero los administradores necesitan utilizarlas, puede permitir su uso solo para un grupo de administradores. Para ello, deberá agregar las unidades extraíbles a la lista de dispositivos de confianza y configurar los permisos de acceso de los usuarios.

No se recomienda agregar más de 1000 dispositivos de confianza, ya que pueden generar inestabilidad en el sistema.

Cómo agregar un dispositivo de confianza en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de propiedades de la directiva, seleccione **Control de actividad local**.

4. En la sección **Control de dispositivos**, haga clic en **Configuración**.
5. En **Configuración de supervisión de dispositivos**, seleccione la pestaña **Dispositivos de confianza**.

   Esto abre la lista de dispositivos de confianza.
6. Active la casilla **Combinar valores al heredar** si desea crear una lista de dispositivos de confianza unificada para todos los equipos de la empresa.

   La lista de dispositivos de confianza de la directiva principal se combinará con las listas de las directivas secundarias. Para que esto ocurra, debe haber habilitado la opción para que los valores se hereden y se combinen. Los dispositivos de confianza de la directiva principal aparecerán en las directivas secundarias, pero solo podrá verlos. No podrá modificarlos ni eliminarlos.
7. Haga clic en el botón **Agregar** y seleccione el método que desee usar para agregar los dispositivos a la lista de confianza:

   - **Generar reglas basadas en los dispositivos conectados**.
   - **Generar reglas basadas en datos del sistema**.
   - **Generar reglas a partir del registro de Kaspersky Security Center**.

   Si la lista de dispositivos está vacía, debe realizar una auditoría de los dispositivos externos. Para ello, ejecute la tarea *Generador de reglas para Control de dispositivos*.

   > Kaspersky Embedded Systems Security no admite agregar dispositivos del tipo **Disquetes** a la lista de confianza.
8. Haga clic en **Agregar reglas para los dispositivos seleccionados**.
9. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados.

Cómo agregar un dispositivo de confianza en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Control de actividad local** → **Control de dispositivos** y haga clic en el botón **Configurar**.

   Se abre la ventana **Control de dispositivos**.
5. En el bloque **Configuración de Control de dispositivos**, haga clic en **Dispositivos de confianza**.

   Esto abre la lista de dispositivos de confianza.

6. Active la casilla **Combinar valores al heredar** si desea crear una lista de dispositivos de confianza unificada para todos los equipos de la empresa.

   La lista de dispositivos de confianza de la directiva principal se combinará con las listas de las directivas secundarias. Para que esto ocurra, debe haber habilitado la opción para que los valores se hereden y se combinen. Los dispositivos de confianza de la directiva principal aparecerán en las directivas secundarias, pero solo podrá verlos. No podrá modificarlos ni eliminarlos.

7. Haga clic en **Desde el registro de KSC**.

   Si la lista de dispositivos está vacía, debe realizar una auditoría de los dispositivos externos. Para ello, ejecute la tarea *Generador de reglas para Control de dispositivos*.

   > Kaspersky Embedded Systems Security no admite agregar dispositivos del tipo **Disquetes** a la lista de confianza.

8. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados.

Cómo agregar un dispositivo de confianza en la Consola de la aplicación

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Control del equipo** → **Control de dispositivos**.

2. En el panel de resultados del nodo **Control de dispositivos**, haga clic en **Propiedades**.

   Se abre la ventana **Propiedades: Control de dispositivos**.

3. En **Configuración de Control de dispositivos**, seleccione la pestaña **Dispositivos de confianza**.

   Esto abre la lista de dispositivos de confianza.

4. Haga clic en el botón **Agregar** y seleccione el método que desee usar para agregar los dispositivos a la lista de confianza:

   - **Generar reglas basadas en los dispositivos conectados**.
   - **Generar reglas basadas en datos del sistema**.
   - **Generar reglas a partir del registro de Kaspersky Security Center**.

   Si la lista de dispositivos está vacía, debe realizar una auditoría de los dispositivos externos. Para ello, ejecute la tarea *Generador de reglas para Control de dispositivos*.

   > Kaspersky Embedded Systems Security no admite agregar dispositivos del tipo **Disquetes** a la lista de confianza.

5. Haga clic en **Agregar reglas para los dispositivos seleccionados**.

6. Guarde los cambios.

Exportar e importar la lista de dispositivos de confianza

Si desea distribuir la lista de dispositivos de confianza a otros equipos de la organización, puede usar el procedimiento de exportación/importación. Puede exportar la lista de dispositivos de confianza a un archivo XML. A continuación, puede modificar el archivo para, por ejemplo, agregar una gran cantidad de dispositivos del mismo tipo. Puede utilizar la función de exportación/importación para realizar una copia de seguridad de la lista de dispositivos de confianza o para migrar la lista a otro servidor.

Kaspersky Embedded Systems Security le permite importar la lita de dispositivos de confianza desde Kaspersky Endpoint Security para Windows. El formato del archivo XML para estas aplicaciones es el mismo.

Cómo exportar e importar una lista de dispositivos de confianza en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de propiedades de la directiva, seleccione **Control de actividad local**.
4. En la sección **Control de dispositivos**, haga clic en **Configuración**.
5. En **Configuración de Control de dispositivos**, seleccione la pestaña **Dispositivos de confianza**.

   Esto abre la lista de dispositivos de confianza.
6. Para exportar la lista de dispositivos de confianza.
   a. Seleccione los dispositivos de confianza que desea exportar.
   b. Haga clic en el botón y seleccione el modo de exportación: exportar la lista completa de dispositivos de confianza o solo dispositivos de confianza seleccionados.
   c. En la ventana que se abre, escriba el nombre del archivo XML en el que se guardará la lista exportada. Seleccione también la carpeta en la que se guardará este archivo.
   d. Guarde el archivo.

      Kaspersky Embedded Systems Security exporta la lista de direcciones de recursos web a un archivo XML.
7. Para importar la lista de dispositivos de confianza:
   a. Haga clic en **Agregar** → **Importar reglas desde archivo XML** y seleccione un modo de importación: agregar o reemplazar.

      En la ventana que se abre, seleccione el archivo XML que desea usar para importar la lista de recursos web.

En el modo Fusionar, la aplicación revisa las listas de dispositivos de confianza y elimina las entradas duplicadas. En el modo Agregar, la aplicación agrega entradas a la lista de aplicaciones de confianza sin buscar duplicados.

b. Abra el archivo.

Kaspersky Embedded Systems Security importa los dispositivos de confianza según el modo seleccionado.

8. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados.

Cómo exportar e importar una lista de dispositivos de confianza en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

Se abre la ventana de propiedades de la directiva.

3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Control de actividad local** → **Control de dispositivos** y haga clic en el botón **Configurar**.

Se abre la ventana **Control de dispositivos**.

5. En el bloque **Configuración de Control de dispositivos**, haga clic en **Dispositivos de confianza**.

Esto abre la lista de dispositivos de confianza.

6. Para exportar la lista de dispositivos de confianza.

a. Seleccione los dispositivos de confianza que desea exportar.

b. Haga clic en el botón **Exportar** y seleccione el modo de exportación: exportar la lista completa de dispositivos de confianza o solo dispositivos de confianza seleccionados.

c. Guarde el archivo.

Kaspersky Embedded Systems Security exporta la lista de direcciones de recursos web a un archivo XML.

7. Para importar la lista de dispositivos de confianza:

a. Haga clic en el botón **Importar** y seleccione un modo de importación: agregar o reemplazar.

b. En la ventana que se abre, seleccione el archivo XML que desea usar para importar la lista de recursos web.

c. Abra el archivo.

Kaspersky Embedded Systems Security importa los dispositivos de confianza según el modo seleccionado.

8. Guarde los cambios. Para aplicar la directiva en los equipos, cierre los candados.

Cómo exportar e importar una lista de dispositivos de confianza en la Consola de la aplicación

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Control del equipo** → **Control de dispositivos**.
2. En el panel de resultados del nodo **Control de dispositivos**, haga clic en **Propiedades**.

   Se abre la ventana **Propiedades: Control de dispositivos**.
3. En **Configuración de Control de dispositivos**, seleccione la pestaña **Dispositivos de confianza**.

   Esto abre la lista de dispositivos de confianza.
4. Para exportar la lista de dispositivos de confianza.

   a. Seleccione los dispositivos de confianza que desea exportar.

   b. Haga clic en el botón y seleccione el modo de exportación: exportar la lista completa de dispositivos de confianza o solo dispositivos de confianza seleccionados.

   c. En la ventana que se abre, escriba el nombre del archivo XML en el que se guardará la lista exportada. Seleccione también la carpeta en la que se guardará este archivo.

   d. Guarde el archivo.

   Kaspersky Embedded Systems Security exporta la lista de direcciones de recursos web a un archivo XML.
5. Para importar la lista de dispositivos de confianza:

   a. Haga clic en **Agregar** → **Importar reglas desde archivo XML** y seleccione un modo de importación: agregar o reemplazar.

   En la ventana que se abre, seleccione el archivo XML que desea usar para importar la lista de recursos web.

   En el modo Fusionar, la aplicación revisa las listas de dispositivos de confianza y elimina las entradas duplicadas. En el modo Agregar, la aplicación agrega entradas a la lista de aplicaciones de confianza sin buscar duplicados.

   b. Abra el archivo.

   Kaspersky Embedded Systems Security importa los dispositivos de confianza según el modo seleccionado.
6. Guarde los cambios.

Firewall

El componente Firewall puede funcionar en los siguientes modos:

- **Observar el estado del Firewall de Windows**. El modo está diseñado para una transición sin problemas de la lógica de la tarea Administración del Firewall en la versión 3.4 o anteriores de la aplicación al Firewall con todas las funciones en la versión 4.0 y posteriores de la aplicación. Cuando se actualizan la versión 3.4 y anteriores de la aplicación, se mantienen las reglas de la tarea Administración del Firewall integrada en el Firewall de Windows. Pero el componente Firewall ya no interactúa con el Firewall de Windows, sino que solo supervisa el filtrado de tráfico del Firewall de Windows y registra los eventos correspondientes en el registro de operaciones del componente. Luego puede crear reglas de Firewall o importar reglas del Firewall de Windows y cambiar el modo de funcionamiento del Firewall a **Informar**.

- **Informar**. La aplicación solo supervisa el funcionamiento de las reglas del Firewall y registra los eventos correspondientes en el registro de operaciones del componente. El modo está diseñado para probar las reglas del Firewall. Puede evaluar su aplicabilidad usando el registro de operaciones del Firewall. Luego, si es necesario, puede ajustar las reglas del Firewall y cambiar el modo de funcionamiento del Firewall a **Bloquear**.

- **Bloquear**. La aplicación filtra el tráfico de red de acuerdo con la configuración del componente y registra los eventos correspondientes en el registro de funcionamiento del componente.

Acerca de las reglas de firewall

Si selecciona el modo **Bloquear**, el componente Firewall filtra el tráfico de red usando las reglas del Firewall.

Las reglas de firewall para aplicaciones controlan las conexiones de red de aplicaciones específicas. El criterio de activación para estas reglas se basa en la ruta de acceso al archivo ejecutable de la aplicación.

Las reglas de firewall para puertos controlan las conexiones de red en las que se utilizan puertos y protocolos (TCP/UDP) puntuales. Los criterios de activación de las reglas son el tipo de protocolo y el puerto o rango de puertos.

> Las reglas de puerto involucran un área de aplicación más amplia que la de las reglas de aplicación. Al permitir las conexiones de red a través de reglas de puertos, se reduce el nivel de seguridad del equipo protegido.

Configurar el firewall

En esta sección, se brindan instrucciones para ajustar la configuración general del componente Firewall y para crear y configurar reglas de Firewall.

Establecer la configuración general de firewall

Ajustar la configuración general del componente Firewall en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la sección **Control de actividad de red**, haga clic en el botón **Configuración** de la subsección **Firewall**.

   Se abre la ventana **Firewall**.
4. En la pestaña **General** en el bloque **Modo de funcionamiento de las reglas de bloqueo**, seleccione el modo de funcionamiento del componente:

   - **Observar el estado del Firewall de Windows**. El modo está diseñado para una transición sin problemas de la lógica de la tarea Administración del Firewall en la versión 3.4 o anteriores de la aplicación al Firewall con todas las funciones en la versión 4.0 y posteriores de la aplicación. Cuando se actualizan la versión 3.4 y anteriores de la aplicación, se mantienen las reglas de la tarea Administración del Firewall integrada en el Firewall de Windows. Pero el componente Firewall ya no interactúa con el Firewall de Windows, sino que solo supervisa el filtrado de tráfico del Firewall de Windows y registra los eventos correspondientes en el registro de operaciones del componente. Luego puede crear reglas de Firewall o importar reglas del Firewall de Windows y cambiar el modo de funcionamiento del Firewall a **Informar**.
   - **Informar**. La aplicación solo supervisa el funcionamiento de las reglas del Firewall y registra los eventos correspondientes en el registro de operaciones del componente. El modo está diseñado para probar las reglas del Firewall. Puede evaluar su aplicabilidad usando el registro de operaciones del Firewall. Luego, si es necesario, puede ajustar las reglas del Firewall y cambiar el modo de funcionamiento del Firewall a **Bloquear**.
   - **Bloquear**. La aplicación filtra el tráfico de red de acuerdo con la configuración del componente y registra los eventos correspondientes en el registro de funcionamiento del componente.
5. En el bloque **Conexiones entrantes**, establezca la configuración para las conexiones de red entrantes:

   - Use la lista desplegable **Acción para conexiones entrantes** para especificar la acción que la aplicación realizará para todas las conexiones de red entrantes, a menos que haya reglas de Firewall para conexiones entrantes que definan lo contrario.
   - De ser necesario, agregue reglas de Firewall para conexiones entrantes.

     Las reglas que defina para las conexiones entrantes en Firewall actuarán como exclusiones. Por ejemplo, si configura una regla de autorización para conexiones de red entrantes y selecciona **Bloquear** en la lista desplegable **Acción para conexiones entrantes**, la aplicación permitirá las conexiones de red entrantes que coincidan con los criterios de la regla.

6. En el bloque **Conexiones salientes**, establezca la configuración para las conexiones de red salientes:

   - Use la lista desplegable **Acción para conexiones salientes** para especificar la acción que la aplicación realizará para todas las conexiones de red salientes, a menos que haya reglas de Firewall para conexiones salientes que definan lo contrario.

   - De ser necesario, agregue reglas de Firewall para conexiones salientes.

     Las reglas que defina para las conexiones salientes en Firewall actuarán como exclusiones. Por ejemplo, si configura una regla de bloqueo para conexiones de red salientes y selecciona **Permitir** en la lista desplegable **Acción para conexiones salientes**, la aplicación bloqueará las conexiones de red salientes que coincidan con los criterios de la regla.

7. Guarde los cambios.

Kaspersky Embedded Systems Security aplica la nueva configuración. La fecha y la hora en que se modificó la configuración se guardarán en el registro de auditoría del sistema.

Ajustar la configuración general del componente Firewall en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.

2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la ficha **Configuración de la aplicación**.

4. En la sección **Control de actividad de red**, haga clic en el botón **Configurar** de la subsección **Firewall**.

   Se abre la ventana **Firewall**.

5. Configure el interruptor en **Firewall HABILITADO**.

6. En el bloque **Modo de funcionamiento de las reglas de bloqueo**, seleccione el modo de funcionamiento del componente:

   - **Observar el estado del Firewall de Windows**. El modo está diseñado para una transición sin problemas de la lógica de la tarea Administración del Firewall en la versión 3.4 o anteriores de la aplicación al Firewall con todas las funciones en la versión 4.0 y posteriores de la aplicación. Cuando se actualizan la versión 3.4 y anteriores de la aplicación, se mantienen las reglas de la tarea Administración del Firewall integrada en el Firewall de Windows. Pero el componente Firewall ya no interactúa con el Firewall de Windows, sino que solo supervisa el filtrado de tráfico del Firewall de Windows y registra los eventos correspondientes en el registro de operaciones del componente. Luego puede crear reglas de Firewall o importar reglas del Firewall de Windows y cambiar el modo de funcionamiento del Firewall a **Informar**.

   - **Informar**. La aplicación solo supervisa el funcionamiento de las reglas del Firewall y registra los eventos correspondientes en el registro de operaciones del componente. El modo está diseñado para probar las reglas del Firewall. Puede evaluar su aplicabilidad usando el registro de operaciones del Firewall. Luego, si es necesario, puede ajustar las reglas del Firewall y cambiar el modo de funcionamiento del Firewall a **Bloquear**.

   - **Bloquear**. La aplicación filtra el tráfico de red de acuerdo con la configuración del componente y registra los eventos correspondientes en el registro de funcionamiento del componente.

7. En el bloque **Conexiones entrantes**, establezca la configuración para las conexiones de red entrantes:

   - Use la lista desplegable **Acción para conexiones entrantes** para especificar la acción que la aplicación realizará para todas las conexiones de red entrantes, a menos que haya reglas de Firewall para conexiones entrantes que definan lo contrario.

   - De ser necesario, agregue reglas de Firewall para conexiones entrantes.

     Las reglas que defina para las conexiones entrantes en Firewall actuarán como exclusiones. Por ejemplo, si configura una regla de autorización para conexiones de red entrantes y selecciona **Bloquear** en la lista desplegable **Acción para conexiones entrantes**, la aplicación permitirá las conexiones de red entrantes que coincidan con los criterios de la regla.

8. En el bloque **Conexiones salientes**, establezca la configuración para las conexiones de red salientes:

   - Use la lista desplegable **Acción para conexiones salientes** para especificar la acción que la aplicación realizará para todas las conexiones de red salientes, a menos que haya reglas de Firewall para conexiones salientes que definan lo contrario.

   - De ser necesario, agregue reglas de Firewall para conexiones salientes.

     Las reglas que defina para las conexiones salientes en Firewall actuarán como exclusiones. Por ejemplo, si configura una regla de bloqueo para conexiones de red salientes y selecciona **Permitir** en la lista desplegable **Acción para conexiones salientes**, la aplicación bloqueará las conexiones de red salientes que coincidan con los criterios de la regla.

9. Guarde los cambios.

Kaspersky Embedded Systems Security aplica la nueva configuración. La fecha y la hora en que se modificó la configuración se guardarán en el registro de auditoría del sistema.

Ajustar la configuración general del componente Firewall en la Consola de la aplicación

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Control del equipo** → **Firewall**.

2. En el panel de resultados del nodo **Firewall**, haga clic en **Propiedades**.

   Se abre la ventana **Propiedades: Firewall**.

3. Seleccione la casilla de verificación **Firewall**.

4. En el bloque **Modo de funcionamiento de las reglas de bloqueo**, seleccione el modo de funcionamiento del componente:

   - **Observar el estado del Firewall de Windows**. El modo está diseñado para una transición sin problemas de la lógica de la tarea Administración del Firewall en la versión 3.4 o anteriores de la aplicación al Firewall con todas las funciones en la versión 4.0 y posteriores de la aplicación. Cuando se actualizan la versión 3.4 y anteriores de la aplicación, se mantienen las reglas de la tarea Administración del Firewall integrada en el Firewall de Windows. Pero el componente Firewall ya no interactúa con el Firewall de Windows, sino que solo supervisa el filtrado de tráfico del Firewall de Windows y registra los eventos correspondientes en el registro de operaciones del componente. Luego puede crear reglas de Firewall o importar reglas del Firewall de Windows y cambiar el modo de funcionamiento del Firewall a **Informar**.

   - **Informar**. La aplicación solo supervisa el funcionamiento de las reglas del Firewall y registra los eventos correspondientes en el registro de operaciones del componente. El modo está diseñado para probar las reglas del Firewall. Puede evaluar su aplicabilidad usando el registro de operaciones del Firewall. Luego, si es necesario, puede ajustar las reglas del Firewall y cambiar el modo de funcionamiento del Firewall a **Bloquear**.

   - **Bloquear**. La aplicación filtra el tráfico de red de acuerdo con la configuración del componente y registra los eventos correspondientes en el registro de funcionamiento del componente.

5. En el bloque **Conexiones entrantes**, establezca la configuración para las conexiones de red entrantes:

   - Use la lista desplegable **Acción para conexiones entrantes** para especificar la acción que la aplicación realizará para todas las conexiones de red entrantes, a menos que haya reglas de Firewall para conexiones entrantes que definan lo contrario.

   - De ser necesario, agregue reglas de Firewall para conexiones entrantes.

     Las reglas que defina para las conexiones entrantes en Firewall actuarán como exclusiones. Por ejemplo, si configura una regla de autorización para conexiones de red entrantes y selecciona **Bloquear** en la lista desplegable **Acción para conexiones entrantes**, la aplicación permitirá las conexiones de red entrantes que coincidan con los criterios de la regla.

6. En el bloque **Conexiones salientes**, establezca la configuración para las conexiones de red salientes:

   - Use la lista desplegable **Acción para conexiones salientes** para especificar la acción que la aplicación realizará para todas las conexiones de red salientes, a menos que haya reglas de Firewall para conexiones salientes que definan lo contrario.

   - De ser necesario, agregue reglas de Firewall para conexiones salientes.

     Las reglas que defina para las conexiones salientes en Firewall actuarán como exclusiones. Por ejemplo, si configura una regla de bloqueo para conexiones de red salientes y selecciona **Permitir** en la lista desplegable **Acción para conexiones salientes**, la aplicación bloqueará las conexiones de red salientes que coincidan con los criterios de la regla.

7. Guarde los cambios.

Kaspersky Embedded Systems Security aplica la nueva configuración. La fecha y la hora en que se modificó la configuración se guardarán en el registro de auditoría del sistema.

Creación y configuración de reglas de Firewall

Crear y configurar reglas de Firewall en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la sección **Control de actividad de red**, haga clic en el botón **Configuración** de la subsección **Firewall**.

   Se abre la ventana **Firewall**.
4. En el bloque **Conexiones entrantes**, haga clic en el botón **Lista de reglas**.

   Se abre la ventana **Reglas para conexiones entrantes**.
5. Cree y configure sus reglas de Firewall para conexiones entrantes.

   1. En la ficha **Aplicaciones**, haga clic en el botón **Agregar**.

      Se abre la ventana **Regla para aplicación**.
   2. Configure los parámetros de la regla:

      a. En el campo **Nombre de la regla**, escriba el nombre de la regla.

      > El nombre de la regla, independientemente de las mayúsculas y minúsculas que contenga, no debe coincidir con los nombres reservados "All", "ICMPv4" e "ICMPv6"; tampoco debe repetirse en la lista de reglas para conexiones de red entrantes.

      b. En la lista **Acción**, seleccione una de las opciones:

      - **Permitir**. Si selecciona esta opción, la aplicación permitirá las conexiones de red entrantes para la aplicación.
      - **Bloquear**. Si selecciona esta opción, la aplicación bloqueará las conexiones de red entrantes para la aplicación.

      c. Marque la casilla **Protocolo** para seleccionar el tipo de protocolo para el cual la aplicación controla las conexiones de red entrantes.

      d. En los bloques **Puertos locales** y **Puertos remotos**, ingrese un puerto o un intervalo de puertos.

      e. En el campo **Ruta de la aplicación**, ingrese la ruta al archivo ejecutable de la aplicación para la que está configurando la regla. Puede indicar la ruta manualmente o puede utilizar el botón **Examinar**.

f. En el campo **Alcance de aplicación de la regla**, ingrese direcciones de red. La aplicación controlará las conexiones entrantes que se originen en las direcciones de red especificadas siguiendo los ajustes de la regla.

> Solo el formato IPv4 es compatible con las direcciones IP.

g. En el bloque **Adaptadores de red**, especifique la lista de adaptadores de red.

h. Haga clic en el botón **Aceptar** para guardar la regla.

3. En la ficha **Puertos locales**, haga clic en el botón **Agregar**.

   Se abre la ventana **Regla para puertos**.

4. Configure los parámetros de la regla:

   a. En el campo **Nombre de la regla**, escriba el nombre de la regla.

   b. En la lista **Acción**, seleccione una de las opciones:

   - **Permitir**. Si selecciona esta opción, la aplicación permitirá las conexiones de red entrantes para los puertos.
   - **Bloquear**. Si selecciona esta opción, la aplicación bloqueará las conexiones de red entrantes para los puertos.

   c. Marque la casilla **Protocolo** para seleccionar el tipo de protocolo para el cual la aplicación controla las conexiones de red entrantes.

   d. En los bloques **Puertos locales** y **Puertos remotos**, ingrese un puerto o un intervalo de puertos.

   e. En el campo **Alcance de aplicación de la regla**, ingrese direcciones de red. La aplicación controlará las conexiones entrantes que se originen en las direcciones de red especificadas siguiendo los ajustes de la regla.

   > Solo el formato IPv4 es compatible con las direcciones IP.

   f. En el bloque **Adaptadores de red**, especifique la lista de adaptadores de red.

   g. Haga clic en el botón **Aceptar** para guardar la regla.

5. Haga clic en el botón **Aceptar** de la ventana **Reglas para conexiones entrantes**.

6. En el bloque **Conexiones salientes**, haga clic en el botón **Lista de reglas**.

   Se abre la ventana **Reglas para conexiones salientes**.

7. Cree y configure sus reglas de Firewall para conexiones salientes.

   1. En la ficha **Aplicaciones**, haga clic en el botón **Agregar**.

      Se abre la ventana **Regla para aplicación**.

2. Configure los parámetros de la regla:

   a. En el campo **Nombre de la regla**, escriba el nombre de la regla.

      El nombre de la regla, independientemente de las mayúsculas y minúsculas que contenga, no debe coincidir con los nombres reservados "All", "ICMPv4" e "ICMPv6"; tampoco debe repetirse en la lista de reglas para conexiones de red salientes.

   b. En la lista **Acción**, seleccione una de las opciones:

      - **Permitir**. Si selecciona esta opción, la aplicación permitirá las conexiones de red salientes para la aplicación.
      - **Bloquear**. Si selecciona esta opción, la aplicación bloqueará las conexiones de red salientes para la aplicación.

   c. Marque la casilla **Protocolo** para seleccionar el tipo de protocolo para el cual la aplicación controla las conexiones de red entrantes.

   d. En los bloques **Puertos locales** y **Puertos remotos**, ingrese un puerto o un intervalo de puertos.

   e. En el campo **Ruta de la aplicación**, ingrese la ruta al archivo ejecutable de la aplicación para la que está configurando la regla. Puede indicar la ruta manualmente o puede utilizar el botón **Examinar**.

   f. En el campo **Alcance de aplicación de la regla**, ingrese direcciones de red. La aplicación controlará las conexiones salientes que tengan como destino las direcciones de red especificadas siguiendo los ajustes de la regla.

      Solo el formato IPv4 es compatible con las direcciones IP.

   g. En el bloque **Adaptadores de red**, especifique la lista de adaptadores de red.

   h. Haga clic en el botón **Aceptar** para guardar la regla.

3. En la ficha **Puertos**, haga clic en el botón **Agregar**.

   Se abre la ventana **Regla para puertos**.

4. Configure los parámetros de la regla:

   a. En el campo **Nombre de la regla**, escriba el nombre de la regla.

   b. En la lista **Acción**, seleccione una de las opciones:

      - **Permitir**. Si selecciona esta opción, la aplicación permitirá las conexiones de red salientes a los puertos.
      - **Bloquear**. Si se selecciona esta opción, la aplicación bloquea las conexiones de red salientes a los puertos.

   c. Marque la casilla **Protocolo** para seleccionar el tipo de protocolo para el cual la aplicación controla las conexiones de red entrantes.

d. En los bloques **Puertos locales** y **Puertos remotos**, ingrese un puerto o un intervalo de puertos.

e. En el campo **Alcance de aplicación de la regla**, ingrese direcciones de red. La aplicación controlará las conexiones salientes que tengan como destino las direcciones de red especificadas siguiendo los ajustes de la regla.

> Solo el formato IPv4 es compatible con las direcciones IP.

f. En el bloque **Adaptadores de red**, especifique la lista de adaptadores de red.

g. Haga clic en el botón **Aceptar** para guardar la regla.

5. Haga clic en el botón **Aceptar** de la ventana **Reglas para conexiones salientes**.

8. Si desea importar o exportar reglas personalizadas desde un archivo XML, use los botones **Importar** o **Exportar** en el bloque **Importar y exportar reglas**.

9. Guarde los cambios.

Kaspersky Embedded Systems Security aplica la nueva configuración. La fecha y la hora en que se modificó la configuración se guardarán en el registro de auditoría del sistema.

Crear y configurar reglas de Firewall en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. En la sección **Control de actividad de red**, haga clic en el botón **Configurar** de la subsección **Firewall**.
   Se abre la ventana **Firewall**.
5. Configure el interruptor en **Firewall HABILITADO**.
6. En el bloque **Conexiones entrantes**, haga clic en el botón **Configurar**.
   Se abre la ventana **Reglas para conexiones entrantes**.
7. Cree y configure sus reglas de Firewall para conexiones entrantes.

   1. En la ficha **Puertos locales**, haga clic en el botón **Agregar**.
      Se abre la ventana **Regla para puertos**.

2. Configure los parámetros de la regla:

   a. En el campo **Nombre de la regla**, escriba el nombre de la regla.

   b. En la lista **Acción**, seleccione una de las opciones:

      - **Permitir**. Si selecciona esta opción, la aplicación permitirá las conexiones de red salientes a los puertos.
      - **Denegar**. Si se selecciona esta opción, la aplicación bloquea las conexiones de red salientes a los puertos.

   c. Marque la casilla **Protocolo** para seleccionar el tipo de protocolo para el cual la aplicación controla las conexiones de red entrantes.

   d. En los bloques **Puertos locales** y **Puertos remotos**, ingrese un puerto o un intervalo de puertos.

   e. En el campo **Alcance de aplicación de la regla**, ingrese direcciones de red. La aplicación controlará las conexiones salientes que tengan como destino las direcciones de red especificadas siguiendo los ajustes de la regla.

      Solo el formato IPv4 es compatible con las direcciones IP.

   f. En el bloque **Adaptadores de red**, especifique la lista de adaptadores de red.

   g. Haga clic en el botón **Aceptar** para guardar la regla.

3. En la ficha **Aplicaciones**, haga clic en el botón **Agregar**.

   Se abre la ventana **Regla para aplicaciones**.

4. Configure los parámetros de la regla:

   a. En el campo **Nombre de la regla**, escriba el nombre de la regla.

      El nombre de la regla, independientemente de las mayúsculas y minúsculas que contenga, no debe coincidir con los nombres reservados "All", "ICMPv4" e "ICMPv6"; tampoco debe repetirse en la lista de reglas para conexiones de red salientes.

   b. En la lista **Acción**, seleccione una de las opciones:

      - **Permitir**. Si selecciona esta opción, la aplicación permitirá las conexiones de red salientes para la aplicación.
      - **Denegar**. Si selecciona esta opción, la aplicación bloqueará las conexiones de red salientes para la aplicación.

   c. Marque la casilla **Protocolo** para seleccionar el tipo de protocolo para el cual la aplicación controla las conexiones de red entrantes.

   d. En los bloques **Puertos locales** y **Puertos remotos**, ingrese un puerto o un intervalo de puertos.

e. En el campo **Ruta de la aplicación**, ingrese manualmente la ruta al archivo ejecutable de la aplicación para la que está configurando la regla.

f. En el campo **Alcance de aplicación de la regla**, ingrese direcciones de red. La aplicación controlará las conexiones salientes que tengan como destino las direcciones de red especificadas siguiendo los ajustes de la regla.

> Solo el formato IPv4 es compatible con las direcciones IP.

g. En el bloque **Adaptadores de red**, especifique la lista de adaptadores de red.

h. Haga clic en el botón **Aceptar** para guardar la regla.

5. Haga clic en el botón **Aceptar** de la ventana **Reglas para conexiones entrantes**.

8. En el bloque **Conexiones salientes**, haga clic en el botón **Configurar**.

   Se abre la ventana **Reglas para conexiones salientes**.

9. Cree y configure sus reglas de Firewall para conexiones salientes.

   1. En la ficha **Puertos locales**, haga clic en el botón **Agregar**.

      Se abre la ventana **Regla para puertos**.

   2. Configure los parámetros de la regla:

      a. En el campo **Nombre de la regla**, escriba el nombre de la regla.

      b. En la lista **Acción**, seleccione una de las opciones:

      - **Permitir**. Si selecciona esta opción, la aplicación permitirá las conexiones de red salientes a los puertos.
      - **Denegar**. Si se selecciona esta opción, la aplicación bloquea las conexiones de red salientes a los puertos.

      c. Marque la casilla **Protocolo** para seleccionar el tipo de protocolo para el cual la aplicación controla las conexiones de red entrantes.

      d. En los bloques **Puertos locales** y **Puertos remotos**, ingrese un puerto o un intervalo de puertos.

      e. En el campo **Alcance de aplicación de la regla**, ingrese direcciones de red. La aplicación controlará las conexiones salientes que tengan como destino las direcciones de red especificadas siguiendo los ajustes de la regla.

      > Solo el formato IPv4 es compatible con las direcciones IP.

      f. En el bloque **Adaptadores de red**, especifique la lista de adaptadores de red.

      g. Haga clic en el botón **Aceptar** para guardar la regla.

3. En la ficha **Aplicaciones**, haga clic en el botón **Agregar**.

   Se abre la ventana **Regla para aplicaciones**.

4. Configure los parámetros de la regla:

   a. En el campo **Nombre de la regla**, escriba el nombre de la regla.

   > El nombre de la regla, independientemente de las mayúsculas y minúsculas que contenga, no debe coincidir con los nombres reservados "All", "ICMPv4" e "ICMPv6"; tampoco debe repetirse en la lista de reglas para conexiones de red salientes.

   b. En la lista **Acción**, seleccione una de las opciones:

   - **Permitir**. Si selecciona esta opción, la aplicación permitirá las conexiones de red salientes para la aplicación.
   - **Denegar**. Si selecciona esta opción, la aplicación bloqueará las conexiones de red salientes para la aplicación.

   c. Marque la casilla **Protocolo** para seleccionar el tipo de protocolo para el cual la aplicación controla las conexiones de red entrantes.

   d. En los bloques **Puertos locales** y **Puertos remotos**, ingrese un puerto o un intervalo de puertos.

   e. En el campo **Ruta de la aplicación**, ingrese manualmente la ruta al archivo ejecutable de la aplicación para la que está configurando la regla.

   f. En el campo **Alcance de aplicación de la regla**, ingrese direcciones de red. La aplicación controlará las conexiones salientes que tengan como destino las direcciones de red especificadas siguiendo los ajustes de la regla.

   > Solo el formato IPv4 es compatible con las direcciones IP.

   g. En el bloque **Adaptadores de red**, especifique la lista de adaptadores de red.

   h. Haga clic en el botón **Aceptar** para guardar la regla.

