ENDPOINT ANTIVIRUS
FOR WINDOWS

Guía del usuario

Microsoft® Windows® 10/8.1/8/7/Vista
Haga clic aquí para descargar la versión más reciente de este documento

ENJOY SAFER TECHNOLOGY™

ESET **ENDPOINT ANTIVIRUS 7**

Atención al cliente internacional: www.eset.com/support

REV. 15/08/2018

Contenido

Contenido

1. ESET Endpoint Antivirus 7

ESET Endpoint Antivirus 7 representa un nuevo enfoque de la seguridad informática realmente integrada. La versión más reciente del motor de análisis ThreatSense® garantiza la protección del ordenador gracias a su velocidad y precisión. Estas características lo convierten en un sistema inteligente que está constantemente en alerta frente a ataques y software malintencionado que puedan poner en peligro su ordenador.

ESET Endpoint Antivirus 7 es una solución de seguridad integral que nació tras un gran esfuerzo por combinar el nivel máximo de protección con un impacto mínimo en el sistema. Las tecnologías avanzadas basadas en la inteligencia artificial son capaces de eliminar proactivamente la infiltración de virus, spyware, troyanos, gusanos, adware, rootkits y otros ataques que albergan en Internet sin dificultar el rendimiento del sistema ni interrumpir la actividad del ordenador.

ESET Endpoint Antivirus 7 está diseñado principalmente para su uso en estaciones de trabajo en empresas pequeñas. El uso de ESET Endpoint Antivirus con ESET Remote Administrator en un entorno empresarial le permitirá administrar fácilmente cualquier número de estaciones de trabajo cliente, aplicar políticas y reglas, controlar detecciones y configurar clientes de forma remota desde cualquier ordenador en red.

1.1 Requisitos del sistema

Para un funcionamiento óptimo de ESET Endpoint Antivirus, el sistema debería cumplir con los siguientes requisitos de hardware y software (configuración predeterminada del producto):

Procesadores compatibles:

• Procesador de 32 bits (x86) o 64 bits (x64), 1 GHz o superior

Sistemas operativos: Microsoft® Windows® 10/8.1/8/7/Vista

• Un sistema operativo y el Service Pack necesario compatible con la versión del producto ESET instalada
• Se deben cumplir los requisitos del sistema operativo y otro software instalado en el ordenador
• 0,3 GB de memoria del sistema libre (consulte la nota 1)
• 1 GB de espacio de disco duro libre (consulte la nota 2)
• Resolución de pantalla mínima de 1024 × 768
• Conexión a Internet o conexión de red de área local a una fuente (consulte la nota 3) de actualizaciones del producto

Aunque el producto podría instalarse y ejecutarse en sistemas que no cumplan estos requisitos, recomendamos realizar pruebas de usabilidad basadas en los requisitos de rendimiento.

NOTA
(1): El producto podría utilizar más memoria si la memoria no se utiliza para otras tareas en un ordenador con muchas infecciones o al importar grandes listas de datos en el producto (p. ej. listas blancas de URL).
(2): El espacio en disco necesario para descargar el instalador, instalar el producto y conservar una copia del paquete de instalación en los datos del programa, así como copias de seguridad de las actualizaciones del producto para admitir la función de reversión. El producto puede utilizar más espacio en disco con configuraciones distintas (p. ej. cuando se almacenan más versiones de copia de seguridad de actualizaciones del producto, volcados de memoria o grandes cantidades de registros) o en un ordenador infectado (p. ej. debido a la función de cuarentena). Se recomienda mantener espacio en disco libre suficiente para permitir las actualizaciones del sistema operativo y del producto ESET.
(3): aunque no se recomienda, el producto se puede actualizar manualmente desde un soporte extraíble.

1.2 Prevención

Cuando trabaje con el ordenador y, especialmente, cuando navegue por Internet, tenga en cuenta que ningún sistema antivirus del mundo puede eliminar completamente el riesgo de amenazas y ataques. Para disfrutar de una protección y una comodidad máximas, es esencial usar correctamente su solución antivirus y cumplir varias reglas útiles:

Actualización regular

De acuerdo con las estadísticas de ESET LiveGrid®, cada día se crean miles de nuevas amenazas únicas para burlar las medidas de seguridad existentes y proporcionar un beneficio a sus autores, todo ello a costa de otros usuarios. Los especialistas del laboratorio de virus de ESET analizan estas amenazas diariamente y preparan y publican actualizaciones para mejorar continuamente el nivel de protección para los usuarios. Para garantizar la máxima eficacia de estas actualizaciones es importante que estén bien configuradas en el sistema. Para obtener más información sobre cómo configurar las actualizaciones, consulte el capítulo Configuración de actualizaciones.

Descarga de parches de seguridad

Los autores de software malintencionado con frecuencia explotan varias vulnerabilidades del sistema para aumentar la eficacia de la propagación de códigos malintencionados. Por ello, las empresas de software vigilan de cerca las nuevas vulnerabilidades en las aplicaciones y publican actualizaciones de seguridad para eliminar amenazas potenciales periódicamente. Es importante descargar estas actualizaciones de seguridad a medida que se publican. Microsoft Windows y los navegadores web como Internet Explorer son dos ejemplos de programas que publican de forma periódica actualizaciones de seguridad.

Copia de seguridad de los datos importantes

Normalmente, a los autores de código malicioso no les importan las necesidades de los usuarios y, con frecuencia, la actividad de los programas malintencionados provoca un funcionamiento incorrecto del sistema operativo y la pérdida de datos importantes. Es importante realizar copias de seguridad periódicas de sus datos importantes y confidenciales en una fuente externa, como un DVD o un disco duro externo. Estas precauciones facilitan y aceleran la recuperación de los datos en caso de fallo del sistema.

Análisis regular del ordenador en busca de virus

El módulo de protección del sistema de archivos en tiempo real se encarga de la detección de los virus, gusanos, troyanos y rootkits, conocidos o no. Esto significa que cada vez que entra en un archivo o lo abre, este se analiza en busca de actividad de código malicioso. Recomendamos que realice un análisis completo del ordenador al menos una vez al mes, ya que las firmas de códigos maliciosos pueden variar y el motor de detección se actualiza todos los días.

Seguimiento de las reglas de seguridad básicas

Esta es la regla más útil y eficaz de todas: sea siempre cauto. Actualmente, muchas amenazas requieren la intervención del usuario para su ejecución y distribución. Si es precavido a la hora de abrir archivos nuevos, se ahorrará mucho tiempo y esfuerzo en la desinfección de amenazas. Estas son algunas directrices útiles:

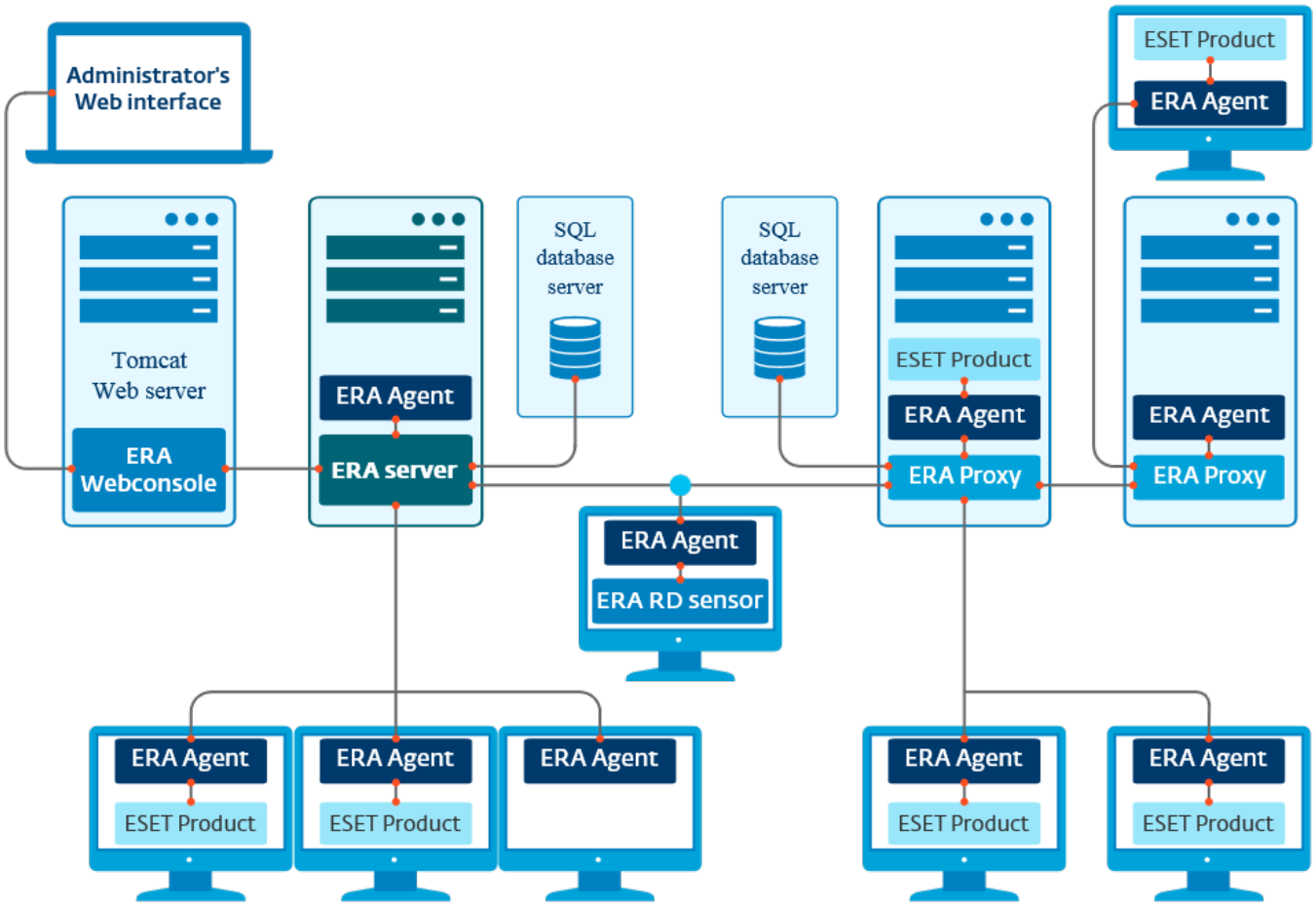
- No visite sitios web sospechosos con varios elementos y anuncios emergentes.
- Tenga cuidado al instalar programas gratuitos, paquetes codec, etc. Use únicamente programas seguros y solo visite sitios web seguros.
- Tenga cuidado a la hora de abrir archivos adjuntos de correo electrónico, especialmente los de mensajes masivos y de remitentes desconocidos.
- No use la cuenta de administrador para realizar su trabajo diario en el ordenador.

2. Documentación para usuarios conectados a través de ESET Remote Administrator

ESET Remote Administrator (ERA) es una aplicación que le permite administrar los productos de ESET en un entorno de red desde una ubicación central. El sistema de administración de tareas de ESET Remote Administrator le permite instalar soluciones de seguridad de ESET en ordenadores remotos y responder rápidamente a nuevos problemas y amenazas. ESET Remote Administrator no proporciona protección frente a código malicioso por sí solo, sino que confía en la presencia de soluciones de seguridad de ESET en cada cliente.

Las soluciones de seguridad de ESET son compatibles con redes que incluyan varios tipos de plataforma. Su red puede incluir una combinación de sistemas operativos actuales de Microsoft, Linux, Mac OS y sistemas operativos de dispositivos móviles (teléfonos móviles y tabletas).

En la imagen siguiente se muestra una arquitectura de ejemplo para una red protegida con soluciones de seguridad de ESET administradas mediante ERA:



NOTA
Para obtener más información, consulte la ayuda en línea de ESET Remote Administrator.

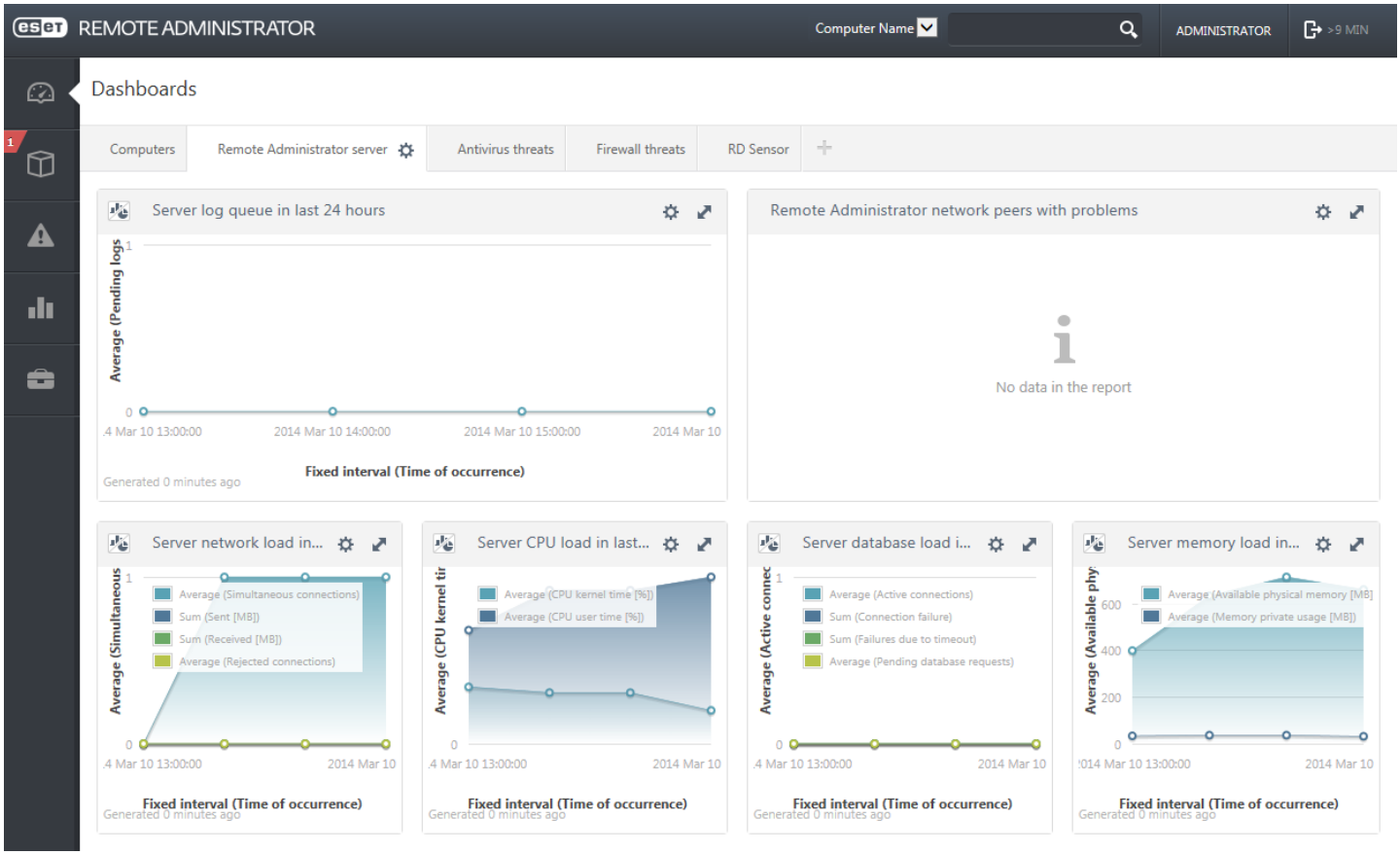
2.1 ESET Remote Administrator Server

ESET Remote Administrator Server es uno de los componentes principales de ESET Remote Administrator. Es la aplicación ejecutiva que procesa todos los datos recibidos de los clientes que se conectan al servidor (a través de ERA Agent). ERA Agent facilita la comunicación entre el cliente y el servidor. Los datos (registros de clientes, configuración, replicación del agente, etc.) se almacenan en una base de datos. ERA Server necesita una conexión estable a un servidor de bases de datos para procesar los datos correctamente. Le recomendamos que instale ERA Server y la base de datos en servidores diferentes para optimizar el rendimiento. El ordenador donde se instale ERA Server debe configurarse de modo que acepte todas las conexiones de agente, proxy y sensor RD, que se verifican mediante certificados. Una vez instalado puede abrir ERA Web Console, aplicación que se conecta a ERA Server (como se indica en el diagrama). Al administrar las soluciones de seguridad de ESET en su red, todas las operaciones relativas a ERA Server se realizan desde la Web Console.

2.2 Web Console

ERA Web Console es una interfaz web de usuario que presenta datos de ERA Server y permite administrar las soluciones de seguridad ESET de su red. A Web Console se accede desde un navegador. Muestra información general del estado de los clientes en la red y se puede utilizar para implementar de forma remota soluciones de ESET en ordenadores no administrados. Puede hacer que el servidor web sea accesible desde Internet para permitir el uso de ESET Remote Administrator desde prácticamente cualquier lugar o dispositivo.

Este es el tablero de Web Console:



La herramienta de **Búsqueda rápida** se encuentra en la parte superior de Web Console. Seleccione en el menú desplegable la opción **Nombre del ordenador**, **IPv4/Dirección IPv6** o **Nombre de la amenaza**, escriba la cadena de búsqueda en el campo de texto, y haga clic en el símbolo de la lupa o pulse **Intro** para buscar. Se abrirá la sección **Grupos**, en la que se muestran los resultados de la búsqueda.

NOTA
Para obtener más información, consulte la ayuda en línea de ESET Remote Administrator.

2.3 Proxy

ERA Proxy es otro de los componentes de ESET Remote Administrator, y tiene dos fines. En el caso de una red de tamaño mediano o de empresa con muchos clientes (por ejemplo, 10 000 clientes o más), puede utilizar ERA Proxy para distribuir la carga entre varios servidores ERA Proxy y así reducir la carga del ERA Server principal. La otra ventaja de ERA Proxy es que lo puede utilizar cuando se conecta a una sucursal remota con un vínculo débil. Esto significa que el ERA Agent de cada cliente no se conecta directamente al ERA Server principal, sino que lo hace a través de ERA Proxy, situado en la misma red local de la sucursal. Esta configuración libera el vínculo de conexión con la sucursal. ERA Proxy acepta conexiones desde todos los ERA Agent locales, recoge sus datos y los carga al ERA Server principal (o a otro ERA Proxy). Esto permite que la red dé cabida a más clientes sin poner en peligro el rendimiento de la red y de las consultas a la base de datos.

Según la configuración de la red, es posible que un ERA Proxy se conecte a otro ERA Proxy y, después, se conecte al ERA Server principal.

Para que ERA Proxy funcione correctamente, el ordenador host donde se instale debe tener instalado un ESET Agent y estar conectado al nivel superior (ya sea un ERA Server o un ERA Proxy superior, si lo hay) de la red.

2.4 Agente

ERA Agent es un componente esencial de ESET Remote Administrator. Las soluciones de seguridad de ESET instaladas en ordenadores cliente (por ejemplo, ESET Endpoint Security) se comunican con ERA Server a través del agente. Esta comunicación permite la administración de las soluciones de seguridad de ESET de todos los clientes remotos desde una ubicación central. El agente recopila información del cliente y la envía al servidor. Cuando el servidor envía una tarea al cliente, la tarea se envía al agente y este se comunica a continuación con el cliente. Toda la comunicación de la red tiene lugar entre el agente y la parte superior de la red de ERA (el servidor y el proxy).

El agente de ESET utiliza uno de estos tres métodos para conectarse al servidor:

1. El agente del cliente se conecta directamente al servidor.
2. El agente del cliente se conecta a través de un proxy que está conectado al servidor.
3. El agente del cliente se conecta al servidor a través de varios proxies.

El agente de ESET se comunica con las soluciones de ESET instaladas en un cliente, recopila información de los programas en dicho cliente y envía al cliente la información de configuración recibida del servidor.

NOTA
El proxy de ESET tiene su propio agente, que gestiona todas las tareas de comunicación entre clientes, otros proxies y el servidor.

2.5 Sensor RD

Sensor RD (Rogue Detection) es un componente de ESET Remote Administrator diseñado para localizar ordenadores en su red. Ofrece un método práctico para añadir ordenadores nuevos a ESET Remote Administrator sin tener que buscarlos y añadirlos manualmente. En Web Console se muestran todos los ordenadores detectados en la red, que se añaden al grupo **Todos** predeterminado. Desde aquí puede realizar otras acciones con los ordenadores clientes individuales.

RD Sensor es un oyente pasivo que detecta los ordenadores que están presentes en la red y envía información sobre ellos a ERA Server. ERA Server evalúa si los PC que se encuentran en la red son desconocidos o ya están administrados.

3. Uso de ESET Endpoint Antivirus exclusivamente

Este apartado de la Guía del usuario se dirige a aquellos usuarios que utilizan ESET Endpoint Antivirus sin ESET Remote Administrator. Todas las características y funciones de ESET Endpoint Antivirus son totalmente accesibles según los derechos de la cuenta del usuario.

3.1 Instalación con ESET AV Remover

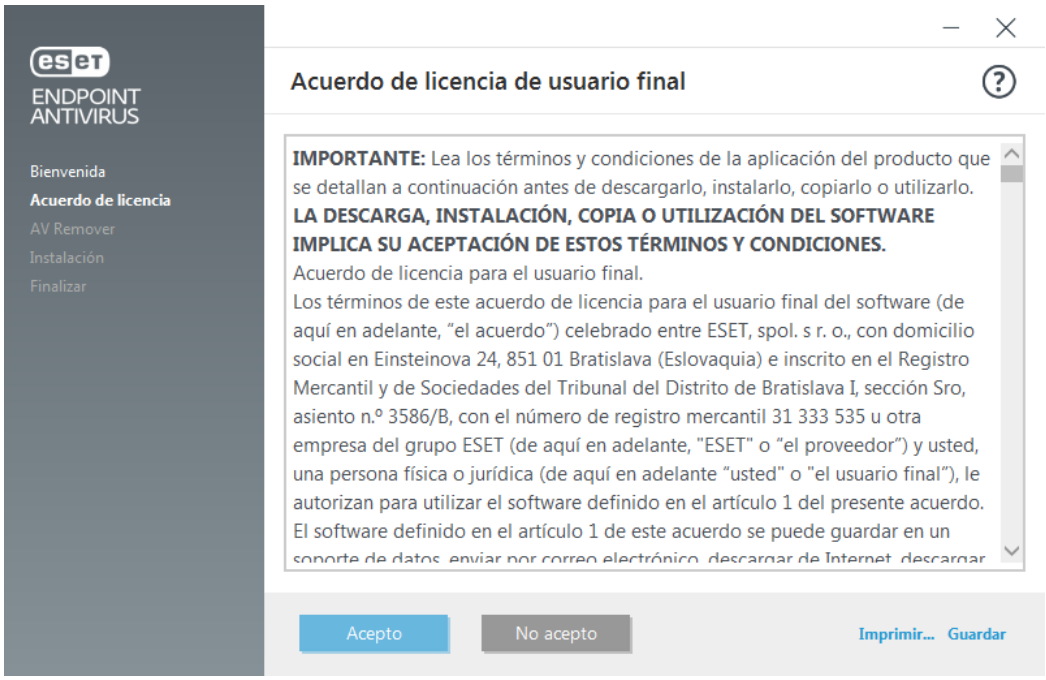
Antes de continuar con el proceso de instalación, es importante que desinstale las posibles aplicaciones de seguridad que tenga en el ordenador. Marque la casilla situada junto a **Quiero desinstalar aplicaciones antivirus con ESET AV Remover** para que ESET AV Remover analice el sistema y quite las aplicaciones de seguridad compatibles que tuviera instaladas. Mantenga la casilla desmarcada y haga clic en **Continuar** para instalar ESET Endpoint Antivirus sin ejecutar ESET AV Remover.

3.1.1 ESET AV Remover

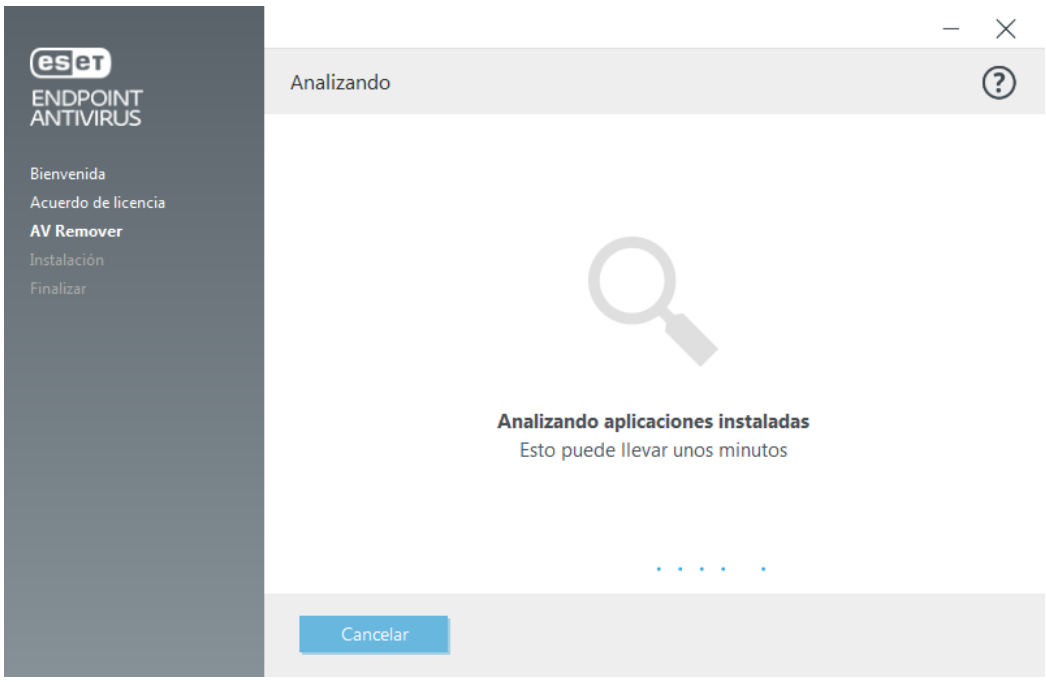
La herramienta ESET AV Remover le ayuda a eliminar casi todos los programas antivirus que haya instalado anteriormente en su sistema. Siga las instrucciones expuestas a continuación para quitar un programa antivirus existente con ESET AV Remover:

1. Para ver una lista del software antivirus que ESET AV Remover puede quitar, visite el artículo de la base de conocimiento de ESET. Descargue la herramienta independiente ESET AV Remover.

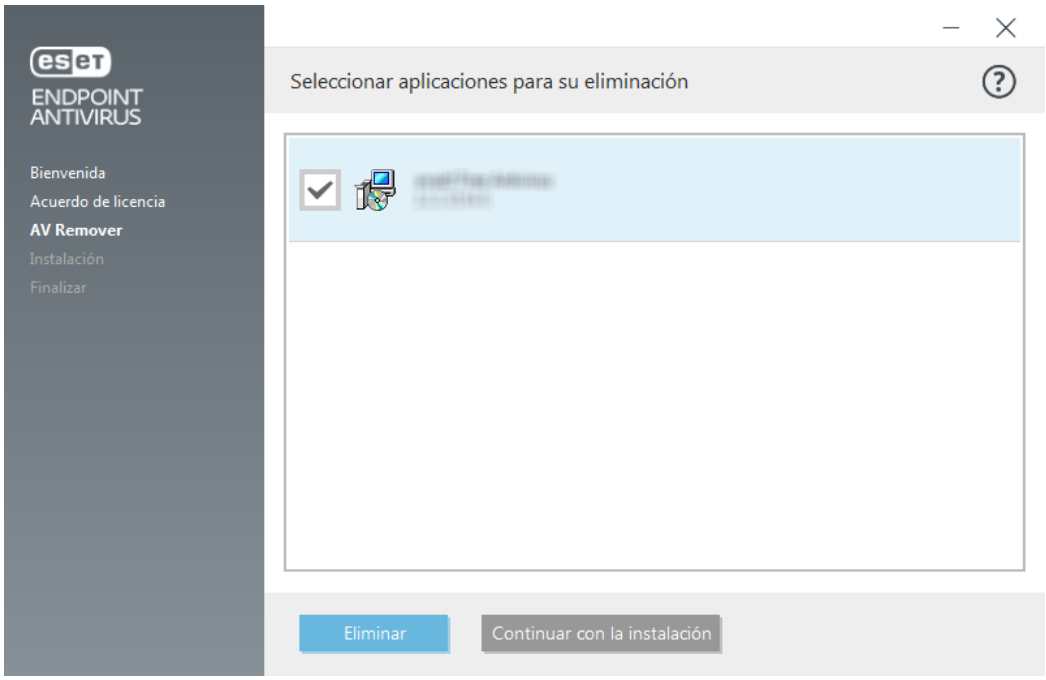
2. Lea el Acuerdo de licencia para el usuario final y haga clic en **Aceptar** para confirmar que acepta dicho acuerdo. Hacer clic en **Rechazar** finalizará la eliminación de la aplicación de seguridad existente del ordenador.



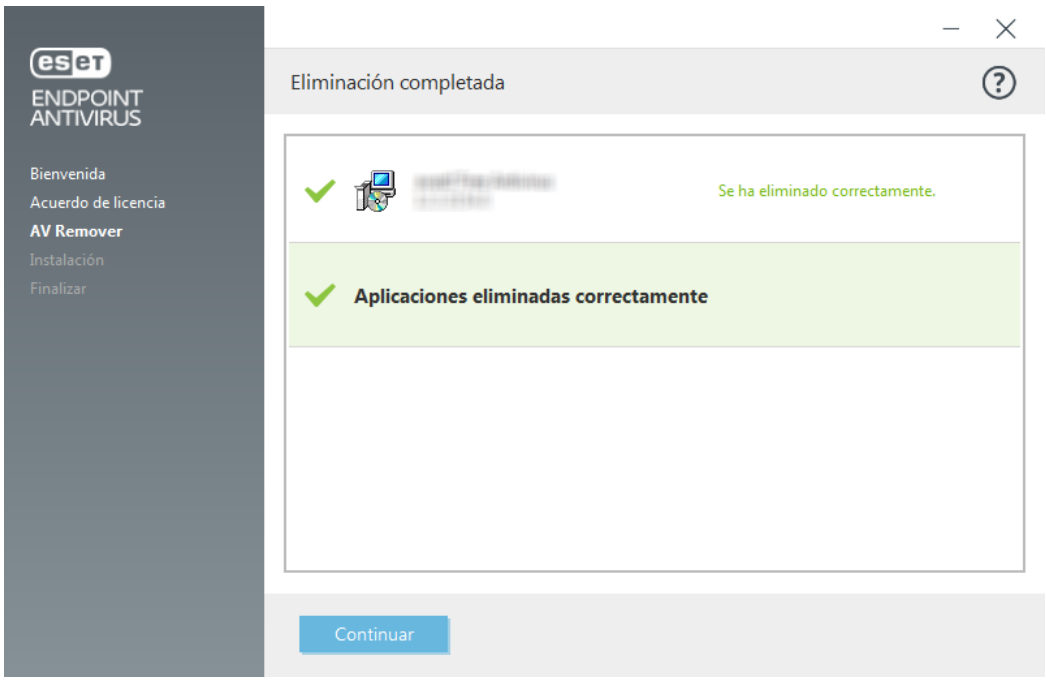
3. ESET AV Remover comenzará a buscar software antivirus en el sistema.