5. Haga clic en el botón **Aceptar** de la ventana **Reglas para conexiones salientes**.

10. Si desea importar o exportar reglas personalizadas desde un archivo XML, use los botones **Importación de reglas** o **Exportación de reglas** en el bloque **Importar y exportar reglas**.

11. Guarde los cambios.

Kaspersky Embedded Systems Security aplica la nueva configuración. La fecha y la hora en que se modificó la configuración se guardarán en el registro de auditoría del sistema.

Crear y configurar reglas de Firewall en la Consola de la aplicación

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Control del equipo** → **Firewall**.
2. En el panel de resultados del nodo **Firewall**, haga clic en **Propiedades**.

   Se abre la ventana **Propiedades: Firewall**.
3. En el bloque **Conexiones entrantes**, haga clic en el botón **Lista de reglas**.

   Se abre la ventana **Reglas para conexiones entrantes**.
4. Cree y configure sus reglas de Firewall para conexiones entrantes.

   1. En la ficha **Aplicaciones**, haga clic en el botón **Agregar**.

      Se abre la ventana **Regla para aplicación**.
   2. Configure los parámetros de la regla:

      a. En el campo **Nombre de la regla**, escriba el nombre de la regla.

      > El nombre de la regla, independientemente de las mayúsculas y minúsculas que contenga, no debe coincidir con los nombres reservados "All", "ICMPv4" e "ICMPv6"; tampoco debe repetirse en la lista de reglas para conexiones de red entrantes.

      b. En la lista **Acción**, seleccione una de las opciones:

      - **Permitir**. Si selecciona esta opción, la aplicación permitirá las conexiones de red entrantes para la aplicación.
      - **Bloquear**. Si selecciona esta opción, la aplicación bloqueará las conexiones de red entrantes para la aplicación.

      c. Marque la casilla **Protocolo** para seleccionar el tipo de protocolo para el cual la aplicación controla las conexiones de red entrantes.

      d. En los bloques **Puertos locales** y **Puertos remotos**, ingrese un puerto o un intervalo de puertos.

      e. En el campo **Ruta de la aplicación**, ingrese la ruta al archivo ejecutable de la aplicación para la que está configurando la regla. Puede indicar la ruta manualmente o puede utilizar el botón **Examinar**.

      f. En el campo **Alcance de aplicación de la regla**, ingrese direcciones de red. La aplicación controlará las conexiones entrantes que se originen en las direcciones de red especificadas siguiendo los ajustes de la regla.

      > Solo el formato IPv4 es compatible con las direcciones IP.

g. En el bloque **Adaptadores de red**, especifique la lista de adaptadores de red.

h. Haga clic en el botón **Aceptar** para guardar la regla.

3. En la ficha **Puertos locales**, haga clic en el botón **Agregar**.

   Se abre la ventana **Regla para puertos**.

4. Configure los parámetros de la regla:

   a. En el campo **Nombre de la regla**, escriba el nombre de la regla.

   b. En la lista **Acción**, seleccione una de las opciones:

   - **Permitir**. Si selecciona esta opción, la aplicación permitirá las conexiones de red entrantes para los puertos.
   - **Bloquear**. Si selecciona esta opción, la aplicación bloqueará las conexiones de red entrantes para los puertos.

   c. Marque la casilla **Protocolo** para seleccionar el tipo de protocolo para el cual la aplicación controla las conexiones de red entrantes.

   d. En los bloques **Puertos locales** y **Puertos remotos**, ingrese un puerto o un intervalo de puertos.

   e. En el campo **Alcance de aplicación de la regla**, ingrese direcciones de red. La aplicación controlará las conexiones entrantes que se originen en las direcciones de red especificadas siguiendo los ajustes de la regla.

   > Solo el formato IPv4 es compatible con las direcciones IP.

   f. En el bloque **Adaptadores de red**, especifique la lista de adaptadores de red.

   g. Haga clic en el botón **Aceptar** para guardar la regla.

5. Haga clic en el botón **Aceptar** de la ventana **Reglas para conexiones entrantes**.

5. En el bloque **Conexiones salientes**, haga clic en el botón **Lista de reglas**.

   Se abre la ventana **Reglas para conexiones salientes**.

6. Cree y configure sus reglas de Firewall para conexiones salientes.

   1. En la ficha **Aplicaciones**, haga clic en el botón **Agregar**.

      Se abre la ventana **Regla para aplicación**.

2. Configure los parámetros de la regla:

   a. En el campo **Nombre de la regla**, escriba el nombre de la regla.

      El nombre de la regla, independientemente de las mayúsculas y minúsculas que contenga, no debe coincidir con los nombres reservados "All", "ICMPv4" e "ICMPv6"; tampoco debe repetirse en la lista de reglas para conexiones de red salientes.

   b. En la lista **Acción**, seleccione una de las opciones:

      - **Permitir**. Si selecciona esta opción, la aplicación permitirá las conexiones de red salientes para la aplicación.
      - **Bloquear**. Si selecciona esta opción, la aplicación bloqueará las conexiones de red salientes para la aplicación.

   c. Marque la casilla **Protocolo** para seleccionar el tipo de protocolo para el cual la aplicación controla las conexiones de red entrantes.

   d. En los bloques **Puertos locales** y **Puertos remotos**, ingrese un puerto o un intervalo de puertos.

   e. En el campo **Ruta de la aplicación**, ingrese la ruta al archivo ejecutable de la aplicación para la que está configurando la regla. Puede indicar la ruta manualmente o puede utilizar el botón **Examinar**.

   f. En el campo **Alcance de aplicación de la regla**, ingrese direcciones de red. La aplicación controlará las conexiones salientes que tengan como destino las direcciones de red especificadas siguiendo los ajustes de la regla.

      Solo el formato IPv4 es compatible con las direcciones IP.

   g. En el bloque **Adaptadores de red**, especifique la lista de adaptadores de red.

   h. Haga clic en el botón **Aceptar** para guardar la regla.

3. En la ficha **Puertos**, haga clic en el botón **Agregar**.

   Se abre la ventana **Regla para puertos**.

4. Configure los parámetros de la regla:

   a. En el campo **Nombre de la regla**, escriba el nombre de la regla.

   b. En la lista **Acción**, seleccione una de las opciones:

      - **Permitir**. Si selecciona esta opción, la aplicación permitirá las conexiones de red salientes a los puertos.
      - **Bloquear**. Si se selecciona esta opción, la aplicación bloquea las conexiones de red salientes a los puertos.

   c. Marque la casilla **Protocolo** para seleccionar el tipo de protocolo para el cual la aplicación controla las conexiones de red entrantes.

d. En los bloques **Puertos locales** y **Puertos remotos**, ingrese un puerto o un intervalo de puertos.

e. En el campo **Alcance de aplicación de la regla**, ingrese direcciones de red. La aplicación controlará las conexiones salientes que tengan como destino las direcciones de red especificadas siguiendo los ajustes de la regla.

Solo el formato IPv4 es compatible con las direcciones IP.

f. En el bloque **Adaptadores de red**, especifique la lista de adaptadores de red.

g. Haga clic en el botón **Aceptar** para guardar la regla.

5. Haga clic en el botón **Aceptar** de la ventana **Reglas para conexiones salientes**.

7. Si desea importar o exportar reglas personalizadas desde un archivo XML, use los botones **Importar** o **Exportar** en el bloque **Importar y exportar reglas**.

8. Para importar reglas del Firewall de Windows, haga clic en **Importar reglas del Firewall de Windows**.

En equipos con Windows 11, versión 24H2, es posible que la aplicación omita ciertas reglas del Firewall de Windows. Debido a las características especiales que tiene esta versión del sistema operativo, es posible que Kaspersky Embedded Systems Security no reconozca los parámetros de algunas reglas de los paquetes de aplicaciones.

9. Guarde los cambios.

Kaspersky Embedded Systems Security aplica la nueva configuración. La fecha y la hora en que se modificó la configuración se guardarán en el registro de auditoría del sistema.

Habilitación y deshabilitación de Reglas de firewall

Crear y configurar reglas de Firewall en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.

2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.

3. En la sección **Control de actividad de red**, haga clic en el botón **Configuración** de la subsección **Firewall**.

Se abre la ventana **Firewall**.

4. En la ventana que se abre, haga clic en el botón **Lista de reglas** en la sección **Conexiones entrantes** o **Conexiones salientes**, según el tipo de regla cuyo estado desea cambiar.

5. En la ventana que se abre, seleccione la pestaña **Aplicaciones** o **Puertos locales**.

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. Para eliminar reglas de la lista, seleccione las reglas y haga clic en **Eliminar**.

7. Guarde los cambios.

Crear y configurar reglas de Firewall en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.

2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la ficha **Configuración de la aplicación**.

4. En la sección **Control de actividad de red**, haga clic en el botón **Configurar** de la subsección **Firewall**.

   Se abre la ventana **Firewall**.

5. En la ventana que se abre, haga clic en el botón **Configurar** en la sección **Conexiones entrantes** o **Conexiones salientes**, según el tipo de regla cuyo estado desea cambiar.

6. En la ventana que se abre, seleccione la pestaña **Puertos locales** o **Aplicaciones**.

   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.

7. Para eliminar reglas de la lista, seleccione las reglas y haga clic en **Eliminar**.

8. Guarde los cambios.

Crear y configurar reglas de Firewall en la Consola de la aplicación

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Control del equipo** → **Firewall**.
2. En el panel de resultados del nodo **Firewall**, haga clic en **Propiedades**.

   Se abre la ventana **Propiedades: Firewall**.
3. En la ventana que se abre, haga clic en el botón **Lista de reglas** en la sección **Conexiones entrantes** o **Conexiones salientes**, según el tipo de regla cuyo estado desea cambiar.
4. En la ventana que se abre, seleccione la pestaña **Aplicaciones** o **Puertos locales**.

   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.
5. Para eliminar reglas de la lista, seleccione las reglas y haga clic en **Eliminar**.
6. Guarde los cambios.

Prevención de ataques BadUSB

El componente Prevención de ataques BadUSB no se instala por defecto. Puede agregar un componente durante la instalación de la aplicación o cambiar el conjunto de componentes de la aplicación después de instalarla.

Algunos virus modifican el firmware de los dispositivos USB para hacer que el sistema operativo considere que el dispositivo USB es un teclado. De esta manera, el virus puede ejecutar comandos en su cuenta de usuario para descargar malware, por ejemplo.

El componente Prevención de ataques BadUSB impide que los dispositivos USB infectados que emulan un teclado se conecten al equipo.

Cuando un dispositivo USB se conecta al equipo y es identificado por el sistema operativo como un teclado, la aplicación le solicita al usuario que ingrese un código numérico generado por la aplicación desde este teclado, o con un Teclado en pantalla, si está disponible. Este procedimiento se conoce como autorización del teclado.

Si el código se ha ingresado correctamente, la aplicación guarda los parámetros de identificación (VID/PID del teclado y el número del puerto al cual se ha conectado) en la lista de teclados autorizados. No es necesario repetir la autorización del teclado cuando el teclado vuelve a conectarse o después del reinicio del sistema operativo.

Si el teclado autorizado se conecta a otro puerto USB del equipo, la aplicación mostrará otra vez una solicitud de autorización para este teclado.

Si se ha ingresado incorrectamente el código numérico, la aplicación genera un nuevo código. Puede configurar el número de intentos ingresando el código numérico. Si el código numérico se ingresa incorrectamente varias veces o se cierra la ventana de autorización del teclado, la aplicación bloquea la entrada desde este teclado. Cuando transcurre el tiempo de bloqueo del dispositivo USB o se reinicia el sistema operativo, la aplicación le solicita al usuario que lleve a cabo nuevamente la autorización del teclado.

La aplicación permite el uso de un teclado autorizado y bloquea un teclado que no haya sido autorizado.

Los dispositivos USB identificados por el sistema operativo como teclados y conectados al equipo antes de la instalación del componente de Prevención de ataques BadUSB se consideran autorizados después de la instalación del componente.

Cómo habilitar y configurar el componente Prevención de ataques BadUSB en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de las propiedades de la directiva, vaya a la sección **Control de actividad local**.
4. En el bloque **Prevención de ataques BadUSB**, haga clic en el botón **Configuración**.
   Se abre la ventana **Prevención de ataques BadUSB**.

5. Utilice la casilla **Prevención de ataques BadUSB** para habilitar o deshabilitar el componente.

6. En la sección **Autorización de dispositivos USB**, configure las siguientes opciones:

   - **Número máximo de intentos de autorización del dispositivo USB**. Bloquear automáticamente el dispositivo USB si el código de autorización se ingresa incorrectamente el número de veces especificado. Los valores válidos son de 1 a 10. Por ejemplo, si permite 5 intentos para ingresar el código de autorización, el dispositivo USB se bloquea después del quinto intento fallido. Kaspersky Embedded Systems Security muestra la duración del bloqueo del dispositivo USB. Una vez transcurrido este tiempo, puede tener 5 intentos para ingresar el código de autorización.

   - **Tiempo de espera al alcanzar el número máximo de intentos (minutos)**. Duración del bloqueo del dispositivo USB después del número especificado de intentos fallidos para ingresar el código de autorización. Los valores válidos son de 1 a 180 (minutos).

7. En la sección **Autorización del dispositivo USB al conectarlo**, configure las siguientes opciones:

   - **No permitir el uso del Teclado en pantalla para la autorización de dispositivos USB**. Si se selecciona la casilla de verificación, la aplicación bloquea el uso del teclado en pantalla para la autorización de dispositivos USB desde el cual no se puede ingresar un código de autorización (p. ej., un escáner de códigos de barra).

   - **Prohibición del uso de un código de barra para la autorización de dispositivos USB**. Si se selecciona la casilla de verificación, la aplicación no muestra el código de barras en la notificación de autorización del escáner de códigos de barras.

8. Cierre los candados para aplicar la directiva en los equipos.

9. Haga clic en **Aceptar** para guardar los cambios.

Cómo habilitar y configurar el componente Prevención de ataques BadUSB en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.

2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la ficha **Configuración de la aplicación**.

4. Seleccione la sección **Control de actividad local**.

5. En el bloque **Prevención de ataques BadUSB**, haga clic en el botón **Configurar**.

   Se abre la ventana **Prevención de ataques BadUSB**.

6. Use el interruptor **Prevención de ataques BadUSB** para habilitar o deshabilitar el componente.

7. Habilite o deshabilite **Prohibición del uso del Teclado en pantalla para la autorización de dispositivos USB HABILITADA** para permitir o bloquear el uso del teclado en pantalla para autorizar dispositivos USB desde el cual no se puede ingresar un código de autorización (p. ej., un escáner de códigos de barra).

8. Habilite o deshabilite **Prohibición del uso del código de barra para la autorización de dispositivos USB HABILITADA** para permitir o bloquear la visualización de un código de barras en la notificación de autorización del lector de códigos de barras.

9. En la sección **Autorización de dispositivos USB**, configure las siguientes opciones:

   - **Número máximo de intentos de autorización del dispositivo USB (1-10)**. Bloquear automáticamente el dispositivo USB si el código de autorización se ingresa incorrectamente el número de veces especificado. Los valores válidos son de 1 a 10. Por ejemplo, si permite 5 intentos para ingresar el código de autorización, el dispositivo USB se bloquea después del quinto intento fallido. Kaspersky Embedded Systems Security muestra la duración del bloqueo del dispositivo USB. Una vez transcurrido este tiempo, puede tener 5 intentos para ingresar el código de autorización.

   - **Tiempo de espera al alcanzar el número máximo de intentos en minutos (1-180)**. Duración del bloqueo del dispositivo USB después del número especificado de intentos fallidos para ingresar el código de autorización. Los valores válidos son de 1 a 180 (minutos).

10. Cierre los candados para aplicar la directiva en los equipos.

11. Haga clic en **Aceptar** para guardar los cambios.

Cómo habilitar y configurar el componente Prevención de ataques BadUSB en la Consola de la aplicación

1. En el árbol de la Consola de la aplicación, seleccione la sección **Control del equipo → Prevención de ataques BadUSB**.

2. Haga clic en el vínculo **Propiedades** del panel de resultados.

   Se abre la ventana **Prevención de ataques BadUSB**.

3. Utilice la casilla **Prevención de ataques BadUSB** para habilitar o deshabilitar el componente.

4. En la sección **Autorización de dispositivos USB**, configure las siguientes opciones:

   - **Número máximo de intentos de autorización del dispositivo USB**. Bloquear automáticamente el dispositivo USB si el código de autorización se ingresa incorrectamente el número de veces especificado. Los valores válidos son de 1 a 10. Por ejemplo, si permite 5 intentos para ingresar el código de autorización, el dispositivo USB se bloquea después del quinto intento fallido. Kaspersky Embedded Systems Security muestra la duración del bloqueo del dispositivo USB. Una vez transcurrido este tiempo, puede tener 5 intentos para ingresar el código de autorización.

   - **Tiempo de espera al alcanzar el número máximo de intentos (minutos)**. Duración del bloqueo del dispositivo USB después del número especificado de intentos fallidos para ingresar el código de autorización. Los valores válidos son de 1 a 180 (minutos).

5. En la sección **Autorización del dispositivo USB al conectarlo**, configure las siguientes opciones:

- **No permitir el uso del Teclado en pantalla para la autorización de dispositivos USB**. Si se selecciona la casilla de verificación, la aplicación bloquea el uso del teclado en pantalla para la autorización de dispositivos USB desde el cual no se puede ingresar un código de autorización (p. ej., un escáner de códigos de barra).

- **Prohibición del uso de un código de barra para la autorización de dispositivos USB**. Si se selecciona la casilla de verificación, la aplicación no muestra el código de barras en la notificación de autorización del escáner de códigos de barras.

6. Haga clic en **Aceptar** para guardar los cambios.

Control de integridad del sistema

Kaspersky Embedded Systems Security 4.0 ahora incluye el componente Control de integridad del sistema en lugar del componente Monitor de integridad de archivos. El componente Control de integridad del sistema incluye todas las funciones de Monitor de integridad de archivos y, además, permite supervisar los cambios del registro y la conexión de los dispositivos externos.

El componente Control de integridad del sistema supervisa los cambios en el sistema operativo que podrían indicar filtraciones de seguridad en el equipo. Cuando se detectan dichos cambios, Kaspersky Embedded Systems Security genera los eventos y las alertas correspondientes, y las envía al administrador. Control de integridad del sistema puede operar en tiempo real y también puede realizar controles de integridad del sistema a pedido.

Control de integridad del sistema en tiempo real

En el modo de tiempo real, Control de integridad del sistema realiza un seguimiento de los cambios en los objetos que incluyó en el alcance del componente (el alcance del monitoreo). Además, Control de integridad del sistema permite bloquear el acceso no autorizado a dichos objetos en tiempo real.

Comprobación de integridad del sistema a pedido

Comprobación de integridad del sistema a pedido es una tarea que se puede ejecutar manualmente o según una programación. Para ejecutar la tarea **Monitor comparativo de integridad del sistema**, debe configurar el alcance del componente (el alcance del monitoreo) y crear una línea de base. Una línea de base es un estado registrado de los objetos en el sistema que la aplicación usa como referencia cuando se compara con el estado actual. Se crea una línea de base cuando se inicia la tarea por primera vez.

Migración de la configuración de Monitor de integridad de archivos

Cuando se actualiza Kaspersky Embedded Systems Security 3.4 o versiones anteriores a la versión 4.0, la configuración de Monitor de acceso al registro y del Monitor de integridad de archivos se migra automáticamente. Como parte de la migración, la aplicación mueve las reglas de monitoreo a Control de integridad del sistema.

Acerca de las reglas de Control de integridad del sistema

Para que funcione Control de integridad del sistema, debe agregar al menos una regla. Una *regla de Control de integridad del sistema* es un conjunto de criterios que definen el acceso de los usuarios a los archivos o al registro. Control de integridad del sistema detecta cambios en los archivos o el registro dentro del *alcance del monitoreo* especificado. El alcance del monitoreo es uno de los criterios de una regla de Control de integridad del sistema.

Control de integridad del sistema permite supervisar los siguientes objetos:

- Archivos
- Registro
- Dispositivos externos

Consideraciones especiales involucradas en la supervisión de archivos

Control de integridad del sistema supervisa los cambios en los archivos y las carpetas, así como los archivos que se agregan al alcance del monitoreo o se eliminan de él. Estos cambios pueden indicar una filtración de seguridad informática. Recomendamos agregar objetos que rara vez se modifican u objetos a los que solo tiene acceso el administrador. Esto ayuda a reducir la cantidad de eventos de Control de integridad del sistema.

Kaspersky Embedded Systems Security supervisa los cambios de archivos y carpetas solo en aquellos discos que estaban conectados cuando comenzó a funcionar Control de integridad del sistema en tiempo real. Si un disco no estaba conectado cuando comenzó a funcionar Control de integridad del sistema en tiempo real, la aplicación no supervisa los cambios de archivos y carpetas en ese disco, incluso si los archivos y las carpetas se agregan al alcance del monitoreo.

Consideraciones especiales involucradas en la supervisión del registro

Control de integridad del sistema supervisa el registro. Estos cambios pueden indicar una filtración de seguridad informática.

Control de integridad del sistema supervisa las siguientes claves raíz del registro:

- `HKCR`
- `HKLM`
- `HKU`
- `HKCC`
- `HKEY_CLASSES_ROOT`
- `HKEY_LOCAL_MACHINE`
- `HKEY_USERS`
- `HKEY_CURRENT_CONFIG`.

Control de integridad del sistema no admite la clave `HKEY_CURRENT_USER`. Puede especificar una clave en `HKEY_USERS` como `HKEY_USERS\<user profile ID>\<key>`.

Consideraciones especiales involucradas en la supervisión de dispositivos externos

Control de integridad del sistema supervisa la conexión y desconexión de dispositivos externos. Esto es necesario para proteger el equipo de las amenazas de seguridad que pueden resultar del intercambio de archivos con dichos dispositivos. Control de integridad del sistema no supervisa el acceso a dispositivos externos y no bloquea el intercambio de archivos. Puede configurar el acceso a los dispositivos utilizando un componente diferente de la aplicación, Control de dispositivos.

Al ejecutar la tarea *Monitor comparativo de integridad del sistema*, la aplicación ignora la reconexión de dispositivos externos si los dispositivos tienen la misma letra de unidad en el sistema operativo. Para que se registren, los dispositivos reconectados deben tener distintas letras de unidad.

Control de integridad del sistema supervisa la conexión de los siguientes tipos de dispositivos externos:

- Unidad extraíble (incluidas las unidades flash USB)
- Disco duro.
- Adaptador de red externo.
- Unidad de CD/DVD/Blu-ray.
- Escáner o cámara.

Control de integridad del sistema en tiempo real

Control de integridad del sistema permite realizar un seguimiento de los cambios del sistema operativo en tiempo real. Puede realizar un seguimiento de cambios que pueden indicar filtraciones de seguridad en el equipo. El componente permite bloquear estos cambios o simplemente registrar eventos de cambio.

Para que funcione Control de integridad del sistema, debe agregar al menos una regla. Una regla de Control de integridad del sistema es un conjunto de criterios que definen el acceso de los usuarios a los archivos y al registro. Control de integridad del sistema detecta cambios en los archivos y el registro dentro del alcance del monitoreo especificado. El alcance del monitoreo es uno de los criterios de una regla de Control de integridad del sistema.

Cómo habilitar y configurar Control de integridad del sistema en tiempo real en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de propiedades de la directiva, seleccione **Inspección del sistema**.
4. En la sección **Control de integridad del sistema**, haga clic en **Configuración**.
5. Seleccione la casilla de verificación **Control de integridad del sistema**.
6. Configure el Monitor de integridad de archivos:
    a. Marque la casilla **Supervisar archivos** en la pestaña **Archivos**.
    b. Bajo **Modo de funcionamiento de las reglas de bloqueo**, seleccione un modo del Monitor de integridad de archivos:
        - **Bloquear**. En este modo, la aplicación realiza acciones en los archivos de acuerdo con las reglas del Monitor de integridad de archivos y genera los eventos correspondientes en el registro de Control de integridad del sistema.
        - **Informar**. En este modo, la aplicación solo genera eventos sobre las reglas del Monitor de integridad de archivos activadas en el registro de Control de integridad del sistema.

c. Agregue las reglas del Monitor de integridad de archivos manualmente usando el botón **Agregar** o importándolos desde un archivo XML. La configuración de las reglas del Monitor de integridad de archivos se describe en la siguiente tabla.

d. En la lista de reglas del Monitor de integridad de archivos, administre las casillas de verificación para dejar las reglas que necesita habilitadas.

7. Configure el Monitor de acceso al registro:

a. Marque la casilla **Supervisar el registro** en la pestaña **Registro**.

b. En **Modo de funcionamiento de las reglas de bloqueo**, seleccione un modo para el Monitor de acceso al registro:

- **Bloquear**. En este modo, la aplicación bloquea las acciones con el registro de acuerdo con las reglas del Monitor de acceso al registro y genera los eventos correspondientes en el registro de Control de integridad del sistema.
- **Informar**. En este modo, la aplicación solo genera eventos sobre las reglas del Monitor de acceso al registro activadas en el registro de Control de integridad del sistema.

c. Agregue las reglas del Monitor de acceso al registro manualmente usando el botón **Agregar** o importándolos desde un archivo XML. La configuración de las reglas del Monitor de acceso al registro se describe en la siguiente tabla.

d. En la lista de reglas del Monitor de acceso al registro, administre las casillas de verificación para dejar las reglas que necesita habilitadas.

8. Configure la supervisión de dispositivos externos:

a. Marque la casilla **Supervisar dispositivos** en la pestaña **Dispositivos**.

b. En la lista desplegable **Nivel de gravedad del evento**, seleccione el nivel de importancia de los eventos de supervisión de dispositivos externos: *Informativo*, *Advertencia* o *Crítico*.

Después de aplicar la configuración de supervisión de dispositivos externos, la aplicación recuerda las conexiones actuales de dispositivos externos. Posteriormente, cuando se conecta o desconecta un dispositivo externo, la aplicación genera un evento correspondiente en el registro del Control de integridad del sistema.

9. Guarde los cambios.

Cómo habilitar y configurar Control de integridad del sistema en tiempo real en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Inspección del sistema** → **Control de integridad del sistema** y haga clic en el botón **Configurar**.

5. Seleccione la casilla de verificación **Control de integridad del sistema**.

6. Configure el Monitor de integridad de archivos:

   a. Marque la casilla **Supervisar archivos** en la pestaña **Archivos**.

   b. Bajo **Modo de funcionamiento de las reglas de bloqueo**, seleccione un modo del Monitor de integridad de archivos:

      - **Bloquear**. En este modo, la aplicación realiza acciones en los archivos de acuerdo con las reglas del Monitor de integridad de archivos y genera los eventos correspondientes en el registro de Control de integridad del sistema.

      - **Informar**. En este modo, la aplicación solo genera eventos sobre las reglas del Monitor de integridad de archivos activadas en el registro de Control de integridad del sistema.

   c. Agregue las reglas del Monitor de integridad de archivos manualmente usando el botón **Agregar** o importándolos desde un archivo XML. La configuración de las reglas del Monitor de integridad de archivos se describe en la siguiente tabla.

   d. En la lista de reglas del Monitor de integridad de archivos, administre las casillas de verificación en la columna **Estado** para dejar las reglas que necesita habilitadas.

7. Configure el Monitor de acceso al registro:

   a. Marque la casilla **Supervisar el registro** en la pestaña **Registro**.

   b. En **Modo de funcionamiento de las reglas de bloqueo**, seleccione un modo para el Monitor de acceso al registro:

      - **Bloquear**. En este modo, la aplicación bloquea las acciones con el registro de acuerdo con las reglas del Monitor de acceso al registro y genera los eventos correspondientes en el registro de Control de integridad del sistema.

      - **Informar**. En este modo, la aplicación solo genera eventos sobre las reglas del Monitor de acceso al registro activadas en el registro de Control de integridad del sistema.

   c. Agregue las reglas del Monitor de acceso al registro manualmente usando el botón **Agregar** o importándolos desde un archivo XML. La configuración de las reglas del Monitor de acceso al registro se describe en la siguiente tabla.

   d. En la lista de reglas del Monitor de acceso al registro, administre las casillas de verificación en la columna **Estado** para dejar las reglas que necesita habilitadas.

8. Configure la supervisión de dispositivos externos:

   a. Marque la casilla **Supervisar dispositivos** en la pestaña **Dispositivos**.

   b. En la lista desplegable **Nivel de gravedad del evento**, seleccione el nivel de importancia de los eventos de supervisión de dispositivos externos: *Informativo*, *Advertencia* o *Crítico*.

      Control de integridad del sistema registra la conexión actual de dispositivos externos. La aplicación comienza a supervisar la conexión y desconexión de dispositivos externos después de que el componente se habilita en la configuración de la aplicación. Posteriormente, cuando se conecta o desconecta un dispositivo externo, la aplicación genera un evento correspondiente.

9. Guarde los cambios.

Cómo habilitar y configurar Control de integridad del sistema en tiempo real en la Consola de la aplicación

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Inspección del sistema** → **Control de integridad del sistema**.
2. En el panel de resultados del nodo **Control de integridad del sistema**, haga clic en **Propiedades**.

   Se abre la ventana **Propiedades: Control de integridad del sistema**.
3. Seleccione la casilla de verificación **Control de integridad del sistema**.
4. Configure el Monitor de integridad de archivos:
   a. Marque la casilla **Supervisar archivos** en la pestaña **Archivos**.
   b. Bajo **Modo de funcionamiento de las reglas de bloqueo**, seleccione un modo del Monitor de integridad de archivos:
      - **Bloquear**. En este modo, la aplicación realiza acciones en los archivos de acuerdo con las reglas del Monitor de integridad de archivos y genera los eventos correspondientes en el registro de Control de integridad del sistema.
      - **Informar**. En este modo, la aplicación solo genera eventos sobre las reglas del Monitor de integridad de archivos activadas en el registro de Control de integridad del sistema.
   c. Agregue las reglas del Monitor de integridad de archivos manualmente usando el botón **Agregar** o importándolos desde un archivo XML. La configuración de las reglas del Monitor de integridad de archivos se describe en la siguiente tabla.
   d. En la lista de reglas del Monitor de integridad de archivos, administre las casillas de verificación para dejar las reglas que necesita habilitadas.
5. Configure el Monitor de acceso al registro:
   a. Marque la casilla **Supervisar el registro** en la pestaña **Registro**.
   b. En **Modo de funcionamiento de las reglas de bloqueo**, seleccione un modo para el Monitor de acceso al registro:
      - **Bloquear**. En este modo, la aplicación bloquea las acciones con el registro de acuerdo con las reglas del Monitor de acceso al registro y genera los eventos correspondientes en el registro de Control de integridad del sistema.
      - **Informar**. En este modo, la aplicación solo genera eventos sobre las reglas del Monitor de acceso al registro activadas en el registro de Control de integridad del sistema.
   c. Agregue las reglas del Monitor de acceso al registro manualmente usando el botón **Agregar** o importándolos desde un archivo XML. La configuración de las reglas del Monitor de acceso al registro se describe en la siguiente tabla.
   d. En la lista de reglas del Monitor de acceso al registro, administre las casillas de verificación para dejar las reglas que necesita habilitadas.

6. Configure la supervisión de dispositivos externos:

   a. Marque la casilla **Supervisar dispositivos** en la pestaña **Dispositivos**.

   b. En la lista desplegable **Nivel de gravedad del evento**, seleccione el nivel de importancia de los eventos de supervisión de dispositivos externos: *Informativo*, *Advertencia* o *Crítico*.

      Después de aplicar la configuración de supervisión de dispositivos externos, la aplicación recuerda las conexiones actuales de dispositivos externos. Posteriormente, cuando se conecta o desconecta un dispositivo externo, la aplicación genera un evento correspondiente en el registro del Control de integridad del sistema.

7. Guarde los cambios.

Configuración de las reglas de Control de integridad del sistema

Parámetro	Descripción
Supervisar las operaciones de archivo en estas áreas	El alcance con el que desea aplicar el Monitor de integridad de archivos. Este campo es obligatorio. Usar máscaras: Kaspersky Embedded Systems Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara: El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco C:, pero no en las subcarpetas. Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT ubicados en carpetas dentro de la `Folder`, excepto la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida. El carácter `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras \ y /, que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las carpetas. Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.
Objetos supervisados	Aquí, puede especificar el nombre o valor de una clave del registro. Usar máscaras: Kaspersky Embedded Systems Security admite los caracteres `*` y `?` al ingresar una máscara:
Operaciones con archivos	• **Detectar**. La aplicación permite acciones en archivos en el alcance de la supervisión. • **Detectar y bloquear**. Lo que hace la aplicación depende del modo del Monitor de integridad de archivos seleccionado. Si seleccionó el modo *Bloquear*, Control de integridad del sistema permite las acciones con archivos del alcance de supervisión. Si seleccionó el modo *Informar*, Control de integridad del sistema permite las acciones con archivos del alcance del supervisión.
Grupos de usuarios o usuarios de confianza	Un usuario de confianza es un usuario al que se le permite realizar acciones con los archivos y las claves del registro en el alcance del monitoreo. Si Kaspersky Embedded Systems Security detecta una acción realizada por un usuario de confianza, Control de integridad del sistema genera un evento Informativo . Puede seleccionar usuarios en Active Directory, en la lista de cuentas en Kaspersky Security Center o ingresando un nombre de usuario local manualmente.
Marcadores de las operaciones sobre archivos/Acciones	Marcadores que describen la acción con los archivos o las claves del registro que supervisará la aplicación.
Detectar operaciones de archivos según todos los marcadores reconocidos/Detectar operaciones de registros según todos los marcadores reconocidos	De manera predeterminada, Kaspersky Embedded Systems Security detecta todos los marcadores de las operaciones del registro/archivo.
Detectar operaciones de archivos según los siguientes marcadores/Detectar operaciones de registros según los siguientes marcadores	En la lista de operaciones de registros/archivos disponibles, seleccione las casillas de verificación ubicadas junto a las operaciones que desea supervisar.

Parámetro	Descripción
Si es posible, calcule una suma de comprobación luego de realizar una operación de archivos. Esta se indicará en el registro de tareas	Si la casilla se selecciona, Kaspersky Embedded Systems Security calcula la suma de control del archivo modificado en caso de que se detecte una operación con archivos con al menos un marcador. Si varios marcadores detectan la operación con archivos, se calcula solo la suma de control del archivo final después de todas las modificaciones. Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security no calcula la suma de control de archivos modificados. Ningún cálculo de la suma de control se realiza en los casos siguientes: • Si el archivo se vuelve no disponible (por ejemplo, debido a un cambio de permisos de acceso). • Si la operación con archivos se detectó en un archivo que fue eliminado posteriormente. De forma predeterminada, la casilla no está activada.
Algoritmo de cálculo de sumas de comprobación	Seleccione uno de los algoritmos de cálculo de la suma de comprobación de la lista desplegable: • Hash MD5 • Hash SHA256
Exclusiones	En la pestaña **Exclusiones**, puede agregar objetos que desea excluir del alcance del monitoreo: • Para una regla del Monitor de integridad de archivos, puede especificar una lista de carpetas. • Para una regla de Monitor de acceso al registro, puede especificar valores o claves del registro. Usar máscaras: **Archivos** Lista de archivos y carpetas supervisados por el componente. Kaspersky Embedded Systems Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara: El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco C:, pero no en las subcarpetas. Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT ubicados en carpetas dentro de la `Folder`, excepto la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida. El carácter `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las carpetas. Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres. **Registro** Kaspersky Embedded Systems Security es compatible con los caracteres `*` y `?` al ingresar una máscara: las entradas de exclusión tienen una prioridad más alta que las entradas del alcance del monitoreo.
Nivel de gravedad del evento	Kaspersky Embedded Systems Security registra eventos de modificación de archivos cada vez que se cambia un archivo o una clave del registro del alcance del monitoreo. Los siguientes niveles de gravedad de eventos están disponibles: **Informativo**, **Advertencia**, **Crítico**.

Comprobación de integridad del sistema a pedido

Comprobación de integridad del sistema a pedido es una tarea que se puede ejecutar manualmente o según una programación. Cuando se ejecuta la tarea *Monitor comparativo de integridad del sistema*, la aplicación compara el estado actual de los objetos incluidos en el alcance del monitoreo con el estado de su *línea de base*. Se crea una línea de base cuando se inicia la tarea por primera vez.

Para que funcione Control de integridad del sistema, debe agregar al menos una regla. Una regla de Control de integridad del sistema es un conjunto de criterios que definen el acceso de los usuarios a los archivos y al registro. Control de integridad del sistema detecta cambios en los archivos y el registro dentro del alcance del monitoreo especificado. El alcance del monitoreo es uno de los criterios de una regla de Control de integridad del sistema.

Configuración del alcance del monitoreo para la tarea Monitor comparativo de integridad del sistema

De manera predeterminada, el alcance del monitoreo de la tarea *Monitor comparativo de integridad del sistema* es el mismo que el alcance del monitoreo de Control de integridad del sistema. Puede configurar un alcance del monitoreo diferente para la tarea.

Control de integridad del sistema no admite la importación de las claves `HKEY_CURRENT_USER` ni `HKEY_CURRENT_CONFIG` para la tarea *Comprobación de integridad del sistema*. Si el alcance del control de la tarea contiene estas claves, la aplicación genera el evento *El alcance del monitoreo incluye objetos incorrectos*.

Cómo configurar un alcance del monitoreo diferente para la tarea Monitor comparativo de integridad del sistema en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Tareas**.
2. Seleccione la tarea *Monitor comparativo de integridad del sistema* necesaria y haga doble clic para abrir las propiedades de la tarea.
3. En la ventana que se abre, seleccione **Configuración**.
4. Configure el monitoreo de archivos:
   a. Marque la casilla **Supervisar archivos** en la pestaña **Archivos**.
   b. Marque las casillas para seleccione las reglas de la lista.
   c. Si es necesario, agregue una nueva regla al hacer clic en el botón **Agregar**. La configuración de la regla Monitor comparativo de integridad del sistema se describe en la siguiente tabla.
   d. También puede importar reglas de otra fuente.
5. Configure el monitoreo del registro:
   a. Marque la casilla **Supervisar el registro** en la pestaña **Registro**.
   b. Marque las casillas para seleccione las reglas de la lista.
   c. Si es necesario, agregue una nueva regla al hacer clic en el botón **Agregar**. La configuración de la regla Monitor comparativo de integridad del sistema se describe en la siguiente tabla.
   d. También puede importar reglas de otra fuente.

6. Configure la supervisión de dispositivos externos:

    a. Marque la casilla **Supervisar dispositivos** en la pestaña **Dispositivos**.

    b. En la lista desplegable **Nivel de gravedad del evento**, seleccione el nivel de importancia de los eventos de supervisión de dispositivos externos: *Informativo*, *Advertencia* o *Crítico*.

    La tarea Monitor comparativo de integridad del sistema registra información sobre los dispositivos externos conectados en el momento en que se crea la línea de base. Posteriormente, cuando se conecta un dispositivo externo, la aplicación genera un evento correspondiente. Cuando se ejecuta la tarea, la aplicación no supervisa la desconexión de los dispositivos externos.

7. Guarde los cambios.

Cómo configurar un alcance del monitoreo diferente para la tarea Monitor comparativo de integridad del sistema en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Tareas**.

2. Seleccione la tarea *Monitor comparativo de integridad del sistema* necesaria y haga doble clic para abrir las propiedades de la tarea.

3. En la ventana que se abre, seleccione **Configuración de la aplicación**.

4. Configure el monitoreo de archivos:

    a. Seleccione la casilla de verificación **Supervisar archivos**.

    b. Marque las casillas para seleccione las reglas de la lista.

    c. Si es necesario, agregue una nueva regla al hacer clic en el botón **Agregar**. La configuración de la regla Monitor comparativo de integridad del sistema se describe en la siguiente tabla.

    d. También puede importar reglas de otra fuente.

5. Configure el monitoreo del registro:

    a. Seleccione la casilla de verificación **Supervisar el registro**.

    b. Marque las casillas para seleccione las reglas de la lista.

    c. Si es necesario, agregue una nueva regla al hacer clic en el botón **Agregar**. La configuración de la regla Monitor comparativo de integridad del sistema se describe en la siguiente tabla.

    d. También puede importar reglas de otra fuente.

6. Configure la supervisión de dispositivos externos:

    a. Seleccione la casilla de verificación **Supervisar dispositivos**.

    b. En la lista desplegable **Nivel de gravedad del evento**, seleccione el nivel de importancia de los eventos de supervisión de dispositivos externos: *Informativo*, *Advertencia* o *Crítico*.

    La tarea *Monitor comparativo de integridad del sistema* registra información sobre los dispositivos externos conectados en el momento en que se crea la línea de base. Posteriormente, cuando se conecta un dispositivo externo, la aplicación genera un evento correspondiente. Cuando se ejecuta la tarea, la aplicación no supervisa la desconexión de los dispositivos externos.

7. Guarde los cambios.

Cómo configurar un alcance del monitoreo diferente para la tarea Monitor comparativo de integridad del sistema en la Consola de la aplicación

Las propiedades de la tarea **Monitor comparativo de integridad del sistema** se pueden editar en la Consola de Kaspersky Embedded Systems Security si la tarea se creó localmente o si la casilla **Permitir el uso de tareas locales** está seleccionada en la sección **Configuración de la aplicación → Ejecutar tareas locales del sistema** de las propiedades de la directiva.

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Inspección del sistema → Monitor comparativo de integridad del sistema**.

2. En el panel de resultados del nodo **Monitor comparativo de integridad del sistema**, haga clic en **Propiedades**.

    Se abre la ventana **Propiedades: Monitor comparativo de integridad del sistema**.

3. Configure el monitoreo de archivos:

    a. Marque la casilla **Supervisar archivos** en la pestaña **Archivos**.

    b. Marque las casillas para seleccione las reglas de la lista.

    c. Si es necesario, agregue una nueva regla al hacer clic en el botón **Agregar**. La configuración de la regla Monitor comparativo de integridad del sistema se describe en la siguiente tabla.

    d. También puede importar reglas de otra fuente.

4. Configure el monitoreo del registro:

    a. Marque la casilla **Supervisar el registro** en la pestaña **Registro**.

    b. Marque las casillas para seleccione las reglas de la lista.

    c. Si es necesario, agregue una nueva regla al hacer clic en el botón **Agregar**. La configuración de la regla Monitor comparativo de integridad del sistema se describe en la siguiente tabla.

    d. También puede importar reglas de otra fuente.

5. Configure la supervisión de dispositivos externos:

   a. Marque la casilla **Supervisar dispositivos** en la pestaña **Dispositivos**.

   b. En la lista desplegable **Nivel de gravedad del evento**, seleccione el nivel de importancia de los eventos de supervisión de dispositivos externos: *Informativo*, *Advertencia* o *Crítico*.

      La tarea Monitor comparativo de integridad del sistema registra información sobre los dispositivos externos conectados en el momento en que se crea la línea de base. Posteriormente, cuando se conecta un dispositivo externo, la aplicación genera un evento correspondiente. Cuando se ejecuta la tarea, la aplicación no supervisa la desconexión de los dispositivos externos.

6. Guarde los cambios.

Configuración de una regla de la tarea Monitor comparativo de integridad del sistema

Parámetro	Descripción
Supervisar las operaciones de archivo en estas áreas	El alcance con el que desea aplicar el Monitor de integridad de archivos. Este campo es obligatorio. Usar máscaras: Kaspersky Embedded Systems Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara: El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco C:, pero no en las subcarpetas. Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT ubicados en carpetas dentro de la `Folder`, excepto la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida. El carácter `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras \ y /, que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las carpetas. Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres.
Objetos supervisados	Aquí, puede especificar el nombre o valor de una clave del registro. Usar máscaras: Kaspersky Embedded Systems Security admite los caracteres `*` y `?` al ingresar una máscara:
Exclusiones	En la pestaña **Exclusiones**, puede agregar objetos que desea excluir del alcance del monitoreo: • Para una regla del Monitor de integridad de archivos, puede especificar una lista de carpetas. • Para una regla de Monitor de acceso al registro, puede especificar valores o claves del registro. Usar máscaras: **Archivos** Lista de archivos y carpetas supervisados por el componente. Kaspersky Embedded Systems Security admite variables de entorno y los caracteres `*` y `?` al ingresar una máscara: El carácter `*` (asterisco) puede usarse para representar cualquier cantidad de caracteres. Los únicos símbolos que no puede representar son las dos barras (`\` y `/`), que se utilizan para delimitar los nombres de los archivos y de las carpetas en las rutas de acceso. Por ejemplo, la máscara `C:\*\*.txt` incluirá todas las rutas a archivos con la extensión TXT localizada en carpetas en el disco C:, pero no en las subcarpetas. Dos caracteres `*` consecutivos toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la carpeta, incluidos los caracteres `\` y `/` (delimitadores de los nombres de archivos y carpetas en rutas a archivos y carpetas). Por ejemplo, la máscara `C:\Folder\**\*.txt` incluirá todas las rutas a archivos con la extensión TXT ubicados en carpetas dentro de la `Folder`, excepto la `Folder` misma. La máscara debe incluir al menos un nivel de anidación. La máscara `C:\**\*.txt` no es válida. El carácter `?` (signo de interrogación) puede usarse para representar casi cualquier carácter individual; se excluyen únicamente las barras (`\` y `/`), que se utilizan en las rutas de acceso para delimitar los nombres de los archivos y las carpetas. Por ejemplo, la máscara `C:\Folder\???.txt` incluirá las rutas a todos los archivos de la carpeta llamada `Folder` que tengan la extensión TXT y cuyo nombre sea de tres caracteres. **Registro** Kaspersky Embedded Systems Security es compatible con los caracteres `*` y `?` al ingresar una máscara: las entradas de exclusión tienen una prioridad más alta que las entradas del alcance del monitoreo.
Nivel de gravedad del evento	Kaspersky Embedded Systems Security registra eventos de modificación de archivos cada vez que se cambia un archivo o una clave del registro del alcance del monitoreo. Los siguientes niveles de gravedad de eventos están disponibles: **Informativo**, **Advertencia**, **Crítico**.

Ejecución de la tarea Monitor comparativo de integridad del sistema

La tarea **Monitor comparativo de integridad del sistema** permite verificar los archivos o las claves del registro para detectar cambios y también verifica la conexión de los dispositivos externos. Para buscar cambios en los archivos, puede ejecutar la tarea **Monitor comparativo de integridad del sistema** en los siguientes modos:

- **Análisis completo**. En este modo, la aplicación verifica todos los atributos y hashes de los archivos.
- **Análisis rápido**. En este modo, la aplicación verifica solo los atributos de los archivos.

El modo en el que se ejecuta la tarea no afecta la comprobación del registro o de los dispositivos externos.

Cómo ejecutar la tarea Monitor comparativo de integridad del sistema en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Nueva tarea**.

   Se inicia el Asistente de tareas. Siga las instrucciones del Asistente.

3. Seleccione **Kaspersky Embedded Systems Security → Monitor comparativo de integridad del sistema**. Seleccione un modo de Control de integridad del sistema:

   - **Análisis completo**. En este modo, la aplicación verifica todos los atributos y hashes de los archivos.
   - **Análisis rápido**. En este modo, la aplicación verifica solo los atributos de los archivos.

4. Seleccione los equipos en los que se ejecutará la tarea. Las siguientes opciones están disponibles:

   - Seleccione los equipos detectados por el Servidor de Administración en la red: dispositivos no asignados. Los dispositivos específicos pueden incluir dispositivos en grupos de administración, así como dispositivos no asignados.
   - Especifique direcciones de dispositivo manualmente o importe direcciones de una lista. Puede especificar los nombres NetBIOS, las direcciones IP y las subredes IP de los dispositivos a los que desea asignar la tarea.
   - Especifique la selección de dispositivos para los que desea ejecutar la tarea.
   - Asignar la tarea a un grupo de administración. En este caso, la tarea se asigna a los equipos incluidos en un grupo de administración creado anteriormente.

5. Seleccione una cuenta para ejecutar la tarea. De manera predeterminada, Kaspersky Embedded Systems Security ejecutará la tarea con los derechos de una cuenta de usuario local.

6. Configure una programación para la tarea; por ejemplo, manualmente o en un día determinado de la semana.

7. Ingrese el nombre de la tarea.

8. Complete el asistente. Si es necesario, seleccione la casilla **Ejecutar la tarea al finalizar el asistente**. Podrá ver el progreso de la tarea en las propiedades de la misma.

Cómo ejecutar la tarea Monitor comparativo de integridad del sistema en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Agregar**.

   Se inicia el Asistente de tareas.

3. Configure los parámetros de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione Kaspersky Embedded Systems Security.

   b. En la lista desplegable **Tipo de tarea**, seleccione **Monitor comparativo de integridad del sistema**.

   c. En el campo **Nombre de la tarea**, escriba una breve descripción (por ejemplo, *Comprobación de integridad del sistema semanal*).

4. En el bloque **Dispositivos a los que se asignará la tarea**, seleccione el alcance de la tarea.

5. Seleccione los dispositivos de acuerdo con la opción de alcance de la tarea seleccionada. Vaya al siguiente paso.

6. Seleccione el algoritmo de cálculo de la suma de comprobación.

7. Seleccione una cuenta para ejecutar la tarea. De manera predeterminada, Kaspersky Embedded Systems Security ejecutará la tarea con los derechos de una cuenta de usuario local.

8. Complete el asistente.

   La nueva tarea aparecerá en la lista de tareas.

9. Haga clic en la tarea nueva.

   Se abre la ventana de propiedades de la tarea.

10. Seleccione la ficha **Configuración de la aplicación**.

11. Seleccione un modo de Comprobación de integridad del sistema:

    - **Análisis completo**. En este modo, la aplicación verifica todos los atributos y hashes de los archivos.
    - **Análisis rápido**. En este modo, la aplicación verifica solo los atributos de los archivos.

12. Guarde los cambios.

13. Active la casilla ubicada junto a la tarea.

14. Haga clic en **Iniciar**.

Exportación e importación de las reglas de Control de integridad del sistema

Puede exportar la lista de reglas de Control de integridad del sistema a un archivo XML. A continuación, puede modificar el archivo para, por ejemplo, agregar una gran cantidad de registros del mismo tipo. Puede utilizar la función de exportación/importación para crear una copia de seguridad de la lista de reglas de Control de integridad del sistema o para migrar la lista a otro servidor.

Control de integridad del sistema no admite la importación de las claves `HKEY_CURRENT_USER` ni `HKEY_CURRENT_CONFIG` para la tarea *Comprobación de integridad del sistema*. Si el alcance del control de la tarea contiene estas claves, la aplicación genera el evento *El alcance del monitoreo incluye objetos incorrectos*.

Cómo exportar e importar una lista de reglas de Control de integridad del sistema en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de propiedades de la directiva, seleccione **Inspección del sistema**.
4. En la sección **Control de integridad del sistema**, haga clic en **Configuración**.
5. Para exportar reglas de archivo/registro:
   a. En la pestaña **Archivos** o **Registro**, seleccione las reglas que desea exportar.
   b. Haga clic en el botón **Exportar** y seleccione **Exportar seleccionados**.
   c. Si no seleccionó ninguna regla y hace clic en **Exportar** → **Exportar**, Kaspersky Embedded Systems Security exporta todas las reglas.
   d. En la ventana que se abre, escriba el nombre del archivo XML en el que se guardará la lista de reglas exportada. Seleccione también la carpeta en la que se guardará este archivo.
   e. Guarde el archivo.
      Kaspersky Embedded Systems Security exportará la lista de reglas al archivo XML.
6. Para importar reglas de archivo/registro:
   a. En la pestaña **Archivos** o **Registro**, haga clic en el botón **Importar**.
      En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de reglas.

b. Abra el archivo.

Cuando ya exista una lista de reglas en el equipo, Kaspersky Embedded Systems Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.

7. Guarde los cambios.

Cómo exportar e importar una lista de reglas de Control de integridad del sistema en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Inspección del sistema** → **Control de integridad del sistema** y haga clic en el botón **Configurar**.

   Se abre la ventana **Configuración de Control de integridad del sistema**.
5. Para exportar reglas de archivo/registro:

   a. En la pestaña **Archivo** o **Registro**, seleccione las reglas que desea exportar.

   b. Haga clic en el botón **Exportar**. En la ventana que se abre, especifique si desea exportar las reglas seleccionadas o todas las reglas. Luego, haga clic en **Exportar**.

   Si no seleccionó ninguna regla, Kaspersky Embedded Systems Security exportará todas las reglas.
6. Kaspersky Embedded Systems Security exportará la lista de reglas al archivo XML.
7. Para importar reglas de archivo/registro:

   a. En la pestaña **Archivo** o **Registro**, haga clic en el botón **Importar desde la versión anterior** si desea importar reglas desde un archivo XML creado en la versión 3.4 o una versión anterior de la aplicación.

   Si importará reglas desde un archivo XML creado en la versión 4.0 o una versión posterior, haga clic en **Importar**.

   b. Cuando ya exista una lista de reglas en el equipo, Kaspersky Embedded Systems Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.

   c. En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de reglas.

   d. Haga clic en **Importar**.
8. Guarde los cambios.

Cómo exportar e importar una lista de reglas de Control de integridad del sistema en la Consola de la aplicación

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Inspección del sistema** → **Control de integridad del sistema**.
2. En el panel de resultados del nodo **Control de integridad del sistema**, haga clic en **Propiedades**.

   Se abre la ventana **Propiedades: Control de integridad del sistema**.
3. Para exportar reglas de archivo/registro:
   a. En la pestaña **Archivos** o **Registro**, seleccione las reglas que desea exportar.
   b. Haga clic en el botón **Exportar** y seleccione **Exportar seleccionados**.
   c. Si no seleccionó ninguna regla y hace clic en **Exportar** → **Exportar**, Kaspersky Embedded Systems Security exporta todas las reglas.
   d. En la ventana que se abre, escriba el nombre del archivo XML en el que se guardará la lista de reglas exportada. Seleccione también la carpeta en la que se guardará este archivo.
   e. Guarde el archivo.

      Kaspersky Embedded Systems Security exportará la lista de reglas al archivo XML.
4. Para importar reglas de archivo/registro:
   a. En la pestaña **Archivos** o **Registro**, haga clic en el botón **Importar**.

      En la ventana que se abre, seleccione el archivo XML que se usará para importar la lista de reglas.
   b. Abra el archivo.

      Cuando ya exista una lista de reglas en el equipo, Kaspersky Embedded Systems Security le preguntará si desea eliminarla o si prefiere complementarla con las entradas del archivo XML.
5. Guarde los cambios.

Visualización de los informes de Control de integridad del sistema

Para analizar el rendimiento de las reglas de Control de integridad del sistema, puede consultar los informes y eventos generados por la aplicación. Kaspersky Embedded Systems Security genera los siguientes informes sobre el componente:

- En la interfaz de la aplicación:
  - El informe Actualización básica.

  Los informes contienen los eventos de Control de integridad del sistema.

- En la Consola de Kaspersky Security Center
  - El informe sobre los equipos en los que se activaron las reglas de monitoreo la mayor cantidad de veces
  - El informe sobre las reglas de monitoreo activadas con mayor frecuencia

    Para generar un informe sobre las reglas de supervisión activadas con mayor frecuencia, la aplicación registra los siguientes eventos:

    - *Se detectó el cambio de un archivo o una carpeta*
    - *Solo estadísticas: operación de archivo no permitida en área controlada*
    - *Operación de archivo permitida en un área controlada realizada por un usuario de confianza*
    - *Operación de archivo no controlada en área controlada*.

    > Para configurar la duración del almacenamiento de estos eventos, en la sección **Configuración de eventos** de la directiva, especifique la duración del evento general de Control de integridad del sistema: *Se detectó el cambio de un archivo o una carpeta*.

De manera predeterminada, se crea un informe para los 30 días anteriores, incluida la fecha en que se crea el informe.

Cómo ver los informes de Control de integridad del sistema en la Consola de administración de Kaspersky Security Center

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el nodo del **Servidor de administración** del árbol de la Consola de administración, seleccione la pestaña **Informes**.
3. Haga clic en **Nueva plantilla de informe**.

   Se inicia el Asistente de nueva plantilla de informe.
4. Siga las instrucciones del Asistente de plantilla de informe. En el paso **Selección del tipo de plantilla de informe**, seleccione el informe Control de integridad del sistema (la sección **Otro**):
   - **Los 10 dispositivos cuyas reglas de Monitor de integridad de archivos / Control de integridad del sistema se desencadenan con mayor frecuencia**.
   - **Las 10 reglas Monitor de integridad de archivos / Control de integridad del sistema que se activaron con mayor frecuencia en los dispositivos**.

   Una vez que haya terminado con el Asistente de nueva plantilla de informe, la plantilla de informe nueva aparecerá en la tabla de la pestaña **Informes**.
5. Abra el informe haciendo doble clic en él.

Se inicia el proceso de generación del informe. El informe se muestra en una ventana nueva.

Cómo ver los informes de Control de integridad del sistema en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Supervisión e informes → Informes**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente de nueva plantilla de informe.
3. En **Plantilla**, en la sección **Otros**, seleccione un informe del Control de integridad del sistema:

   - **Los 10 dispositivos cuyas reglas de Monitor de integridad de archivos / Control de integridad del sistema se desencadenan con mayor frecuencia**.
   - **Las 10 reglas Monitor de integridad de archivos / Control de integridad del sistema que se activaron con mayor frecuencia en los dispositivos**.

   Una vez que haya terminado con el Asistente de nueva plantilla de informe, la plantilla de informe nueva aparecerá en la tabla.
4. Seleccione y ejecute el informe.

Se inicia el proceso de generación del informe. El informe se muestra en una ventana nueva.

Para ver los eventos generados por la aplicación, también puede usar las selecciones de eventos de la consola de Kaspersky Security Center.

Inspección de registros

Inspección de registro monitorea la integridad del entorno protegido en función del análisis del registro de eventos de Windows. Cuando la aplicación detecta indicios de un comportamiento atípico en el sistema, informa al administrador, ya que este comportamiento puede indicar un intento de ciberataque.

Kaspersky Embedded Systems Security analiza los registros de eventos de Windows y detecta las infracciones de acuerdo con las reglas. El componente incluye reglas predefinidas. Las reglas predefinidas funcionan con análisis heurístico. También puede agregar sus propias reglas (reglas personalizadas). Cuando se activa una regla, la aplicación crea un evento con el estado *Crítico*.

Si desea utilizar Inspección de registro, asegúrese de que la directiva de auditoría esté configurada y que el sistema registre los eventos relevantes (para obtener información, consulte el Sitio web de soporte técnico de Microsoft.).

Parámetro	Descripción
Reglas predefinidas	Lista de reglas de Inspección de registro. Las reglas predefinidas incluyen plantillas de actividad anormal en el equipo protegido. La actividad anormal puede implicar un intento de ataque.
Reglas personalizadas	Lista de reglas de Inspección de registro que agregó el usuario. Puede establecer sus propios criterios de activación de las reglas de Inspección de registro. Para hacerlo, debe ingresar un ID de evento y seleccionar una fuente de evento. Puede seleccionar un origen de eventos entre los registros estándar: *Application*, *Security* o *System*. También puede especificar el registro de una aplicación de terceros.

Agregar reglas personalizadas

Puede establecer sus propios criterios de activación de las reglas de Inspección de registro. Para hacerlo, debe ingresar un ID de evento y seleccionar una fuente de evento. Puede buscar el ID del evento en el sitio web de soporte técnico de Microsoft. Puede seleccionar un origen de eventos entre los registros estándar: *Application*, *Security* o *System*. También puede especificar el registro de una aplicación de terceros. Puede averiguar el nombre del registro de la aplicación de terceros con la herramienta Visor de eventos. Los registros de aplicaciones de terceros se guardan en la carpeta Registros de aplicaciones y servicios (por ejemplo, el registro de *Windows PowerShell*).

La aplicación no comprueba si el registro especificado está realmente presente en el Registro de eventos de Windows. Si hay un error en el nombre del registro, la aplicación no monitorea los eventos de ese registro.

La lista de reglas personalizadas ya incluye varias reglas que crearon expertos de Kaspersky.

Para agregar una regla personalizada en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de propiedades de la directiva, seleccione **Inspección del sistema**.

4. En la sección **Inspección de registros**, haga clic en **Configuración**.
5. Seleccione la casilla de verificación **Inspección de registros**.
6. En la pestaña **Reglas personalizadas**, seleccione la casilla **Aplicar reglas personalizadas en Inspección de registros**.
7. Active las casillas ubicadas junto a las reglas personalizadas que desee habilitar.
8. Si es necesario, haga clic en **Agregar** para crear sus reglas personalizadas.
9. Esto abre una ventana, donde debe configurar la regla personalizada:
   - **Nombre de la regla**.
   - **Nombre del registro**. Registros de eventos de Windows. Estos son los registros disponibles: *Application*, *Security* o *System*.
   - **Fuente**. Registros de aplicaciones de terceros. Puede averiguar el nombre del registro de la aplicación de terceros con la herramienta Visor de eventos. Los registros de aplicaciones de terceros se guardan en la carpeta Registros de aplicaciones y servicios (por ejemplo, el registro de Windows PowerShell).
   - **Identificadores de eventos**. ID de eventos en el Registro de eventos de Windows. Puede buscar el ID del evento en la documentación técnica de Microsoft.
10. Guarde los cambios.

Para agregar una regla personalizada en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Inspección del sistema** → **Inspección de registros** y haga clic en el botón **Configurar**.
5. Seleccione la casilla de verificación **Habilitar la Inspección de registros**.
6. En la pestaña **Reglas personalizadas**, seleccione la casilla **Aplicar reglas personalizadas en Inspección de registros**.
7. Configure las reglas personalizadas con los interruptores:
8. Si es necesario, haga clic en **Agregar** para crear sus reglas personalizadas.
9. Esto abre una ventana, donde debe configurar la regla personalizada:
   - **Nombre de la regla**.
   - **Nombre de Registro de eventos de Windows**. Registros de eventos de Windows. Estos son los registros disponibles: *Application*, *Security* o *System*.

- **Origen**. Registros de aplicaciones de terceros. Puede averiguar el nombre del registro de la aplicación de terceros con la herramienta Visor de eventos. Los registros de aplicaciones de terceros se guardan en la carpeta Registros de aplicaciones y servicios (por ejemplo, el registro de Windows PowerShell).
- **Id. del evento**. ID de eventos en el Registro de eventos de Windows. Puede buscar el ID del evento en la documentación técnica de Microsoft.

10. Guarde los cambios.

Cómo agregar una regla personalizada en la Consola de la aplicación

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Inspección del sistema** → **Inspección de registros**.
2. En el panel de resultados del nodo **Inspección de registros**, haga clic en **Propiedades**.

   Se abrirá la ventana **Propiedades: Inspección de registros**.
3. Seleccione la casilla de verificación **Inspección de registros**.
4. En la pestaña **Reglas personalizadas**, seleccione la casilla **Aplicar reglas personalizadas en Inspección de registros**.
5. Active las casillas ubicadas junto a las reglas personalizadas que desee habilitar.
6. Si es necesario, haga clic en **Agregar** para crear sus reglas personalizadas.
7. Esto abre una ventana, donde debe configurar la regla personalizada:
   - **Nombre de la regla**.
   - **Nombre del registro**. Registros de eventos de Windows. Estos son los registros disponibles: *Application*, *Security* o *System*.
   - **Fuente**. Registros de aplicaciones de terceros. Puede averiguar el nombre del registro de la aplicación de terceros con la herramienta Visor de eventos. Los registros de aplicaciones de terceros se guardan en la carpeta Registros de aplicaciones y servicios (por ejemplo, el registro de Windows PowerShell).
   - **Identificadores de eventos**. ID de eventos en el Registro de eventos de Windows. Puede buscar el ID del evento en la documentación técnica de Microsoft.
8. Guarde los cambios.

Como resultado, cuando se activa la regla, Kaspersky Embedded Systems Security crea un evento *Crítico*.

Configuración de reglas predefinidas

Las reglas predefinidas incluyen plantillas de actividad anormal en el equipo protegido. La actividad anormal puede implicar un intento de ataque. Las reglas predefinidas funcionan con análisis heurístico. Inspección de registro tiene siete reglas predefinidas disponibles. Puede habilitarlas o deshabilitarlas. Las reglas predefinidas no se pueden eliminar.

Puede configurar los criterios de activación de las reglas que monitorean eventos para las siguientes operaciones:

- Detección de ataques de fuerza bruta a contraseñas
- Detección de inicios de sesión en la red

Cómo configurar reglas predefinidas en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de propiedades de la directiva, seleccione **Inspección del sistema**.
4. En la sección **Inspección de registros**, haga clic en **Configuración**.
5. Seleccione la casilla de verificación **Inspección de registros**.
6. En la pestaña **Reglas predefinidas**, seleccione la casilla **Aplicar reglas predefinidas en Inspección de registros**.
7. Para configurar reglas predefinidas, seleccione o anule la selección de las casillas de verificación:
   - **Hay patrones de posibles ataques de fuerza bruta en el sistema**.
   - **Se detectó una actividad inusual durante un inicio de sesión en la red**.
   - **Hay patrones de un posible abuso del Registro de eventos de Windows**.
   - **Se detectaron acciones atípicas de parte de un nuevo servicio instalado**.
   - **Se detectó un inicio de sesión atípico que usa credenciales explícitas**.
   - **Hay patrones de un posible ataque PAC falsificado de Kerberos (MS14-068) en el sistema**.
   - **Se detectaron cambios sospechosos en el grupo de administradores integrado y con privilegios**.
8. Si es necesario, configure la regla **Hay patrones de posibles ataques de fuerza bruta en el sistema**:
   a. Haga clic en el botón **Configuración** junto a la regla.
   b. En la ventana que se abre, especifique el número de intentos y el período en el cual se deben realizar los intentos para ingresar una contraseña a fin de que se active la regla.
   c. Haga clic en **Aceptar**.
9. Si seleccionó la regla **Se detectó una actividad inusual durante un inicio de sesión en la red**, deberá configurarla:
   a. Haga clic en el botón **Configuración** junto a la regla.
   b. En la ventana que se abre, en el bloque **Detección de inicios de sesión en la red**, especifique el inicio y el final del intervalo de tiempo.

Kaspersky Embedded Systems Security considera los intentos de inicio de sesión realizados durante el intervalo definido como actividad anormal.

De manera predeterminada, el intervalo no se establece, y la aplicación no supervisa los intentos de inicio de sesión. Para que la aplicación supervise constantemente los intentos de inicio de sesión, establezca el intervalo entre las 12:00 a. m. y las 11:59 p. m. El inicio y el final del intervalo no deben coincidir. Si coinciden, la aplicación no supervisa los intentos de inicio de sesión.

c. Cree la lista de usuarios de confianza y direcciones IP de confianza (IPv4 e IPv6).

Puede seleccionar usuarios en Active Directory, en la lista de cuentas en Kaspersky Security Center o ingresando un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio. Kaspersky Embedded Systems Security no monitorea los intentos de inicio de sesión de estos usuarios y equipos.

> La exclusión de equipos de confianza por dirección IP no funciona en la aplicación que se ejecuta en Windows XP.

d. Haga clic en **Aceptar**.

10. Guarde los cambios.

Cómo configurar reglas predefinidas en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Inspección del sistema** → **Inspección de registros** y haga clic en el botón **Configurar**.
5. Seleccione la casilla de verificación **Habilitar la Inspección de registros**.
6. En la pestaña **Reglas predefinidas**, seleccione la casilla **Aplicar reglas predefinidas en Inspección de registros**.
7. Configure las reglas predefinidas con los interruptores:
   - **Hay patrones de posibles ataques de fuerza bruta en el sistema**.
   - **Se detectó una actividad inusual durante un inicio de sesión en la red**.
   - **Hay patrones de un posible abuso del Registro de Eventos de Windows**.
   - **Se detectaron acciones atípicas de parte de un nuevo servicio instalado**.
   - **Se detectó un inicio de sesión atípico que usa credenciales explícitas**.
   - **Hay patrones de un posible ataque PAC falsificado de Kerberos (MS14-068) en el sistema**.
   - **Se detectaron cambios sospechosos en el grupo de administradores integrado y con privilegios**.

8. En la pestaña **Extendido**, establezca la siguiente configuración:

   - Número de intentos y un periodo en el cual se deben realizar los intentos para ingresar una contraseña a fin de que se active la regla **Hay patrones de posibles ataques de fuerza bruta en el sistema**.
   - Para que se active la regla **Se detectó una actividad inusual durante un inicio de sesión en la red**, especifique el inicio y final del intervalo de tiempo durante el cual la aplicación considera todos los intentos de inicio de sesión como actividad anormal.

     De manera predeterminada, el intervalo no se establece, y la aplicación no supervisa los intentos de inicio de sesión. Para que la aplicación supervise constantemente los intentos de inicio de sesión, establezca el intervalo entre las 12:00 a. m. y las 11:59 p. m. El inicio y el final del intervalo no deben coincidir. Si coinciden, la aplicación no supervisa los intentos de inicio de sesión.