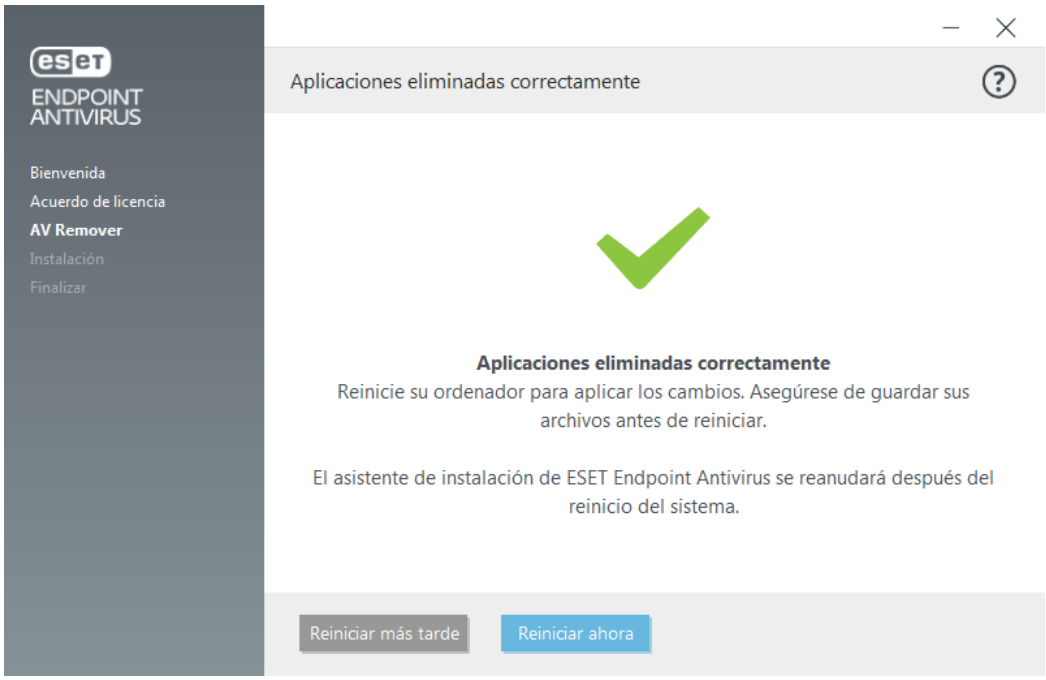
4. Seleccione las aplicaciones antivirus que aparezcan en la lista y haga clic en Quitar. Este proceso puede llevar unos minutos.



5. Una vez finalizado el procedimiento de desinstalación de aplicaciones, haga clic en **Continuar**.



6. Reinicie el ordenador para aplicar los cambios. Si la desinstalación no ha finalizado correctamente, consulte el apartado La desinstalación mediante ESET AV Remover finalizó con un error de esta guía.



3.1.2 Desinstalación mediante ESET AV Remover finalizada con error

Si no puede quitar un programa antivirus con ESET AV Remover, recibirá una notificación en la que se le indica que la aplicación que está intentando quitar podría no ser compatible con ESET AV Remover. Consulte la lista de productos compatibles o acceda a los desinstaladores de software antivirus para Windows populares en la base de conocimiento de ESET para comprobar si el programa en cuestión puede quitarse.

Si la desinstalación del producto de seguridad no se pudo completar correctamente o alguno de sus componentes se ha desinstalado solo de forma parcial, aparecerá la opción **Reiniciar y analizar de nuevo**. Confirme el Control de cuentas de usuario tras el inicio, y continúe con el proceso de análisis y desinstalación.

En caso de ser necesario, póngase en contacto con el servicio de atención al cliente de ESET para abrir una solicitud de asistencia técnica y facilitar el archivo **AppRemover.log** a los técnicos de ESET. El archivo **AppRemover.log** se encuentra en la carpeta **eset**. Desde el Explorador de Windows, diríjase a *%TEMP%* para acceder a esta carpeta. El servicio de atención al cliente de ESET responderá a la mayor brevedad posible para ayudarle a resolver el problema.

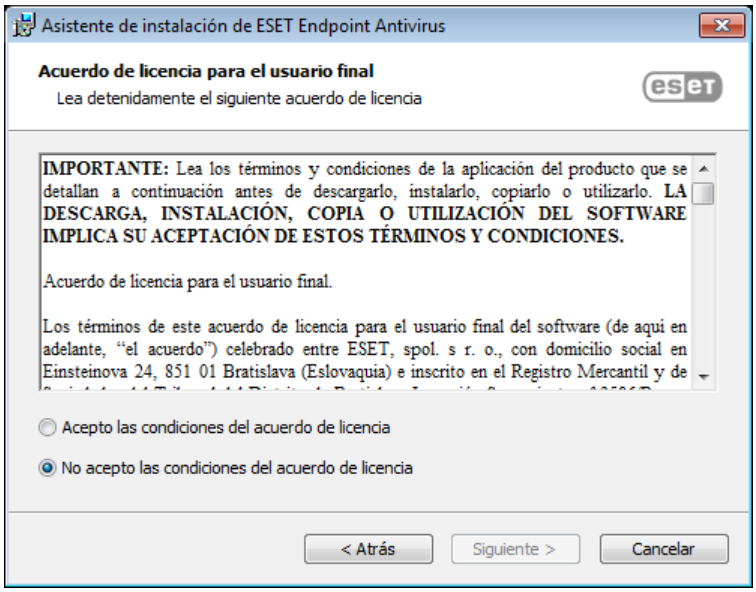
3.2 Instalación

Cuando ejecute el instalador, el asistente de instalación le proporcionará instrucciones para realizar la instalación.

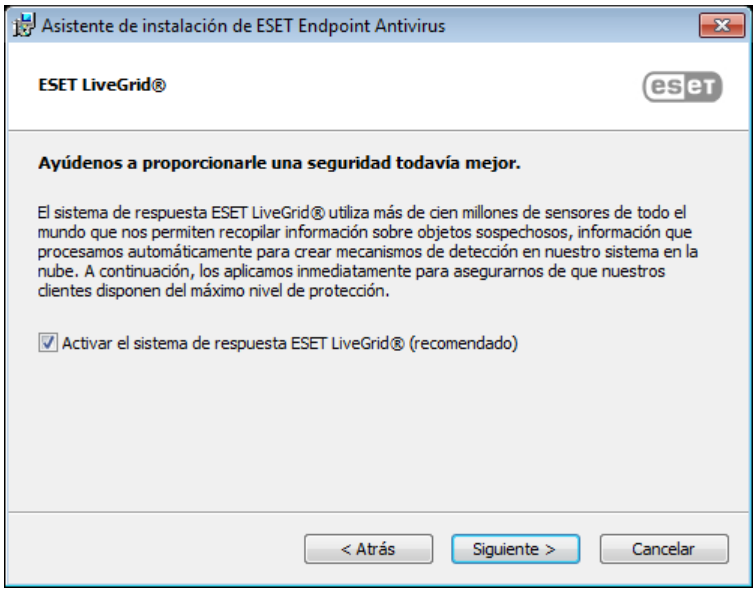
IMPORTANTE

Asegúrese de que no tiene instalados otros programas antivirus en el ordenador. Si instala más de dos soluciones antivirus en un solo ordenador, estas pueden entrar en conflicto. Le recomendamos que desinstale del sistema uno de los programas antivirus. Consulte nuestro artículo de la base de conocimiento para ver una lista de herramientas de desinstalación para software antivirus habitual (disponible en inglés y algunos otros idiomas).

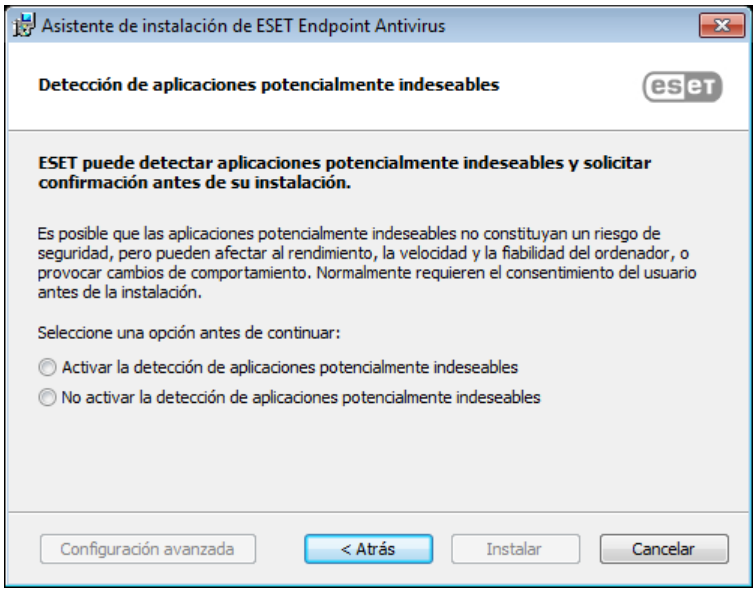
En el paso siguiente, se muestra el acuerdo de licencia para el usuario final. Léalo y haga clic en **Aceptar** para confirmar que acepta dicho acuerdo. Haga clic en **Siguiente** para aceptar los términos y continuar con la instalación.



Tras seleccionar "Acepto..." y hacer clic en **Siguiente**, se le pedirá que active el sistema de respuesta ESET LiveGrid®. ESET LiveGrid® garantiza que ESET recibe notificaciones inmediatas sobre las nuevas amenazas para que podamos proteger mejor a nuestros clientes. El sistema permite el envío de nuevas amenazas al laboratorio de virus de ESET, donde se analizan, procesan y agregan a la base de firmas de virus.



El paso siguiente del proceso de instalación consiste en configurar la detección de aplicaciones potencialmente indeseables, que no siempre son maliciosas, pero pueden perjudicar el comportamiento del sistema operativo. Consulte el capítulo Aplicaciones potencialmente indeseables para ver más detalles. Si desea acceder a más opciones de configuración, haga clic en **Configuración avanzada** (por ejemplo, para instalar su producto de ESET en una carpeta específica o activar el análisis automático tras la instalación).



El último paso es hacer clic en **Instalar** para confirmar la instalación.

3.2.1 Instalación avanzada

La instalación avanzada le permite personalizar varios parámetros de instalación que no están disponibles durante el proceso de instalación típico.

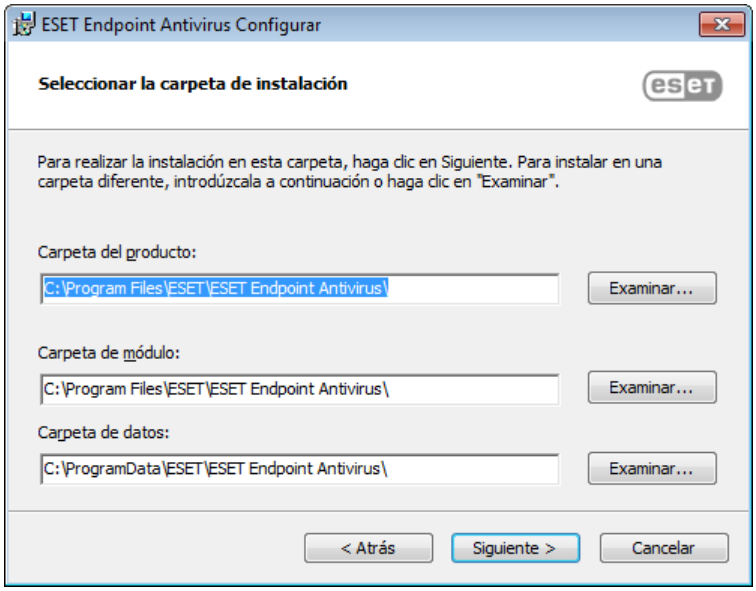
Una vez que haya seleccionado su preferencia para la detección de aplicaciones potencialmente indeseables y hecho clic en **Configuración avanzada**, se le solicitará que seleccione una ubicación para la carpeta de instalación del producto. De forma predeterminada, el programa se instala en el directorio siguiente:

C:\Archivos de programa\ESET\ESET Endpoint Antivirus

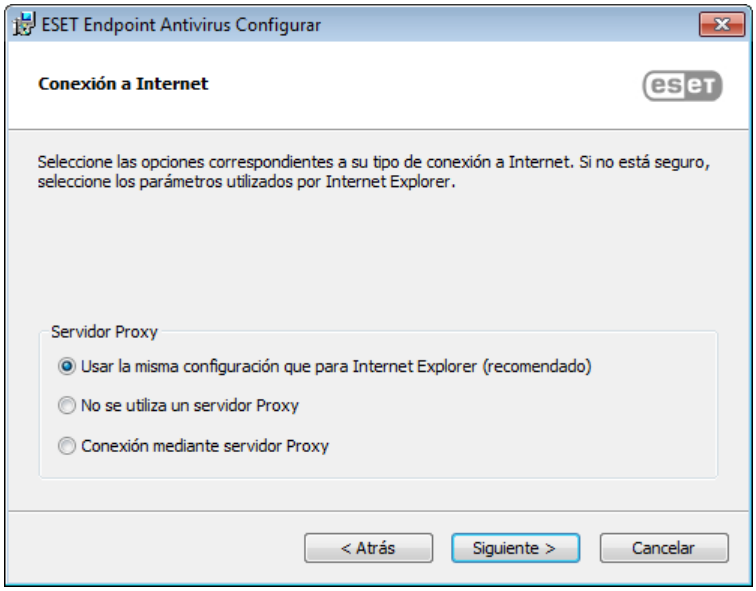
Puede especificar una ubicación para los datos y los módulos del programa. De forma predeterminada, estos se instalan en los directorios siguientes, respectivamente:

C:\Archivos de programa\ESET\ESET Endpoint Antivirus
C:\ProgramData\ESET\ESET Endpoint Antivirus

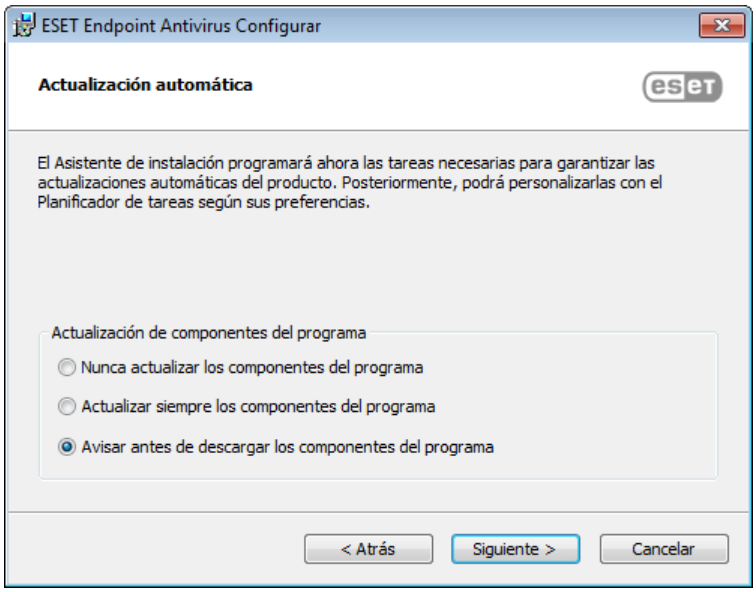
Haga clic en **Examinar** para cambiar estas ubicaciones (no recomendado).



Para configurar el servidor Proxy, seleccione **Conexión mediante servidor Proxy** y haga clic en **Siguiente**. Introduzca la dirección IP o URL de su servidor Proxy en el campo **Dirección**. Si no está seguro de si utiliza un servidor Proxy para conectarse a Internet, seleccione **Usar la misma configuración que para Internet Explorer (recomendado)** y haga clic en **Siguiente**. Si no utiliza un servidor Proxy, seleccione **No se utiliza un servidor Proxy**. Encontrará más información en Servidor Proxy.

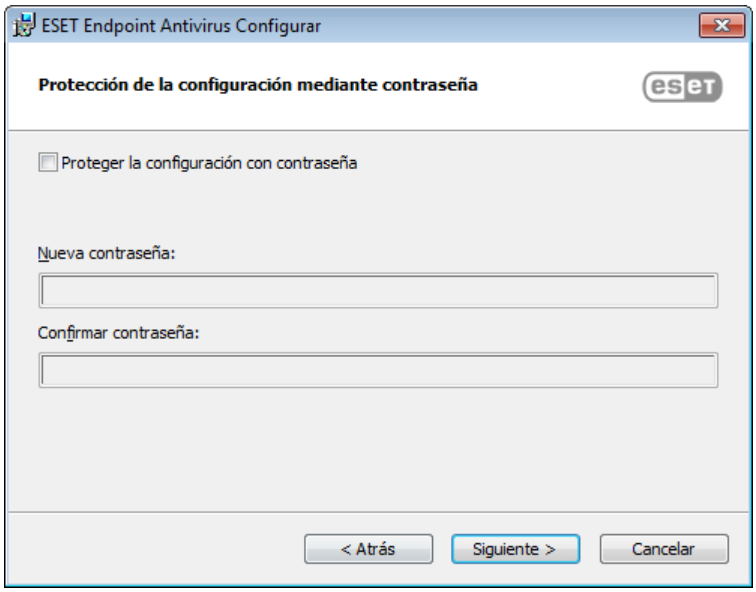


La instalación personalizada le permite definir la gestión de las actualizaciones automáticas del programa en el sistema. Haga clic en **Cambiar** para acceder a la configuración avanzada.