9. Cree la lista de usuarios de confianza y direcciones IP de confianza (IPv4 e IPv6) en las pestañas correspondientes.

   Puede seleccionar a los usuarios de la lista de cuentas o ingresar un nombre de usuario local manualmente.

   La exclusión de equipos de confianza por dirección IP no funciona en la aplicación que se ejecuta en Windows XP.

10. Guarde los cambios.

Cómo configurar reglas predefinidas en la Consola de la aplicación

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Inspección del sistema** → **Inspección de registros**.
2. En el panel de resultados del nodo **Inspección de registros**, haga clic en **Propiedades**.

   Se abrirá la ventana **Propiedades: Inspección de registros**.
3. Seleccione la casilla de verificación **Inspección de registros**.
4. En la pestaña **Reglas predefinidas**, seleccione la casilla **Aplicar reglas predefinidas en Inspección de registros**.
5. Para configurar reglas predefinidas, seleccione o anule la selección de las casillas de verificación:

   - **Hay patrones de posibles ataques de fuerza bruta en el sistema**.
   - **Se detectó una actividad inusual durante un inicio de sesión en la red**.
   - **Hay patrones de un posible abuso del Registro de eventos de Windows**.
   - **Se detectaron acciones atípicas de parte de un nuevo servicio instalado**.
   - **Se detectó un inicio de sesión atípico que usa credenciales explícitas**.
   - **Hay patrones de un posible ataque PAC falsificado de Kerberos (MS14-068) en el sistema**.
   - **Se detectaron cambios sospechosos en el grupo de administradores integrado y con privilegios**.

6. Si es necesario, configure la regla **Hay patrones de posibles ataques de fuerza bruta en el sistema**:

   a. Haga clic en el botón **Configuración** junto a la regla.

   b. En la ventana que se abre, especifique el número de intentos y el período en el cual se deben realizar los intentos para ingresar una contraseña a fin de que se active la regla.

   c. Haga clic en **Aceptar**.

7. Si seleccionó la regla **Se detectó una actividad inusual durante un inicio de sesión en la red**, deberá configurarla:

   a. Haga clic en el botón **Configuración** junto a la regla.

   b. En la ventana que se abre, en el bloque **Detección de inicios de sesión en la red**, especifique el inicio y el final del intervalo de tiempo.

   Kaspersky Embedded Systems Security considera los intentos de inicio de sesión realizados durante el intervalo definido como actividad anormal.

   De manera predeterminada, el intervalo no se establece, y la aplicación no supervisa los intentos de inicio de sesión. Para que la aplicación supervise constantemente los intentos de inicio de sesión, establezca el intervalo entre las 12:00 a. m. y las 11:59 p. m. El inicio y el final del intervalo no deben coincidir. Si coinciden, la aplicación no supervisa los intentos de inicio de sesión.

   c. Cree la lista de usuarios de confianza y direcciones IP de confianza (IPv4 e IPv6).

   Puede seleccionar usuarios en Active Directory, en la lista de cuentas en Kaspersky Security Center o ingresando un nombre de usuario local manualmente. Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio. Cree la lista de usuarios desde Active Directory. Kaspersky Embedded Systems Security no monitorea los intentos de inicio de sesión de estos usuarios y equipos.

   > La exclusión de equipos de confianza por dirección IP no funciona en la aplicación que se ejecuta en Windows XP.

   d. Haga clic en **Aceptar**.

8. Guarde los cambios.

Como resultado, cuando se activa la regla, Kaspersky Embedded Systems Security crea un evento *Crítico*.

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 dispositivo protegido.

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 dispositivos protegidos, RAM y objetos de ejecución automática.

Kaspersky Embedded Systems Security proporciona las siguientes tareas de Análisis a pedido:

- De forma predeterminada, la tarea *Análisis de áreas críticas* se realiza cada semana según una 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 del proceso. Kaspersky Embedded Systems Security aplica la configuración de seguridad que corresponde al nivel **Informar**. Puede modificar la configuración de la tarea *Análisis de áreas críticas*.

- La tarea Comprobación de integridad de la aplicación se realiza todos los días. 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 indican el número de módulos comprobados y el número de módulos 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.

- La tarea *Análisis de unidades extraíbles* analiza todos los archivos que ejecuta o copia, incluso si el archivo está ubicado en una unidad extraíble. Para evitar la propagación de virus y otros programas malintencionados, puede configurar análisis automáticos de unidades extraíbles cuando están conectadas al equipo.

- La tarea *Análisis completo* se realiza semanalmente. La tarea garantiza un análisis exhaustivo del dispositivo protegido, incluidos el almacenamiento de copias de seguridad del sistema, los sectores de arranque y las bases de datos de correo.

Además, puede crear tareas de Análisis a pedido personalizadas, por ejemplo, una tarea para analizar las carpetas compartidas en el dispositivo protegido.

Kaspersky Embedded Systems Security puede ejecutar varias tareas de Análisis a pedido de manera simultánea.

Acerca del área del análisis de la tarea y la configuración de seguridad

En la Consola de la aplicación, el área de análisis de la tarea Análisis a pedido seleccionada se muestra en forma de lista de recursos de archivos del dispositivo protegido que Kaspersky Embedded Systems Security puede controlar.

Los elementos o nodos se muestran en una visualización en forma de lista de los recursos del archivo del dispositivo protegido de la siguiente manera:

☑ El nodo se incluye en el alcance del análisis.

☐ El nodo se excluye del área del análisis.

Configuración de seguridad

En la tarea de Análisis a pedido seleccionada, la configuración de seguridad predeterminada puede modificarse si se la establece como configuración común para toda el área de protección o de análisis, o como una configuración diferente para los distintos nodos o elementos de la lista de recursos de archivos del dispositivo.

Si el mismo objeto figura en varias entradas del alcance de protección y estas entradas tienen diferentes niveles de seguridad, la última regla de la lista tendrá prioridad. Por ejemplo, considere un alcance de protección que incluye dos entradas: **Todos los discos duros** (nivel de seguridad **Informar**) y `*\Users\*\Downloads\*` (nivel de seguridad **Personalizada**). La aplicación analiza los discos duros según el nivel Informar, excepto la carpeta `Downloads`. La aplicación analiza la carpeta `Downloads` según la configuración que se especificó manualmente porque esta entrada es la última en la lista del alcance de la protección.

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 área de 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 la lista de los recursos de archivos del dispositivo protegido (el nivel de seguridad cambia a **Personalizada**).

Áreas del análisis predefinidas

La lista de recursos del archivo del dispositivo protegido para la tarea de Análisis a pedido seleccionada se muestran en la ventana **Alcance del análisis**.

La lista de recursos de archivos muestra los nodos a los cuales tiene acceso de lectura según las opciones de seguridad configuradas de Microsoft Windows.

Kaspersky Embedded Systems Security contiene las áreas del análisis predefinidas siguientes:

- **Todos los discos duros**. Kaspersky Embedded Systems Security analiza objetos en los discos duros del dispositivo protegido. Todos los discos duros, discos, carpetas o archivos individuales se pueden incluir en el área del análisis o excluir de él.
- **Todas las unidades extraíbles**. Kaspersky Embedded Systems Security analiza archivos en dispositivos externos, por ejemplo, unidades extraíbles o CD. Todas las unidades extraíbles, discos, carpetas o archivos individuales pueden incluirse en el área del análisis o excluirse de ella.
- **Todas las unidades de 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 dispositivo protegido. Para incluir objetos de unidades de red en el área del análisis, especifique la ruta a la carpeta que corresponde a la unidad de red en formato UNC.

- **Memoria del núcleo**. 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.
- **Procesos en ejecución y 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 dispositivo protegido.
- **Sectores de arranque del disco**. Kaspersky Embedded Systems Security analiza los sectores de arranque de discos duros y unidades extraíbles.
- **Mi correo electrónico**. Kaspersky Embedded Systems Security analiza archivos relevantes para el cliente de correo de Outlook: archivos de datos (PST), archivos de datos sin conexión (OST).
- **Copia de seguridad del sistema**. Kaspersky Embedded Systems Security analiza el contenido de la carpeta de Información de volumen del sistema.

Las áreas de análisis estándar se muestran en el árbol de recursos de archivos de red de forma predeterminada. Se pueden agregar a la lista de recursos de archivos en red cuando se la crea en la configuración de áreas de análisis.

De forma predeterminada, las tareas de Análisis a pedido se ejecutan según las diferentes áreas:

- Tarea de *Análisis de áreas críticas*:
  - **Todos los discos duros** (no incluye las carpetas de Windows).
  - **Todas las unidades extraíbles**.
  - **Memoria del núcleo**.
  - **Procesos en ejecución y objetos de inicio**.
- Tarea de *Análisis a pedido*:
  - **Todos los discos duros** (no incluye las carpetas de Windows).
  - **Todas las unidades extraíbles**.

- **Memoria del núcleo**.
- **Procesos en ejecución y objetos de inicio**.

- Tarea de *Análisis completo*:
  - **Todos los discos duros** (no incluye las carpetas de Windows).
  - **Todas las unidades extraíbles**.
  - **Memoria del núcleo**.
  - **Procesos en ejecución y objetos de inicio**.
  - **Copia de seguridad del sistema**.
  - **Sectores de arranque del disco**.
  - **Mi correo electrónico**.

Análisis de archivos almacenados en línea

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 de 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 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 dispositivo 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 dispositivo 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 contengan archivos en la nube al área de la protección 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 inicio de aplicaciones: puede crear reglas de autorización y de denegación para archivos y con la tarea Generador de reglas de 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 alcance de generación de reglas que realiza la aplicación, ya que no están presentes físicamente en su disco duro. Como no se puede crear 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. Así, 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.

Acerca de los niveles de seguridad predefinidos

La configuración de seguridad **Utilizar análisis heurístico** no se incluye en la configuración para los niveles de seguridad predefinidos. Si cambia esta configuración, no se cambiará el nivel de seguridad predeterminado que seleccionó.

Puede aplicar uno de cuatro niveles de seguridad predefinidos a un nodo seleccionado en el árbol de recursos de archivos del dispositivo: **Máximo rendimiento**, **Recomendado**, **Máxima protección** e **Informar**. Cada uno de estos niveles contiene su propia configuración de seguridad predefinida (consulte la tabla a continuación).

Máximo rendimiento

El nivel de seguridad **Máximo rendimiento** se recomienda si su red tiene medidas de seguridad adicionales para los dispositivos protegidos, por ejemplo, firewalls y directivas de seguridad existentes, además de usar Kaspersky Embedded Systems Security en estaciones de trabajo y dispositivos protegidos.

Recomendado

El nivel de seguridad **Recomendado** garantiza la mejor combinación de protección e impacto en el rendimiento de los dispositivos protegidos. Los expertos de Kaspersky recomiendan este nivel porque es adecuado para proteger los dispositivos en la mayoría de las redes corporativas. 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 dispositivo.

Informar

Se recomienda el nivel de seguridad **Informar** si potencialmente hay varios equipos infectados en la red corporativa y bloquearlos podría interrumpir considerablemente el funcionamiento de la organización.

Niveles de seguridad predefinidos y los valores de configuración de seguridad correspondientes

Opciones	Nivel de seguridad			
Máximo rendimiento	Recomendado	Máxima protección	Informar	
Tipos de objetos	Objetos analizados según su formato	Todos los objetos	Todos los objetos	Todos los objetos
Analizar solo archivos nuevos y modificados	Habilitado	Deshabilitado	Deshabilitado	Deshabilitado
Acción que se realizará con los objetos infectados y otros objetos	Desinfectar. Si falla la desinfección, eliminar	Realizar la acción recomendada por los expertos de Kaspersky	Desinfectar. Si falla la desinfección, eliminar	Informar
Análisis de archivos compuestos	Analizar paquetes de distribución y archivos de Microsoft Office	Analizar todos los archivos de almacenamiento, paquetes de distribución y archivos de Microsoft Office	Analizar todos los archivos de almacenamiento, paquetes de distribución y archivos de Microsoft Office	Analizar todos los archivos de almacenamiento, paquetes de distribución y archivos de Microsoft Office
La denominación "objeto crítico del sistema" hace referencia a aquellos archivos que el sistema operativo y Kaspersky Embedded Systems Security requieren para funcionar. Estos archivos no se pueden eliminar. Los procesos asociados con dichos objetos no se pueden finalizar.				
Aplicar la acción a los tipos de objetos seleccionados	De manera predeterminada, se analizan todos los tipos de objetos	De manera predeterminada, se analizan todos los tipos de objetos	De manera predeterminada, se analizan todos los tipos de objetos	De manera predeterminada, se analizan todos los tipos de objetos
Si se detecta un objeto integrado, eliminar todo el archivo compuesto que la aplicación no pueda modificar	No	No	No	No
Excluir archivos	No	No	No	No
No detectar objetos por tipo	No	No	No	No

Opciones	Nivel de seguridad			
Detener el análisis si demora más de (s)	60 segundos.	No	No	No
Omitir objetos compuestos de más de (MB)	8 MB	No	No	No
Usar tecnología iSwift	Sí	Sí	Sí	Sí
Usar tecnología iChecker	Sí	Sí	Sí	Sí

Análisis de unidades extraíbles

Puede configurar el análisis de discos extraíbles conectados al dispositivo protegido mediante un puerto USB.

Los análisis de Kaspersky Embedded Systems Security conectaron discos extraíbles cuando se registran como dispositivos externos USB en el sistema operativo. La aplicación no analiza una unidad extraíble si la conexión está bloqueada por la tarea Control de dispositivos.

Kaspersky Embedded Systems Security permite el acceso a las unidades extraíbles durante el análisis.

Los resultados de análisis de cada unidad extraíble pueden consultarse en el registro de la tarea Análisis a pedido creada cuando se conecta la unidad extraíble.

Puede cambiar la configuración del componente Análisis de unidades extraíbles (consulte la tabla a continuación).

Configuración de Análisis de unidades extraíbles

Parámetro	Valor predeterminado	Descripción
Analizar unidades extraíbles al conectarlas via USB	Desactivada	Puede activar o desactivar el análisis de las unidades extraíbles después de conectarlas al dispositivo protegido por USB.
Analizar las unidades extraíbles si el tamaño no excede (MB)	4096 MB	Puede reducir el área del componente si configura el volumen máximo de datos del disco analizado. Kaspersky Embedded Systems Security no analiza una unidad extraíble si el volumen de datos almacenados excede el valor especificado.
Analizar con nivel de seguridad	Máxima protección	Puede configurar tareas creadas de Análisis a pedido a través de uno de los tres niveles de seguridad: • **Máxima protección** • **Recomendado** • **Máximo rendimiento** • **Informar**. 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 locales del sistema y personalizadas.

Parámetro	Valor predeterminado	Descripción
Área del análisis	Aplicado en tareas locales del sistema y personalizadas: • **Análisis de áreas críticas**: el dispositivo protegido completo, excluidas las carpetas compartidas y determinados archivos del sistema operativo. • **Análisis a pedido** (tareas personalizadas): el dispositivo protegido completo. • **Análisis completo**: un análisis detallado del dispositivo protegido.	Se puede cambiar el área del análisis. El alcance del análisis no se puede configurar para las tareas locales del sistema **Análisis de unidades extraíbles** y **Control de integridad de la aplicación**.
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 de recursos de archivos del dispositivo protegido, puede realizar lo siguiente: • Seleccionar un nivel de seguridad predefinido diferente • Cambiar manualmente la configuración de seguridad
Utilizar análisis heurístico	Para el nivel de análisis **Medio** de *Análisis de áreas críticas*, las tareas *Análisis a pedido* y *Análisis completo*.	Se puede habilitar o deshabilitar el Analizador heurístico y configurar el nivel de análisis.
La configuración para iniciar una tarea con permisos específicos	La tarea se inicia con una cuenta de sistema.	Puede modificar la configuración de inicio de tareas con permisos de cuenta específicos para todas las tareas Análisis a pedido personalizadas o del sistema, excepto la tarea *Comprobación de integridad de la aplicación*.
Ejecutar tarea en segundo plano	No aplicado	Puede configurar el nivel de prioridad de las tareas de Análisis a pedido.
Considerar la tarea como Análisis de áreas críticas	Para *Análisis a pedido*, las tareas *Análisis de áreas críticas* y *Análisis completo*.	Puede configurar el nivel de prioridad de las tareas de Análisis a pedido.
No ejecutar varias tareas de análisis al mismo tiempo	No aplicado	Puede configurar el nivel de prioridad de las tareas de Análisis a pedido.
Programación de inicio de tareas	Para las tareas locales del sistema: *Análisis de áreas críticas*, *Comprobación de integridad de la aplicación* y *Análisis completo*: **Mensualmente**.	Puede configurar las opciones para el inicio programado de tareas.

Administrar las tareas de Análisis a pedido

En esta sección, se describe cómo navegar por la interfaz y configurar la tarea Análisis a pedido en el dispositivo protegido.

Navegación

Obtenga información sobre cómo dirigirse a la configuración de la tarea requerida a través de la interfaz que elija.

Cómo abrir el asistente de la tarea de Análisis a pedido

Para crear una tarea nueva de Análisis a pedido:

[Abrir el Asistente de tarea nueva para crear una tarea de Análisis a pedido en la Consola de administración de Kaspersky Security Center](#)

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 dispositivo protegido.

   c. En el panel de resultados, en la pestaña **Dispositivos**, abra el menú contextual para el dispositivo 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. Seleccione la pestaña **Tareas**.

   d. Haga clic en **Nueva tarea**.

   Se abre la ventana **Nuevo asistente de tarea**.

3. Para crear una tarea para un grupo personalizado de dispositivos protegidos:

   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. Seleccione la pestaña **Resultados de selección *nombre de selección***.

   c. En la lista desplegable **Realizar acción**, seleccione **Tarea nueva**.

   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** y configure la tarea según 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: Análisis a pedido**.

[Abrir el Asistente de tarea nueva para crear una tarea de Análisis a pedido en Kaspersky Security Center Web Console]

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Dispositivos administrados**.
2. Haga clic en el nombre del dispositivo protegido.
3. En la ventana **<Nombre del dispositivo>** que se abre, seleccione la pestaña **Tareas**.
4. Haga clic en el botón **Agregar**.

   Se abre la ventana **Nuevo asistente de tarea**.
5. En la lista desplegable **Aplicación**, seleccione **Kaspersky Embedded Systems Security**.
6. En la lista desplegable **Tipo de tarea**, seleccione la tarea **Análisis a pedido**.
7. Haga clic en **Siguiente**.

Ajuste la configuración de la tarea como sea necesario.

Para empezar a crear una tarea nueva de Análisis a pedido de grupo:

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Tareas**.
2. Haga clic en la pestaña **Grupos** para seleccionar el grupo de administración para el cual desea crear una tarea.
3. Haga clic en el botón **Agregar**.

   Se abre la ventana **Nuevo asistente de tarea**.
4. En la lista desplegable **Aplicación**, seleccione **Kaspersky Embedded Systems Security**.
5. En la lista desplegable **Tipo de tarea**, seleccione la tarea **Análisis a pedido**.
6. Haga clic en **Siguiente**.

Ajuste la configuración de la tarea como sea necesario.

Para empezar a crear una tarea nueva de Análisis a pedido para un grupo personalizado:

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Selecciones de dispositivos**.
2. Elija la selección para la cual desea crear una tarea.
3. Haga clic en el botón **Iniciar**.
4. En la ventana **Resultados de la selección**, seleccione los dispositivos para los que desea crear una tarea.
5. Haga clic en el botón **Nueva tarea**.

6. En la lista desplegable **Aplicaciones**, seleccione **Kaspersky Embedded Systems Security**.
7. En la lista desplegable **Tipo de tarea**, seleccione la tarea **Análisis a pedido**.
8. Haga clic en **Siguiente**.

Ajuste la configuración de la tarea como sea necesario.

Para configurar una tarea de Análisis a pedido existente:

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Tareas**.
2. Haga clic en el nombre de la tarea en la lista de tareas de Kaspersky Security Center.

Se abre la ventana **<Nombre de la tarea>**.

Cómo abrir la configuración de la tarea de Análisis a pedido

Para abrir la configuración de la aplicación para la tarea de Análisis a pedido en un solo dispositivo protegido:

Para abrir la configuración general de la tarea de Análisis a pedido en la Consola 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 al cual pertenece el dispositivo protegido.
3. Seleccione la pestaña **Dispositivos**.
4. Haga doble clic en el nombre del dispositivo protegido para el cual desea configurar el área de análisis.

   Se abre la ventana **Propiedades: <Nombre del dispositivo protegido>**.
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: Análisis a pedido**.

Ajuste la configuración de la tarea como sea necesario.

Para abrir la configuración general de la tarea de Análisis a pedido en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Dispositivos administrados**.
2. Seleccione el grupo de administración al cual pertenece el dispositivo protegido.

3. Haga clic en el nombre del dispositivo protegido.
4. En la ventana **<Nombre del dispositivo>** que se abre, seleccione la pestaña **Tareas**.
5. En la lista de tareas creadas para el dispositivo, seleccione la tarea de Análisis a pedido que creó.
6. Abra la pestaña **Configuración de la aplicación**.

Para abrir la configuración general de la tarea de Análisis a pedido en la Consola de la aplicación

1. En el árbol de la Consola de la aplicación, expanda el nodo **Análisis a pedido**.
2. Seleccione el nodo secundario que corresponde a la tarea que desea configurar.
3. En el nodo secundario del panel de resultados, haga clic en el vínculo **Propiedades**.
   Se abre la ventana **Propiedades: <Nombre de la tarea>**.

Creación de una tarea de Análisis a pedido

Crear una tarea de Análisis a pedido en la Consola de administración de Kaspersky Security Center

1. Inicie el Asistente de nueva tarea.
2. En la ventana **Seleccionar el tipo de tarea**, seleccione **Análisis a pedido** y haga clic en **Siguiente**.
3. Cree un área del análisis en la ventana **Alcance del análisis**:

   De manera predeterminada, el área del análisis incluye áreas críticas del dispositivo protegido. 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 alcance del análisis, seleccione el elemento de la lista correspondiente y haga clic en **Eliminar**.
   - Para incluir un área del análisis predeterminada, disco, carpeta, objeto de red o archivo en el área del análisis:

     a. Haga clic en **Agregar**.

     b. En la ventana **Seleccionar alcance del análisis**, seleccione el alcance predefinido del análisis en la lista y haga clic en **Aceptar**.

- Para excluir subcarpetas o archivos del alcance del análisis:

  a. Seleccione una carpeta (o disco) que haya agregado en la ventana **Alcance del análisis**.

  b. Haga clic en **Modificar**.

  c. Deshabilite la casilla **Incluir subcarpetas**.

- Para cambiar la configuración de seguridad del área del análisis:

  a. Seleccione el alcance del análisis para el cual desea editar la configuración y haga clic en **Configurar**.

  b. En la ventana que se abre, seleccione uno de los niveles de seguridad predefinidos o haga clic en el botón **Configuración** para configurar seguridad manualmente.

  Las opciones de seguridad se configuran de la misma manera que en la tarea Protección de archivos en tiempo real.

4. Configure el analizador heurístico y la integración con otros componentes:

   - Configure el uso del analizador heurístico.
   - Seleccione la casilla **Ejecutar tarea en segundo plano** si desea asignar una prioridad *Baja* al proceso de trabajo en el que se ejecutará la tarea.

     De manera predeterminada, los procesos de trabajo en que se ejecutan las tareas de Kaspersky Embedded Systems Security reciben la prioridad *Media* (Normal).

   - Seleccione la casilla **Considerar la tarea como Análisis de áreas críticas** si desea usar la tarea como una tarea *Análisis de áreas críticas*.
   - Seleccione la casilla **No ejecutar varias tareas de análisis al mismo tiempo** para optimizar la carga en el equipo.

5. En la ventana **Seleccionar dispositivos a los que se asignará la tarea**, especifique la lista de dispositivos y haga clic en **Siguiente**.
6. En la ventana **Seleccione una cuenta con la que ejecutar la tarea**, especifique una cuenta y haga clic en **Siguiente**.
7. En la ventana **Configurar programación de tarea**, configure la programación de la tarea y haga clic en **Siguiente**.
8. Ingrese el nombre de la tarea.

   El nombre de la tarea no debe tener más de 100 caracteres y no puede contener los siguientes símbolos: " * < > & \ : |

9. Se abre la ventana **Finalizar la creación de la tarea**. Haga clic en **Finalizar** para terminar de crear la tarea.

Se creará la nueva tarea Análisis a pedido para el dispositivo protegido o el grupo de dispositivos protegidos seleccionados.

Crear una tarea de Análisis a pedido en Kaspersky Security Center Web Console

1. Inicie el Asistente de nueva tarea.
2. En la ventana **Nueva tarea**, en la lista desplegable **Aplicación**, seleccione **Kaspersky Embedded Systems Security**.
3. En la lista desplegable **Tipo de tarea**, seleccione **Análisis a pedido** y haga clic en **Siguiente**.
4. Seleccione el alcance de la tarea y haga clic en **Siguiente**.
5. En la ventana **Seleccione una cuenta con la que ejecutar la tarea**, especifique una cuenta y haga clic en **Siguiente**.
6. Ingrese el nombre de la tarea.

   El nombre de la tarea no debe tener más de 100 caracteres y no puede contener los siguientes símbolos: " * < > & \ : |
7. Se abre la ventana **Finalizar la creación de la tarea**. Haga clic en **Finalizar** para terminar de crear la tarea.

Se creará la nueva tarea Análisis a pedido para el dispositivo protegido o el grupo de dispositivos protegidos seleccionados.

Crear una tarea de Análisis a pedido en la Consola de la aplicación

Las tareas personalizadas para un solo dispositivo protegido pueden generarse en el nodo **Análisis a pedido**.

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 la opción **Crear tarea**.

   Se abre la ventana **Crear tarea**.
3. Escriba un nombre para la tarea y haga clic en **Aceptar**.

Se crea la tarea Análisis a pedido para un dispositivo protegido individual.

Ejecución de una tarea de Análisis a pedido en segundo plano

De manera predeterminada, los procesos en que se ejecutan las tareas de Kaspersky Embedded Systems Security reciben la prioridad *Media (Normal)*.

El proceso que ejecutará una tarea de Análisis a pedido se le puede asignar la prioridad *Baja*. Si se degrada la prioridad del proceso, se aumenta el tiempo requerido para ejecutar la tarea, pero puede tener un efecto beneficioso en el rendimiento de los procesos de otros programas en ejecución.

Varias tareas en segundo plano pueden estar en ejecución en un único proceso de trabajo con prioridad baja.

Para cambiar la prioridad de una tarea de Análisis a pedido existente, seleccione o desactive la casilla **Ejecutar tarea en segundo plano** en la configuración de la tarea.

La configuración de la tarea se guarda y se aplica inmediatamente a una tarea en ejecución. Si la tarea no se está ejecutando, la configuración modificada se aplica en el siguiente inicio.

Registro de la ejecución de un Análisis de áreas críticas

De forma predeterminada, el estado de protección del dispositivo se muestra en el panel de resultados del nodo **Kaspersky Embedded Systems Security** y se actualiza cada semana después de finalizar la tarea *Análisis de áreas críticas*.

La hora en la que se actualiza el estado de protección del dispositivo está relacionada con la programación de la tarea Análisis a pedido para la cual se seleccionó la casilla **Considerar la tarea como Análisis de áreas críticas**.

Configurar el alcance del análisis en la tarea de Análisis a pedido

Si modifica el alcance del análisis en las tareas *Análisis al inicio del sistema operativo* y *Análisis de áreas críticas*, puede restablecer el alcance del análisis predeterminado en estas tareas al restaurar Kaspersky Embedded Systems Security con el Asistente de instalación.

Configurar el alcance del análisis para la tarea de Análisis a pedido en la Consola de administración de Kaspersky Security Center

1. Abra la ventana **Propiedades: Análisis a pedido**.
2. Seleccione la sección **Alcance del análisis**.
3. Para agregar alcances al alcance del análisis, seleccione las casillas.
4. Si desea agregar un alcance del análisis que no está en la lista:
   a. Haga clic en **Agregar**.
   b. En la ventana que se muestra, seleccione un alcance, un disco individual, una carpeta o una ubicación de la red.
   c. Si desea incluir subcarpetas en el alcance del análisis, seleccione la casilla **Incluir subcarpetas**.
5. Para excluir nodos individuales del área del análisis, desactive las casillas de verificación al lado de los nombres de estos nodos.
6. Para editar un alcance del análisis, selecciónelo en la lista y haga clic en **Editar**.

7. Para ocultar un alcance del análisis agregado previamente de la lista de recursos del archivo de red, seleccione el alcance del análisis y haga clic en **Eliminar**.

   El área del análisis se excluye del área de la tarea de Análisis a pedido cuando se elimina de la lista de recursos de archivos en red.

8. Haga clic en **Aceptar**.

Se cierra la ventana Configuración de área del análisis. Se guardan las opciones configuradas recientemente.

Configurar el alcance del análisis para la tarea de Análisis a pedido en Kaspersky Security Center Web Console

1. Abra la ventana **Análisis a pedido**.
2. Seleccione la ficha **Configuración de la aplicación**.
3. Para agregar alcances al alcance del análisis, seleccione las casillas y active el interruptor.
4. Si desea agregar un alcance del análisis que no está en la lista:
   a. Haga clic en **Agregar**.
   b. En la ventana que se muestra, seleccione un alcance, un disco individual, una carpeta o una ubicación de la red.
   c. Si desea incluir subcarpetas en el alcance del análisis, seleccione la casilla **Subcarpetas**.
5. Para excluir nodos individuales del área del análisis, desactive las casillas de verificación al lado de los nombres de estos nodos.
6. Para editar un alcance del análisis, selecciónelo en la lista y haga clic en **Modificar alcance**.
7. Para ocultar un alcance del análisis agregado previamente de la lista de recursos del archivo de red, seleccione el alcance del análisis y haga clic en **Eliminar**.

   El área del análisis se excluye del área de la tarea de Análisis a pedido cuando se elimina de la lista de recursos de archivos en red.

8. Haga clic en **Guardar**.

Se cierra la ventana Configuración de área del análisis. Se guardan las opciones configuradas recientemente.

Configurar el alcance del análisis para la tarea de Análisis a pedido en la Consola de la aplicación

1. En el árbol de la Consola de la aplicación, expanda el nodo **Análisis a pedido**.
2. Seleccione el nodo secundario correspondiente a una tarea de Análisis a pedido que desea configurar.
3. En el panel de resultados del nodo seleccionado, haga clic en el vínculo **Configurar el área de protección**.
4. Para agregar alcances al alcance del análisis, en la ventana que se muestra, seleccione las casillas.
5. Si desea agregar un alcance del análisis que no está en la lista:
   a. Haga clic en **Agregar**.
   b. En la ventana que se muestra, seleccione un alcance, un disco individual, una carpeta o una ubicación de la red.
   c. Si desea incluir subcarpetas en el alcance del análisis, seleccione la casilla **Incluir subcarpetas**.
6. Para excluir nodos individuales del área del análisis, desactive las casillas de verificación al lado de los nombres de estos nodos.
7. Para editar un alcance del análisis, selecciónelo en la lista y haga clic en **Modificar alcance**.
8. Para ocultar un alcance del análisis agregado previamente de la lista de recursos del archivo de red, seleccione el alcance del análisis y haga clic en **Eliminar**.

   El área del análisis se excluye del área de la tarea de Análisis a pedido cuando se elimina de la lista de recursos de archivos en red.

9. Haga clic en **Aceptar**.

Se cierra la ventana Configuración de área del análisis. Se guardan las opciones configuradas recientemente.

Establecer la configuración de la tarea de Análisis a pedido

Cómo configurar la tarea Análisis a pedido en la Consola de administración de Kaspersky Security Center

1. Abra las propiedades de la tarea Análisis a pedido.
2. Seleccione la sección **Opciones**.
3. Desactive o seleccione la casilla de verificación **Utilizar análisis heurístico**.
4. Si es necesario, cambie el nivel de análisis.

5. Seleccione la casilla **Ejecutar tarea en segundo plano** si desea asignar una prioridad *Baja* al proceso de trabajo en el que se ejecutará la tarea.

   De manera predeterminada, los procesos de trabajo en que se ejecutan las tareas de Kaspersky Embedded Systems Security reciben la prioridad *Media* (Normal).

6. Seleccione la casilla **Considerar la tarea como Análisis de áreas críticas** si desea usar la tarea como una tarea *Análisis de áreas críticas*.

7. Seleccione la casilla **No ejecutar varias tareas de análisis al mismo tiempo** para optimizar la carga en el equipo.

8. Guarde los cambios.

Cómo configurar la tarea Análisis a pedido en Kaspersky Security Center Web Console

1. Abra las propiedades de la tarea Análisis a pedido.

2. Seleccione la sección **Configuración de la aplicación**.

3. Vaya a la sección **Configuración**.

4. Desactive o seleccione la casilla de verificación **Utilizar análisis heurístico**.

5. Si es necesario, seleccione el nivel de análisis en la lista desplegable **Nivel del análisis heurístico**.

6. Seleccione la casilla **Ejecutar tarea en segundo plano** si desea asignar una prioridad *Baja* al proceso de trabajo en el que se ejecutará la tarea.

   De manera predeterminada, los procesos de trabajo en que se ejecutan las tareas de Kaspersky Embedded Systems Security reciben la prioridad *Media* (Normal).

7. Seleccione la casilla **Considerar la tarea como Análisis de áreas críticas** si desea usar la tarea como una tarea *Análisis de áreas críticas*.

8. Seleccione la casilla **No ejecutar varias tareas de análisis al mismo tiempo** para optimizar la carga en el equipo.

9. Guarde los cambios.

Cómo configurar la tarea Análisis a pedido en la Consola de la aplicación

1. En el árbol de la Consola de la aplicación, expanda el nodo **Análisis a pedido**.

2. Seleccione el nodo secundario correspondiente a una tarea de Análisis a pedido que desea configurar.

3. En el panel de resultados del nodo seleccionado, haga clic en **Propiedades**.

4. Seleccione la ficha **Configuración de la tarea**.
5. Desactive o seleccione la casilla de verificación **Utilizar análisis heurístico**.
6. Si es necesario, cambie el nivel de análisis.
7. Seleccione la casilla **Ejecutar tarea en segundo plano** si desea asignar una prioridad *Baja* al proceso de trabajo en el que se ejecutará la tarea.

   De manera predeterminada, los procesos de trabajo en que se ejecutan las tareas de Kaspersky Embedded Systems Security reciben la prioridad *Media* (Normal).

8. Seleccione la casilla **Considerar la tarea como Análisis de áreas críticas** si desea usar la tarea como una tarea *Análisis de áreas críticas*.
9. Seleccione la casilla **No ejecutar varias tareas de análisis al mismo tiempo** para optimizar la carga en el equipo.
10. Guarde los cambios.

Configuración del Análisis de unidades extraíbles

Configurar el Análisis de unidades extraíbles en la Consola 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 configurar la tarea.
3. Seleccione la pestaña **Directivas**.
4. Haga doble clic en el nombre de la directiva que desea configurar.

   En la ventana de las propiedades de la directiva, vaya a la sección **Adicional**.
5. Haga clic en **Configuración** en la subsección **Análisis de unidades extraíbles**.

   Se abre la ventana **Análisis de unidades extraíbles**.

6. Haga lo siguiente:

   - Seleccione la casilla de verificación **Analizar unidades extraíbles al conectarlas 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 tamaño no excede (MB)** y especifique el valor máximo en el campo de la derecha.
   - En la lista desplegable **Analizar con nivel de seguridad**, seleccione el nivel de seguridad que reúna los parámetros con los que desee ejecutar las tareas de Análisis de unidades extraíbles.

7. Haga clic en **Aceptar**.

La configuración especificada se guarda y se aplica.

Configurar el Análisis de unidades extraíbles en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a la sección **Adicional**.
5. Haga clic en **Configurar** en **Análisis de unidades extraíbles**.

   Se abre la ventana **Análisis de unidades extraíbles**.
6. Haga lo siguiente:

   - Seleccione la casilla de verificación **Analizar unidades extraíbles al conectarlas 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 tamaño no excede (MB)** y especifique el valor máximo en el campo de la derecha.
   - En la lista desplegable **Analizar con nivel de seguridad**, seleccione el nivel de seguridad que reúna los parámetros con los que desee ejecutar las tareas de Análisis de unidades extraíbles.

7. Haga clic en **Aceptar**.

La configuración especificada se guarda y se aplica.

Configurar el Análisis de unidades extraíbles en 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** y seleccione **Análisis de unidades extraíbles**.

   Se abre la ventana **Análisis de unidades extraíbles**.

2. Haga lo siguiente:

   - Seleccione la casilla de verificación **Analizar unidades extraíbles al conectarlas 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 tamaño no excede (MB)** y especifique el valor máximo en el campo de la derecha.
   - En la lista desplegable **Analizar con nivel de seguridad**, seleccione el nivel de seguridad que reúna los parámetros con los que desee ejecutar las tareas de Análisis de unidades extraíbles.

3. Haga clic en **Aceptar**.

Selección de niveles de seguridad predefinidos para tareas de Análisis a pedido

Se puede aplicar uno de los siguientes tres niveles de seguridad predefinidos a un nodo seleccionado en la lista de recursos de archivos del dispositivo protegido: **Máximo rendimiento**, **Recomendado** y **Máxima protección**.

Seleccionar uno de los niveles de seguridad predefinidos en la Consola de administración de Kaspersky Security Center

1. Abra las propiedades de la tarea Análisis a pedido.
2. Seleccione la sección **Alcance del análisis**.
3. En la lista del dispositivo protegido, seleccione un elemento incluido en el área del análisis para configurar un nivel de seguridad predefinido.
4. Haga clic en **Configurar**.
5. En la ventana que se abre, en la pestaña **Nivel de seguridad**, seleccione el nivel de seguridad que se aplicará.
6. Haga clic en **Aceptar**.
7. En la ventana **Propiedades: Análisis a pedido**, haga clic en el botón **Aceptar**.

La configuración de la tarea se guarda y se aplica inmediatamente a una tarea en ejecución. Si la tarea no se está ejecutando, la configuración modificada se aplica en el siguiente inicio.

Seleccionar uno de los niveles de seguridad predefinidos en la Consola de la aplicación

1. En el árbol de la Consola de la aplicación, expanda el nodo **Análisis a pedido**.
2. Seleccione el nodo secundario correspondiente a una tarea de Análisis a pedido que desea configurar.
3. En el panel de resultados del nodo seleccionado, haga clic en **Configurar el área de protección**.
4. En la lista de recursos de archivos de la red del dispositivo protegido, seleccione un nodo o elemento para el que desea establecer el nivel de seguridad predefinido.
5. Asegúrese que el nodo o elemento seleccionado se incluya en el área del análisis.
6. Haga clic en **Configurar**.
7. En la ventana que se abre, seleccione el nivel de seguridad de su elección.

   La ventana muestra la lista de opciones de seguridad correspondientes al nivel de seguridad seleccionado.
8. 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.

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 al nivel de seguridad predefinido **Recomendado**.

Los valores predeterminados de la configuración de seguridad se pueden modificar configurándolos como valores comunes para toda el área del análisis, o como valores diferentes para los diversos elementos de la lista de recursos de archivos del dispositivo protegido o nodos del árbol.

Administrar manualmente la configuración de seguridad en la Consola de administración de Kaspersky Security Center

1. Abra las propiedades de la tarea Análisis a pedido.
2. Seleccione la sección **Alcance del análisis**.
3. En la lista de dispositivos protegidos, seleccione un elemento incluido en el alcance del análisis administrar la configuración de seguridad.
4. Haga clic en **Configurar**.
5. En la ventana que se abre, en la pestaña **Nivel de seguridad**, seleccione el nivel de seguridad que se aplicará.

6. Seleccione el recurso cuya configuración de seguridad desea ajustar.

7. Haga clic en **Configurar**.

8. En la ventana que se abre, seleccione el nivel de seguridad requerido y haga clic en **Configuración**.

9. En la pestaña **General**, especifique la siguiente configuración:

   - Objetos que deberían incluirse en el alcance de la protección:
     - **Todos los objetos**
     - **Objetos analizados según su formato**
     - **Objetos analizados según la lista de extensiones de la base de datos antivirus**
   - En el bloque **Optimización**, seleccione o desactive la casilla de verificación **Proteger solo los archivos nuevos y modificados**.
   - En la sección **Análisis de archivos compuestos**, especifique los objetos compuestos que desea incluir en el área de análisis:
     - **Analizar archivos de almacenamiento**
     - **Analizar paquetes de distribución**
     - **Analizar archivos de Microsoft Office**
     - **Analizar archivos de formato de correo electrónico**

10. En la pestaña **Acciones**, especifique la siguiente configuración:

    - Seleccione la acción que se debe realizar en los objetos infectados y otros objetos detectados:
      - **Desinfectar**
      - **Desinfectar; eliminar si falla la desinfección**
      - **Eliminar**
      - **Recomendada**
      - **Informar**
    - Configure las acciones que se deben realizar en los objetos según el tipo de objeto detectado:
      a. Desactive o seleccione la casilla de verificación **Aplicar la acción a los tipos de objetos seleccionados**.
      b. Haga clic en **Configuración** y seleccione los tipos de objetos que se deben detectar.
    - Configure las acciones en los archivos compuestos que no están disponibles para su modificación: desactive o seleccione la casilla **Si se detecta un objeto integrado, eliminar todo el archivo compuesto que la aplicación no pueda modificar**.

11. En la pestaña **Rendimiento**, especifique la siguiente configuración:
    - En el bloque **Exclusiones**:
        - Desactive o seleccione la casilla de verificación **Excluir archivos**.
        - Desactive o seleccione la casilla de verificación **No detectar objetos por tipo**.
          Haga clic en el botón **Modificar** en cada para parámetro agregar exclusiones.
    - En el bloque **Configuración avanzada**:
        - **Detener el análisis si demora más de (s)**
        - **No analizar objetos compuestos de más de (MB)**
        - **Usar la tecnología iSwift**
        - **Usar la tecnología iChecker**
12. Guarde la nueva configuración de seguridad.

Administrar manualmente la configuración de seguridad en Kaspersky Security Center Web Console

1. Abra las propiedades de la tarea Análisis a pedido.
2. Seleccione la sección **Configuración de la aplicación**.
3. Vaya a la sección **Alcance del análisis**.
4. En la lista de recursos de archivos de la red del dispositivo protegido, seleccione un elemento para el que desea administrar la configuración de seguridad. Asegúrese de que el elemento seleccionado se incluya en el alcance del análisis.
5. Haga clic en **Modificar**.
6. Seleccione un modo de protección de objetos en la lista desplegable:
    - **Todos los objetos**
    - **Objetos analizados según su formato**
    - **Objetos analizados según la lista de extensiones de la base de datos antivirus**
7. Seleccione o desactive la casilla **Proteger solo los archivos nuevos y modificados** y especifique si desea incluir Subcarpetas en el análisis.
8. Administre la configuración de la protección de objetos compuestos:
    - **Analizar archivos de almacenamiento**
    - **Analizar paquetes de distribución**

- Analizar archivos de Microsoft Office
- Analizar archivos de formato de correo electrónico

9. Seleccione la acción que se debe realizar en los objetos infectados y otros objetos detectados:
   - **Desinfectar**
   - **Desinfectar; eliminar si falla la desinfección**
   - Eliminar
   - Recomendada
   - Informar
10. Configure las acciones que se deben realizar en los objetos según el tipo de objeto detectado:
    a. Desactive o seleccione la casilla de verificación Aplicar la acción a los tipos de objetos seleccionados.
    b. Haga clic en **Configuración** y seleccione los tipos de objetos que se deben detectar.
11. Configure las acciones en los archivos compuestos que no están disponibles para su modificación: desactive o seleccione la casilla Si se detecta un objeto integrado, eliminar todo el archivo compuesto que la aplicación no pueda modificar.
12. En el bloque **Exclusiones**:
    - Desactive o seleccione la casilla de verificación Excluir archivos.
    - Desactive o seleccione la casilla de verificación No detectar objetos por tipo.
13. En el bloque **Agregar clave**:
    - Detener el análisis si demora más de (s)
    - No analizar objetos compuestos de más de (MB)
    - Usar la tecnología iSwift
    - Usar la tecnología iChecker
14. Guarde la nueva configuración de seguridad.

Administrar manualmente la configuración de seguridad en la Consola de la aplicación

1. En el árbol de la Consola de la aplicación, expanda el nodo **Análisis a pedido**.
2. Seleccione el nodo secundario correspondiente a una tarea de Análisis a pedido que desea configurar.
3. En el panel de resultados del nodo seleccionado, haga clic en **Configurar el área de protección**.

4. En la lista de recursos de archivos de la red del dispositivo protegido, seleccione un elemento para el que desea administrar la configuración de seguridad.

5. Asegúrese de que el elemento seleccionado se incluya en el alcance del análisis.

6. Haga clic en **Configurar**.

7. En la ventana que se abre, seleccione el nivel de seguridad requerido y haga clic en **Configuración**.

8. En la pestaña **General**, especifique la siguiente configuración:

   - Objetos que deberían incluirse en el alcance de la protección:
     - **Todos los objetos**.
     - **Objetos analizados según su formato**.
     - **Objetos analizados según la lista de extensiones de la base de datos antivirus**.
   - En el bloque **Optimización**, seleccione o desactive la casilla de verificación **Proteger solo los archivos nuevos y modificados**.
   - En la sección **Análisis de archivos compuestos**, especifique los objetos compuestos que desea incluir en el área de análisis:
     - **Analizar archivos de almacenamiento**.
     - **Analizar paquetes de distribución**.
     - **Analizar archivos de Microsoft Office**.
     - **Analizar archivos de formato de correo electrónico**.

9. En la pestaña **Acciones**, especifique la siguiente configuración:

   - Seleccione la acción que se debe realizar en los objetos infectados y otros objetos detectados:
     - **Desinfectar**
     - **Desinfectar; eliminar si falla la desinfección**
     - **Eliminar**.
     - **Recomendada**.
     - **Informar**.

- Configure las acciones que se deben realizar en los objetos según el tipo de objeto detectado:

  a. Desactive o seleccione la casilla de verificación **Aplicar la acción a los tipos de objetos seleccionados**.

  b. Haga clic en **Configuración** y seleccione los tipos de objetos que se deben detectar.

- Configure las acciones en los archivos compuestos que no están disponibles para su modificación: desactive o seleccione la casilla **Si se detecta un objeto integrado, eliminar todo el archivo compuesto que la aplicación no pueda modificar**.

10. En la pestaña **Rendimiento**, especifique la siguiente configuración:

    - En el bloque **Exclusiones**:

      - Desactive o seleccione la casilla de verificación **Excluir archivos**.
      - Desactive o seleccione la casilla de verificación **No detectar objetos por tipo**.

      Haga clic en el botón **Modificar** en cada para parámetro agregar exclusiones.

    - En el bloque **Configuración avanzada**:

      - **Detener el análisis si demora más de (s)**.
      - **No analizar objetos compuestos de más de (MB)**.
      - **Usar la tecnología iSwift**.
      - **Usar la tecnología iChecker**.

11. Guarde la nueva configuración de seguridad.

Estadísticas de la tarea de Análisis a pedido

Mientras se ejecuta la tarea de Análisis a pedido, puede visualizar información sobre la cantidad de objetos procesados por Kaspersky Embedded Systems Security desde que se inició.

Esta información permanecerá disponible aún si se pausa la tarea. Puede ver las estadísticas de la tarea en el registro de tareas.

Para ver las estadísticas de una tarea de Análisis a pedido:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Análisis a pedido**.

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 resultados 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.

Campo	Descripción
Detectados	Número de objetos detectados por Kaspersky Embedded Systems Security. Por ejemplo, si Kaspersky Embedded Systems Security detecta un objeto malicioso en cinco archivos, el valor de este campo aumenta en uno.
Objetos infectados y otros objetos	Número de objetos que Kaspersky Embedded Systems Security encontró y clasificó como infectados o número de archivos encontrados de software legítimo que no se excluyeron del alcance del análisis y se clasificaron como software legítimo que los intrusos pueden utilizar para dañar el dispositivo o sus datos personales.
No se desinfectó el objeto	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 desinfectados	Número de objetos desinfectados por Kaspersky Embedded Systems Security.
Objetos eliminados	Cantidad de objetos eliminados correctamente por Kaspersky Embedded Systems Security.
Objetos no analizados	Cantidad de objetos en el área 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.
Archivos comprimidos	Cantidad de archivos analizados por Kaspersky Embedded Systems Security.
Objetos empaquetados	Cantidad de objetos comprimidos analizados 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 porque el formato estaba dañado.
Errores de procesamiento	Cantidad de objetos en los que se produjo un error durante su procesamiento.
Objetos no eliminados	Cantidad de objetos que Kaspersky Embedded Systems Security intentó eliminar sin éxito debido a que, por ejemplo, el acceso al objeto estaba bloqueado por otra aplicación.
Objetos no procesados	Cantidad total de objetos que Kaspersky Embedded Systems Security no procesó.

También puede ver las estadísticas de la tarea Análisis a pedido en el registro de tareas seleccionado si hace clic en el vínculo **Abrir registro de tareas** en la sección **Administración** del panel de resultados.

Le recomendamos procesar manualmente los eventos incluidos en la pestaña **Eventos** en el registro de tareas al finalizar la tarea.

Base de datos y actualización de módulos del programa de Kaspersky Embedded Systems Security

En esta sección se ofrece información acerca de las tareas de actualización y la reversión de actualizaciones de Kaspersky Embedded Systems Security, así como instrucciones para la configuración de la tarea.

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

Actualizar bases de datos y módulos de la aplicación

La actualización de las bases de datos y de los módulos de la aplicación Kaspersky Embedded Systems Security garantiza una protección actualizada del equipo. Todos los días aparecen nuevos virus y otros tipos de malware en todo el mundo. Las bases de datos de Kaspersky Embedded Systems Security contienen información sobre amenazas y sobre las formas de neutralizarlas. Para detectar amenazas rápidamente, se recomienda actualizar las bases de datos y los módulos de la aplicación con regularidad.

Las actualizaciones regulares requieren una licencia en vigencia. Si no hay una licencia actual, se podrá realizar una única actualización.

Kaspersky Embedded Systems Security descarga las actualizaciones de las bases de datos y los módulos de la aplicación desde los servidores de actualizaciones HTTP o FTP de Kaspersky, el servidor de administración de Kaspersky Security Center u otros orígenes de actualizaciones.

Puede descargar actualizaciones para cada dispositivo protegido o usar un dispositivo protegido como intermediario. Las actualizaciones se copiarán al dispositivo que actúe como intermediario y luego se distribuirán a los dispositivos protegidos restantes. Si administra la seguridad de los dispositivos de su organización de manera centralizada con Kaspersky Security Center, puede utilizar el Servidor de administración como proxy para descargar las actualizaciones.

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 de las últimas actualizaciones instaladas. Si las bases de datos de Kaspersky Embedded Systems Security se dañan, se pueden revertir manualmente a las actualizaciones anteriormente instaladas.

Al realizar una actualización, se descargan e instalan en el equipo los siguientes objetos:

- Bases de datos de Kaspersky Embedded Systems Security. La protección del equipo se brinda con bases de datos que contienen firmas de virus y otras amenazas e información sobre maneras de neutralizarlas. Los componentes de protección utilizan esta información al realizar búsquedas de archivos infectados en el equipo y neutralizarlos. Las bases de datos se actualizan constantemente con registros de amenazas nuevas y métodos para contrarrestarlas. Por lo tanto, le recomendamos actualizar las bases de datos con regularidad.

  Además de las bases de datos de Kaspersky Embedded Systems Security, también se actualizan los controladores de red que permiten a los componentes de la aplicación interceptar el tráfico de la red.

- Módulos de la aplicación. Además de las bases de datos de Kaspersky Embedded Systems Security, también se pueden actualizar los módulos de la aplicación. La actualización de los módulos de la aplicación repara vulnerabilidades en Kaspersky Embedded Systems Security y agrega funciones nuevas o mejora funciones existentes.

Durante la actualización, los módulos de la aplicación y las bases de datos del equipo se comparan con la versión actualizada en el origen de actualizaciones. Si las bases de datos y los módulos de la aplicación actuales difieren de las respectivas versiones actualizadas, la parte faltante de las actualizaciones se instala en el equipo.

Si las bases de datos están obsoletas, es posible que el tamaño del paquete de actualización sea considerable, lo que puede ocasionar un mayor tráfico web (hasta varias docenas de MB).

La información sobre el estado actual de las bases de datos de Kaspersky Embedded Systems Security se muestra en la ventana principal de la aplicación o en la información sobre herramientas que ve cuando pasa el cursor sobre el ícono de la aplicación en el área de notificaciones.

La información sobre los resultados de la actualización y sobre todos los eventos que ocurren durante la ejecución de la tarea de actualización se registra en el registro de tareas de actualización.

Acerca de las tareas de Actualización

Kaspersky Embedded Systems Security tiene dos tareas de actualización: Actualizar y Reversión de la actualización.

De forma predeterminada, Kaspersky Embedded Systems Security se conecta con el origen de actualizaciones cada una hora. Puede configurar todas las tareas de actualización, excepto la tarea Reversión de la actualización. 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 manera predeterminada, Kaspersky Embedded Systems Security copia las bases de datos y, si están disponibles, los módulos de la aplicación del origen de actualizaciones al dispositivo 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.

Reversión de la actualización

La tarea hace que Kaspersky Embedded Systems Security vuelva a los módulos de la aplicación y las bases de datos anteriores.

La tarea Reversión de la actualización está deshabilitada de manera predeterminada.

Esquemas de actualización para las bases de datos y los módulos de Kaspersky Embedded Systems Security

La elección del origen de actualizaciones en la tarea de actualización depende del esquema elegido para actualizar las bases de datos y los módulos de software en la organización.

Los módulos y bases de datos de Kaspersky Embedded Systems Security se pueden actualizar en los dispositivos protegidos mediante los esquemas siguientes:

- Descargar actualizaciones directamente de Internet a cada dispositivo protegido (Esquema 1).
- Descargar actualizaciones de Internet a un dispositivo intermediario y distribuirlas a dispositivos protegidos desde ese dispositivo.

  Cualquier dispositivo que tenga las siguientes aplicaciones instaladas puede funcionar como intermediario:

  - Kaspersky Embedded Systems Security (Esquema 2).
  - Servidor de administración de Kaspersky Security Center (Esquema 3).

  > La actualización mediante un dispositivo intermediario no solo reduce el tráfico de Internet, sino que también proporciona seguridad adicional para los dispositivos protegidos de la red.

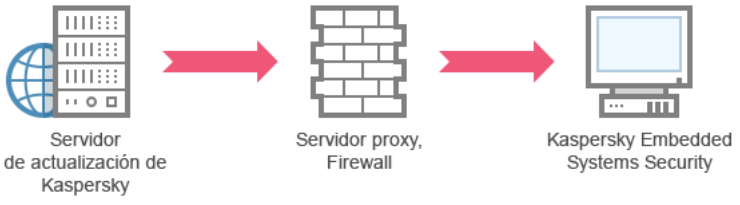
Los esquemas de actualización enumerados se describen a continuación.

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 dispositivo protegido, en la configuración de la tarea de Actualización de bases de datos, especifique los servidores de actualizaciones de Kaspersky como el origen de actualizaciones.

Se pueden configurar otros servidores HTTPS o HTTP que tengan una carpeta de actualización como el origen de actualizaciones.



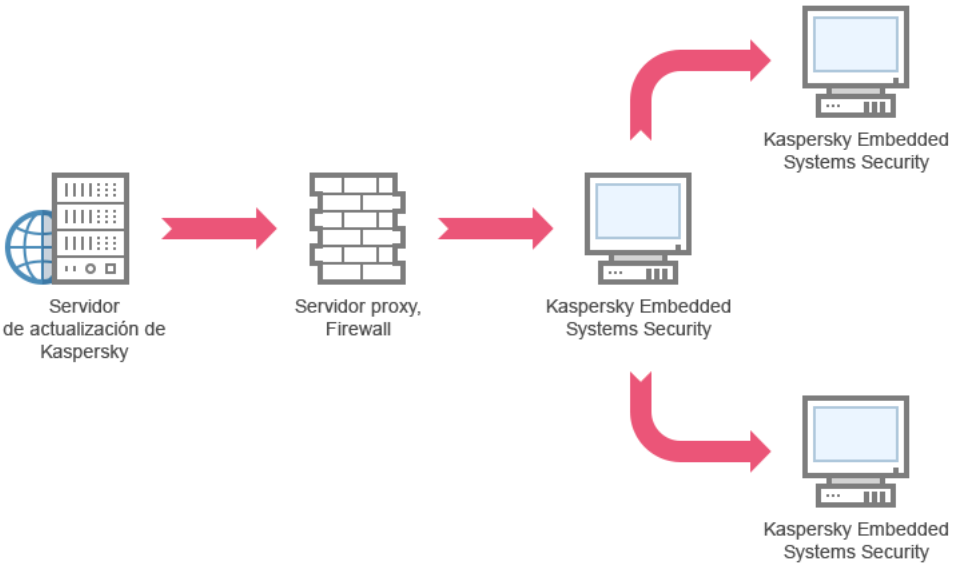
Esquema 1: Actualización de bases de datos y módulos directamente desde Internet

Esquema 2. Actualización de bases de datos y módulos a través de uno de los dispositivos protegidos

Para configurar la recepción de actualizaciones para Kaspersky Embedded Systems Security mediante uno de los dispositivos protegidos:

1. Copie las actualizaciones en el dispositivo protegido seleccionado.
   - Configure la configuración de la tarea de Actualización en el dispositivo protegido seleccionado:
     a. Especifique el servidor de actualizaciones de Kaspersky 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 dispositivos protegidos:
   - Configure la tarea de Actualización en cada uno de los dispositivos protegidos.
     Como origen de actualizaciones, especifique la carpeta en la unidad del dispositivo intermediario en la cual se descargarán las actualizaciones.

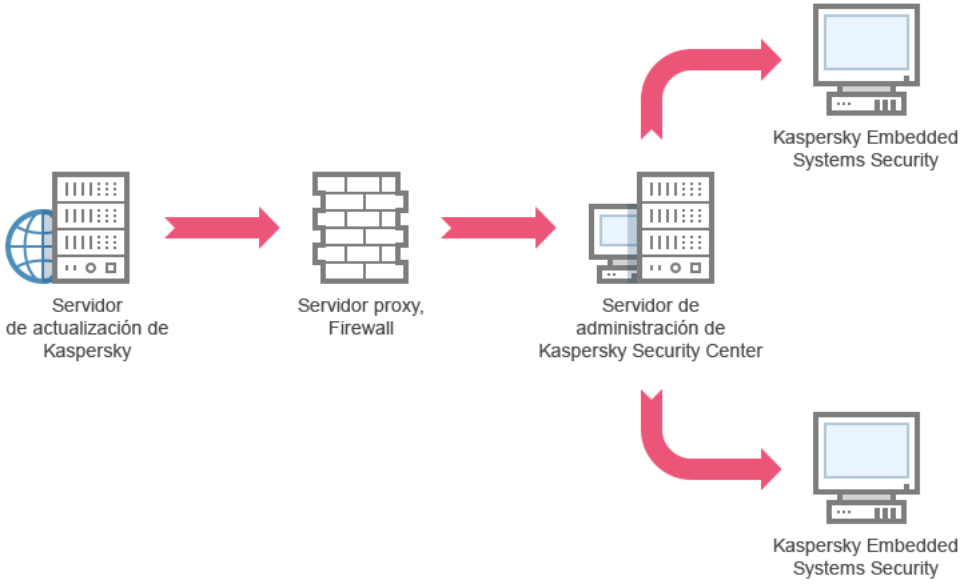
Kaspersky Embedded Systems Security obtendrá actualizaciones mediante uno de los dispositivos protegidos.



Esquema 2: Actualización de bases de datos y módulos a través de uno de los dispositivos protegidos

Esquema 3. Actualización de bases de datos y módulos a través del Servidor de administración de Kaspersky Security Center

Si utiliza Kaspersky Security Center para administrar de forma centralizada la protección antivirus de los dispositivos, puede descargar las actualizaciones a través del Servidor de administración de Kaspersky Security Center instalado en la red local.



Esquema 3: Actualización de bases de datos y módulos a través del Servidor de administración de Kaspersky Security Center

Para configurar la recepción de actualizaciones para Kaspersky Embedded Systems Security mediante el Servidor de administración de Kaspersky Security Center:

1. Instale el Agente de red en cada uno de los dispositivos protegidos. El Agente de red es un componente de software incluido en el kit de distribución de Kaspersky Security Center. Esto garantiza la interacción entre el Servidor de administración y Kaspersky Embedded Systems Security en el dispositivo protegido. Se proporciona información detallada sobre el Agente de red y su configuración con Kaspersky Security Center en la *Ayuda de Kaspersky Security Center*.

2. Descargue las actualizaciones de los servidores de actualizaciones de Kaspersky en el Servidor de administración de Kaspersky Security Center.

   - Configure la tarea de Recuperar actualizaciones por el servidor de administración para el conjunto especificado de dispositivos protegidos.

     Especifique el servidor de actualizaciones de Kaspersky como el origen de actualizaciones.

3. Distribuir actualizaciones a los dispositivos 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 dispositivos protegidos:

   - Configure la tarea de Actualización en cada uno de los dispositivos protegidos:

     a. Especifique el servidor de administración de Kaspersky Security Center como origen de actualizaciones.

     b. Configure la programación de la tarea de ser necesario.

Kaspersky Embedded Systems Security obtendrá actualizaciones mediante el Servidor de administración de Kaspersky Security Center.

Configuración de tareas de Actualización

Cómo configurar la tarea de Actualización en la Consola de administración de Kaspersky Security Center

1. En la Consola de administración de Kaspersky Security Center, vaya a la tarea de actualización local o de grupo que desea configurar.
2. Abra la sección **Configuración**.
3. En **Configuración de actualización en modo local** para Kaspersky Embedded Systems Security conectado al Servidor de administración de Kaspersky Security Center, configure orígenes de actualizaciones:
   a. Haga clic en **Configuración**.
      Se abre la ventana **Actualización de bases de datos y módulos de la aplicación**.
   b. Active la casilla ubicada junto a los orígenes de actualizaciones que desee usar:
      - Servidor de administración de Kaspersky Security Center
      - Servidores de actualizaciones de Kaspersky

      Si es necesario, haga clic en el botón **Agregar** para agregar un origen de actualizaciones personalizado.
   c. Si selecciona varios orígenes de actualizaciones, use los botones **Arriba** y **Abajo** para ordenar los orígenes de actualizaciones por prioridad. Kaspersky Embedded Systems Security accede a los orígenes de actualizaciones siguiendo estrictamente el orden configurado y realiza la tarea de actualización usando el paquete de actualización del primer origen de actualizaciones disponible.
      De manera predeterminada, Kaspersky Embedded Systems Security usa el servidor de Kaspersky Security Center como el primer origen de actualizaciones. Esto ayuda a conservar el tráfico al actualizar. Si no se aplica una directiva al equipo, los servidores de Kaspersky se seleccionan como el primer origen de actualizaciones en la configuración de la tarea Actualización local, ya que es posible que la aplicación no tenga acceso a Kaspersky Security Center.
   d. Si seleccionó **Servidores de actualizaciones de Kaspersky** como origen de actualizaciones, seleccione el principio que Kaspersky Embedded Systems Security debe seguir cuando selecciona un servidor de actualizaciones de Kaspersky:
      - **Detección automática**. La aplicación usa el servidor de actualizaciones de Kaspersky disponible más cercano.
      - **Seleccionar de la lista**. La aplicación usa el servidor de actualizaciones de Kaspersky en el país que se seleccionó en la lista.
   e. En la ventana **Actualización de bases de datos y módulos de la aplicación**, haga clic en el botón **Aceptar**.
4. Configure las actualizaciones de bases de datos de la aplicación:
   a. Seleccione o desactive la casilla **Descargar actualizaciones de las bases de datos de la aplicación**.

b. Seleccione o desactive la casilla **Reducir la carga de lectura y escritura en disco**.

c. Si seleccionó la casilla **Reducir la carga de lectura y escritura en disco**, en el campo **RAM usada para la optimización, MB**, especifique la cantidad de RAM en megabytes. 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 640 MB. El tamaño de RAM mínimo es 400 MB.

Cuando ejecuta la tarea Actualización con la optimización del subsistema del disco habilitada, puede producirse una de las siguientes situaciones:

- Si el valor es demasiado pequeño, la cantidad de memoria RAM asignada podría ser insuficiente para completar la tarea de actualización de bases de datos (por ejemplo, durante la primera actualización); lo que conducirá a la finalización de la tarea con un error.

  En este caso, se recomienda asignar más memoria RAM para la función de optimización del subsistema del disco.

- Si el valor es demasiado grande, al comienzo de la tarea de Actualización de bases de datos, podría ser imposible crear una unidad virtual de un tamaño seleccionado en la memoria RAM. Como consecuencia, la función de optimización del subsistema del disco se deshabilita automáticamente y la tarea de Actualización de bases de datos se ejecuta sin la función de optimización.

  En este caso, se recomienda asignar menos memoria RAM para la función de optimización del subsistema del disco.

5. Configure actualizaciones del módulo de software de la aplicación:

a. Seleccione o desactive la casilla **Descargar actualizaciones de módulos de la aplicación**.

b. Seleccione el tipo de actualización del módulo de la aplicación que desea aplicar.

- **Instalar actualizaciones críticas y aprobadas**. Si esta opción está seleccionada, cuando haya actualizaciones de los módulos de la aplicación disponibles Kaspersky Embedded Systems Security instala las actualizaciones críticas en forma automática y todas las otras actualizaciones de los módulos de la aplicación solo luego de que se haya aprobado en forma local su instalación, mediante la interfaz de la aplicación o por parte de Kaspersky Security Center.

- **Instalar solo actualizaciones aprobadas**. Si esta opción está seleccionada, cuando haya actualizaciones de los módulos de la aplicación disponibles Kaspersky Embedded Systems Security instala las actualizaciones solo luego de que se haya aprobado en forma local su instalación, mediante la interfaz de la aplicación o por parte de Kaspersky Security Center. De forma predeterminada, esta opción está seleccionada.

Si las actualizaciones de los módulos de aplicación requieren la revisión y aceptación de los términos del Contrato de licencia para usuario final, la aplicación instala las actualizaciones una vez que se hayan aceptado los términos del Contrato de licencia para usuario final.

6. Configure la copia de actualizaciones en una carpeta para el almacenamiento local:

a. Seleccione o desactive la casilla **Copiar actualizaciones en una carpeta para almacenamiento local**.

b. Seleccione el contenido de las actualizaciones que desea que la aplicación copie en la carpeta de almacenamiento local:

- **Copiar actualizaciones de las bases de datos**. La aplicación descarga solo actualización de bases de datos.
- **Copiar actualizaciones críticas de módulos de la aplicación**. La aplicación descarga solo actualizaciones críticas del módulo de la aplicación.
- **Copiar actualizaciones de bases de datos y actualizaciones críticas de módulos de la aplicación**. La aplicación descarga actualización de bases de datos y actualizaciones críticas del módulo de la aplicación.

c. Especifique la carpeta local o de red a la cual Kaspersky Embedded Systems Security distribuirá las actualizaciones descargadas.

7. Guarde los cambios.

Cómo configurar la tarea de Actualización en la Consola de la aplicación

1. En el árbol de la Consola de la aplicación, abra el nodo **Actualización** → **Actualización de bases de datos y módulos de la aplicación**.
2. Haga clic en el vínculo **Propiedades** del panel de resultados.

   Se abre la ventana **Propiedades: Actualización de bases de datos y módulos de la aplicación**.
3. En **Configuración de actualización en modo local** para Kaspersky Embedded Systems Security conectado al Servidor de administración de Kaspersky Security Center, configure orígenes de actualizaciones:

   a. Haga clic en **Configuración**.

   Se abre la ventana **Actualización de bases de datos y módulos de la aplicación**.

   b. Active la casilla ubicada junto a los orígenes de actualizaciones que desee usar:

   - Servidor de administración de Kaspersky Security Center
   - Servidores de actualizaciones de Kaspersky

   Si es necesario, haga clic en el botón **Agregar** para agregar un origen de actualizaciones personalizado.

   c. Si selecciona varios orígenes de actualizaciones, use los botones **Arriba** y **Abajo** para ordenar los orígenes de actualizaciones por prioridad. Kaspersky Embedded Systems Security accede a los orígenes de actualizaciones siguiendo estrictamente el orden configurado y realiza la tarea de actualización usando el paquete de actualización del primer origen de actualizaciones disponible.