Si no desea que se actualicen los componentes del programa, seleccione **Nunca actualizar los componentes del programa**. Seleccione **Preguntar antes de descargar componentes del programa** para ver una ventana de confirmación cada vez que el sistema intente descargar los componentes del programa. Para descargar las actualizaciones de componentes del programa de forma automática, seleccione **Actualizar siempre los componentes del programa**.

En la próxima ventana de instalación tiene la opción de definir una contraseña para proteger la configuración del programa. Seleccione **Proteger la configuración con contraseña** e introduzca la contraseña en los campos **Contraseña nueva** y **Confirmar contraseña**. Necesitará esta contraseña para acceder a la configuración de ESET Endpoint Antivirus o cambiarla. Si ambos campos coinciden, haga clic en **Siguiente** para continuar.



Haga clic en **Instalar** para iniciar la instalación.

3.3 Instalación del producto desde ERA (línea de comandos)

Las siguientes opciones están pensadas para usarlas **solo para la interfaz de usuario con nivel reducido**, **básico y ninguno**. Consulte la documentación de la versión de **msiexec** utilizada para los modificadores correspondientes de la línea de comandos.

Parámetros admitidos:

APPDIR=<ruta de acceso>
- ruta de acceso: ruta de acceso de un directorio válido
- Directorio de instalación de la aplicación.
- Por ejemplo: `ees_nt64_ENU.msi /qn APPDIR=C:\ESET\ ADDLOCAL=DocumentProtection`

APPDATADIR=<ruta de acceso>
- ruta de acceso: ruta de acceso de un directorio válido
- Directorio de instalación de los datos de la aplicación.

MODULEDIR=<ruta de acceso>
- ruta de acceso: ruta de acceso de un directorio válido
- Directorio de instalación del módulo.

ADDLOCAL=<lista>
- Instalación de componentes: lista de características no obligatorias que se pueden instalar localmente.
- Uso con los paquetes .msi de ESET: `ees_nt64_ENU.msi /qn ADDLOCAL=<list>`
- Para obtener más información sobre la propiedad ADDLOCAL, consulte https://msdn.microsoft.com/es-es/library/aa367536(v=vs.85).aspx

Reglas

- La **lista ADDLOCAL** es una lista separada por comas de los nombres de todas las características que se van a instalar.
- Al seleccionar una característica para instalarla, se debe incluir en la lista y de forma explícita toda la ruta de acceso (todas las características principales).
- Consulte las reglas adicionales para obtener la información sobre el uso correcto.

Presencia de características

- **Obligatoria**: la característica se instalará siempre.
- **Opcional**: la característica puede no seleccionarse para no instalarla.
- **Invisible**: característica lógica obligatoria para que otras características funcionen correctamente.
- **Marcador de posición**: característica que no tiene repercusión en el producto, pero que debe incluirse con características secundarias.

El árbol de características de Endpoint 6.1 es el siguiente:

Árbol de características	Nombre de la característica	Presencia de características
Ordenador	Ordenador	Obligatoria
Ordenador/Antivirus y antispyware	Antivirus	Obligatoria
Ordenador/Antivirus y antispyware > Protección del sistema de archivos en tiempo real	RealtimeProtection	Obligatoria
Ordenador/Antivirus y antispyware > Análisis del ordenador	Analizar	Obligatoria
Ordenador/Antivirus y antispyware > Protección de documentos	Protección de documentos	Opcional
Control del ordenador/dispositivo	DeviceControl	Opcional
Red	Red	Marcador de posición
Red/Cortafuegos	Cortafuegos	Opcional
Web y correo electrónico	WebAndEmail	Marcador de posición

Filtrado de protocolos de web y correo electrónico	ProtocolFiltering	Invisible
Protección de la web y el correo electrónico/acceso a la web	WebAccessProtection	Opcional
Protección de la web y el correo electrónico/cliente de correo electrónico	EmailClientProtection	Opcional
Protección de la web y el correo electrónico/cliente de correo electrónico/complementos de correo electrónico	MailPlugins	Invisible
Protección de la web y el correo electrónico/cliente de correo electrónico/antispam	Antispam	Opcional
Control de la web y el correo electrónico/web	WebControl	Opcional
Mirror de actualización	UpdateMirror	Opcional
Asistencia técnica de Microsoft NAP	MicrosoftNAP	Opcional

Reglas adicionales

- Si se selecciona alguna de las características de **WebAndEmail** para su instalación, la característica invisible **ProtocolFiltering** debe incluirse en la lista de forma explícita.
- Si se selecciona alguna de las características secundarias **EmailClientProtection** para su instalación, la característica invisible **MailPlugins** debe incluirse en la lista de forma explícita.

Ejemplos:

```
ees_nt64_ENU.msi /qn ADDLOCAL=WebAndEmail,WebAccessProtection,ProtocolFiltering
```

```
ees_nt64_ENU.msi /qn ADDLOCAL=WebAndEmail,EmailClientProtection,Antispam,MailPlugins
```

Lista de propiedades CFG_:

CFG_POTENTIALLYUNWANTED_ENABLED=1/0
• 0: desactivado, 1: activado
• PUA

CFG_LIVEGRID_ENABLED=1/0
• 0: desactivado, 1: activado
• LiveGrid

CFG_EPFW_MODE=0/1/2/3
• 0: automático, 1: interactivo, 2: política, 3: aprendizaje

CFG_PROXY_ENABLED=0/1
• 0: desactivado, 1: activado

CFG_PROXY_ADDRESS=<ip>
• Dirección IP proxy.

CFG_PROXY_PORT=<puerto>
• Número de puerto de proxy.

CFG_PROXY_USERNAME=<usuario>
• Nombre de usuario para autenticación.

CFG_PROXY_PASSWORD=<contraseña>
• Contraseña de autenticación.

Instalación mediante SCCM, desactivar cuadro de diálogo de activación:

ACTIVATION_DLG_SUPPRESS=1
• 1 - Activado (no se muestra el cuadro de diálogo de activación)
• 0 - Desactivado (se muestra el cuadro de diálogo de activación)

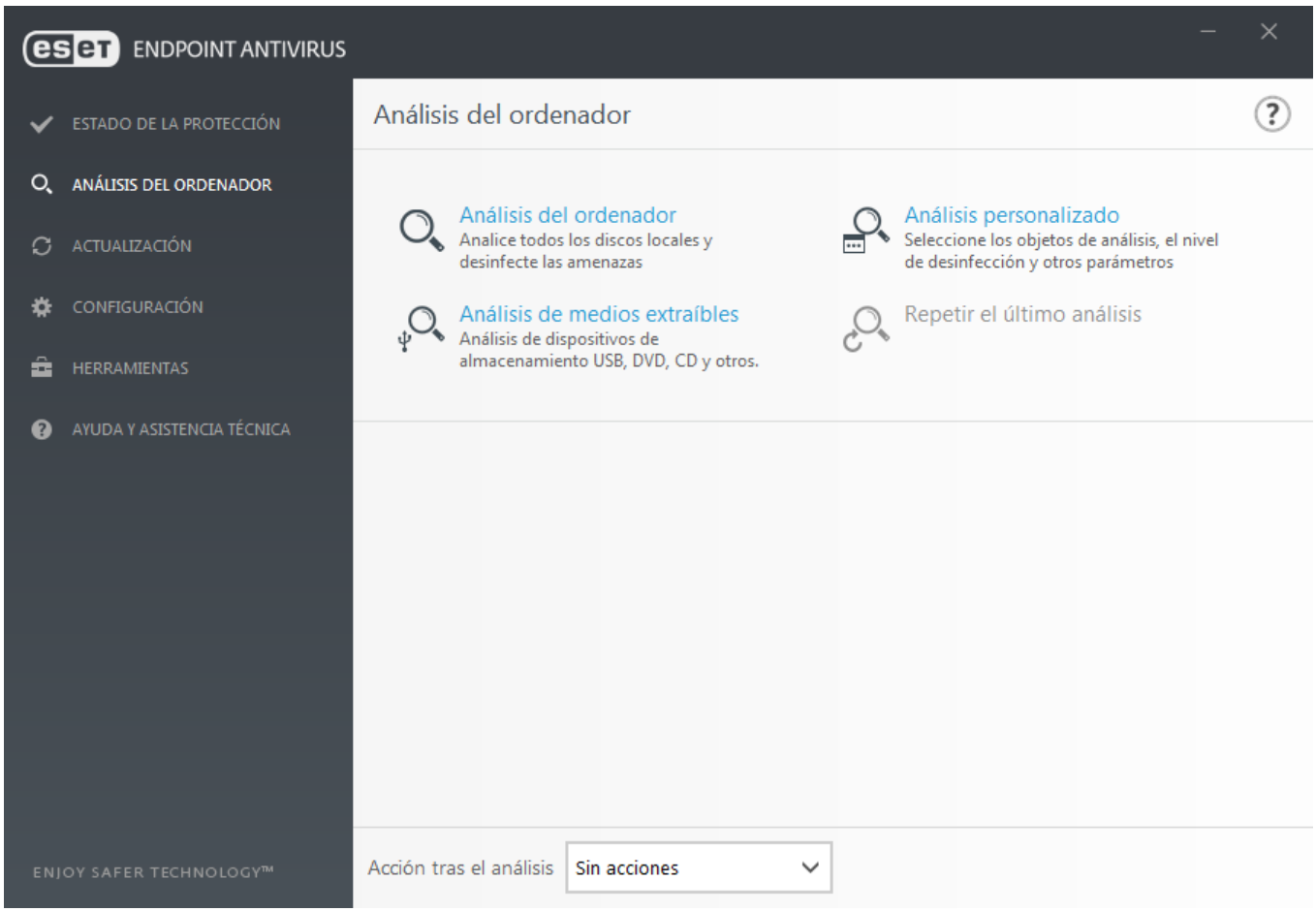
3.4 Activación del producto

Cuando haya finalizado la instalación, se le solicitará que active el producto.

Seleccione uno de los métodos disponibles para activar ESET Endpoint Antivirus. Consulte Cómo activar ESET Endpoint Antivirus para obtener más información.

3.5 Análisis del ordenador

Le recomendamos que realice análisis periódicos del ordenador, o programe un análisis periódico, para detectar amenazas. En la ventana principal del programa, haga clic en **Análisis del ordenador** y, a continuación, en **Análisis estándar**. Encontrará más información sobre los análisis del ordenador en Análisis del ordenador.



3.6 Actualización a una versión más reciente

Las versiones nuevas de ESET Endpoint Antivirus ofrecen mejoras o solucionan problemas que no se pueden arreglar con las actualizaciones automáticas de los módulos de programa. La actualización a una versión más reciente se puede realizar de varias maneras:

1. Actualización automática mediante una actualización del programa.
   Las actualizaciones del programa se distribuyen a todos los usuarios y pueden afectar a determinadas configuraciones del sistema, de modo que se envían tras un largo período de pruebas que garantizan su correcto funcionamiento en todas las configuraciones posibles del sistema. Si necesita instalar una versión más reciente en cuanto se publica, utilice uno de los métodos que se indican a continuación.
2. Actualización manual mediante la descarga e instalación de una versión más reciente sobre la instalación existente.
3. Actualización manual, a través de la implementación automática en un entorno de red mediante ESET Remote Administrator.

3.7 Guía para principiantes

En este capítulo se proporciona una descripción general inicial de ESET Endpoint Antivirus y su configuración básica.

3.7.1 Interfaz de usuario

La ventana principal del programa ESET Endpoint Antivirus se divide en dos secciones principales. En la ventana principal, situada a la derecha, se muestra información relativa a la opción seleccionada en el menú principal de la izquierda.

A continuación, se muestra una descripción de las opciones del menú principal:

Estado de la protección: proporciona información sobre el estado de protección de ESET Endpoint Antivirus.

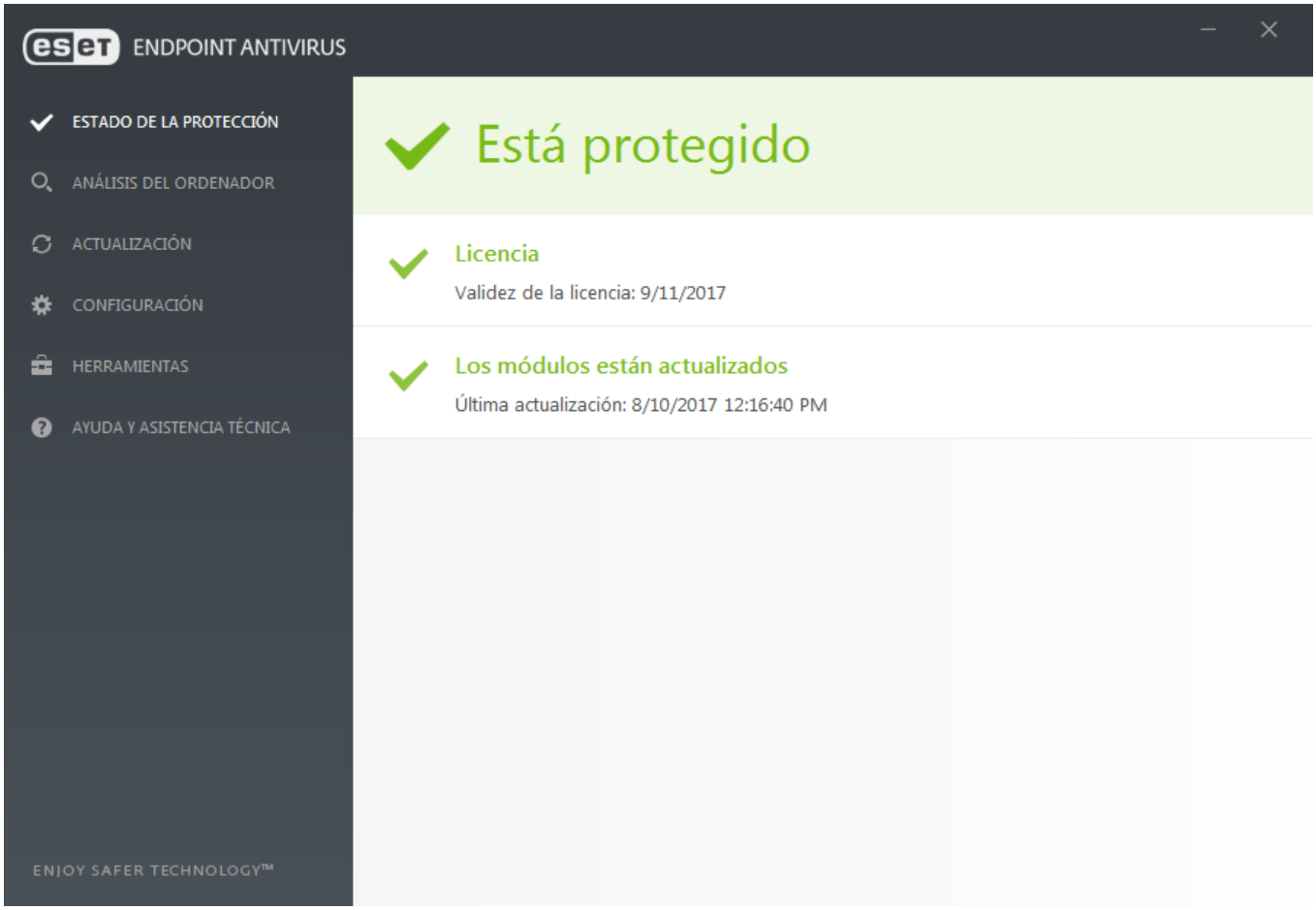
Análisis del ordenador: esta opción le permite configurar e iniciar el análisis estándar, el análisis personalizado o el análisis de medios extraíbles. También se puede repetir el último análisis ejecutado.

Actualización: muestra información sobre el motor de detección.

Configuración: seleccione esta opción para ajustar su ordenador o configuración de seguridad de la Web y el correo electrónico.

Herramientas: proporciona acceso a Archivos de registro, Estadísticas de protección, Observar actividad, Procesos en ejecución, Planificador de tareas, Cuarentena, ESET SysInspector y ESET SysRescue para crear un CD de recuperación. También puede enviar una muestra para su análisis.