   De manera predeterminada, Kaspersky Embedded Systems Security usa el servidor de Kaspersky Security Center como el primer origen de actualizaciones. Esto ayuda a conservar el tráfico al actualizar. Si no se aplica una directiva al equipo, los servidores de Kaspersky se seleccionan como el primer origen de actualizaciones en la configuración de la tarea Actualización local, ya que es posible que la aplicación no tenga acceso a Kaspersky Security Center.

d. Si seleccionó **Servidores de actualizaciones de Kaspersky** como origen de actualizaciones, seleccione el principio que Kaspersky Embedded Systems Security debe seguir cuando selecciona un servidor de actualizaciones de Kaspersky:

- **Detección automática**. La aplicación usa el servidor de actualizaciones de Kaspersky disponible más cercano.
- **Seleccionar de la lista**. La aplicación usa el servidor de actualizaciones de Kaspersky en el país que se seleccionó en la lista.

e. En la ventana **Actualización de bases de datos y módulos de la aplicación**, haga clic en el botón **Aceptar**.

4. Configure las actualizaciones de bases de datos de la aplicación:

a. Seleccione o desactive la casilla **Descargar actualizaciones de las bases de datos de la aplicación**.

b. Seleccione o desactive la casilla **Reducir la carga de lectura y escritura en disco**.

c. Si seleccionó la casilla **Reducir la carga de lectura y escritura en disco**, en el campo **RAM usada para la optimización, MB**, especifique la cantidad de RAM en megabytes. 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 640 MB. El tamaño de RAM mínimo es 400 MB.

Cuando ejecuta la tarea Actualización con la optimización del subsistema del disco habilitada, puede producirse una de las siguientes situaciones:

- Si el valor es demasiado pequeño, la cantidad de memoria RAM asignada podría ser insuficiente para completar la tarea de actualización de bases de datos (por ejemplo, durante la primera actualización); lo que conducirá a la finalización de la tarea con un error.

  En este caso, se recomienda asignar más memoria RAM para la función de optimización del subsistema del disco.

- Si el valor es demasiado grande, al comienzo de la tarea de Actualización de bases de datos, podría ser imposible crear una unidad virtual de un tamaño seleccionado en la memoria RAM. Como consecuencia, la función de optimización del subsistema del disco se deshabilita automáticamente y la tarea de Actualización de bases de datos se ejecuta sin la función de optimización.

  En este caso, se recomienda asignar menos memoria RAM para la función de optimización del subsistema del disco.

5. Configure actualizaciones del módulo de software de la aplicación:

a. Seleccione o desactive la casilla **Descargar actualizaciones de módulos de la aplicación**.

b. Seleccione el tipo de actualización del módulo de la aplicación que desea aplicar.

- **Instalar actualizaciones críticas y aprobadas**. Si esta opción está seleccionada, cuando haya actualizaciones de los módulos de la aplicación disponibles Kaspersky Embedded Systems Security instala las actualizaciones críticas en forma automática y todas las otras actualizaciones de los módulos de la aplicación solo luego de que se haya aprobado en forma local su instalación, mediante la interfaz de la aplicación o por parte de Kaspersky Security Center.
- **Instalar solo actualizaciones aprobadas**. Si esta opción está seleccionada, cuando haya actualizaciones de los módulos de la aplicación disponibles Kaspersky Embedded Systems Security instala las actualizaciones solo luego de que se haya aprobado en forma local su instalación, mediante la interfaz de la aplicación o por parte de Kaspersky Security Center. De forma predeterminada, esta opción está seleccionada.

Si las actualizaciones de los módulos de aplicación requieren la revisión y aceptación de los términos del Contrato de licencia para usuario final, la aplicación instala las actualizaciones una vez que se hayan aceptado los términos del Contrato de licencia para usuario final.

6. Configure la copia de actualizaciones en una carpeta para el almacenamiento local:

   a. Seleccione o desactive la casilla **Copiar actualizaciones en una carpeta para almacenamiento local**.

   b. Seleccione el contenido de las actualizaciones que desea que la aplicación copie en la carpeta de almacenamiento local:

   - **Copiar actualizaciones de las bases de datos**. La aplicación descarga solo actualización de bases de datos.
   - **Copiar actualizaciones críticas de módulos de la aplicación**. La aplicación descarga solo actualizaciones críticas del módulo de la aplicación.
   - **Copiar actualizaciones de bases de datos y actualizaciones críticas de módulos de la aplicación**. La aplicación descarga actualización de bases de datos y actualizaciones críticas del módulo de la aplicación.

   c. Especifique la carpeta local o de red a la cual Kaspersky Embedded Systems Security distribuirá las actualizaciones descargadas.

7. Guarde los cambios.

Cómo configurar la tarea de Actualización en Kaspersky Security Center Web Console

1. En Web Console, vaya a la tarea de actualización local o de grupo que desee configurar.
2. Abra la sección **Configuración**.
3. Seleccione la pestaña **Modo local** para configurar la tarea Actualización para Kaspersky Embedded Systems Security conectado al Servidor de administración de Kaspersky Security Center.
4. Configure los orígenes de actualizaciones:

   a. En **Orígenes de actualizaciones**, seleccione la casilla junto a los orígenes de actualizaciones que desee usar:

   - **Servidor de administración de Kaspersky Security Center**
   - **Servidores de actualizaciones de Kaspersky**

   Si es necesario, haga clic en el botón **Agregar** para agregar un origen de actualizaciones personalizado.

b. Si selecciona varios orígenes de actualizaciones, use los botones **Arriba** y **Abajo** para ordenar los orígenes de actualizaciones por prioridad. Kaspersky Embedded Systems Security accede a los orígenes de actualizaciones siguiendo estrictamente el orden configurado y realiza la tarea de actualización usando el paquete de actualización del primer origen de actualizaciones disponible.

De manera predeterminada, Kaspersky Embedded Systems Security usa el servidor de Kaspersky Security Center como el primer origen de actualizaciones. Esto ayuda a conservar el tráfico al actualizar. Si no se aplica una directiva al equipo, los servidores de Kaspersky se seleccionan como el primer origen de actualizaciones en la configuración de la tarea Actualización local, ya que es posible que la aplicación no tenga acceso a Kaspersky Security Center.

5. Configure las actualizaciones de bases de datos de la aplicación:

a. Seleccione o desactive la casilla **Descargar actualizaciones de las bases de datos de la aplicación**.

b. Seleccione o desactive la casilla **Reducir la carga de lectura y escritura en disco**.

c. Si seleccionó la casilla **Reducir la carga de lectura y escritura en disco**, en el campo **RAM usada para la optimización, MB**, especifique la cantidad de RAM en megabytes. 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 640 MB. El tamaño de RAM mínimo es 400 MB.

Cuando ejecuta la tarea Actualización con la optimización del subsistema del disco habilitada, puede producirse una de las siguientes situaciones:

- Si el valor es demasiado pequeño, la cantidad de memoria RAM asignada podría ser insuficiente para completar la tarea de actualización de bases de datos (por ejemplo, durante la primera actualización); lo que conducirá a la finalización de la tarea con un error.

  En este caso, se recomienda asignar más memoria RAM para la función de optimización del subsistema del disco.

- Si el valor es demasiado grande, al comienzo de la tarea de Actualización de bases de datos, podría ser imposible crear una unidad virtual de un tamaño seleccionado en la memoria RAM. Como consecuencia, la función de optimización del subsistema del disco se deshabilita automáticamente y la tarea de Actualización de bases de datos se ejecuta sin la función de optimización.

  En este caso, se recomienda asignar menos memoria RAM para la función de optimización del subsistema del disco.

6. Configure actualizaciones del módulo de software de la aplicación:

a. Seleccione o desactive la casilla **Descargar actualizaciones de módulos de la aplicación**.

b. Seleccione el tipo de actualización del módulo de la aplicación que desea aplicar.

- **Instalar actualizaciones críticas y aprobadas**. Si esta opción está seleccionada, cuando haya actualizaciones de los módulos de la aplicación disponibles Kaspersky Embedded Systems Security instala las actualizaciones críticas en forma automática y todas las otras actualizaciones de los módulos de la aplicación solo luego de que se haya aprobado en forma local su instalación, mediante la interfaz de la aplicación o por parte de Kaspersky Security Center.

- **Instalar solo actualizaciones aprobadas**. Si esta opción está seleccionada, cuando haya actualizaciones de los módulos de la aplicación disponibles Kaspersky Embedded Systems Security instala las actualizaciones solo luego de que se haya aprobado en forma local su instalación, mediante la interfaz de la aplicación o por parte de Kaspersky Security Center. De forma predeterminada, esta opción está seleccionada.

Si las actualizaciones de los módulos de aplicación requieren la revisión y aceptación de los términos del Contrato de licencia para usuario final, la aplicación instala las actualizaciones una vez que se hayan aceptado los términos del Contrato de licencia para usuario final.

7. Configure la copia de actualizaciones en una carpeta para el almacenamiento local:

   a. Seleccione o desactive la casilla **Copiar las actualizaciones a la siguiente carpeta**.

   b. Seleccione el contenido de las actualizaciones que desea que la aplicación copie en la carpeta de almacenamiento local:

   - **Copiar actualizaciones de las bases de datos**. La aplicación descarga solo actualización de bases de datos.
   - **Copiar actualizaciones críticas de módulos de la aplicación**. La aplicación descarga solo actualizaciones críticas del módulo de la aplicación.
   - **Copiar actualizaciones de bases de datos y actualizaciones críticas de módulos de la aplicación**. La aplicación descarga actualización de bases de datos y actualizaciones críticas del módulo de la aplicación.

   c. Especifique la carpeta local o de red a la cual Kaspersky Embedded Systems Security distribuirá las actualizaciones descargadas.

8. Guarde los cambios.

Actualización SMU de la aplicación

Para actualizar la aplicación usando el servicio de actualización de Kaspersky (Seamless Update; SMU), no es necesario ejecutar el instalador, a diferencia de otros métodos de actualización. Kaspersky Embedded Systems Security recibe la nueva versión de la aplicación junto con las bases de datos antivirus del mismo origen.

Una actualización de SMU permite actualizar la aplicación a la última versión en todos los equipos de la organización. Antes de aplicar una actualización de SMU, recomendamos probar la nueva versión de la aplicación en algunos equipos. Para hacerlo, debe actualizar la aplicación en estos equipos manualmente (por ejemplo, de forma local con el Asistente de configuración). No puede seleccionar equipos específicos al realizar una actualización de SMU.

El personal de Kaspersky determina el cronograma de actualizaciones de la aplicación. Para asegurarse de que la nueva versión de la aplicación se ejecute sin problemas, Kaspersky ofrece actualizaciones por etapas. Esto significa que puede obtener la actualización de SMU hasta dos meses después del lanzamiento de una nueva versión.

Puede administrar la actualización de SMU de la aplicación con la tarea *Actualización de bases de datos y módulos de la aplicación*. Para tener la nueva versión de la aplicación incluida en el mismo paquete que las bases de datos antivirus, debe permitir la actualización de los *módulos de la aplicación* en la configuración de la tarea Actualización de bases de datos y módulos de la aplicación.

Pasos de una actualización de SMU de la aplicación

1. **Después de publicar una nueva versión de la aplicación o actualizar un módulo, Kaspersky distribuye la actualización.**

2. **El usuario debe aprobar la actualización de la aplicación.**

   Si el equipo está conectado a Kaspersky Security Center, la actualización estará disponible en Kaspersky Security Center, en la sección **Actualizaciones para bases de datos y módulos de software de Kaspersky**. Para obtener más información sobre la aprobación de actualizaciones, consulte la Ayuda de Kaspersky Security Center.

   Si el equipo no está conectado a Kaspersky Security Center, la actualización está disponible en la Consola de la aplicación. Para aprobar la actualización, vaya a la sección **Actualización → Actualización de aplicación**, seleccione una versión de la aplicación y, si es necesario, acepte los términos y condiciones de los contratos.

3. **Kaspersky Embedded Systems Security ejecuta la tarea Actualización de bases de datos y módulos de la aplicación según una programación.**

Como resultado, Kaspersky Embedded Systems Security actualiza la aplicación en modo "silencioso".

Reversión de actualizaciones de bases de datos de Kaspersky Embedded Systems Security

Antes de que se realicen las actualizaciones de las bases de datos, Kaspersky Embedded Systems Security crea copias de seguridad de las bases de datos anteriormente usadas. Si una 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, puede regresar a las actualizaciones instaladas anteriormente mediante la tarea *Reversión de la última actualización*.

Para ejecutar la tarea Reversión de la última actualización:

1. En el árbol de la Consola de la aplicación, abra la sección **Actualización → Reversión de la última actualización**.

2. En el panel de resultados, haga clic en el vínculo **Inicio**.

Estadísticas de las tareas de actualización

Mientras se ejecuta la tarea Actualización, se muestra la información en tiempo real sobre la cantidad de datos descargados desde que se inició la tarea, así como otras estadísticas de ejecución de la tarea.

Cuando la tarea finaliza o se detiene, la información está disponible en el registro de tareas.

Para ver las estadísticas de la tarea Actualización:

En el árbol de la Consola de la aplicación, abra la sección **Actualización → Actualización de bases de datos y módulos de la aplicación**.

En el panel de resultados, en **Estadísticas**, puede encontrar información sobre la cantidad total de datos obtenidos.

Creación de copias de seguridad de los objetos

En esta sección se proporciona información sobre cómo realizar una copia de seguridad de los objetos maliciosos detectados antes de la desinfección o eliminación.

Creación de copias de seguridad de los objetos. Copia de seguridad

Kaspersky Embedded Systems Security guarda copias cifradas de objetos desinfectados o eliminados en la carpeta Copias de seguridad.

Si el objeto forma parte de un objeto compuesto (por ejemplo, parte de un archivo de almacenamiento), Kaspersky Embedded Systems Security guardará el 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 disponible en el disco duro.

Los archivos se pueden restaurar de la Copia de seguridad a su carpeta original o a una carpeta diferente en el dispositivo protegido. Un archivo se puede restaurar de la Copia de seguridad, por ejemplo, si un archivo infectado contiene información importante. Sin embargo, Kaspersky Embedded Systems Security no puede desinfectarlo sin dañar su integridad y perder la información.

Restaurar archivos de Copia de seguridad puede dar lugar a una infección en el dispositivo protegido.

Ver objetos en Copia de seguridad

Esta sección proporciona información acerca de cómo ver la lista de archivos en Copia de seguridad.

Cómo ver objetos de Copia de seguridad en la Consola de administración de Kaspersky Security Center

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Adicional** → **Depósitos**.
3. Vaya a la carpeta **Copias de seguridad**.
4. La información sobre los objetos colocados en Copia de seguridad se muestra en el panel derecho de la consola.

Cómo ver objetos de Copia de seguridad en Kaspersky Security Center Web Console

1. Abra Web Console.
2. En el árbol de la consola, seleccione **Operaciones** → **Depósitos**.
3. Vaya a la carpeta **Copias de seguridad**.
4. La información sobre los objetos colocados en Copia de seguridad se muestra en el panel derecho de la consola.

Cómo ver objetos de Copia de seguridad en la Consola de la aplicación

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Depósitos** → **Copias de seguridad**.
2. La información sobre los objetos colocados en Copia de seguridad se muestra en el panel derecho de la consola.

Para encontrar el objeto necesario en la lista de Objetos en Copia de seguridad,

ordene o filtre los objetos.

Cómo ordenar archivos en Copia de seguridad

De manera predeterminada, los archivos en Copia de seguridad se ordenan por la fecha de copia de seguridad en orden cronológico inverso. Para buscar el archivo requerido, puede ordenarlos de acuerdo con el contenido de cualquiera de las columnas en el panel de resultados.

Cómo ordenar archivos de Copias de seguridad en la Consola de administración de Kaspersky Security Center

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Adicional** → **Depósitos**.
3. Vaya a la carpeta **Copias de seguridad**.
4. En la lista de archivos, seleccione el encabezado de la columna que desea usar para ordenar los objetos.

Los archivos en Copia de seguridad se ordenarán según el criterio seleccionado.

Cómo ordenar archivos de Copias de seguridad en Kaspersky Security Center Web Console

1. Abra Web Console.
2. En el árbol de la consola, seleccione **Operaciones** → **Depósitos**.
3. Vaya a la carpeta **Copias de seguridad**.
4. En la lista de archivos, seleccione el encabezado de la columna que desea usar para ordenar los objetos.

Los archivos en Copia de seguridad se ordenarán según el criterio seleccionado.

Cómo ordenar archivos de Copias de seguridad en la Consola de la aplicación

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Depósitos** → **Copias de seguridad**.
2. En la lista de archivos, seleccione el encabezado de la columna que desea usar para ordenar los objetos.

Los archivos en Copia de seguridad se ordenarán según el criterio seleccionado.

Filtrado de archivos en Copia de seguridad

Para buscar un archivo en Copias de seguridad, puede filtrar los archivos para que la lista muestre solo los archivos que satisfacen el criterio de filtrado (filtros) que especificó.

Filtrar archivos de Copias de seguridad en la Consola de administración de Kaspersky Security Center

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Adicional** → **Depósitos**.
3. Vaya a la carpeta **Copias de seguridad**.
4. En el panel derecho, haga clic en el vínculo **No se especificó un filtro**.
5. Haga clic en **Ajustar filtro** y, en la ventana **Configuración de filtrado**, seleccione las columnas para el filtrado.
6. Especifique los operadores y valores para las columnas seleccionadas.

7. Se guardarán los filtros creados.
8. Para que vuelvan a aparecer todos los objetos en Copias de seguridad, en la ventana **Configuración de filtrado**, haga clic en **Borrar todo**.

Filtrar archivos de Copias de seguridad en Kaspersky Security Center Web Console

1. Abra Web Console.
2. En el árbol de la consola, seleccione **Operaciones** → **Depósitos**.
3. Vaya a la carpeta **Copias de seguridad**.
4. Haga clic en el ícono del filtro y haga clic en el botón **Agregar** en la pestaña **Filtros**.
5. Seleccione una propiedad de filtrado.
6. Especifique una condición y un valor para la propiedad seleccionada.
7. Haga clic en **Aplicar**.

   Se guarda la configuración de filtro.
8. Para que vuelvan a aparecer todos los objetos en Copias de seguridad, en la pestaña **Filtros**, haga clic en **Borrar todo**.

Cómo filtrar archivos en Copias de seguridad en la Consola de la aplicación

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Depósitos** → **Copias de seguridad**.
2. En la tabla de archivos, seleccione el encabezado de la columna y haga clic en el ícono del filtro en la esquina superior izquierda.
3. Configure el filtro y haga clic en **Aceptar**.

   Se guarda la configuración de filtro.

Restauración de archivos desde copias de seguridad

Kaspersky Embedded Systems Security almacena archivos en la carpeta Copia de seguridad en forma cifrada para proteger el dispositivo protegido contra cualquier posible efecto peligroso.

Se puede restaurar cualquier archivo de la copia de seguridad.

Es posible que se deba restaurar un archivo en los casos siguientes:

- El archivo original 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.
- Usted considera que el archivo no es peligroso para el dispositivo protegido y desea utilizarlo. Si no desea que Kaspersky Embedded Systems Security considere a este archivo infectado durante los análisis subsiguientes, puede excluirlo del procesamiento en la tarea de Protección de archivos en tiempo real y las tareas de Análisis a pedido.

Restaurar archivos de Copia de seguridad puede dar lugar a una infección en el dispositivo protegido.

Al restaurar un archivo, puede seleccionar dónde guardarlo: en su ubicación original (opción predeterminada), en la carpeta utilizada especialmente para colocar los objetos restaurados en el dispositivo protegido o en una carpeta personalizada que se encuentre, bien en el dispositivo protegido en el que esté instalada la Consola de la aplicación.

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.

Restaurar archivos de Copias de seguridad en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Adicional** → **Depósitos**.
2. Vaya a la carpeta **Copias de seguridad**.
3. Realice una de las siguientes acciones:
   - Para restaurar un objeto, seleccione **Restaurar** en el menú contextual del nombre del objeto.
   - 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.
4. El objeto se restaurará en la carpeta original.

Restaurar archivos de Copias de seguridad en Kaspersky Security Center Web Console

1. Abra Web Console.
2. En el árbol de la consola, seleccione **Operaciones** → **Depósitos**.
3. Vaya a la carpeta **Copias de seguridad**.
4. Seleccione objetos de la lista y haga clic en el botón **Restaurar**.
5. El objeto se restaurará en la carpeta original.

Restaurar archivos desde Copias de seguridad en la Consola de la aplicación

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Depósitos** → **Copias de seguridad**.
2. En el panel de resultados del nodo **Copias 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.
3. En la ventana **Restaurar objeto**, especifique la carpeta en la que se guardará el objeto restaurado 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.

4. Realice una de las siguientes acciones:
   - 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 durante la instalación de la aplicación, seleccione **Restaurar a la carpeta de restauración predeterminada**.
   - Para guardar un objeto en una carpeta diferente del dispositivo protegido en el que esté instalada la Consola de la aplicación, seleccione **Restaurar a una carpeta en equipo local** y seleccione la carpeta en cuestión (o especifique la ruta a dicha carpeta).
5. 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).
6. Para aplicar las condiciones de restauración especificadas en los restantes objetos seleccionados, active la casilla de verificación **Aplicar a todos los objetos seleccionados**.
7. Haga clic en **Aceptar**.
8. 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 sustituir el objeto existente con el objeto restaurado.
    - **Cambiar nombre**, para guardar un objeto restaurado con otro nombre. En el campo de entrada, introduzca el nombre de archivo del nuevo objeto restaurado y la ruta completa.
    - **Agregar un sufijo al nombre**, para cambiar el nombre del objeto restaurado al agregar un sufijo a su nombre de archivo. Escriba el sufijo en el campo de entrada.

    b. Si eligió varios objetos para restaurar, seleccione la casilla de verificación **Aplicar a todos los objetos seleccionados** para aplicar la acción seleccionada (**Reemplazar** o **Cambiar nombre**) al resto de los objetos seleccionados. Si seleccionó **Cambiar 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 incluirá la información sobre la operación de restauración.

Si no seleccionó **Aplicar a todos los objetos seleccionados** en la ventana **Restaurar objeto**, la ventana **Restaurar objeto** puede abrirse de nuevo. Utilice esta ventana para especificar la ubicación donde se guardará el objeto seleccionado.

Eliminación de archivos de Copia de seguridad

Eliminar archivos de Copias de seguridad en la Consola de administración de Kaspersky Security Center

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Adicional** → **Depósitos**.
3. Vaya a la carpeta **Copias de seguridad**. En el panel derecho se muestra la lista de objetos de Copias de seguridad.
4. Realice una de las siguientes acciones:
    - Para eliminar un objeto, seleccione **Eliminar** en el menú contextual del objeto.
    - Para eliminar varios objetos, seleccione los objetos que desea eliminar mediante la tecla CTRL o MAYÚS, haga clic con el botón secundario en uno de los objetos seleccionados y seleccione **Eliminar** en el menú contextual.
5. Los objetos seleccionados se eliminan de Copias de seguridad.

Eliminar archivos desde Copias de seguridad en Kaspersky Security Center Web Console

1. Abra Web Console.
2. En el árbol de la consola, seleccione **Operaciones** → **Depósitos**.
3. Vaya a la carpeta **Copias de seguridad**.
4. Seleccione objetos de la lista y haga clic en el botón **Eliminar**.
5. Los objetos seleccionados se eliminan de Copias de seguridad.

Eliminar archivos desde Copias de seguridad en la Consola de la aplicación

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Depósitos** → **Copias de seguridad**.
2. En el panel derecho se muestra la lista de objetos de Copias de seguridad.
3. Realice una de las siguientes acciones:
   - Para eliminar un objeto, seleccione **Eliminar** en el menú contextual del objeto.
   - Para eliminar varios objetos, seleccione los objetos que desea eliminar mediante la tecla CTRL o MAYÚS, haga clic con el botón secundario en uno de los objetos seleccionados y seleccione **Eliminar** en el menú contextual.
4. Los objetos seleccionados se eliminan de Copias de seguridad.

Envío de objetos probablemente infectados a Kaspersky para su análisis

Si el comportamiento de un objeto le da motivos para sospechar que contiene una amenaza y Kaspersky Embedded Systems Security considera que el objeto 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 objeto a Kaspersky para análisis. Los analistas de antivirus de Kaspersky lo analizarán y si detectan una amenaza nueva, la agregarán a un registro que la identificará en las bases de datos. Cuando vuelva a analizar el objeto después de que la base de datos se haya actualizado, es probable que Kaspersky Embedded Systems Security identifique el objeto como infectado y pueda desinfectarlo. No solo podrá conservar el objeto, sino que también evitará un ataque de virus.

Para enviar un objeto para su análisis a los expertos de Kaspersky en la Consola de administración de Kaspersky Security Center

1. Abra la Consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione **Adicional** → **Depósitos**.

3. Vaya a la carpeta **Copia de seguridad**.
4. Realice una de las siguientes acciones:
   - Para enviar un objeto, seleccione **Enviar a Kaspersky** en el menú contextual del nombre del objeto.
   - Para enviar varios objetos, seleccione los objetos que desea enviar mediante la tecla CTRL o MAYÚS, haga clic con el botón secundario en uno de los objetos seleccionados y seleccione **Enviar a Kaspersky** en el menú contextual.
5. Seleccione la carpeta para guardar el objeto en su computadora.
6. Después de esto, se le pedirá que vaya al Kaspersky Threat Intelligence Portal y cargue el objeto guardado para obtener información completa sobre él.

Para enviar un objeto para su análisis a los expertos de Kaspersky en Kaspersky Security Center Web Console

1. Abra Web Console.
2. En el árbol de la consola, seleccione **Operaciones** → **Depósitos**.
3. Vaya a la carpeta **Copia de seguridad**.
4. Seleccione objetos de la lista y haga clic en el botón **Enviar a Kaspersky**.
5. Seleccione la carpeta para guardar el objeto en su computadora.
6. Después de esto, se le pedirá que vaya al Kaspersky Threat Intelligence Portal y cargue el objeto guardado para obtener información completa sobre él.

Kaspersky Security Center Web Console o la Consola de administración de Kaspersky Security Center no se pueden usar para enviar objetos en Copia de seguridad a Kaspersky para analizar si se migraron después de actualizar la versión 3.4 o anteriores a la versión 4.0 o posteriores.

Configuración de Copia de seguridad

Cómo configurar Copia de seguridad en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Adicional** → **Depósitos** y haga clic en **Configuración**.
4. Seleccione la ficha **Copias de seguridad**.

5. Especifique la configuración de Copia de seguridad.

   - Conservar objetos como máximo
   - Limitar el tamaño de Copia de seguridad a
   - Limitar el valor umbral del espacio disponible a

     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.

6. Guarde los cambios.

Cómo configurar Copia de seguridad en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Seleccione **Adicional** → **Depósitos** y haga clic en el botón **Configurar**.
5. Seleccione la ficha **Copias de seguridad**.
6. Especifique la configuración de Copia de seguridad.

   - Conservar objetos como máximo
   - Limitar el tamaño de Copia de seguridad a

     Si el tamaño de los objetos en Copia de seguridad supera el tamaño máximo de Copia de seguridad, Kaspersky Embedded Systems Security le notificará sobre esto y, al mismo tiempo, continuará colocando objetos en Copia de seguridad.
7. Guarde los cambios.

Cómo configurar Copia de seguridad en la Consola de la aplicación

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Depósitos** → **Copias de seguridad**.
2. En el panel de resultados del nodo **Copias de seguridad**, haga clic en **Propiedades**.

3. En la ventana **Propiedades: Copias de seguridad**, especifique la configuración de Copia de seguridad:

- Conservar objetos como máximo
- Limitar el tamaño de Copia de seguridad a
- Limitar el valor umbral del espacio disponible a

> 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.

4. Guarde los cambios.

Estadísticas de Copia de seguridad

Puede visualizar la información sobre el estado actual de la Copia de seguridad, es decir, estadísticas de Copia de seguridad.

Para ver las estadísticas de Copia de seguridad:

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Depósitos** → **Copias de seguridad**.
2. En el panel de resultados del nodo **Copias de seguridad**, haga clic en **Estadísticas**.

Esto abre **Copia de seguridad.Ventana Estadísticas**. La ventana **Copia de seguridad: estadísticas** muestra información sobre el estado actual de Copia de seguridad (consulte la tabla siguiente).

Información sobre el estado actual de la Copia de seguridad

Campo	Descripción
Tamaño actual de Copia de seguridad	Tamaño total de los datos en la carpeta Copia de seguridad; la aplicación calcula el tamaño del archivo en forma cifrada.
Cantidad total de objetos	Cantidad total actual de objetos en Copia de seguridad.

Bloqueo de acceso a los recursos de red. Sesiones en la red bloqueadas

En esta sección se describe cómo bloquear dispositivos remotos y configurar las opciones de la Lista de sesiones en la red bloqueadas.

Lista de sesiones de red bloqueadas

De manera predeterminada, la Lista de sesiones de red bloqueadas está disponible para su uso si alguno de los siguientes componentes está instalado: Protección contra amenazas de red o Detección de comportamiento. Estos componentes descubren intentos remotos de cifrar, abrir o ejecutar objetos en el dispositivo protegido o en las carpetas compartidas de almacenamiento conectado a la red de acuerdo con la lista de sesiones en la red bloqueadas. La información sobre las sesiones en la red bloqueadas de todos los dispositivos protegidos se envía a Kaspersky Security Center. Kaspersky Embedded Systems Security bloquea la sesión actual y, en términos de la sesión actual, provoca que las carpetas compartidas o las carpetas de almacenamiento conectadas a la red no estén disponibles.

La lista de sesiones en la red bloqueadas se completa cuando al menos una de las siguientes tareas se inicia en modo activo (en condiciones específicas):

- Para la tarea *Protección contra amenazas de red*: se detecta la actividad típica de los ataques de red.

  La lista de equipos bloqueados se vacía cada vez que Kaspersky Embedded Systems Security se reinicia o cuando se modifica la configuración de Protección contra amenazas de red.

- Para la tarea *Detección de comportamiento*: se detecta el cifrado malicioso por parte de un dispositivo que accede a los recursos de archivos de la red.

Una vez que se detecta una actividad malintencionada o un intento de cifrado, la tarea envía información sobre la sesión en la red atacante a la lista de sesiones en la red bloqueadas y la aplicación crea un evento de *advertencia* para la sesión actual del host atacante. Se bloqueará cualquier intento de esta sesión de acceder a las carpetas de red compartidas protegidas.

Si el identificador único local (LUID) de un host que inició la sesión en la red atacante se agrega a la lista de sesiones en la red bloqueadas, Kaspersky Embedded Systems Security determina la dirección IP de este host y la agrega a la lista de sesiones en la red bloqueadas en lugar del LUID del host atacante.

De manera predeterminada, Kaspersky Embedded Systems Security elimina las sesiones en la red bloqueadas de la lista 30 minutos después de que se agregaron a la lista. El acceso a los recursos de archivos en red se restaura automáticamente después de que se eliminan las sesiones en la red de la lista de sesiones en la red bloqueadas. Puede especificar el periodo de tiempo después del cual las sesiones de red bloqueadas se desbloquean automáticamente.

Tenga en cuenta que cuando restringe el acceso a la administración de almacenamiento de cualquier cuenta de usuario, la lista de sesiones en la red seguirá estando disponible. La configuración de las sesiones en la red bloqueadas no se puede cambiar a menos que la cuenta de usuario seleccionada tenga **Modificar permisos** para administrar Kaspersky Embedded Systems Security.

Administrar la lista de sesiones de red bloqueadas

Para agregar sesiones en la red que muestren cualquier actividad maliciosa o de cifrado a la lista de sesiones en la red bloqueadas y bloquear el acceso a los recursos de archivos en red para esas sesiones, se debe habilitar al menos uno de los siguientes componentes:

- Protección contra amenazas de red
- Detección de comportamiento

Habilitar el bloqueo de hosts no confiables en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Control de actividad de red → Configuración de Protección contra amenazas de red** y haga clic en **Configuración**.
4. En la ventana que se abre, seleccione la casilla **Protección contra amenazas de red**.
5. En la pestaña **General**, habilite el modo **Bloquear**.
6. Seleccione la casilla de verificación **Bloquear dispositivos atacantes durante** y especifique la duración del bloqueo.
7. Guarde los cambios.

Para configurar el bloqueo de sesiones de red no confiables para el componente de Detección de comportamiento en las propiedades de la directiva:

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de la directiva, seleccione **Protección del equipo en tiempo real →Detección de comportamiento** y haga clic en **Configuración**.
4. En la ventana que se abre, seleccione la casilla **Detección de comportamiento**.
5. Vaya a la pestaña **Protección de carpetas compartidas** y seleccione la casilla **Proteger carpetas compartidas**.
6. Seleccione **Bloquear la conexión durante** y especifique la duración del bloqueo.
7. Si es necesario, especifique los alcances y las exclusiones de la protección por dirección IP y máscara.
8. Guarde los cambios.

Habilitar el bloqueo de hosts no confiables en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Control de actividad de red** → **Protección contra amenazas de red** y haga clic en el botón **Configurar**.
5. En la ventana que se abre, seleccione la casilla **Habilitar protección contra amenazas de red**.
6. Habilite el modo **Bloquear**.
7. Seleccione la casilla de verificación **Bloquear dispositivos atacantes durante** y especifique la duración del bloqueo.
8. Si es necesario, especifique exclusiones por dirección IP.
9. Guarde los cambios.

Para configurar el bloqueo de sesiones de red no confiables para el componente de Detección de comportamiento:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Protección del equipo en tiempo real** → **Detección de comportamiento** y haga clic en el botón **Configurar**.
5. En la ventana que se abre, seleccione la casilla **Habilitar Detección de comportamiento**.
6. Vaya a la pestaña **Protección de carpetas compartidas** y seleccione la casilla **Habilitar protección de carpetas compartidas contra el cifrado externo**.
7. Seleccione **Bloquear conexión** y especifique la duración del bloqueo en la sección **Al detectar intentos de cifrado externo en las carpetas compartidas.**
8. Si es necesario, especifique los alcances y las exclusiones de la protección por dirección IP y máscara.
9. Guarde los cambios.

Habilitar el bloqueo de hosts no confiables en la Consola de la aplicación

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Protección del equipo en tiempo real** → **Protección contra amenazas de red**.
2. En el panel de resultados del nodo **Protección contra amenazas de red**, haga clic en **Propiedades**.

   Se abre la ventana **Propiedades: Protección contra amenazas de red**.
3. En la ventana que se abre, seleccione la casilla **Protección contra amenazas de red**.
4. En la pestaña **General**, habilite el modo **Bloquear**.
5. Seleccione la casilla de verificación **Bloquear dispositivos atacantes durante** y especifique la duración del bloqueo.
6. Guarde los cambios.

Para configurar el bloqueo de sesiones de red no confiables para el componente de Detección de comportamiento:

1. En el árbol de la Consola de Kaspersky Embedded Systems Security, seleccione **Protección del equipo en tiempo real** → **Anticifrador**.
2. En el panel de resultados del nodo **Detección de comportamiento**, haga clic en **Propiedades**.
3. En la ventana que se abre, seleccione la casilla **Detección de comportamiento**.
4. Vaya a la pestaña **Protección de carpetas compartidas** y seleccione la casilla **Proteger carpetas compartidas**.
5. Seleccione **Bloquear la conexión durante** y especifique la duración del bloqueo.
6. Si es necesario, especifique los alcances y las exclusiones de la protección por dirección IP y máscara.
7. Guarde los cambios.

Configurar la lista de sesiones en la red bloqueadas en la Consola de la aplicación

1. En el árbol de la Consola de la aplicación, expanda el nodo **Depósitos**.
2. Seleccione el nodo secundario **Sesiones de red bloqueadas**.
3. En el panel de resultados, haga clic en el botón **Propiedades**.
4. En la ventana que se abre, seleccione la casilla **Bloquear dispositivos atacantes durante** y especifique la duración del bloqueo.
5. Para restaurar el acceso a todas las sesiones de red bloqueadas, haga clic en **Desbloquear todas** en la parte superior de la ventana.

   Se eliminarán y desbloquearán todas las sesiones en la red.

6. Para eliminar las sesiones de red de la lista de sesiones de red bloqueadas, en la lista del panel de resultados, seleccione una o más sesiones y haga clic en **Desbloquear seleccionada** en la parte superior de la ventana.

   Las sesiones en la red seleccionadas se desbloquean.

Registro de eventos. Registros de Kaspersky Embedded Systems Security

Esta sección proporciona información sobre cómo trabajar con los registros de Kaspersky Embedded Systems Security.

Modos de registrar eventos de Kaspersky Embedded Systems Security

Los eventos de Kaspersky Embedded Systems Security se dividen en dos grupos:

- Eventos relacionados con la operación de los componentes de la aplicación, 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 funcionamiento de los componentes de la aplicación**. Los registros contienen información sobre eventos que ocurrieron durante el funcionamiento de los componentes de la aplicación.
- **Registro de auditoría del sistema**. El registro de auditoría del sistema contiene información sobre los eventos relacionados con la administración de Kaspersky Embedded Systems Security. Y también contiene información sobre eventos asociados con la violación de la seguridad o los intentos de violación de la seguridad en el dispositivo protegido.
- **Registro de eventos**. El registro de eventos contiene información sobre los eventos requeridos para diagnosticar fallas en el funcionamiento de Kaspersky Embedded Systems Security. El registro de eventos está disponible en el Visor de eventos de Microsoft Windows.

Los archivos que se pueden descargar mediante los siguientes vínculos contienen tablas con las listas completas de los eventos de Kaspersky Embedded Systems Security de las siguientes categorías:

- Eventos que Kaspersky Embedded Systems Security escribe en el registro de eventos.

   DESCARGAR WEL-EVENTS.ZIP

- Eventos que Kaspersky Embedded Systems Security envía al Servidor de administración.

   DESCARGAR KSC-EVENTS.ZIP

Configuración de los parámetros del registro

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 del registro de tareas y el archivo de registro de auditoría del sistema.
- Umbrales de generación de eventos para *Las bases de datos están desactualizadas*, *Las bases de datos están obsoletas* 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.

Cómo configurar registros en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de propiedades de la directiva, seleccione **Registros y notificaciones**.
4. En la sección **Registros de tareas**, haga clic en **Configuración**.

   Se abre la ventana **Notificaciones**.
5. En esta ventana, seleccione el registro que desea configurar y especifique la configuración para eventos individuales:
   - Dónde se guardan los eventos: informe local o registro de eventos de Windows.
   - Notificaciones de eventos: notificar por correo electrónico, notificar mediante el servicio de terminales o notificar mediante un archivo ejecutable.
   - Si desea enviar el evento a un servidor SIEM o a Kaspersky Security Center.
6. Configurar los umbrales de generación de eventos haciendo clic en **Configuración de umbrales de generación de eventos**.
7. En la ventana que se abre, especifique el número de días después de los cuales se deben registrar los siguientes eventos: *Las bases de datos están desactualizadas*, *Las bases de datos están obsoletas* y *Hace mucho tiempo que no se realiza un análisis de áreas críticas*.
8. Configurar la conexión del servidor SIEM haciendo clic en **Configuración de notificaciones de SIEM**.

9. Configurar las notificaciones de correo electrónico haciendo clic en **Configuración de notificaciones por correo**.
10. Guarde los cambios.

Cómo configurar registros en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Registros y notificaciones** → **Registros de tareas** y haga clic en el botón **Configurar**.
5. En la ventana que se abre, en la pestaña **Notificaciones** , seleccione el registro que desea configurar y especifique la configuración para eventos individuales:
   - Dónde se guardan los eventos: informe local o registro de eventos de Windows.
   - Notificaciones de eventos: notificar por correo electrónico, notificar mediante el servicio de terminales o notificar mediante un archivo ejecutable.
   - Si desea enviar el evento a un servidor SIEM o a Kaspersky Security Center.
6. Configurar las notificaciones de correo electrónico en la pestaña **Configuración de notificaciones por correo**.
7. Configurar la conexión del servidor SIEM en la pestaña **Integración con SIEM**.
8. Guarde los cambios.

Cómo configurar registros en la Consola de la aplicación:

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 **Notificaciones**.
3. En esta ventana, seleccione el registro que desea configurar y especifique la configuración para eventos individuales:
   - Dónde se guardan los eventos: informe local o registro de eventos de Windows.
   - Notificaciones de eventos: notificar por correo electrónico, notificar mediante el servicio de terminales o notificar mediante un archivo ejecutable.
   - Si desea enviar el evento a un servidor SIEM o a Kaspersky Security Center.

4. Configurar los umbrales de generación de eventos haciendo clic en **Configuración de umbrales de generación de eventos**.

5. En la ventana que se abre, especifique el número de días después de los cuales se deben registrar los siguientes eventos: *Las bases de datos están desactualizadas (días)*, *Las bases de datos están extremadamente desactualizadas (días)* y *Hace mucho tiempo que no se realiza un análisis de áreas críticas (días)*.

6. Configurar la conexión del servidor SIEM haciendo clic en **Configuración de notificaciones de SIEM**.

7. Configurar las notificaciones de correo electrónico haciendo clic en **Configuración de notificaciones por correo**.

8. Guarde los cambios.

Ordenar eventos en el registro

De manera predeterminada, los eventos en el registro se muestran en orden cronológico inverso.

Para ordenar eventos en el registro:

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Registros y notificaciones**.

2. Seleccione el registro requerido.

3. En el panel de resultados, seleccione el encabezado de la columna que desee usar para ordenar los eventos en la lista.

Los resultados ordenados se guardarán hasta que visualice de nuevo el registro.

Filtrado de eventos en el registro

Puede configurar el registro para que muestre solo los registros de eventos que cumplen con las condiciones de filtrado (filtros) que especificó.

Para filtrar eventos en el registro:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Registros y notificaciones**.

2. Seleccione el registro para el que desea configurar un filtro y, en el panel de resultados, haga clic en **Filtrar**.

   Se abre la ventana **Configuración de filtro**.

3. Para agregar un filtro, siga estos pasos:

   a. En la lista **Nombre del campo**, seleccione la columna que desee usar para filtrar 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 **Valor del campo**, seleccione un valor para el filtro.

d. Haga clic en **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:

   - 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**.

5. Haga clic en el botón **Aceptar** para guardar las condiciones de filtrado de los eventos de registro.

La lista de eventos del registro muestra solo los eventos que cumplen las condiciones de filtrado. Los resultados filtrados se guardarán hasta que visualice de nuevo el registro.

Para deshabilitar el filtro:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Registros y notificaciones**.
2. Seleccione el registro para el que desea eliminar un filtro y haga clic en **Eliminar filtro**.

A continuación, el registro mostrará todos los eventos.

Eliminar eventos del registro

De manera predeterminada, Kaspersky Embedded Systems Security conserva los registros durante 30 días. Se puede cambiar el periodo de almacenamiento para los registros en un registro.

Para eliminar eventos del registro:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Registros y notificaciones**.
2. Seleccione el registro del que desea eliminar eventos y, en el panel de resultados, haga clic en **Borrar**.
3. Confirme la operación de borrado.

Se borra el registro.

Exportar información desde el registro

Puede exportar los datos de un registro a un archivo con formato TXT o CSV.

Para exportar eventos de registros:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Registros y notificaciones**.
2. Seleccione un registro y, en el panel de resultados, haga clic en el botón **Exportar registros**.

   Se abre la ventana **Guardar como**.

3. Especifique el nombre, la ubicación, el tipo del archivo al que desea exportar los datos del registro.

4. Haga clic en **Guardar**.

La información de los registros se guarda en el archivo especificado.

Registro de auditoría del sistema

Kaspersky Embedded Systems Security realiza una auditoría del sistema de los eventos relacionados con la administración de Kaspersky Embedded Systems Security. La aplicación registra información sobre 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 las tareas Análisis a pedido. La aplicación también registra información sobre eventos asociados con la violación de la seguridad o los intentos de violación de la seguridad en el dispositivo protegido. Los registros de todos esos eventos se muestran en el panel de resultados cuando se selecciona el nodo **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 30 días. Se puede cambiar el periodo de almacenamiento para los registros en un registro.

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.

Registros de tareas

La información sobre el funcionamiento de los componentes y las tareas de Kaspersky Embedded Systems Security se muestra en la Consola de la aplicación en el panel de resultados cuando selecciona un nodo con el nombre del componente o la tarea en la sección **Registros y notificaciones**.

De manera predeterminada, Kaspersky Embedded Systems Security mantiene registros de componentes y tareas durante 30 días. Para las tareas, desde el momento de su finalización. Se puede cambiar el periodo de almacenamiento para los eventos del registro de componentes y tareas.

Puede especificar una carpeta diferente de la predeterminada para que Kaspersky Embedded Systems Security almacene los archivos que contienen los registros de componentes y tareas. También puede seleccionar los eventos que Kaspersky Embedded Systems Security asentará en los registros de componentes y tareas.

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 tareas, puede ver información detallada sobre todos los eventos que han ocurrido en las tareas desde que iniciaron, 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 una tarea y, en el panel de resultados, seleccione la pestaña **Estadísticas**.

Ver el 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 que son necesarios para diagnosticar las 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 informativo es el más detallado y registra todos los eventos. El Nivel Crítico es el menos detallado y solo registra los eventos críticos.

Para consultar el registro del evento de Kaspersky Embedded Systems Security:

1. Haga clic en el botón **Iniciar**, ingrese el comando `mmc` en la barra de búsqueda y presione la tecla **Enter**.

   Se abre 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 dispositivo protegido 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 la Consola de administración de Microsoft, 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.

Acerca de la integración de SIEM

Para reducir la carga en dispositivos de rendimiento reducido y reducir el riesgo de la degradación del sistema como consecuencia del aumento en los tamaños 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). Almacena y analiza los eventos recibidos y realiza otras acciones de administración de registros.

Puede usar la integración de SIEM en dos modos:

- Duplicar eventos en el servidor syslog: en este modo, todos los eventos de rendimiento de la tarea cuya publicación se establece en la configuración de registros, así como todos los eventos de auditoría del sistema, continúan almacenándose en el dispositivo protegido hasta después de que se envían al servidor SIEM.

  Recomendamos utilizar este modo para reducir todo lo posible la carga en el dispositivo protegido.

- Eliminar copias locales de eventos: en este modo, todos los eventos que se registran durante el funcionamiento de la aplicación y se publican en el servidor SIEM se eliminan del dispositivo protegido.

  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 el servidor SIEM. La aplicación admite la conversión al formato de datos estructurado y al formato JSON.

Recomendamos seleccionar el formato de eventos basados en la configuración del servidor SIEM utilizado.

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 establecer las configuraciones correspondientes.

Puede reducir el riesgo de que los eventos no se envíen al servidor SIEM si configura conexiones a varios servidores SIEM.

Kaspersky Embedded Systems Security se conecta al primer servidor de SIEM de la lista. Si un intento de conexión falla, Kaspersky Embedded Systems Security intentará conectarse a otros servidores de la lista, uno por uno.

Kaspersky Embedded Systems Security también utiliza eventos de auditoría del sistema para notificarle sobre intentos fallidos de conexión al servidor SIEM y sobre errores al enviar eventos al servidor SIEM.

Cómo configurar la integración con SIEM en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. Seleccione la sección **Registros y notificaciones**.
4. En el bloque **Integración con SIEM**, haga clic en el botón **Configuración**.

   Se abre la ventana **Integración con SIEM**.
5. En el bloque **Configuración de la integración**, seleccione la casilla **Habilitar la transmisión de eventos de seguridad a un servidor SIEM**.

6. Configure la conexión del servidor SIEM en el bloque **Configuración de conexión con los servidores SIEM**:

    a. Haga clic en **Agregar**.

    b. En la ventana **Agregar servidor** que se abre, ingrese la dirección del servidor de SIEM (IPv4, DNS), el puerto y el protocolo de conexión.

    c. Haga clic en **Configuración de seguridad de conexiones TCP**.

    d. En la ventana **Configuración de seguridad de conexiones TCP** que se abre, configure la conexión del servidor SIEM (consulte la tabla a continuación).

7. Si es necesario, seleccione la casilla **Eliminar copias locales de eventos que se enviaron a un servidor syslog remoto** en el bloque **Configuración de la transmisión de eventos a un servidor de SIEM**. Si se selecciona la casilla, la aplicación elimina las copias locales de eventos después de que se han publicado correctamente en el servidor SIEM. Este modo se recomienda en dispositivos de rendimiento reducido. Si se desactiva la casilla, la aplicación solo envía eventos al servidor SIEM. Las copias de los de registros continúan almacenándose a nivel local. De forma predeterminada, la casilla no está activada.

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

8. En el bloque **Formato de eventos**, seleccione el formato al cual desee convertir los eventos de la aplicación de modo que se puedan enviar al servidor SIEM. De forma predeterminada, la opción **Convertir eventos a STRUCTURED-DATA** está seleccionada. Recomendamos seleccionar el formato de eventos basados en la configuración del servidor SIEM utilizado.

9. Cierre el candado para aplicar la directiva en los equipos.

10. Haga clic en **Aceptar** para guardar los cambios.

Cómo configurar la integración con SIEM en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.

2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

    Se abre la ventana de propiedades de la directiva.

3. Seleccione la ficha **Configuración de la aplicación**.

4. Seleccione la sección **Registros y notificaciones**.

5. En el bloque **Integración con SIEM**, haga clic en el botón **Configurar**.

    Se abre la ventana **Integración con SIEM**.

6. Seleccione la casilla de verificación **Habilitar la transmisión de eventos de seguridad a un servidor SIEM**.

7. Configure la conexión del servidor SIEM en el bloque **Configuración de conexión con los servidores SIEM**:

   a. Haga clic en **Agregar**.

   b. En la ventana **Servidor de SIEM** que se abre, ingrese la dirección del servidor de SIEM (IPv4, DNS), el puerto y el protocolo de conexión.

   c. En el bloque **Protección de la conexión**, haga clic en el vínculo **Configuración de conexión con los servidores SIEM**.

   d. En la ventana **Configuración de conexión con los servidores SIEM** que se abre, configure la conexión del servidor SIEM (consulte la tabla a continuación).

   e. En el bloque **Formato de eventos**, seleccione el formato al cual desee convertir los eventos de la aplicación de modo que se puedan enviar al servidor SIEM. De forma predeterminada, la opción **Convertir eventos a STRUCTURED-DATA** está seleccionada. Recomendamos seleccionar el formato de eventos basados en la configuración del servidor SIEM utilizado.

   f. Si es necesario, seleccione la casilla **Eliminar copias locales de eventos que se enviaron a un servidor syslog remoto** en el bloque **Configuración de conexión**. Si se selecciona la casilla, la aplicación elimina las copias locales de eventos después de que se han publicado correctamente en el servidor SIEM. Este modo se recomienda en dispositivos de rendimiento reducido. Si se desactiva la casilla, la aplicación solo envía eventos al servidor SIEM. Las copias de los de registros continúan almacenándose a nivel local. De forma predeterminada, la casilla no está activada.

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

8. Cierre el candado para aplicar la directiva en los equipos.

9. Haga clic en **Aceptar** para guardar los cambios.

Cómo configurar la integración con SIEM en la Consola de la aplicación

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Registros y notificaciones**.

2. Seleccione **Integración con SIEM**.

   Se abre la ventana **Integración con SIEM**.

3. En el bloque **Configuración de la integración**, seleccione la casilla **Habilitar la transmisión de eventos de seguridad a un servidor SIEM**.

4. Configure la conexión del servidor SIEM en el bloque **Configuración de conexión con los servidores SIEM**:

   a. Haga clic en **Agregar**.

   b. En la ventana **Agregar servidor** que se abre, ingrese la dirección del servidor de SIEM (IPv4, DNS), el puerto y el protocolo de conexión.

   c. Haga clic en **Configuración de seguridad de conexiones TCP**.

   d. En la ventana **Configuración de seguridad de conexiones TCP** que se abre, configure la conexión del servidor SIEM (consulte la tabla a continuación).

5. Si es necesario, seleccione la casilla **Eliminar copias locales de eventos que se enviaron a un servidor syslog remoto** en el bloque **Configuración de la transmisión de eventos a un servidor de SIEM**. Si se selecciona la casilla, la aplicación elimina las copias locales de eventos después de que se han publicado correctamente en el servidor SIEM. Este modo se recomienda en dispositivos de rendimiento reducido. Si se desactiva la casilla, la aplicación solo envía eventos al servidor SIEM. Las copias de los de registros continúan almacenándose a nivel local. De forma predeterminada, la casilla no está activada.

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

6. En el bloque **Formato de eventos**, seleccione el formato al cual desee convertir los eventos de la aplicación de modo que se puedan enviar al servidor SIEM. De forma predeterminada, la opción **Convertir eventos a STRUCTURED-DATA** está seleccionada. Recomendamos seleccionar el formato de eventos basados en la configuración del servidor SIEM utilizado.

7. Haga clic en **Aceptar** para guardar los cambios.

Configuración de conexión del servidor SIEM

Parámetro	Descripción
Tiempo de espera (s)	Tiempo de espera máximo de respuesta del servidor de SIEM. Cuando se agota el tiempo de espera, Kaspersky Embedded Systems Security intenta conectarse a un servidor de SIEM diferente.
Certificado TLS del servidor	Certificado TLS para establecer una conexión de confianza con el servidor de SIEM. Puede obtener un certificado TLS desde la interfaz de administración SIEM.
Usar autenticación bidireccional	Autenticación bidireccional al establecer una conexión segura entre Kaspersky Embedded Systems Security y SIEM. Para usar la autenticación bidireccional, debe habilitarla en la configuración de SIEM y, a continuación, obtener un criptocontenedor y establecer una contraseña para protegerlo. Un criptocontenedor es un archivo de almacenamiento PFX con un certificado y una clave privada. Después de establecer la configuración de SIEM, también debe habilitar la casilla de verificación de la autenticación bidireccional en la configuración de Kaspersky Embedded Systems Security y cargar un criptocontenedor protegido con contraseña. El contenedor criptográfico debe tener protección con contraseña. No es posible agregar un contenedor criptográfico con una contraseña en blanco.

Métodos de notificación de administrador y usuario

Puede configurar la aplicación para notificar al administrador y a los usuarios que acceden al dispositivo acerca de lo siguientes eventos en el funcionamiento de Kaspersky Embedded Systems Security y el estado de la protección antivirus en el dispositivo.

- El administrador puede recibir información sobre eventos de tipos seleccionados.
- Los usuarios de LAN que acceden a un dispositivo y los usuarios de dispositivos terminales pueden recibir información sobre eventos del tipo *Objeto detectado* en la tarea de Protección de archivos en tiempo real.

Las notificaciones para administradores y usuarios se pueden activar mediante diversos métodos:

- Herramientas de servicio de terminales.

  Se puede aplicar este método para notificar a los usuarios de dispositivos protegidos terminales si el dispositivo protegido se utiliza como terminal.

- Ejecución de un archivo ejecutable.

  Este método ejecuta un archivo ejecutable que se almacena en la unidad local del dispositivo protegido cuando ocurre un evento.

- Envío por correo electrónico.

  Este método utiliza el correo electrónico para transmitir los mensajes.

Puede crear el texto de un mensaje para los tipos de eventos individuales. Puede incluir un campo de información para describir un evento. De manera predeterminada, la aplicación utiliza un mensaje predeterminado 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.

Cómo configurar las notificaciones de eventos en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de propiedades de la directiva, seleccione **Registros y notificaciones**.
4. En la sección **Registros de tareas**, haga clic en **Configuración**.

   Se abre la ventana **Notificaciones**.
5. Seleccione el evento para el que desea seleccionar un método de notificación y haga clic en **Configuración de notificaciones**.

   Se abre la ventana **Configuración de notificaciones**.
6. Para recibir una notificación por correo electrónico, en la pestaña **Correo electrónico**, puede agregar el texto del mensaje de notificación del evento.

   Para agregar campos con información sobre un evento, haga clic en el botón **Variable** y seleccione los campos relevantes de la lista desplegable. En la tabla de esta sección se describen campos con información sobre los eventos.

   Para restaurar el texto del mensaje del evento predeterminado, haga clic en el botón **Predeterminado**.
7. Para recibir una notificación mediante un archivo ejecutable, en la pestaña **Archivo ejecutable**, seleccione un archivo ejecutable en la unidad local del dispositivo protegido (o ingrese la ruta completa a dicho archivo). El archivo se ejecutará en el dispositivo protegido cuando ocurra el evento. 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.
8. Para recibir una notificación mediante el servicio de terminales, en la pestaña **Servicio de terminales**, puede agregar el texto del mensaje de notificación del evento.

Para agregar campos con información sobre un evento, haga clic en el botón **Variable** y seleccione los campos relevantes de la lista desplegable. En la tabla de esta sección se describen campos con información sobre los eventos.

Para restaurar el texto del mensaje del evento predeterminado, haga clic en el botón **Predeterminado**.

9. Guarde los cambios.

Cómo configurar las notificaciones de evento en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Registros y notificaciones** → **Registros de tareas** y haga clic en el botón **Configurar**.
5. En la ventana que se abre, haga clic en el evento para el que desea seleccionar un método de notificación.

   Se abre la ventana **Configuración de notificaciones**.
6. Para recibir una notificación por correo electrónico, en la sección **Notificar a los usuarios**, seleccione la casilla **Por correo electrónico** y agregue el texto del mensaje de notificación del evento.

   Para agregar campos con información sobre un evento, haga clic en el botón **Agregar variable** y seleccione los elementos relevantes de la lista. En la tabla de esta sección se describen campos con información sobre los eventos.

   Para restaurar el texto del mensaje del evento predeterminado, haga clic en el botón **Restablecer**.
7. Para recibir una notificación mediante un archivo ejecutable, en la sección **Notificar a los administradores**, seleccione la casilla **Mediante un archivo ejecutable** e ingrese la ruta completa a un archivo en un disco local del dispositivo protegido. El archivo se ejecutará en el dispositivo protegido cuando ocurra el evento. 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.
8. Para recibir una notificación mediante el servicio de terminales, en la sección **Notificar a los administradores**, seleccione la casilla **Mediante el servicio de terminales** y agregue el texto del mensaje de notificación del evento.

   Para agregar campos con información sobre un evento, haga clic en el botón **Agregar variable** y seleccione los elementos relevantes de la lista. En la tabla de esta sección se describen campos con información sobre los eventos.

   Para restaurar el texto del mensaje del evento predeterminado, haga clic en el botón **Restablecer**.
9. Guarde los cambios.

Cómo configurar notificaciones de eventos en la Consola de la aplicación

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 **Notificaciones**.
3. Seleccione el evento para el que desea seleccionar un método de notificación y haga clic en **Configuración de notificaciones**.

   Se abre la ventana **Configuración de notificaciones**.
4. Para recibir una notificación por correo electrónico, en la pestaña **Correo electrónico**, puede agregar el texto del mensaje de notificación del evento.

   Para agregar campos con información sobre un evento, haga clic en el botón **Variable** y seleccione los campos relevantes de la lista desplegable. En la tabla de esta sección se describen campos con información sobre los eventos.

   Para restaurar el texto del mensaje del evento predeterminado, haga clic en el botón **Predeterminado**.
5. Para recibir una notificación mediante un archivo ejecutable, en la pestaña **Archivo ejecutable**, seleccione un archivo ejecutable en la unidad local del dispositivo protegido (o ingrese la ruta completa a dicho archivo). El archivo se ejecutará en el dispositivo protegido cuando ocurra el evento. 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.
6. Para recibir una notificación mediante el servicio de terminales, en la pestaña **Servicio de terminales**, puede agregar el texto del mensaje de notificación del evento.

   Para agregar campos con información sobre un evento, haga clic en el botón **Variable** y seleccione los campos relevantes de la lista desplegable. En la tabla de esta sección se describen campos con información sobre los eventos.

   Para restaurar el texto del mensaje del evento predeterminado, haga clic en el botón **Predeterminado**.
7. Guarde los cambios.

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. Cuando se detecta un objeto, este nombre se incluye en el nombre completo otorgado por Kaspersky Embedded Systems Security al objeto detectado. Puede ver el nombre completo de un objeto detectado en el registro de tareas.
%VIRUS_TYPE%	El tipo de objeto detectado según la clasificación de Kaspersky, como "virus" o "troyano". Esta cadena se incluye en el nombre completo que se muestra para el objeto detectado cuando Kaspersky Embedded Systems Security encuentra un objeto infectado o probablemente infectado. Puede ver el nombre completo de un objeto detectado en el registro de tareas.
%USER_COMPUTER%	En las tareas de Protección de archivos en tiempo real y Protección de almacenamiento de red RPC, el nombre del dispositivo protegido del usuario que accedió al objeto en el dispositivo.

Variable	Descripción
%USER_NAME%	En las tareas de Protección de archivos en tiempo real y Protección de almacenamiento de red RPC, el nombre del usuario que accedió al objeto en el dispositivo.
%FROM_COMPUTER%	Nombre del dispositivo 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 (solo para evento de "Error interno de tarea").
%TASK_NAME%	Nombre de la tarea (solo para eventos relacionados con el rendimiento de la tarea).
%PROTOCOL%	El protocolo que se está utilizando.
%MESSAGE%	Texto del mensaje.
%DEVICE_INSTANCEPATH%	Ruta a la instancia del dispositivo.
%DEVICE_VID%	ID del proveedor del dispositivo.
%DEVICE_PID%	Tipo de controlador.
%DEVICE_SERIALNUMBER%	Número de serie del dispositivo.

Configuración de notificaciones de correo electrónico

Cómo configurar las notificaciones de correo electrónico en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la ventana de propiedades de la directiva, seleccione **Registros y notificaciones**.
4. En la sección **Registros de tareas**, haga clic en **Configuración**.

   Se abre la ventana **Notificaciones**.
5. Haga clic en **Configuración de notificaciones por correo**.
6. En la ventana que se abre, seleccione la casilla **Enviar notificaciones de eventos**.
7. En **Enviar notificaciones en nombre de**, especifique la información del remitente: dirección del remitente, servidor SMTP, puerto del servidor SMTP, nombre de usuario y contraseña.
8. En **Destinatario de la notificación**, especifique la dirección de correo electrónico del destinatario.
9. Especifique el modo de envío: **Si sucede el evento** o **Mediante programación (programación no especificada)**. Para configurar la programación, haga clic en **Modificar**.
10. Guarde los cambios.

Cómo configurar las notificaciones de correo electrónico en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Vaya a **Registros y notificaciones** → **Registros de tareas** y haga clic en el botón **Configurar**.
5. En la ventana que se abre, seleccione la pestaña **Configuración de notificaciones por correo**.
6. Seleccione la casilla de verificación **Enviar notificaciones de eventos**.
7. Especifique la información del remitente: dirección del remitente, servidor SMTP, puerto del servidor SMTP, nombre de usuario y contraseña.
8. Especifique la dirección de correo electrónico del destinatario.
9. Especifique el modo de envío: **Si ocurren eventos** o **Mediante programación**. Si corresponde, configure la programación.
10. Guarde los cambios.

Cómo configurar las notificaciones de correo electrónico en la Consola de la aplicación

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 **Notificaciones**.
3. Haga clic en **Configuración de notificaciones por correo**.
4. En la ventana que se abre, seleccione la casilla **Enviar notificaciones de eventos**.
5. En **Enviar notificaciones en nombre de**, especifique la información del remitente: dirección del remitente, servidor SMTP, puerto del servidor SMTP, nombre de usuario y contraseña.
6. En **Destinatario de la notificación**, especifique la dirección de correo electrónico del destinatario.
7. Especifique el modo de envío: **Si sucede el evento** o **Mediante programación (programación no especificada)**. Para configurar la programación, haga clic en **Modificar**.
8. Guarde los cambios.

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.

Cómo configurar la integración con el Servidor de administración en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. En la sección **Registros y notificaciones**, haga clic en el botón **Configuración** de la subsección **Interacción con Servidor de administración**.
4. En la ventana que se abre, elija los tipos de objetos sobre los cuales Kaspersky Embedded Systems Security enviará información al Servidor de administración de Kaspersky Security Center:
   - **Acerca de los archivos almacenados en Copias de seguridad**
   - **Acerca de los archivos no procesados**
   - **Acerca de los dispositivos instalados**
   - **Acerca de la cadena de desarrollo de la amenaza**
5. Guarde los cambios.

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

Cómo configurar la interacción con el Servidor de administración en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. En la sección **Registros y notificaciones**, haga clic en el botón **Configurar** de la subsección **Interacción con Servidor de administración**.

5. En la ventana que se abre, elija los tipos de objetos sobre los cuales Kaspersky Embedded Systems Security enviará información al Servidor de administración de Kaspersky Security Center:

   - **Archivos guardados en Copia de seguridad**
   - **Acerca de los archivos no procesados**
   - **Sesiones de red bloqueadas**
   - **Dispositivos y redes Wi-Fi**

6. Guarde los cambios.

Managed Detection and Response

Kaspersky Embedded Systems Security admite la integración con la solución Managed Detection and Response.

Kaspersky Managed Detection and Response (también conocido como MDR) brinda protección las 24 horas del día contra el creciente volumen de amenazas que eluden las barreras de seguridad automatizadas a las organizaciones que luchan por encontrar el conocimiento y el personal adecuados, o que tienen recursos internos limitados. A diferencia de ofertas similares en el mercado, este servicio aprovecha un historial probado de investigación de ataques dirigidos eficaz para garantizar una defensa continua incluso contra las amenazas más complejas. El servicio permite mejorar la resistencia corporativa a las ciberamenazas, al tiempo que libera los recursos existentes para centrar su atención en otras tareas.

MDR usa datos de telemetría recibidos de puntos de conexión y aprendizaje automático. MDR envía los datos de los incidentes a los expertos de Kaspersky. A continuación, los expertos pueden procesar el incidente y, por ejemplo, agregar una nueva entrada a las bases de datos antivirus. Alternativamente, los expertos pueden emitir recomendaciones sobre el procesamiento del incidente y, por ejemplo, sugerir que se aísle el equipo de la red. Para obtener más detalles sobre el funcionamiento de la solución, consulte la Ayuda de Kaspersky Managed Detection and Response.

Configuración de integración de MDR

Kaspersky Managed Detection and Response requiere habilitar el modo extendido del componente Kaspersky Security Network. De lo contrario, Kaspersky Managed Detection and Response no recibirá los datos de telemetría necesarios para su correcto funcionamiento.

Para que Kaspersky Managed Detection and Response funcione con el Servidor de administración a través de Kaspersky Security Center Web Console, también debe establecer una nueva conexión segura, una *conexión en segundo plano*. Kaspersky Managed Detection and Response le solicita que establezca una conexión en segundo plano cuando despliega la solución. Asegúrese de que la conexión en segundo plano esté establecida.

Establecer una conexión en segundo plano en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Configuración** → **Integración**.
2. Vaya a la sección **Integración**.
3. Active el interruptor de **Conexión en segundo plano para la integración Habilitada**.
4. Guarde los cambios.

El proceso de integración con Kaspersky Managed Detection and Response se divide en los siguientes pasos:

1. **Instalación del componente Managed Detection and Response**

   Para la integración de Kaspersky Embedded Systems Security con la solución Managed Detection and Response se utiliza el componente Managed Detection and Response. Para instalar este componente, en la configuración del paquete de instalación o en el Asistente de configuración, o al cambiar el conjunto de componentes de la aplicación en el Panel de control de Windows, seleccione **Managed Detection and Response** en el paso de selección de componentes.

2 Configuración de Kaspersky Private Security Network

A partir de la actualización de julio de 2025, la solución Managed Detection and Response admite el funcionamiento sin el archivo de configuración de KPSN. Para obtener más detalles sobre cómo la solución MDR usa Kaspersky Security Network, consulte la Ayuda de Kaspersky Managed Detection and Response.

Si la configuración no cumple con los requisitos para ejecutarse sin los archivos de configuración de KPSN, cargue el archivo de configuración de KPSN en las propiedades del Servidor de administración. Encontrará el archivo de configuración de KPSN en el archivo ZIP del archivo de configuración de MDR. También puede **cargar un archivo de configuración de KPSN mediante la línea de comandos.**

1. En el dispositivo, ejecute un intérprete de línea de comandos (por ejemplo, cmd.exe) con los permisos del administrador local.
2. Con el comando `cd`, vaya a la carpeta donde se encuentra el archivo kavshell.exe.

   Por ejemplo, `cd C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0` y presione **ENTER**.

   También puede agregar la ruta del archivo ejecutable a la variable del sistema %PATH% durante lainstalación de la aplicación y ejecutar el comando sin navegar a la carpeta de la aplicación.
3. Ejecute el siguiente comando:

   ```
   KAVSHELL KSN [/global] [/private <ruta completa al archivo de configuración de KSN privado>] [/login=<nombre de la cuenta de usuario actual>] [/pwd=</contraseña de inicio de sesión o contraseña de KLAdmin si /no se especifica el nombre de usuario>]
   ```

   Ejemplo:

   ```
   KAVSHELL KSN /private C:\kpsn_config.pkcs7
   ```

Para más información sobre cómo configurar Kaspersky Private Security Network, consulte la Ayuda de Kaspersky Security Center.

3 Activar Kaspersky Managed Detection and Response

Para activar la solución Managed Detection and Response en Kaspersky Embedded Systems Security, necesita una licencia separada para el complemento Kaspersky Managed Detection and Response for Embedded Systems Security. Para obtener más detalles sobre la activación de la solución, consulte la Ayuda de Kaspersky Managed Detection and Response.

Kaspersky Embedded Systems Security no admite archivos de configuración de MDR (archivos BLOB). Todos los activos se colocarán en el inquilino raíz.