Ayuda y asistencia técnica: proporciona acceso a los archivos de ayuda, la base de conocimiento de ESET y el sitio web de ESET. Aquí también se proporcionan enlaces para abrir una solicitud de soporte de atención al cliente, herramientas de soporte e información sobre la actividad del producto.

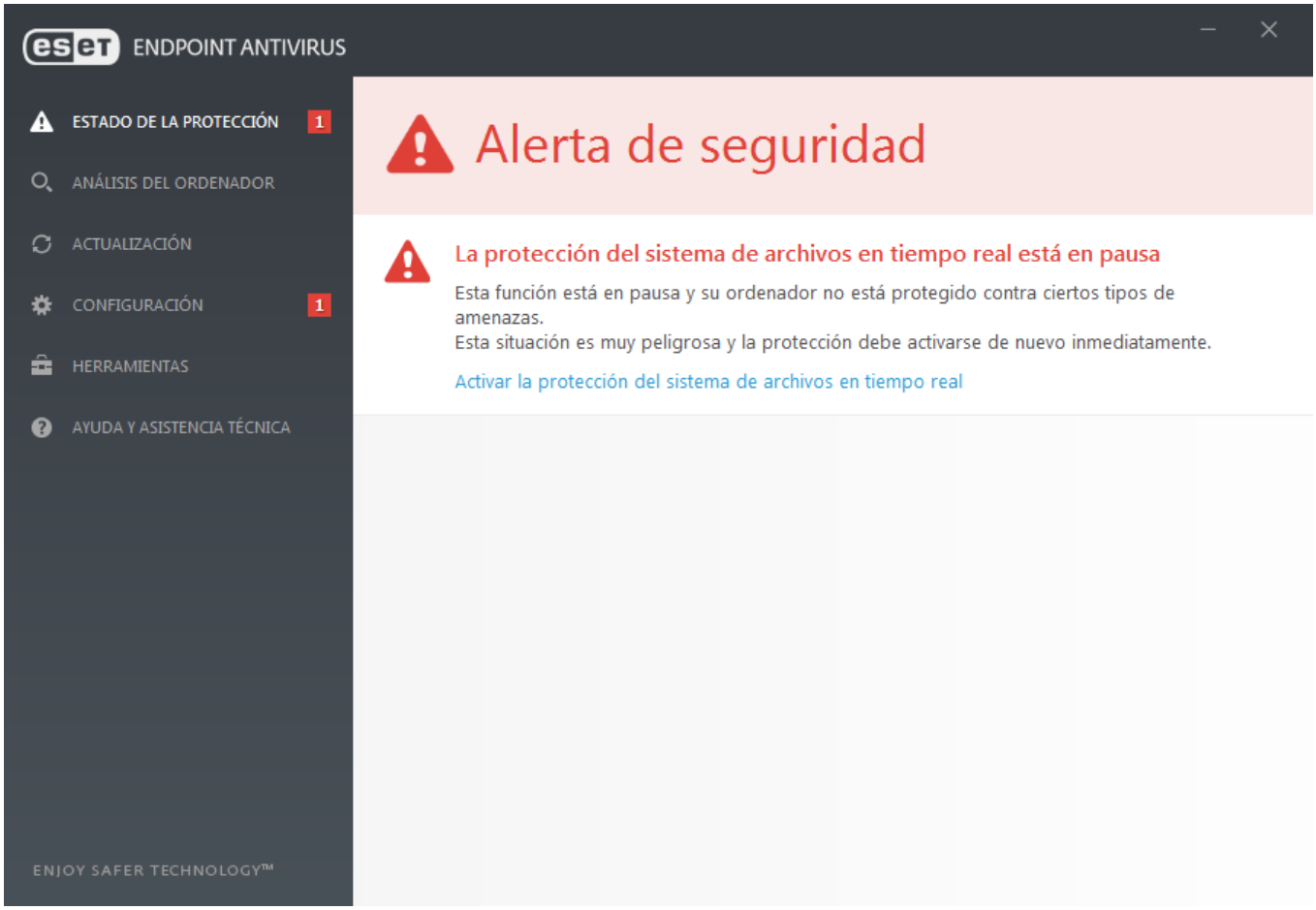


En la pantalla **Estado de la protección** se proporciona información sobre el nivel de seguridad y de protección actual del ordenador. El icono de estado verde de **Máxima protección** indica que se garantiza la protección máxima.

En la ventana de estado también se proporcionan enlaces rápidos a las características más habituales de ESET Endpoint Antivirus e información sobre la última actualización.

¿Qué hacer si el programa no funciona correctamente?

Una marca de verificación verde aparecerá junto a todos los módulos del programa que estén totalmente operativos. Si un módulo necesita atención, aparecerá un signo de exclamación rojo o un icono de notificación naranja. En la parte superior de la ventana aparecerá información adicional sobre el módulo, incluyendo nuestra recomendación sobre cómo restaurar todas las funcionalidades. Para cambiar el estado de un módulo, haga clic en **Configuración** en el menú principal y, a continuación, en el módulo deseado.



 El icono del signo de exclamación rojo (!) indica que no se garantiza la protección máxima del ordenador. Podría encontrarse con este tipo de notificación en las siguientes situaciones:

- **La protección antivirus y antiespía está en pausa**: haga clic en **Iniciar todos los módulos de protección antivirus y antispyware** para volver a activar la protección antivirus y antiespía en el panel **Estado de protección** o **Activar la protección antivirus y antiespía** en el panel **Configuración** en la ventana principal del programa.
- **La protección antivirus no está operativa**: se ha producido un error al inicializar el análisis de virus. La mayoría de los módulos de ESET Endpoint Antivirus no funcionarán correctamente.
- **La protección Anti-Phishing no está operativa**: esta función no está operativa porque otros módulos necesarios del programa no están activos.
- **El Motor de detección está obsoleto**: está utilizando un motor de detección obsoleto. Actualice el motor de detección.
- **El producto no está activado** o **La licencia ha expirado**: esto se indica mediante el icono de estado de la protección, que se vuelve rojo. Una vez que expire la licencia, el programa no se puede actualizar. Le recomendamos que siga las instrucciones de la ventana de alerta para renovar la licencia.
- **El sistema de prevención de intrusiones basado en el host (HIPS) está desactivado**: este problema se indica cuando HIPS está desactivado en Configuración avanzada. Su ordenador no está protegido contra ciertos tipos de amenazas y la protección debería volver a activarse de forma inmediata haciendo clic en **Activar HIPS**.
- **ESET LiveGrid® está desactivado**: este problema se indica cuando ESET LiveGrid® está desactivado en Configuración avanzada.
- **No hay actualizaciones regulares programadas**: ESET Endpoint Antivirus no buscará ni recibirá actualizaciones importantes a menos que programe la tarea de actualización.
- **Anti-Stealth está desactivado**: haga clic en **Activar Anti-Stealth** para volver a activar esta funcionalidad.
- **La protección del sistema de archivos en tiempo real está en pausa**: el usuario desactivó la protección en tiempo real. Su ordenador no está protegido frente a amenazas. Haga clic en **Activar protección en tiempo real** para volver a activar esta funcionalidad.

 La "i" naranja indica que un problema no grave del producto de ESET requiere su atención. Los posibles motivos son:

- **La protección del tráfico de Internet está desactivada**: haga clic en la notificación de seguridad para volver a activar la protección del tráfico de Internet y, a continuación, haga clic en **Activar la protección del acceso a la Web**.
- **Su licencia caducará en breve**: esto se indica mediante el icono de estado de la protección, que muestra un signo de exclamación. Cuando expire la licencia, el programa no se podrá actualizar y el icono del estado de la protección se volverá rojo.
- **La protección antispam está en pausa**: haga clic en **Habilitar la protección antispam** para volver a activar esta función.
- **El Control web está en pausa**: haga clic en **Habilitar control de acceso web** para volver a activar esta función.
- **Anulación de política activa**: la configuración definida por la política está anulada temporalmente, posiblemente hasta que finalice la solución de problemas. Solo el usuario autorizado podrá anular la configuración de la política. Para obtener más información, consulte Cómo utilizar el modo de anulación.
- **Se pausó el control de dispositivos**: haga clic en **Activar el control de dispositivos** para volver a activar esta función.

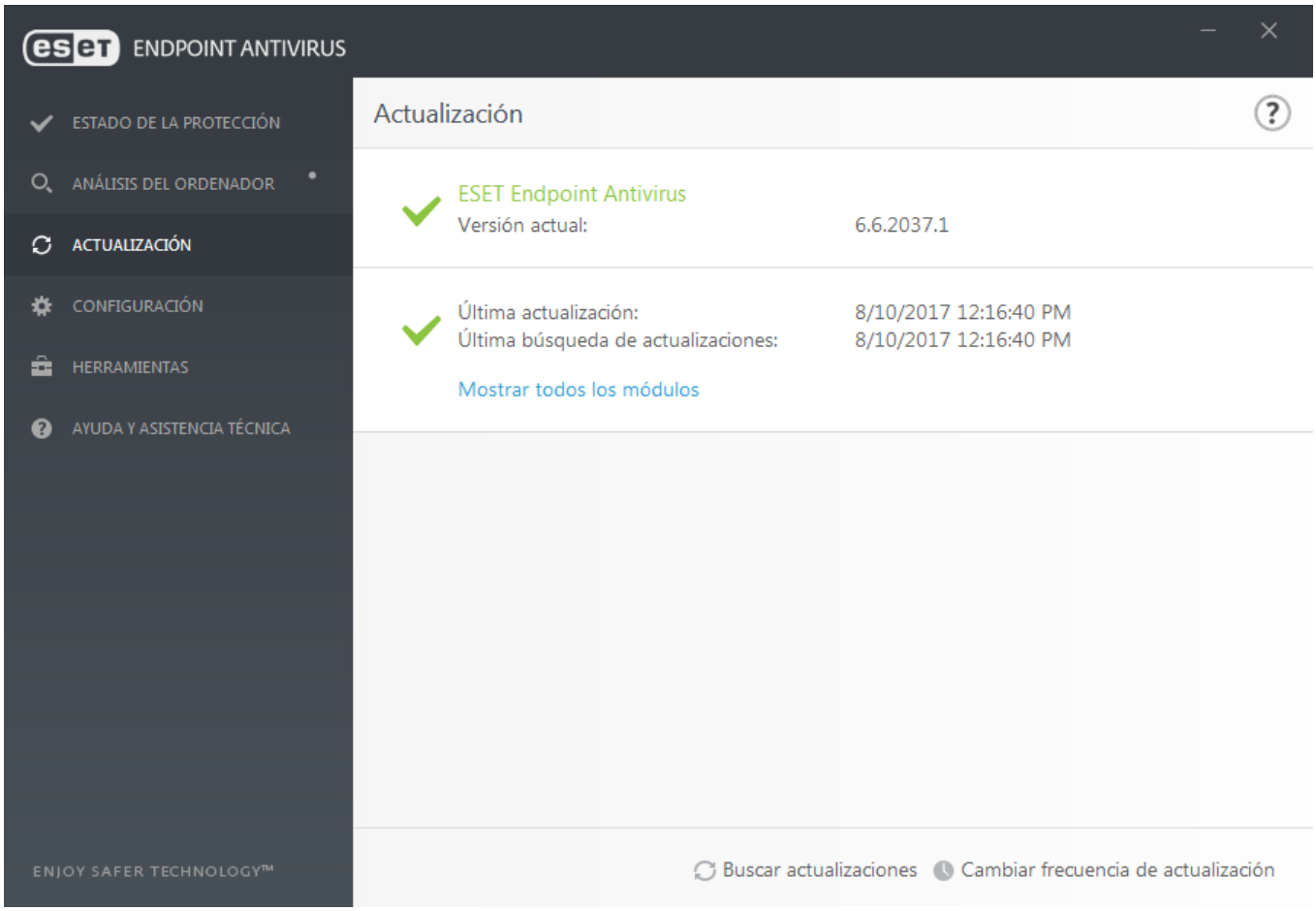
Si no consigue solucionar el problema con estas sugerencias, haga clic en **Ayuda y asistencia técnica** para acceder a los archivos de ayuda o realice una búsqueda en la base de conocimiento de ESET. Si sigue necesitando ayuda, puede enviar una solicitud de atención al cliente de ESET. El servicio de atención al cliente de ESET responderá a sus preguntas y le ayudará a encontrar una solución rápidamente.

NOTA
Si un estado pertenece a una función bloqueada por la política de ERA, no podrá hacer clic en el enlace.

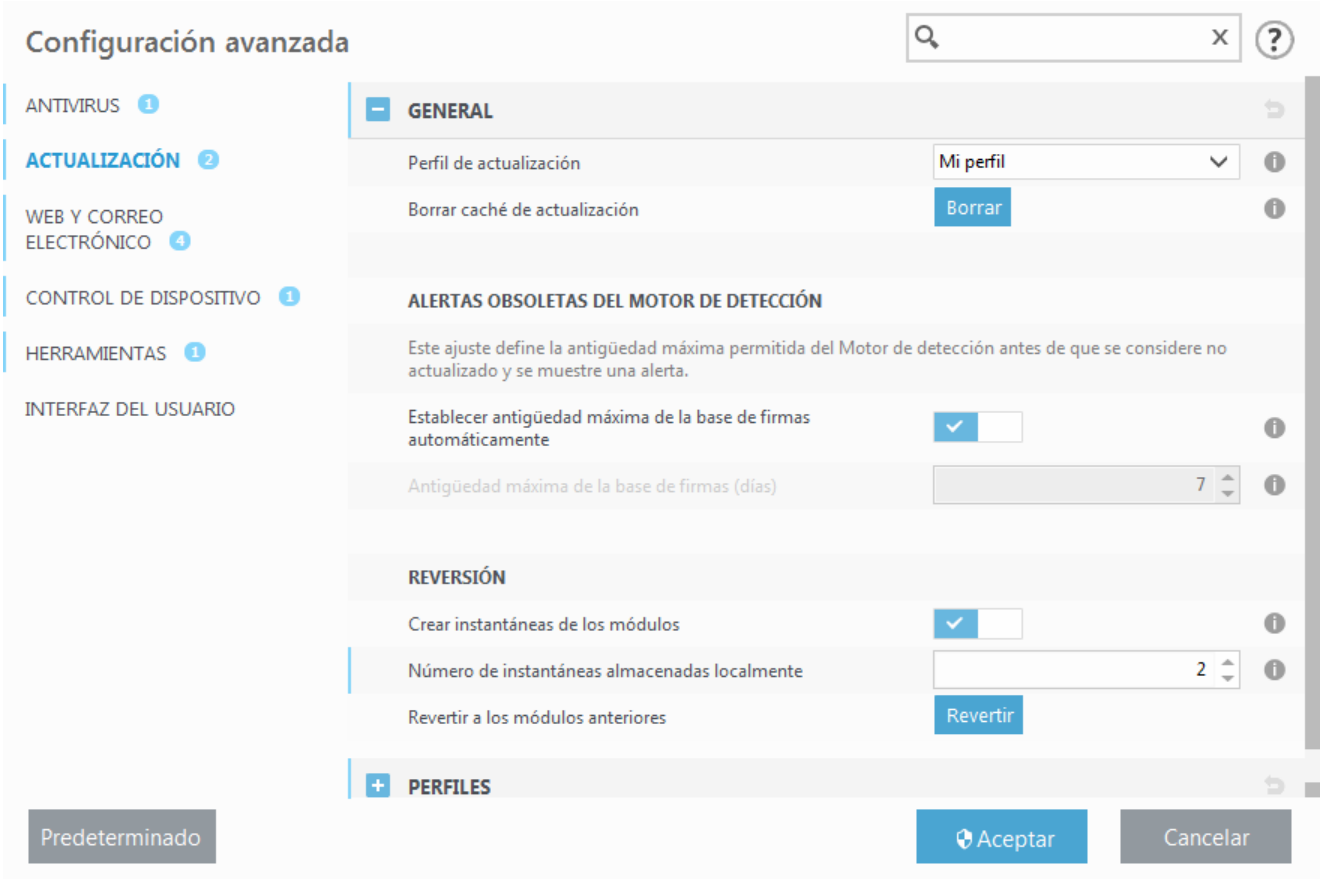
3.7.2 Configuración de actualizaciones

La actualización de los módulos es una parte importante de mantener una protección completa contra el código malicioso. Preste especial atención a la configuración y al funcionamiento de las actualizaciones. En el menú principal, seleccione **Actualizar** > **Actualizar ahora** para comprobar si hay alguna actualización de los módulos más reciente.

Si no introduce su **Clave de licencia**, no podrá recibir actualizaciones nuevas y se le pedirá que active su producto.



La ventana Configuración avanzada (haga clic en **Configuración** > **Configuración avanzada** en el menú principal o pulse **F5** en el teclado) ofrece más opciones de actualización. Para configurar las opciones avanzadas de actualización, como el modo de actualización, el acceso al servidor Proxy, las conexiones de red local y la creación de copias del motor de detección, haga clic en el botón **Actualización** del árbol de configuración avanzada. Si tiene problemas con la actualización, haga clic en el botón **Borrar** para vaciar la caché de actualización temporal. El menú **Servidor de actualización** está establecido en **AUTOSELECT** de forma predeterminada. Si utiliza un servidor ESET, le recomendamos que deje seleccionada la opción **Elegir automáticamente**. Si no desea que aparezca la notificación de la bandeja del sistema en la esquina inferior derecha de la pantalla, seleccione **Desactivar la notificación de la actualización correcta**.



Para optimizar la funcionalidad, es importante que el programa se actualice automáticamente. Esto solo es posible si se introduce la **clave de licencia** correcta en **Ayuda y asistencia técnica** > **Activar producto**.

Si no introdujo la **clave de licencia** tras la instalación, puede hacerlo en cualquier momento. Para obtener más información detallada sobre la activación, consulte Cómo activar ESET Endpoint Antivirus e introduzca las credenciales que recibió al adquirir el producto de seguridad de ESET en la ventana **Detalles de la licencia**.

3.8 Preguntas habituales

Este capítulo abarca algunas de las preguntas más frecuentes y los problemas encontrados. Haga clic en el título del tema para obtener información sobre cómo solucionar el problema:

Cómo actualizar ESET Endpoint Antivirus
Cómo activar ESET Endpoint Antivirus
Cómo utilizar las credenciales actuales para activar un producto nuevo
Cómo eliminar un virus de mi PC
Cómo crear una tarea nueva en Tareas programadas
Cómo programar una tarea de análisis (cada 24 horas)
Cómo conectar mi producto a ESET Remote Administrator
Cómo configurar un Mirror

Si no encuentra su problema en las páginas de ayuda anteriores, realice una búsqueda por palabra clave o por frase para describir el problema en las páginas de Ayuda de ESET Endpoint Antivirus.

Si no encuentra la solución a su problema o consulta en las páginas de Ayuda, consulte la base de conocimiento de ESET, donde encontrará respuesta a las preguntas y los problemas más habituales.

¿Cómo puedo eliminar el troyano Sirefef (ZeroAccess)?
Lista de comprobación para la solución de problemas del mirror de actualización
¿Qué direcciones y puertos del cortafuegos de terceros debo abrir para garantizar la compatibilidad con todas las funciones de mi producto de ESET?

Si es necesario, puede ponerse en contacto con nuestro centro de soporte técnico en línea para comunicarle sus consultas o problemas. El vínculo al formulario de contacto a través de Internet está disponible en el panel **Ayuda y soporte** de la ventana principal del programa.

3.8.1 Cómo actualizar ESET Endpoint Antivirus

ESET Endpoint Antivirus se puede actualizar de forma manual o automática. Para activar la actualización, haga clic en **Activar ahora** en la sección **Actualizar** del menú principal.

Los parámetros de instalación predeterminados crean una tarea de actualización automática que se lleva a cabo cada hora. Para cambiar el intervalo, vaya a **Herramientas** > **Planificador de tareas** (para obtener más información sobre el Planificador de tareas, haga clic aquí).

3.8.2 Cómo activar ESET Endpoint Antivirus

Cuando haya finalizado la instalación, se le solicitará que active el producto.

Hay varios métodos de activar su producto. La disponibilidad de una situación concreta de activación en la ventana de activación puede variar en función del país, además de los medios de distribución (CD/DVD, página web de ESET, etc.).

Para activar su copia de ESET Endpoint Antivirus directamente desde el programa, haga clic en el icono de la bandeja del sistema y seleccione **Activar licencia del producto** en el menú. El producto también se puede activar desde el menú principal, en **Ayuda y asistencia técnica** > **Activar producto** o **Estado de la protección** > **Activar producto**.

Puede utilizar cualquiera de estos métodos para activar ESET Endpoint Antivirus:

- **Clave de licencia**: se trata de una cadena única que presenta el formato XXXX-XXXX-XXXX-XXXX-XXXX y sirve para identificar al propietario de la licencia y activar la licencia.
- **Administrador de seguridad**: es una cuenta creada en el portal de ESET License Administrator con credenciales (dirección de correo electrónico y contraseña). Este método le permite gestionar varias licencias desde una ubicación.
- **Archivo de licencia sin conexión**: se trata de un archivo generado automáticamente que se transferirá al producto de ESET para proporcionar información sobre la licencia. Si una licencia le permite descargar un archivo de licencia (.lf) sin conexión, ese archivo se puede utilizar para realizar la activación sin conexión. El número de licencias sin conexión se restará del número total de licencias disponibles. Si desea obtener más información sobre la generación de un archivo sin conexión, consulte la Guía del usuario de ESET License Administrator.

Haga clic en **Activar más tarde** si su ordenador es miembro de una red administrada y el administrador realizará la activación remota desde ESET Remote Administrator. Si desea activar este cliente más tarde, también puede usar esta opción.

Si dispone de un nombre de usuario y una contraseña y no conoce cómo activar ESET Endpoint Antivirus, haga clic en **Tengo un nombre de usuario y una contraseña, ¿qué tengo que hacer?**. Se le redirigirá a ESET License Administrator, donde puede convertir sus credenciales en una clave de licencia.

Puede cambiar su licencia del producto en cualquier momento. Para ello, haga clic en **Ayuda y asistencia técnica** > **Administrar licencia** en la ventana principal del programa. Verá el ID de la licencia pública utilizado para que ESET identifique su producto y para que el servicio de soporte técnico de ESET identifique la licencia. El nombre de usuario con el que se ha registrado el ordenador en la sección **Acerca de**; esta puede mostrarse al hacer clic con el botón derecho del ratón en el icono de la bandeja del sistema.

NOTA
ESET Remote Administrator puede activar ordenadores cliente de forma silenciosa con las licencias que le proporcione el administrador. Si desea acceder a instrucciones para ello, consulte la ESET Remote Administrator Guía del usuario.

3.8.3 Cómo utilizar las credenciales actuales para activar un producto nuevo

Si ya tiene un nombre de usuario y una contraseña y desea recibir una clave de licencia, visite el portal de ESET License Administrator, donde puede convertir sus credenciales en una nueva clave de licencia.

3.8.4 Cómo eliminar un virus de mi PC

Si su ordenador muestra señales de una infección por código malicioso, por ejemplo, es más lento o se bloquea a menudo, se recomienda que haga lo siguiente:

1. En la ventana principal del programa, haga clic en **Análisis del ordenador**.
2. Haga clic en **Análisis estándar** para iniciar la exploración del sistema.
3. Una vez finalizado el análisis, revise el registro con el número de archivos analizados, infectados y desinfectados.
4. Si solo desea analizar determinadas partes del disco, haga clic en **Análisis personalizado** y especifique los objetos que desee analizar en busca de virus.

Si desea información adicional, visite nuestro artículo de la base de conocimientos de ESET, que se actualiza periódicamente.

3.8.5 Cómo crear una tarea nueva en el Planificador de tareas

Para crear una tarea nueva en **Herramientas** > **Planificador de tareas**, haga clic en **Agregar tarea** o haga clic con el botón derecho y seleccione **Agregar** en el menú contextual. Están disponibles cinco tipos de tareas programadas:

- **Ejecutar aplicación externa**: programa la ejecución de una aplicación externa.
- **Mantenimiento de registros**: los archivos de registro también contienen restos de los registros eliminados. Esta tarea optimiza periódicamente los registros incluidos en los archivos para aumentar su eficacia.
- **Verificación de archivos en el inicio del sistema**: comprueba los archivos que se pueden ejecutar al encender o iniciar el sistema.
- **Crear un informe del estado del sistema**: crea una instantánea del ordenador de ESET SysInspector recopila información detallada sobre los componentes del sistema (por ejemplo controladores, aplicaciones) y evalúa el nivel de riesgo de cada componente.
- **Análisis del ordenador a petición**: analiza los archivos y las carpetas del ordenador.
- **Actualización**: programa una tarea de actualización mediante la actualización de los módulos.

La **actualización** es una de las tareas programadas más frecuentes, por lo que a continuación explicaremos cómo se agrega una nueva tarea de actualización:

En el menú desplegable **Tarea programada**, seleccione **Actualización**. Introduzca el nombre de la tarea en el campo **Nombre de la tarea** y haga clic en **Siguiente**. Seleccione la frecuencia de la tarea. Están disponibles las opciones siguientes: **Una vez**, **Reiteradamente**, **Diariamente**, **Semanalmente** y **Cuando se cumpla la condición.** Seleccione **No ejecutar la tarea si está funcionando con batería** para minimizar los recursos del sistema mientras un ordenador portátil esté funcionando con batería. La tarea se ejecutará en la fecha y hora especificadas en el campo **Ejecución de la tarea**. A continuación, defina la acción que debe llevarse a cabo si la tarea no se puede realizar o completar a la hora programada. Están disponibles las opciones siguientes:

- **En la siguiente hora programada**
- **Lo antes posible**
- **Inmediatamente, si la hora desde la última ejecución excede un valor especificado** (el intervalo se puede definir con el cuadro **Tiempo desde la última ejecución**)

En el paso siguiente, se muestra una ventana de resumen que contiene información acerca de la tarea programada actualmente. Haga clic en **Finalizar** cuando haya terminado de hacer cambios.

Aparecerá un cuadro de diálogo que permite al usuario elegir los perfiles que desea utilizar para la tarea programada. Aquí puede definir los perfiles principal y alternativo. El perfil alternativo se utiliza cuando la tarea no se puede completar con el perfil principal. Haga clic en **Finalizar** para confirmar la operación; la nueva tarea se agregará a la lista de tareas programadas actualmente.

3.8.6 Cómo programar una tarea de análisis (cada 24 horas)

Para programar una tarea periódica, abra la ventana principal del programa y haga clic en **Herramientas** > **Planificador de tareas**. A continuación, dispone de las instrucciones básicas para programar una tarea que analice los discos locales cada 24 horas.

Para programar una tarea:

1. Haga clic en **Agregar** en la pantalla principal del Planificador de tareas.
2. Seleccione **Análisis de estado inactivo** en el menú desplegable.
3. Escriba un nombre para la tarea y seleccione **Reiteradamente**.
4. Seleccione la opción para ejecutar la tarea cada 24 horas.
5. Seleccione la acción que debe realizarse si se produce un error al ejecutar la tarea programada por cualquier motivo.
6. Revise el resumen de la tarea programada y haga clic en **Finalizar**.
7. En el menú desplegable **Objetos**, seleccione **Discos locales**.
8. Haga clic en **Finalizar** para aplicar la tarea.

3.8.7 Cómo conectar ESET Endpoint Antivirus a ESET Remote Administrator

Cuando haya instalado ESET Endpoint Antivirus en su ordenador y desee conectarse a través de ESET Remote Administrator, asegúrese de que también tiene instalado ERA Agent en la estación de trabajo cliente. ERA Agent es una parte esencial de todas las soluciones cliente que se comunican con ERA Server. ESET Remote Administrator utiliza la herramienta RD Sensor para buscar ordenadores en la red. En Web Console se muestran todos los ordenadores de la red que detecte el sensor RD.

Cuando se haya implementado el agente, puede realizar la instalación remota de los productos de seguridad de ESET en los ordenadores cliente. Los pasos exactos de la instalación remota se describen en la Guía del usuario de ESET Remote Administrator.

3.8.8 Cómo configurar un Mirror

ESET Endpoint Antivirus se puede configurar para que almacene copias de los archivos de actualización del motor de detección y distribuya las actualizaciones a otras estaciones de trabajo que ejecuten ESET Endpoint Security o ESET Endpoint Antivirus.

Configuración de ESET Endpoint Antivirus como servidor Mirror para proporcionar actualizaciones mediante un servidor HTTP interno

Pulse **F5** para acceder a Configuración avanzada y despliegue **Actualización** > **Básico**. Asegúrese de que el **Servidor de actualización** está establecido en **AUTOSELECT**. Seleccione **Crear mirror de actualización** y **Proporcionar archivos de actualización mediante el servidor HTTP interno** en **Configuración avanzada** > **Básico** > **Mirror**.

Configuración de un servidor Mirror para proporcionar actualizaciones a través de una carpeta de red compartida

Cree una carpeta compartida en un dispositivo local o de red. Todos los usuarios que utilicen soluciones de seguridad de ESET deben tener acceso de lectura a esta carpeta, que además debe permitir la escritura desde la cuenta de SISTEMA local. Active **Crear mirror de actualización** en **Configuración avanzada** > **Básico** > **Mirror**. Examine y seleccione la carpeta compartida creada.

NOTA
si no desea efectuar la actualización a través del servidor HTTP interno, desactive **Proporcionar archivos de actualización mediante el servidor HTTP interno**.

3.8.9 Cómo actualizar a Windows 10 con ESET Endpoint Antivirus

ADVERTENCIA
Se recomienda encarecidamente actualizar a la versión más reciente de su producto de ESET y a continuación descargar las actualizaciones de módulos más recientes antes de actualizar a Windows 10. De esta forma se asegurará de disponer de la máxima protección y de conservar la configuración del programa y la información de licencia durante la actualización a Windows 10.

Versión 6.x y posteriores:

Haga clic en el vínculo adecuado a continuación para descargar e instalar la versión más reciente con el fin de prepararse para la actualización a Microsoft Windows 10:

Descargar ESET Endpoint Security 6 32 bits Descargar ESET Endpoint Antivirus 6 32 bits

Descargar ESET Endpoint Security 6 64 bits Descargar ESET Endpoint Antivirus 6 64 bits

Versión 5.x y anteriores:

Haga clic en el vínculo adecuado a continuación para descargar e instalar la versión más reciente con el fin de prepararse para la actualización a Microsoft Windows 10:

Descargar ESET Endpoint Security 5 32 bits Descargar ESET Endpoint Antivirus 5 32 bits

Descargar ESET Endpoint Security 5 64 bits Descargar ESET Endpoint Antivirus 5 64 bits

Versiones en otros idiomas:

Si está buscando una versión en otro idioma de su producto ESET Endpoint, visite nuestra página de descargas.

NOTA
Más información sobre la compatibilidad de los productos de ESET con Windows 10.