4 Habilitar el componente Managed Detection and Response

Cómo habilitar Managed Detection and Response en la Consola de administración de Kaspersky Security Center

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Directivas**.
2. Seleccione la directiva correspondiente y haga doble clic para abrir las propiedades de la directiva.
3. Seleccione la sección **Servidores de colección de telemetría**.

4. En el bloque **Managed Detection and Response**, haga clic en el botón **Configuración**.

   Se abre la ventana **Managed Detection and Response**.

5. Seleccione la casilla de verificación **Managed Detection and Response**.

6. Guarde los cambios.

Cómo habilitar el componente Managed Detection and Response en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.

2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la ficha **Configuración de la aplicación**.

4. Seleccione la sección **Servidores de colección de telemetría**.

5. En el bloque **Managed Detection and Response**, haga clic en el botón **Configuración**.

   Se abre la ventana **Managed Detection and Response**.

6. Seleccione la casilla de verificación **Managed Detection and Response DESHABILITADA**.

7. Guarde los cambios.

Cómo habilitar el componente Managed Detection and Response en la Consola de la aplicación

1. En el árbol de la Consola de la aplicación, seleccione la sección **Servidores de colección de telemetría** → **Managed Detection and Response**.

2. Haga clic en el vínculo **Propiedades** del panel de resultados.

   Se abre la ventana **Managed Detection and Response** en la pestaña **General**.

3. Seleccione la casilla de verificación **Managed Detection and Response**.

4. Guarde los cambios.

Cómo habilitar Managed Detection and Response desde la línea de comandos

1. En el dispositivo, ejecute un intérprete de línea de comandos (por ejemplo, cmd.exe) con los permisos del administrador local.

2. Con el comando `cd`, vaya a la carpeta donde se encuentra el archivo kavshell.exe.

   Por ejemplo, `cd C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0` y presione **ENTER**.

   También puede agregar la ruta del archivo ejecutable a la variable del sistema %PATH% durante la instalación de la aplicación y ejecutar el comando sin navegar a la carpeta de la aplicación.

3. Ejecute el siguiente comando:

```
KAVSHELL MDR /<enable|disable|show> [/login:<nombre de la cuenta de usuario actual>] [/pwd:</contraseña de inicio de sesión o contraseña de KLAdmin si /no se especifica el nombre de usuario>]
```

Parámetros de comando para habilitar Managed Detection and Response

Parámetro	Descripción
`MDR /<enable|disable|show>`	Argumento requerido. Permite habilitar, deshabilitar y ver el estado de Managed Detection and Response
`/LOGIN=<nombre de cuenta de usuario>`	Argumento opcional. Le permite especificar el nombre de la cuenta de usuario con permisos suficientes. Si no se especifica esta opción, la aplicación le solicita el nombre de usuario en la siguiente línea. No es necesario que ingrese este valor si ingresó la contraseña de KLAdmin.
`/PWD=</contraseña de inicio de sesión o contraseña de KLAdmin si /no se especifica el nombre de usuario>`	Le permite especificar la contraseña de la cuenta de usuario de KLAdmin o una cuenta de usuario con permisos suficientes. Si no se especifica esta opción, la aplicación le pedirá la contraseña en la siguiente línea.

Contacto con Soporte técnico

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

Cómo acceder al Servicio de soporte técnico

Si no puede encontrar una solución a su problema en la documentación o en ninguna de las fuentes de información sobre Kaspersky Embedded Systems Security, le recomendamos que se ponga en contacto con Soporte técnico. Soporte técnico responderá sus preguntas acerca de la instalación y el uso de Kaspersky Embedded Systems Security.

Kaspersky se compromete a brindar asistencia técnica para Kaspersky Embedded Systems Security a lo largo de su ciclo de vida (el cual se detalla en esta página). Antes de ponerse en contacto con el soporte técnico, lea primero las reglas de soporte.

Puede comunicarse con el Servicio de soporte técnico de las siguientes maneras:

- Visitando el sitio web del soporte técnico
- Enviando una solicitud al Servicio de soporte técnico de Kaspersky por medio del portal de Kaspersky CompanyAccount.

Soporte técnico mediante Kaspersky CompanyAccount

Kaspersky CompanyAccount es un portal para empresas que usan aplicaciones de Kaspersky. Kaspersky CompanyAccount está diseñado para facilitar la interacción entre usuarios y especialistas de Kaspersky 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 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 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.

Proporcionar información de diagnóstico extendida a los especialistas del Servicio de soporte técnico

Para que el soporte y la solución de problemas de la aplicación tengan mayor eficacia, los especialistas del Servicio de soporte técnico pueden pedirle que cambie la configuración de la aplicación temporalmente a fines de depuración durante el diagnóstico. Para ello, es posible que deba hacer lo siguiente:

- Activar la funcionalidad que procesa y almacena la información de diagnóstico extendida.
- Ajustar la configuración de componentes individuales de software, que no están disponibles a través de los elementos estándares de la interfaz del usuario.
- Cambiar la configuración de almacenamiento y transmisión de la información de diagnóstico que se procesó.
- Configurar la intercepción y el registro del tráfico de red.

Los especialistas del Servicio de soporte técnico anunciarán la información que se requiere para realizar las acciones mencionadas (descripción de la secuencia de pasos, configuración modificable, archivos de configuración, scripts, funciones adicionales de la línea de comandos, módulos de depuración, servicios especializados, etc.), así como la composición de los datos analizados a fines de depuración. La información avanzada de diagnóstico se guarda en el equipo del usuario. No se lleva a cabo la transferencia automática de los datos almacenados a Kaspersky.

Después de informar un problema a los especialistas del Servicio de soporte técnico, 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. Los especialistas del Servicio de soporte técnico de Kaspersky también pueden pedirle que cree un archivo de seguimiento y envíe un archivo de volcado de memoria.

Luego de analizar los datos que envíe, los especialistas de soporte técnico pueden crear un script AVZ y enviárselo. Mediante los scripts AVZ es 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.

Las acciones mencionadas solo pueden realizarse bajo la supervisión de los especialistas del Servicio de soporte técnico siguiendo las instrucciones que envían. La modificación sin asistencia de la configuración de la aplicación de maneras no descritas en la documentación de la aplicación o en las recomendaciones de los especialistas del Servicio de soporte técnico puede generar retrasos y mal funcionamiento del sistema operativo, disminución del nivel de protección del equipo, así como una infracción de la disponibilidad e integridad de la información procesada.

Seguimiento de la operación de aplicaciones

Los *archivos de seguimiento de la aplicación* contienen un registro detallado de las acciones que la aplicación realiza, así como de los mensajes sobre los eventos que ocurren cuando la aplicación está en funcionamiento. Durante el proceso de seguimiento, la aplicación crea un conjunto de archivos con datos sobre el funcionamiento de diferentes componentes de la aplicación.

Los archivos de rastreo le permiten hacer un seguimiento del proceso de ejecución de comandos de aplicaciones paso a paso y determinar la etapa del funcionamiento de una aplicación en la cual se produce un error.

Los archivos de seguimiento quedarán guardados en el equipo mientras la aplicación esté instalada; cuando desinstale la aplicación, los archivos se eliminarán de forma permanente. También puede eliminar los archivos de rastreo manualmente. Para ello, debe deshabilitar el seguimiento y detener la aplicación.

Los archivos de rastreo guardados pueden contener datos confidenciales. Usted es responsable de velar por la seguridad de estos archivos y controlar el acceso a los datos.

De manera predeterminada, los archivos de seguimiento, excepto los archivos de seguimiento del Agente de autenticación, se almacenan en la carpeta %ProgramData%\Kaspersky Lab\KESS.4.0\Traces.

El nombre de los archivos de seguimiento tiene este formato: KESS<4.0_dateXX.XX_timeXX.XX_pidXXX.><tipo de archivo de seguimiento>.log.

Puede ver los datos guardados en los archivos de rastreo.

Todos los archivos de rastreo tienen los siguientes datos comunes:

- Hora del evento
- Número del hilo de ejecución

  El archivo de seguimiento del Agente de autenticación no contiene esta información.
- Componente de la aplicación que causó el evento
- Gravedad del evento (evento informativo, advertencia, evento crítico, error)
- Una descripción del evento que involucra la ejecución del comando por un componente de la aplicación y el resultado de la ejecución de ese comando.

Kaspersky Embedded Systems Security guarda las contraseñas de usuario en un archivo de seguimiento solo en forma cifrada.

Cómo habilitar y configurar el seguimiento de la aplicación en la Consola de administración de Kaspersky Security Center

1. En el árbol de la consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados**.
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 de las propiedades de la directiva, vaya a la sección **Diagnóstico de mal funcionamiento**.
6. En el bloque **Configuración de resolución de problemas**, haga clic en el botón **Configuración**.

   Se abre la ventana **Configuración de resolución de problemas** en la pestaña **Configuración de seguimiento de aplicaciones**.
7. Seleccione la casilla de verificación **Habilitar seguimiento**.
8. Si es necesario, en el campo **Carpeta de archivos de seguimiento**, especifique la ruta completa a una carpeta local donde Kaspersky Embedded Systems Security para Windows guardará los archivos de rastreo.

   > La carpeta debe crearse de antemano y es necesario que la cuenta SYSTEM pueda escribir en ella. La ruta no puede hacer referencia a una unidad, una carpeta de red o una variable de entorno.
9. En la lista desplegable **Nivel de detalle**, seleccione el nivel de detalle de la información para depuración:

   - **Crítico** significa que el archivo de rastreo guarda solo los mensajes acerca de errores fatales.
   - **Diagnóstico** significa que el archivo de rastreo guarda mensajes acerca de todos los errores y las advertencias.
   - **Importante** significa que el archivo de rastreo guarda mensajes acerca de todos los errores, advertencias e información adicional.
   - **Normal** significa que el archivo de rastreo guarda mensajes acerca de todos los errores, advertencias, así como información acerca del funcionamiento normal de la aplicación (predeterminado).
   - **Detallado** significa que el archivo de rastreo guarda toda la información acerca del funcionamiento de la aplicación.

   El nivel de detalle que se requiere para solucionar cualquier posible problema es determinado por un especialista del servicio de soporte técnico.
10. El nivel de detalle predeterminado es **Normal**.

11. Especifique el **Tamaño máximo de los archivos de seguimiento (MB)**.

    Valores disponibles: de 1 a 4095 MB. De forma predeterminada, el tamaño máximo de los archivos de seguimiento es de 100 MB.

12. Para que los archivos de seguimiento antiguos se eliminen cuando se alcance el número máximo de archivos, seleccione la casilla **Eliminar los archivos de seguimiento más antiguos**.

13. Especifique el **Cantidad máxima de archivos para un registro de seguimiento**.

    Valores disponibles: de 1 a 999. De manera predeterminada, el número máximo de archivos es 5. El campo está disponible si la casilla de verificación **Eliminar los archivos de seguimiento más antiguos** está seleccionada.

14. Guarde los cambios.

15. Reinicie Kaspersky Embedded Systems Security.

Para detener el seguimiento de la aplicación:

En las propiedades de la directiva, en la ventana **Configuración de resolución de problemas**, en la pestaña **Configuración de seguimiento de aplicaciones**, desactive la casilla **Habilitar seguimiento**.

Cómo habilitar y configurar el seguimiento de la aplicación en la Consola de la aplicación

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 resultados del nodo.
   - Seleccione **Propiedades de la aplicación** en el menú contextual del nodo.

   Se abre la ventana **Propiedades de la aplicación**.

2. Seleccione la ficha **Diagnóstico de mal funcionamiento**.

3. En el bloque **Configuración de resolución de problemas**, haga clic en el botón **Configuración**.

   Se abre la ventana **Configuración de resolución de problemas**.

4. Seleccione la pestaña de configuración del seguimiento:

   - **Configuración de seguimiento de aplicaciones**. Kaspersky Embedded Systems Security inicia el seguimiento de la aplicación.
   - **Configuración de seguimiento de la consola de aplicaciones**. Si la Consola de la aplicación y Kaspersky Embedded Systems Security están instalados en equipos diferentes, puede iniciar el seguimiento solo para la Consola de la aplicación.

5. Seleccione la casilla de verificación **Habilitar seguimiento**.

   El campo **Carpeta de archivos de seguimiento** contiene la ruta completa a la carpeta local en la que Kaspersky Embedded Systems Security guarda los archivos de rastreo de manera predeterminada. Puede especificar otra ruta.

6. En la lista desplegable **Nivel de detalle**, seleccione el nivel de detalle de la información para depuración:

   - **Crítico** significa que el archivo de rastreo guarda solo los mensajes acerca de errores fatales.
   - **Diagnóstico** significa que el archivo de rastreo guarda mensajes acerca de todos los errores y las advertencias.
   - **Importante** significa que el archivo de rastreo guarda mensajes acerca de todos los errores, advertencias e información adicional.
   - **Normal** significa que el archivo de rastreo guarda mensajes acerca de todos los errores, advertencias, así como información acerca del funcionamiento normal de la aplicación (predeterminado).
   - **Detallado** significa que el archivo de rastreo guarda toda la información acerca del funcionamiento de la aplicación.

   El nivel de detalle que se requiere para solucionar cualquier posible problema es determinado por un especialista del servicio de soporte técnico.

   El nivel de detalle predeterminado es **Normal**.

7. Especifique el **Tamaño máximo de los archivos de seguimiento (MB)**.

   Valores disponibles: de 1 a 4095 MB. De forma predeterminada, el tamaño máximo de los archivos de seguimiento es de 100 MB.

8. Para que los archivos de seguimiento antiguos se eliminen cuando se alcance el número máximo de archivos, seleccione la casilla **Eliminar los archivos de seguimiento más antiguos**.

9. Especifique el **Cantidad máxima de archivos para un registro de seguimiento**.

   Valores disponibles: de 1 a 999. De manera predeterminada, el número máximo de archivos es 5. El campo está disponible si la casilla de verificación **Eliminar los archivos de seguimiento más antiguos** está seleccionada.

10. Guarde los cambios.

11. Reinicie Kaspersky Embedded Systems Security.

Para detener el seguimiento de la aplicación:

En las propiedades de la aplicación, en la ventana **Configuración de resolución de problemas**, en la pestaña **Configuración de seguimiento de aplicaciones**, desactive la casilla **Habilitar seguimiento**.

Cómo habilitar y configurar el seguimiento de la aplicación en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la ficha **Configuración de la aplicación**.
4. Seleccione la sección **Diagnóstico de mal funcionamiento**.
5. En el bloque **Configuración de resolución de problemas**, seleccione la casilla **Habilitar seguimiento de la aplicación**.
6. Si es necesario, especifique la ruta completa a una carpeta local donde Kaspersky Embedded Systems Security guardará los archivos de seguimiento.

   > La carpeta debe crearse de antemano y es necesario que la cuenta SYSTEM pueda escribir en ella. La ruta no puede hacer referencia a una unidad, una carpeta de red o una variable de entorno.
7. En la lista desplegable **Nivel**, seleccione el nivel de detalle de la información para depuración.
8. Especifique el **Tamaño máximo de los archivos de seguimiento (MB)**.

   Valores disponibles: de 1 a 4095 MB. De forma predeterminada, el tamaño máximo de los archivos de seguimiento es de 100 MB.
9. Para que los archivos de seguimiento antiguos se eliminen cuando se alcance el número máximo de archivos, seleccione la casilla **Eliminar los archivos de seguimiento más antiguos**.
10. Especifique el **Cantidad máxima de archivos para un registro de seguimiento**.

    Valores disponibles: de 1 a 999. De manera predeterminada, el número máximo de archivos es 5. El campo está disponible si la casilla de verificación **Eliminar los archivos de seguimiento más antiguos** está seleccionada.
11. Guarde los cambios.
12. Reinicie Kaspersky Embedded Systems Security.

Para detener el seguimiento de la aplicación:

En las propiedades de la directiva que está configurando, en la sección **Diagnóstico de mal funcionamiento**, desactive la casilla **Habilitar seguimiento de la aplicación**.

Cómo habilitar y configurar el seguimiento de la aplicación en la Interfaz de diagnóstico compacto

Cómo habilitar y configurar el seguimiento de la aplicación en la línea de comandos

1. Abra el símbolo del sistema (cmd.exe) como administrador.
2. Con el comando cd, vaya a la carpeta donde se encuentra el archivo kavshell.exe.

   Por ejemplo: cd C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.0.0
3. Ejecute el siguiente comando:

   KAVSHELL TRACE /ON|/OFF /F:<carpeta para almacenar archivos de rastreo> [/LVL:debug|info|warning|error|critical] [/S:<tamaño máximo del archivo de rastreo en megabytes>] [/R:<cantidad máxima de archivos de rastreo antes de reemplazarlos por otros nuevos>]

Registrar volcados de memoria

El archivo de volcado de memoria contiene toda información sobre la memoria operativa de los procesos de Kaspersky Embedded Systems Security en el momento en que se falló la aplicación.

Los archivos de volcado de memoria se almacenan en su equipo de una forma modificada que no puede leerse mientras la aplicación está en uso y se eliminan en forma permanente cuando se desinstala la aplicación.

Los archivos de volcado guardados pueden contener datos confidenciales. Usted es responsable de velar por la seguridad de estos archivos y controlar el acceso a los datos.

De manera predeterminada, los archivos de volcado de memoria se almacenan en la siguiente carpeta: %ProgramData%\Kaspersky Lab\KESS.4.0\Traces.

Cómo habilitar o deshabilitar el registro de volcado de memoria en la Consola de administración de Kaspersky Security Center

1. En el árbol de la consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados**.
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 de las propiedades de la directiva, vaya a la sección **Diagnóstico de mal funcionamiento**.

6. En el bloque **Configuración de resolución de problemas**, haga clic en el botón **Configuración**.

   Se abre la ventana **Configuración de resolución de problemas** en la pestaña **Configuración de seguimiento de aplicaciones**.

7. Seleccione la ficha **Configuración de volcado de la aplicación**.

8. Seleccione o desactive la casilla **Crear archivo de volcado** para habilitar o deshabilitar el volcado de memoria en caso de mal funcionamiento.

9. Si es necesario, en el campo **Carpeta de archivos de volcado**, ingrese la ruta completa a la carpeta local donde Kaspersky Embedded Systems Security guardará los archivos de volcado de memoria.

   La carpeta debe crearse de antemano y es necesario que la cuenta SYSTEM pueda escribir en ella. La ruta no puede hacer referencia a una unidad, una carpeta de red o una variable de entorno.

10. Guarde los cambios.

Cómo habilitar o deshabilitar el registro de volcado de memoria en la Consola de la aplicación

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 resultados del nodo.
   - Seleccione **Propiedades de la aplicación** en el menú contextual del nodo.

   Se abre la ventana **Propiedades de la aplicación**.

2. Seleccione la ficha **Diagnóstico de mal funcionamiento**.

3. En el bloque **Configuración de resolución de problemas**, haga clic en el botón **Configuración**.

   Se abre la ventana **Configuración de resolución de problemas**.

4. Seleccione la pestaña de configuración del volcado:

   - **Configuración de volcado de la aplicación**. Kaspersky Embedded Systems Security registra todos los archivos de volcado de la aplicación.
   - **Configuración de volcado de la consola de aplicaciones**. Si la Consola de la aplicación y Kaspersky Embedded Systems Security están instalados en equipos diferentes, puede registrar los archivos de volcado solo para la Consola de la aplicación.

5. Seleccione o desactive la casilla **Crear archivo de volcado** para habilitar o deshabilitar el volcado de memoria en caso de mal funcionamiento.

   De manera predeterminada, los archivos de volcado de memoria se almacenan en la siguiente carpeta: %ProgramData%\Kaspersky Lab\KESS.4.0\Traces. Puede especificar otra ruta.

6. Guarde los cambios.

Cómo habilitar o deshabilitar el registro de volcado de memoria en Kaspersky Security Center Web Console

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.

2. Haga clic en el nombre de la directiva de Kaspersky Embedded Systems Security.

   Se abre la ventana de propiedades de la directiva.

3. Seleccione la ficha **Configuración de la aplicación**.

4. Seleccione la sección **Diagnóstico de mal funcionamiento**.

5. En **Configuración de archivo de volcado**, seleccione o desactive la casilla **Crear archivo de volcado** para habilitar o deshabilitar el volcado de memoria en caso de mal funcionamiento.

6. Si es necesario, especifique la ruta completa a la carpeta local donde Kaspersky Embedded Systems Security guardará los archivos de volcado de memoria.

   > La carpeta debe crearse de antemano y es necesario que la cuenta SYSTEM pueda escribir en ella. La ruta no puede hacer referencia a una unidad, una carpeta de red o una variable de entorno.

7. Guarde los cambios.

También puede habilitar o deshabilitar el registro de volcado de memoria en la Interfaz de diagnóstico compacto.

Fuentes de información acerca de Kaspersky Embedded Systems Security

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
- Página de Kaspersky Embedded Systems Security en el sitio web de soporte técnico (base de conocimientos)
- Ayuda en línea
- Debates sobre la aplicación en el Foro

Si no encontró una solución para su problema, comuníquese con el Servicio de soporte técnico de Kaspersky.

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

En la página de Kaspersky Embedded Systems Security, encontrará 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 de la base de conocimientos contiene artículos que brindan información útil, recomendaciones y respuestas a las preguntas más frecuentes sobre la adquisición, la instalación y el uso de la aplicación.

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

Ayuda en línea de Kaspersky Embedded Systems Security

La ayuda en línea contiene información acerca de la configuración y el uso de Kaspersky Embedded Systems Security.

Debates sobre la aplicación en el Foro

Si su pregunta no requiere una respuesta urgente, puede debatir sobre eso con los expertos de Kaspersky y otros usuarios en nuestro Foro.

En el foro, puede ver los temas existentes, publicar sus propios comentarios y crear nuevos temas de debate.

Glosario

Actualización

El proceso de sustituir o agregar archivos nuevos (bases de datos o módulos de la aplicación) obtenidos de los servidores de actualizaciones de Kaspersky.

Analizador heurístico

Una tecnología para detectar amenazas sobre la información que aún no se ha agregado a las bases de datos de Kaspersky. 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 de almacenamiento

Uno o varios archivos empaquetados en un solo archivo comprimido. Se necesita una aplicación especializada llamada archivador para comprimir y descomprimir datos.

Archivo infectable

Un archivo que, por su estructura o formato, puede ser usado por intrusos como "contenedor" para almacenar y propagar código malicioso. Por lo general, son archivos ejecutables con extensiones de archivo tales como .com, .exe y .dll. Existe un riesgo bastante alto de intrusión de código malicioso en estos archivos.

Bases de datos antivirus

Las bases de datos que contienen información sobre las amenazas conocidas de seguridad al equipo por parte de Kaspersky como de la fecha de lanzamiento de la base de datos antivirus. Las firmas de la bases de datos antivirus ayudan a detectar código malicioso en los objetos analizados. Los especialistas de Kaspersky crean las bases de datos de antivirus y las actualizan a cada hora.

Clave activa

Clave que está utilizando la aplicación.

Configuración de tareas

Configuración de la aplicación específica para cada tipo de tarea.

Copia de seguridad

Espacio de almacenamiento especial destinado a guardar copias de seguridad de los objetos antes de que se los desinfecte o elimine.

Cuarentena

Carpeta a la que la aplicación Kaspersky 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.

Desinfección

Método de procesamiento de objetos infectados cuyo resultado es la recuperación completa o parcial de los datos. No todos los objetos infectados se pueden desinfectar.

Directiva

Una directiva define la configuración de la aplicación y gestiona la capacidad de configurar la aplicación en los equipos de un grupo de administración. Debe crearse una directiva particular para cada aplicación. Puede crear múltiples 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.

Estado de protección

El estado de protección vigente en un momento dado, el cual caracteriza el nivel de seguridad del dispositivo.

Falso positivo

Situación en la cual una aplicación de Kaspersky considera que un objeto no infectado lo está porque su código es similar al de un virus.

Importancia de un evento

Propiedad de un evento encontrada durante la operación de una aplicación de Kaspersky. Hay cuatro niveles de importancia:

- Evento crítico
- Fallo funcional
- Advertencia
- Mensaje informativo.

Los eventos de un mismo tipo pueden tener niveles de gravedad diferentes según la situación en la cual ocurren.

Kaspersky Security Network (KSN)

Infraestructura de servicios en la nube que brinda acceso a la base de conocimientos en línea de Kaspersky sobre la reputación de archivos, recursos web y software. El uso de los datos de Kaspersky Security Network permite que las aplicaciones de Kaspersky respondan más rápido a las amenazas, mejora el rendimiento de algunos componentes de protección y reduce la posibilidad de encontrar falsos positivos.

Máscara de archivo

Representación de un nombre de archivo en la que se utilizan caracteres genéricos. Los principales caracteres utilizados en las máscaras de archivo son * y ? (Donde * representa cualquier cantidad de caracteres, y ? representa un solo carácter).

Nivel de seguridad

Un nivel de seguridad es un conjunto predefinido de ajustes de configuración para los componentes.

Objeto infectado

Objeto en el que una sección de código coincide completamente con una sección del código de una amenaza conocida. Los expertos de Kaspersky recomiendan no trabajar con estos 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.

Periodo de vigencia de la licencia

El período de tiempo durante el cual puede utilizar las funciones de la aplicación y los servicios adicionales. La cantidad de funciones y de servicios adicionales disponibles depende del tipo de licencia.

Servidor de administración

Un componente de Kaspersky Security Center que almacena de forma central información sobre todas las aplicaciones de Kaspersky que se instalan en la red corporativa y que administra esas aplicaciones.

SIEM

Siglas en inglés del término "administración de información y eventos de seguridad". Se trata de una solución para administrar la información y los eventos del sistema de seguridad de una organización.

Tarea

Las funciones que realiza la aplicación de Kaspersky como tareas, por ejemplo: Protección de archivos en tiempo real, Análisis completo y Actualización de bases de datos.

Tarea local

Una tarea que se define y se ejecuta en un equipo cliente individual.

Vulnerabilidad

Una falla en un sistema operativo o una aplicación que pueden utilizar los programadores de malware para penetrar en el sistema operativo o la aplicación y corromper su integridad. La presencia de una gran cantidad de vulnerabilidades en el sistema operativo lo vuelven poco fiable, pues los virus que penetran en el sistema operativo pueden modificar el propio sistema y las aplicaciones que en él se instalan.

Información acerca de código de terceros

La información acerca del código de terceros se incluye en el archivo legal_notices.txt, ubicado en la carpeta de instalación de la aplicación.

Avisos de marca registrada

Las marcas registradas y las marcas de servicio son propiedad de sus respectivos dueños.

Apache es una marca comercial registrada o una marca comercial de Apache Software Foundation.

Citrix XenApp y XenDesktop son marcas comerciales registradas o marcas comerciales de Cloud Software Group, Inc. o sus filiales en los Estados Unidos o en otros países.

CVE es una marca registrada de The MITRE Corporation.

Dell Technologies, Dell, Dell Compellent y otras marcas comerciales son marcas comerciales de Dell Inc. o sus subsidiarias.

EMC, Celerra, Isilon, OneFS y VNX son marcas comerciales registradas o marcas comerciales de EMC Corporation en los Estados Unidos u otros países.

Hitachi es una marca comercial de Hitachi, Ltd.

Linux es la marca comercial registrada de Linus Torvalds en los Estados Unidos y otros países.

Microsoft, Active Directory, Internet Explorer, Excel, Hyper-V, JScript, MultiPoint, Outlook, PowerShell, Windows, Windows Server y Windows Vista son marcas comerciales del grupo de empresas Microsoft.

NetApp y Data ONTAP son marcas comerciales o marcas registradas de NetApp, Inc. en los Estados Unidos o en otros países.

Oracle es una marca registrada de Oracle o de sus empresas vinculadas.

UNIX es una marca comercial registrada en los Estados Unidos y otros países, licenciada exclusivamente a través de X/Open Company Limited.

Apéndices

En esta sección encontrará contenidos que complementan la información principal del documento.

Extensiones de archivos para un análisis rápido

com: archivo ejecutable de una aplicación que no supera los 64 KB

exe: archivo ejecutable o archivo autoextraíble

sys: archivo de sistema de Microsoft Windows

prg – texto de programas para dBase™, Clipper o Microsoft FoxPro Visual®, o un programa WAVmaker

bin: archivo binario

bat: archivo de lote

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

dpl: biblioteca Borland Delphi comprimida

dll: biblioteca de vínculos dinámicos

scr: pantalla inicial de Microsoft Windows

cpl: módulo del panel de control de Microsoft Windows

ocx: objeto de Microsoft OLE (Object Linking and Embedding)

tsp: programa que se ejecuta en modo de tiempo dividido

drv: controlador de dispositivos

vxd: controlador de dispositivos virtuales de Microsoft Windows

pif: archivo de información del programa

lnk: archivo de vínculos de Microsoft Windows

reg: archivo de claves del registro del sistema de Microsoft Windows

ini: archivo de configuración que contiene datos de la configuración para Microsoft Windows, Windows NT y algunas aplicaciones

cla: clase de Java

vbs – script de Visual Basic®

vbe: extensión de video del BIOS

js, jse: texto fuente de JavaScript

htm: documento del hipertexto

htt: encabezado de hipertexto de Microsoft Windows

hta – programa de hipertexto para Microsoft Internet Explorer®

asp: script de Active Server Pages

chm: archivo HTML compilado

pht: archivo HTML con scripts PHP integrados

php: script que se integra en archivos HTML

wsh: archivo de Microsoft Windows Script Host

wsf: script de Microsoft Windows

the: archivo del tapiz de escritorio de Microsoft Windows 95

hlp: archivo de ayuda de Windows

msg: mensaje de correo electrónico de Microsoft Mail

plg: mensaje de correo electrónico

mbx: mensaje de correo electrónico guardado de Microsoft Office Outlook

doc*: documentos de Microsoft Office Word, por ejemplo: doc para documentos de Microsoft Office Word, docx para documentos de Microsoft Office Word 2007 compatibles con XML, y docm para documentos de Microsoft Office Word 2007 compatibles con macros

dot*: plantillas de documentos de Microsoft Office Word, por ejemplo: dot para plantillas de documentos de Microsoft Office Word, dotx para plantillas documentos de Microsoft Office Word 2007 y dotm para plantillas de documentos de Microsoft Office Word 2007 compatibles con macros

fpm: programa de base de datos, archivo de inicio de Microsoft Visual FoxPro

rtf: documento con formato de texto enriquecido

shs: fragmento del manipulador de objetos de desecho de la Shell de Windows

dwg – base de datos de planos de AutoCAD®

msi: paquete de Microsoft Windows Installer

otm: proyecto de VBA para Microsoft Office Outlook

pdf: documento de Adobe Acrobat

swf – objeto del paquete de Shockwave® Flash

jpg, jpeg: formato de gráfico de imagen comprimida

emf: archivo con formato de metarchivo mejorado

ico: archivo de icono de objeto

ov? - archivos ejecutables de Microsoft Office Word

xl*: documentos y archivos de Microsoft Office Excel, por ejemplo: xls, la extensión correspondiente a Microsoft Office Excel, xlc para diagramas, xlt para plantillas de documentos, xlsx para libros de Microsoft Office Excel 2007, xltm para libros de Microsoft Office Excel 2007 compatibles con macros, xlsb para libros de Microsoft Office Excel 2007 en formato binario (no XML), xltx para plantillas de Microsoft Office Excel 2007, xlsm para plantillas de Microsoft Office Excel 2007 compatibles con macros y xlam para complementos de Microsoft Office Excel 2007 compatibles con macros

pp* – documentos y archivos de Microsoft Office PowerPoint®, por ejemplo: pps para diapositivas de Microsoft Office PowerPoint, ppt para presentaciones, pptx para presentaciones de Microsoft Office PowerPoint 2007, pptm para presentaciones de Microsoft Office PowerPoint 2007 compatibles con macros, potx para plantillas de presentaciones de Microsoft Office PowerPoint 2007, potm para plantillas de presentaciones de Microsoft Office PowerPoint 2007 compatibles con macros, ppsx para presentaciones de diapositivas de Microsoft Office PowerPoint 2007, ppsm para presentaciones de diapositivas de Microsoft Office PowerPoint 2007 compatibles con macros y ppam para complementos de Microsoft Office PowerPoint 2007 compatibles con macros

md* – documentos y archivos de Microsoft Office Access®, por ejemplo: mda para grupos de trabajo de Microsoft Office Access y mdb para bases de datos

sldx: una diapositiva de Microsoft PowerPoint 2007

sldm: una diapositiva de Microsoft PowerPoint 2007 compatible con macros

thmx: un tema de Microsoft Office 2007

Cuentas de usuario en las reglas del componente de la aplicación

Para configurar algunos componentes de la aplicación, debe agregar reglas especiales donde puede seleccionar los usuarios a los que la aplicación aplicará la regla.

Se deben agregar reglas para configurar los siguientes componentes de la aplicación:

- Control de inicio de aplicaciones
- Control de dispositivos
- Detección de comportamiento.
- Control de integridad del sistema

Puede agregar usuarios de las siguientes maneras:

- Seleccionar de Active Directory (recomendado)
- Seleccionar de la lista de usuarios de Kaspersky Security Center
- Agregar manualmente

Kaspersky recomienda usar cuentas de usuario locales solo en casos especiales cuando no es posible usar cuentas de usuario de dominio. Para obtener detalles sobre los riesgos de seguridad del uso de cuentas locales, consulte la Base de conocimientos de Microsoft. Usted es completamente responsable de la seguridad de un equipo si se usan cuentas de usuario locales; esto incluye, en especial, la responsabilidad de controlar y restringir el acceso a la configuración de la aplicación.

La aplicación usa el SID (Identificador de seguridad) del usuario para identificar a los usuarios. Al usar cuentas de usuario de Active Directory o de la lista de usuarios de Kaspersky Security Center, la aplicación determina el SID en el Servidor de administración. Esto significa que la aplicación no coloca una carga adicional en el equipo para identificar a un usuario. Si agregó más de 1000 cuentas de usuario locales a una regla de la aplicación, las aplicaciones se comunican con el controlador de dominio para identificar al usuario. Esto significa que la carga en el equipo aumenta. Para optimizar el impacto en el rendimiento del equipo, se recomienda usar cuentas de usuario de Active Directory o de la lista de usuarios de Kaspersky Security Center.

Kaspersky Embedded Systems Security admite cuentas de usuarios y de grupo integradas (por ejemplo, el grupo "Todos") en las reglas. Debido a las características específicas de la detección de SID de usuarios, la aplicación permite usar cuentas integradas que se agregaron desde Active Directory o solo desde la lista de usuarios de Kaspersky Security Center. Las reglas en las que la cuenta integrada se agrega manualmente no funcionan.