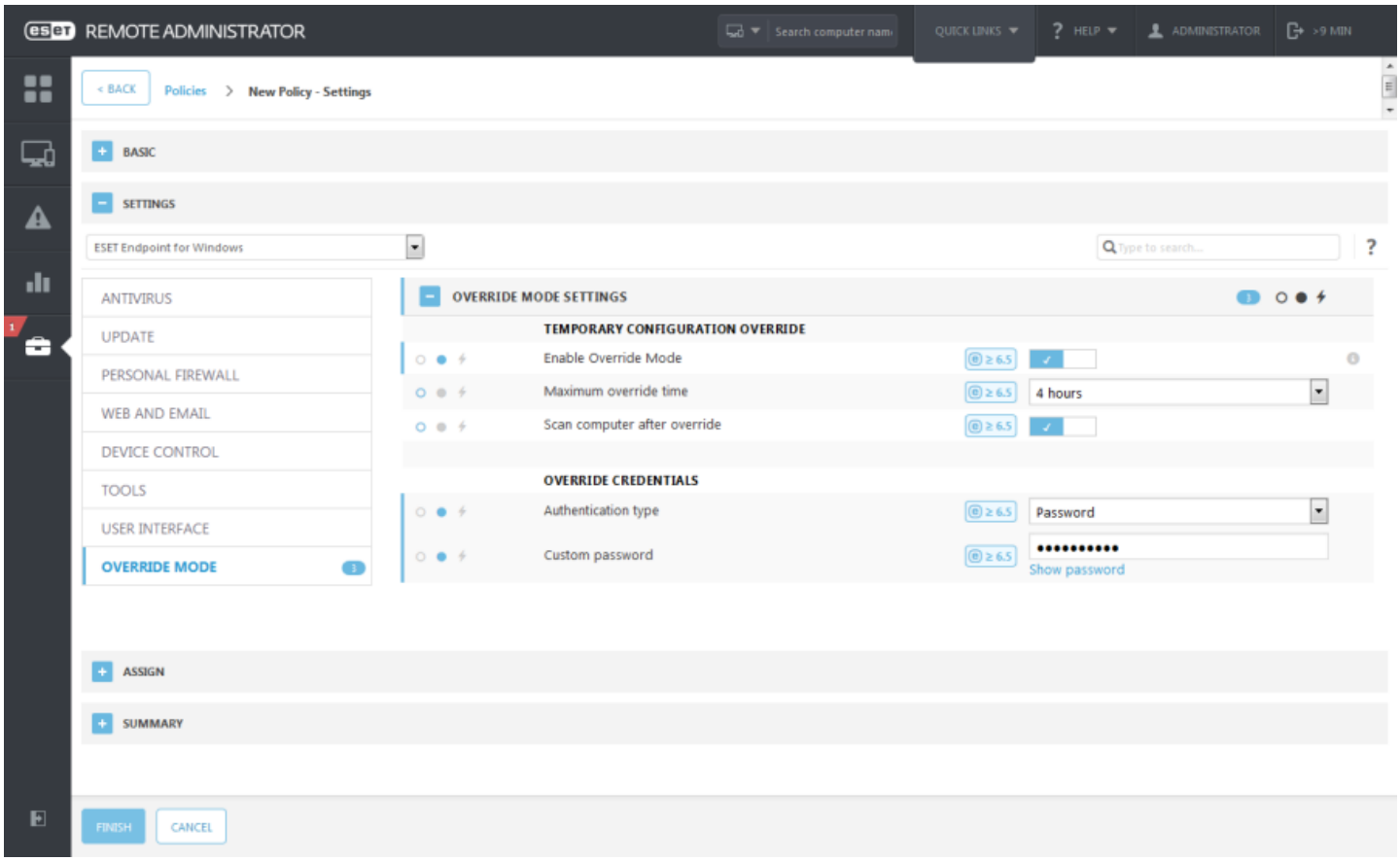
3.8.10 Cómo utilizar el modo de anulación

Los usuarios con productos ESET Endpoint (versión 6.5 y superiores) para Windows instalados en sus máquinas podrán utilizar la función de anulación. El modo de anulación permite a los usuarios de nivel de ordenador cliente cambiar la configuración del producto ESET instalado, incluso si hay una política aplicada a dicha configuración. El modo de anulación puede activarse para determinados usuarios de AD o protegerse mediante contraseña. La función no puede activarse durante más de cuatro horas directamente.

ADVERTENCIA
El modo de anulación no puede detenerse desde ERA Web Console una vez activado. La anulación solo se desactiva cuando transcurre el tiempo de anulación, o cuando se desactiva en el propio cliente.

Para configurar el **Modo de anulación**:

1. Vaya a **Admin** > **Políticas** > **Nueva política**.
2. En la sección **Básico**, escriba un **Nombre** y una **Descripción** para esta política.
3. En la sección **Configuración**, seleccione **ESET Endpoint para Windows**.
4. Haga clic en **Modo de anulación** y configure reglas para el modo de anulación.
5. En la sección **Asignar**, seleccione el ordenador o el grupo de ordenadores a los que se aplicará esta política.
6. Revise la configuración en la sección **Resumen** y haga clic en **Finalizar** para aplicar la política.



Una vez aplicada la política de anulación desde el ERA Server al ERA Agent, aparecerá un botón en la configuración avanzada (de Endpoint en el cliente): Anular política.

1. Haga clic en **Anular política**.
2. Defina el tiempo y haga clic en **Aplicar**.
3. Permita derechos superiores para la aplicación de ESET.
4. Escriba la contraseña determinada por la política (o ninguna contraseña si el usuario de Active Directory se ha definido en la política).
5. Permita derechos superiores para la aplicación de ESET.
6. Ahora el modo de anulación está activado.
7. Para finalizar, haga clic en **Finalizar anulación**.

CONSEJO

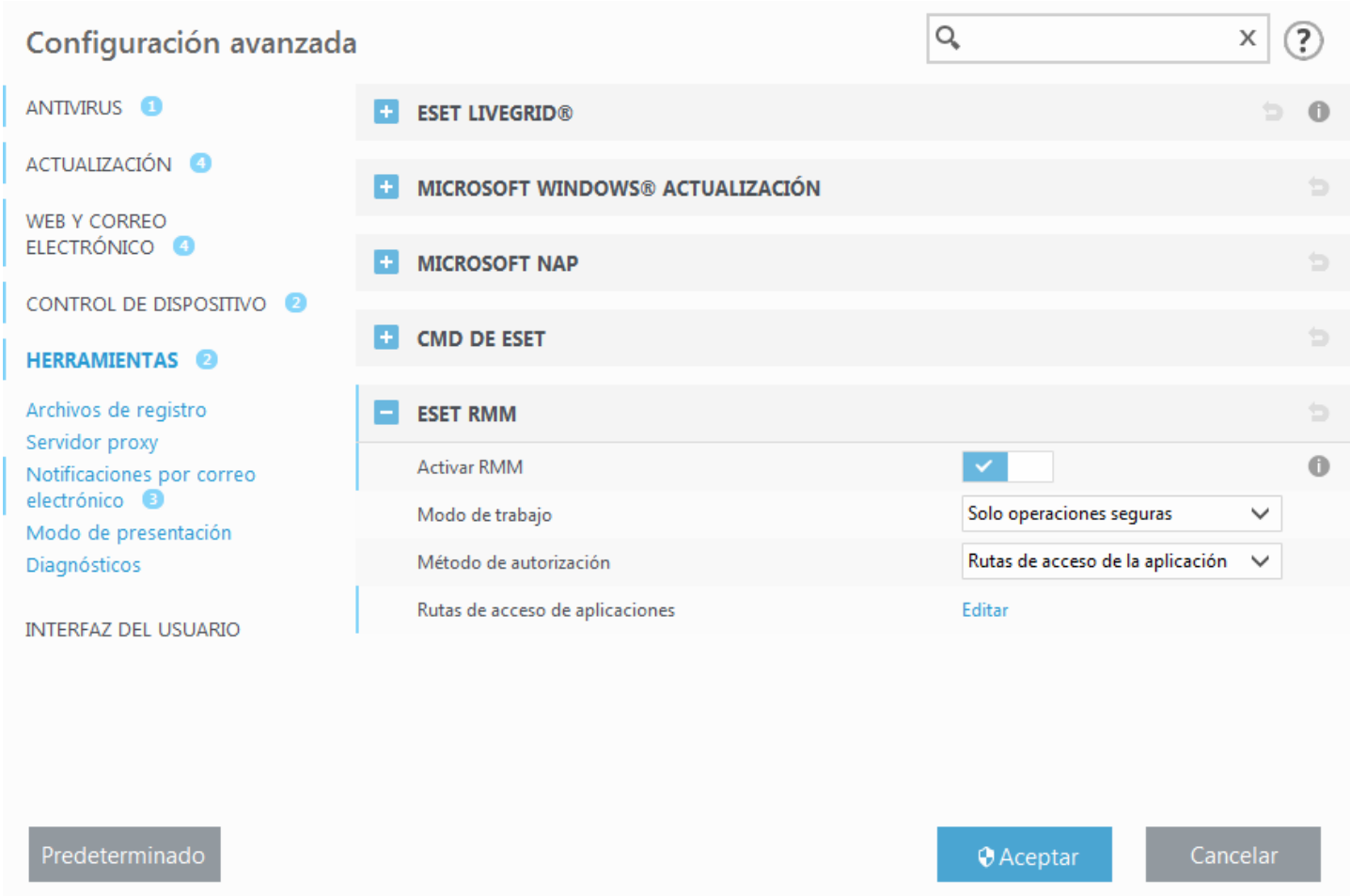
Si *John* tiene un problema porque la configuración de Endpoint está bloqueando algunas funciones importantes o el acceso web en su máquina, el Administrador podrá permitir que *John* anule su política de Endpoint existente y ajuste la configuración manualmente en su máquina. Después, ERA podrá solicitar la nueva configuración, por lo que el Administrador podrá crear una nueva política a raíz de la misma.

Para hacerlo, siga estos pasos:

1. Vaya a **Admin** > **Políticas** > **Nueva política**.
2. Complete los campos **Nombre** y **Descripción**. En la sección **Configuración**, seleccione **ESET Endpoint para Windows**.
3. Haga clic en **Modo de anulación**, active el modo de anulación durante una hora y seleccione *John* como usuario de AD.
4. Asigne la política al *Ordenador de John* y haga clic en **Finalizar** para guardar la política.
5. *John* deberá activar el **Modo de anulación** en su ESET Endpoint y cambiar la configuración manualmente en su máquina.
6. En ERA Web Console, vaya a **Ordenadores**, seleccione *Ordenador de John* y haga clic en **Mostrar detalles**.
7. En la sección **Configuración**, haga clic en **Solicitar configuración** para programar una tarea de cliente para obtener la configuración del cliente lo antes posible.
8. Poco después aparecerá la nueva configuración. Haga clic en el producto cuya configuración desea guardar y, a continuación, haga clic en **Abrir configuración**.
9. Puede revisar la configuración y, a continuación, hacer clic en **Convertir en política**.
10. Complete los campos **Nombre** y **Descripción**.
11. En la sección **Configuración**, puede modificar la configuración en caso necesario.
12. En la sección **Asignar**, puede asignar esta política al *Ordenador de John* (o a otros).
13. Haga clic en **Finalizar** para guardar la configuración.
14. No olvide eliminar la política de anulación cuando ya no la necesite.

3.8.11 Cómo activar supervisión y administración remotas

La supervisión y administración remotas (RMM) es el proceso de supervisar y controlar sistemas de software (como los de escritorios, servidores y dispositivos móviles) con un agente instalado localmente al que se puede acceder mediante un proveedor de servicios de administración.



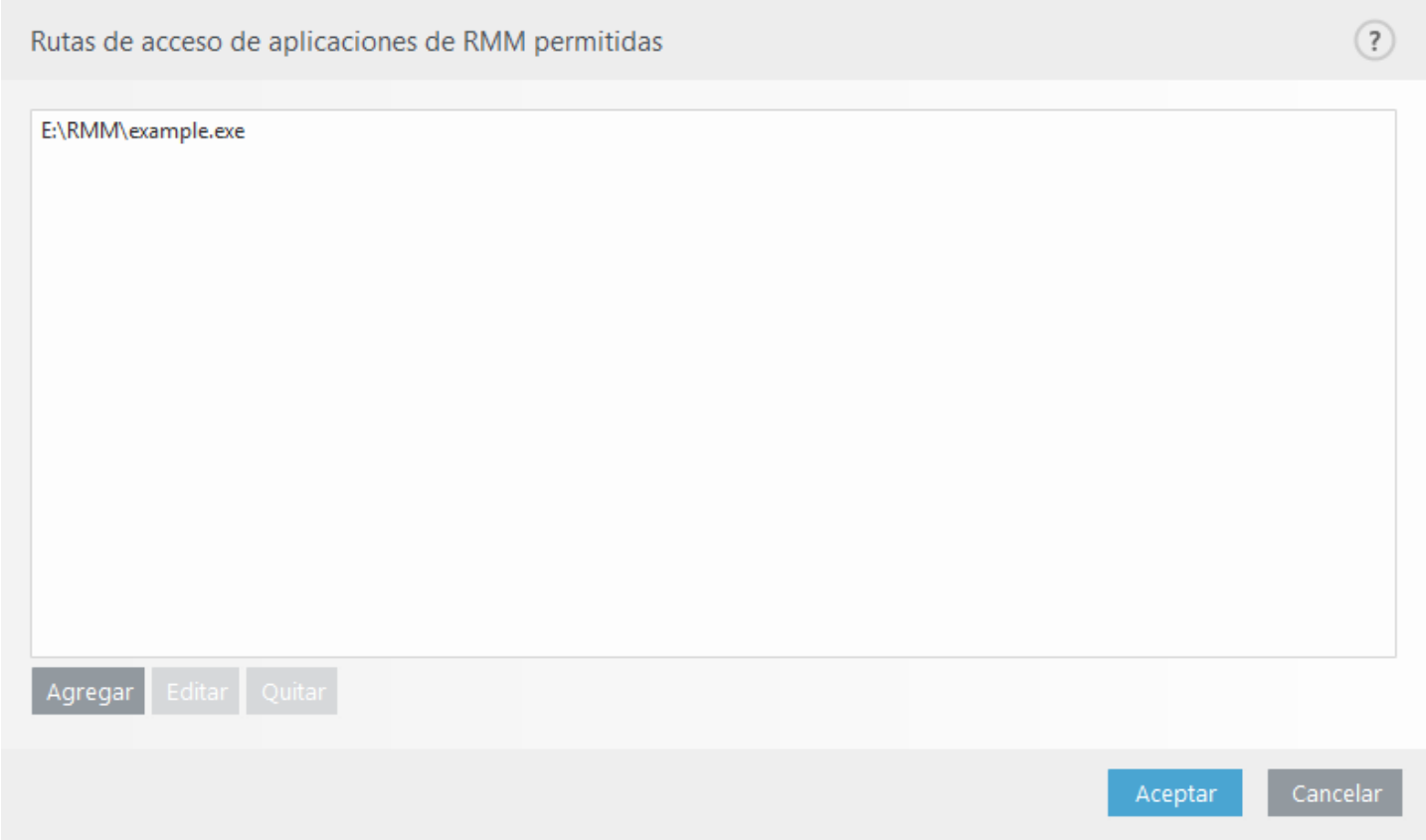
De forma predeterminada, ESET RMM está desactivado. Para activar ESET RMM, pulse **F5** para acceder a Configuración avanzada, haga clic en **Herramientas**, expanda **ESET RMM** y active el conmutador situado junto a **Activar RMM**.

Modo de trabajo: seleccione el modo de trabajo de RMM desde el menú desplegable. Hay dos opciones disponibles: **Solo operaciones seguras** y **Todas las operaciones**.

Método de autorización: defina el método de autorización de RMM. Para utilizar la autorización, seleccione **Ruta de acceso de la aplicación** en el menú desplegable; de lo contrario, seleccione **Ninguno**.

ADVERTENCIA
RMM siempre debe utilizar la autorización para evitar que el software malintencionado desactive o se salte la protección de ESET Endpoint.

Rutas de acceso de la aplicación: si ha seleccionado **Ruta de acceso de la aplicación** como método de autorización, haga clic en **Modificar** para abrir la ventana de configuración de **Rutas de acceso de aplicaciones de RMM permitidas**.



Agregar: cree una nueva ruta de acceso de aplicaciones de RMM permitidas. Escriba la ruta o haga clic en el botón **...** para seleccionar un ejecutable.
Modificar: modifique una ruta de acceso permitida existente. Utilice **Modificar** si la ubicación del ejecutable ha cambiado a otra carpeta.
Eliminar: elimine una ruta de acceso permitida existente.

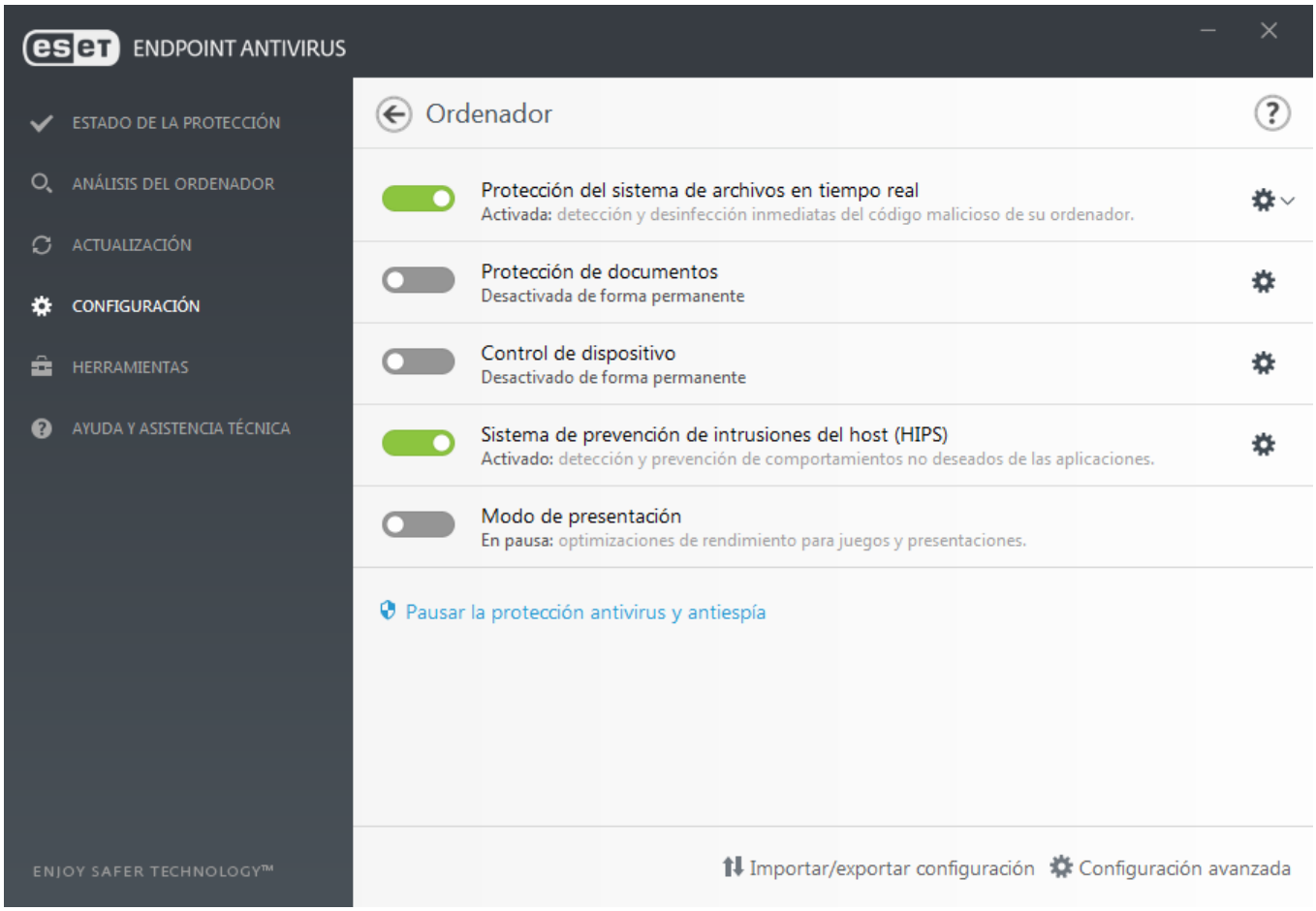
La instalación de ESET Endpoint Antivirus predeterminada contiene el archivo ermm.exe ubicado en el directorio de la aplicación Endpoint (ruta predeterminada *c:\Program Files\ESET\ESET Security*). El archivo ermm.exe intercambia datos con RMM Plugin, que se comunica con RMM Agent, vinculado a un RMM Server.

- ermm.exe: utilidad de línea de comandos desarrollada por ESET que permite administrar productos Endpoint y comunicarse con cualquier RMM Plugin.
- RMM Plugin es una aplicación de terceros que se ejecuta localmente en el sistema Endpoint para Windows. El complemento se ha diseñado para comunicarse con un RMM Agent concreto (p. ej., solo Kaseya) y con ermm.exe.
- RMM Agent es una aplicación de terceros (p. ej., de Kaseya) que se ejecuta localmente en el sistema Endpoint para Windows. El agente se comunica con RMM Plugin y con RMM Server.
- RMM Server se ejecuta como un servicio en un servidor de terceros. Los sistemas de RMM compatibles son Kaseya, Labtech, Autotask, Max Focus y Solarwinds N-able.

3.9 Uso de ESET Endpoint Antivirus

Las opciones de configuración de ESET Endpoint Antivirus le permiten ajustar el nivel de protección del ordenador, la Web y el correo electrónico.

NOTA
Al crear una política desde ESET Remote Administrator Web Console puede seleccionar el indicador de cada ajuste. Los ajustes que tengan el indicador Forzar tendrán prioridad y no podrán sobrescribirse con una política posterior (aunque también tenga este indicador establecido). Esta práctica garantiza que el ajuste no se verá modificado (por ejemplo, por el usuario o por posteriores políticas a la hora de ejecutar la fusión). Para obtener más información, consulte la ayuda en línea de Indicadores de ERA.



El menú **Configuración** incluye las siguientes secciones:

- **Ordenador**
- **Web y correo electrónico**

La configuración de protección de **Ordenador** le permite activar o desactivar los siguientes componentes:

- **Protección del sistema de archivos en tiempo real**: todos los archivos se analizan en busca de código malicioso en el momento de abrirlos, crearlos o ejecutarlos en el ordenador.
- **Protección de documentos**: la función de protección de documentos analiza los documentos de Microsoft Office antes de que se abran, además de los archivos descargados automáticamente con Internet Explorer, como los elementos de Microsoft ActiveX.
- **HIPS**: el sistema HIPS controla los sucesos del sistema operativo y reacciona según un conjunto de reglas personalizado.
- **Modo de presentación**: es una función pensada para aquellos usuarios que exigen un uso del software sin interrupciones y sin ventanas emergentes, así como un menor uso de la CPU. Cuando se active el modo de presentación, recibirá un mensaje de alerta (posible riesgo de seguridad) y la ventana principal del programa se volverá naranja.
- **Protección Anti-Stealth**: detecta programas peligrosos (como los rootkits) que pueden ocultarse del sistema operativo. Esto implica que no es posible detectarlos mediante las técnicas habituales.

La configuración de protección de **Web y correo electrónico** le permite activar o desactivar los siguientes componentes:

- **Protección del acceso a la Web**: si esta opción está activada, se analiza todo el tráfico a través de HTTP o HTTPS para detectar la presencia de software malicioso.
- **Protección del cliente de correo electrónico**: controla las comunicaciones recibidas a través de los protocolos POP3 e IMAP.
- **Protección Anti-Phishing**: le protege frente a intentos de adquirir contraseñas, datos bancarios y otra información confidencial por parte de sitios web que suplantan a sitios legítimos.

Si desea desactivar temporalmente algún módulo individual, haga clic en el conmutador verde  situado junto al módulo deseado. Tenga en cuenta que esto puede disminuir el nivel de protección del ordenador.

Para volver a activar la protección de un componente de seguridad desactivado, haga clic en el conmutador rojo  .

Cuando se aplique la política de ERA, verá el icono del candado  junto a un componente específico. La política aplicada por ESET Remote Administrator podrá sobrescribirse de forma local tras la autenticación por parte del usuario conectado (por ejemplo, el administrador). Para obtener más información, consulte la ayuda en línea de ESET Remote Administrator.

NOTA
Todas las medidas de protección que se desactiven de esta manera se volverán activar al reiniciar el ordenador.

Para acceder a la configuración detallada de un componente de seguridad determinado, haga clic en la rueda dentada que aparece junto a cualquier componente**.**

En la parte inferior de la ventana de configuración encontrará opciones adicionales. Para cargar los parámetros de configuración con un archivo de configuración *.xml*, o para guardar los parámetros de configuración actuales en un archivo de configuración, utilice la opción **Importar/exportar configuración**. Consulte Importar/exportar configuración para obtener más información detallada.

Si desea acceder a opciones más detalladas, haga clic en **Configuración avanzada** o pulse **F5**.

3.9.1 Ordenador

El módulo **Ordenador** está disponible en **Configuración** > **Ordenador**. En él se muestra una visión general de los módulos de protección que se describen en el capítulo anterior. En esta sección están disponibles los parámetros siguientes:

Haga clic en la rueda dentada situada junto a **Protección del sistema de archivos en tiempo real** y haga clic en **Modificar exclusiones** para abrir la ventana de configuración Exclusión, donde puede especificar los archivos y carpetas que no desea incluir en el análisis.

NOTA
El estado de la protección de documentos no estará disponible hasta que lo active en **Configuración avanzada** (F5) > **Antivirus** > **Protección de documentos**. Tras activarla tendrá que reiniciar el ordenador desde el panel Configuración Ordenador haciendo clic en **Reiniciar** dentro de Control de dispositivos, o desde el panel Estado de la protección haciendo clic en **Reiniciar el ordenador**.

Pausar la protección antivirus y antiespía: cuando desactive la protección antivirus y antiespía de forma temporal, utilice el menú desplegable para seleccionar el período de tiempo durante el que desea que el componente seleccionado esté desactivado y, a continuación, haga clic en **Aplicar** para desactivar el componente de seguridad. Para volver a activar la protección, haga clic en **Activar la protección antivirus y antiespía**.

Configuración del análisis del ordenador: haga clic para ajustar los parámetros del análisis del ordenador (análisis ejecutado manualmente).

3.9.1.1 Motor de detección

La protección antivirus protege contra ataques maliciosos al sistema mediante el control de las comunicaciones por Internet, el correo electrónico y los archivos. Si se detecta una amenaza, el módulo antivirus puede bloquearla para después desinfectarla, eliminarla o ponerla en cuarentena.

Para configurar las opciones avanzadas del módulo antivirus, haga clic en **Configuración avanzada** o pulse **F5**.

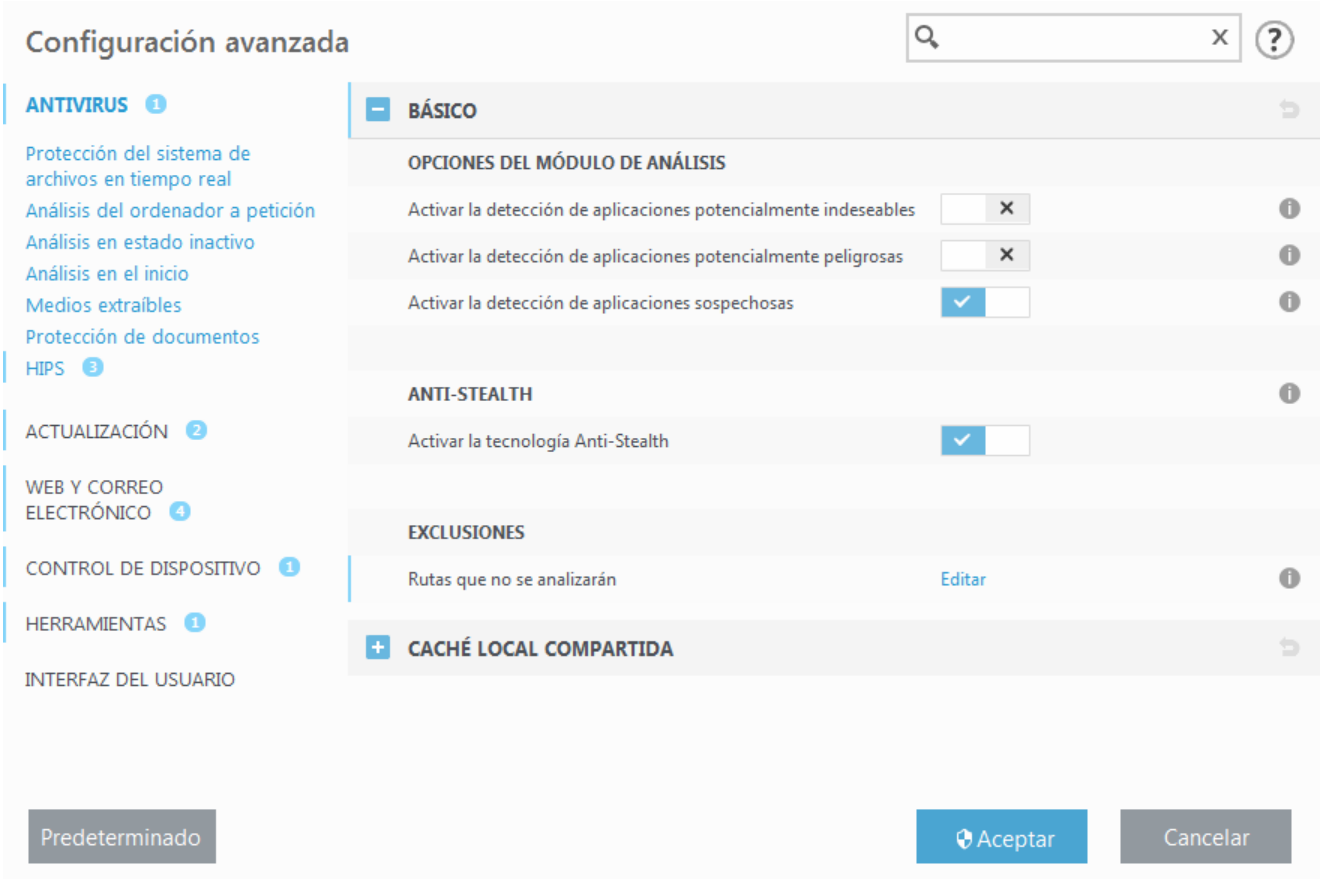
Las opciones de análisis de todos los módulos de protección (por ejemplo, Protección del sistema de archivos en tiempo real, protección del acceso a la Web, etc.) le permiten activar o desactivar la detección de los siguientes elementos:

- Las **aplicaciones potencialmente indeseables** (PUA) no tienen por qué ser maliciosas, pero pueden afectar negativamente al rendimiento del ordenador.
  Puede obtener más información sobre estos tipos de aplicaciones en el glosario.
- Por **aplicaciones potencialmente peligrosas** se entienden programas de software comercial legítimo que pueden utilizarse con fines maliciosos. Entre los ejemplos de este tipo de programas encontramos herramientas de acceso remoto, aplicaciones para detectar contraseñas y registradores de pulsaciones (programas que registran cada tecla pulsada por un usuario). Esta opción está desactivada de manera predeterminada.
  Puede obtener más información sobre estos tipos de aplicaciones en el glosario.
- Entre las **aplicaciones sospechosas** se incluyen programas comprimidos con empaquetadores o protectores. Los autores de código malicioso con frecuencia explotan estos tipos de protectores para evitar ser detectados.

La **tecnología Anti-Stealth** es un sofisticado sistema de detección de programas peligrosos como rootkits, que pueden ocultarse del sistema operativo. Esto implica que no es posible detectarlos mediante las técnicas habituales.

Las **exclusiones** le permiten excluir archivos y carpetas del análisis. Para garantizar que se analizan todos los objetos en busca de amenazas, le recomendamos que solo cree exclusiones cuando sea absolutamente necesario. Puede que haya situaciones en las que necesite excluir un objeto, como durante el análisis de entradas de una base de datos grande que ralentice el ordenador o software que entre en conflicto con el análisis. Para excluir un objeto del análisis, consulte Exclusiones.

Activar análisis avanzado mediante AMSI: herramienta Interfaz de análisis contra el código malicioso de Microsoft que permite que los desarrolladores de aplicaciones creen nuevas defensas contra el código malicioso (solo para Windows 10).



3.9.1.1.1 Detección de una amenaza

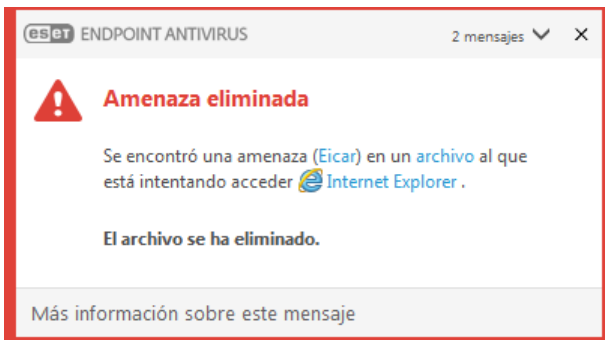
Las amenazas pueden acceder al sistema desde varios puntos de entrada, como páginas web, carpetas compartidas, correo electrónico o dispositivos extraíbles (USB, discos externos, CD, DVD, disquetes, etc.).

Comportamiento estándar

Como ejemplo general de cómo ESET Endpoint Antivirus gestiona las amenazas, estas se pueden detectar mediante:

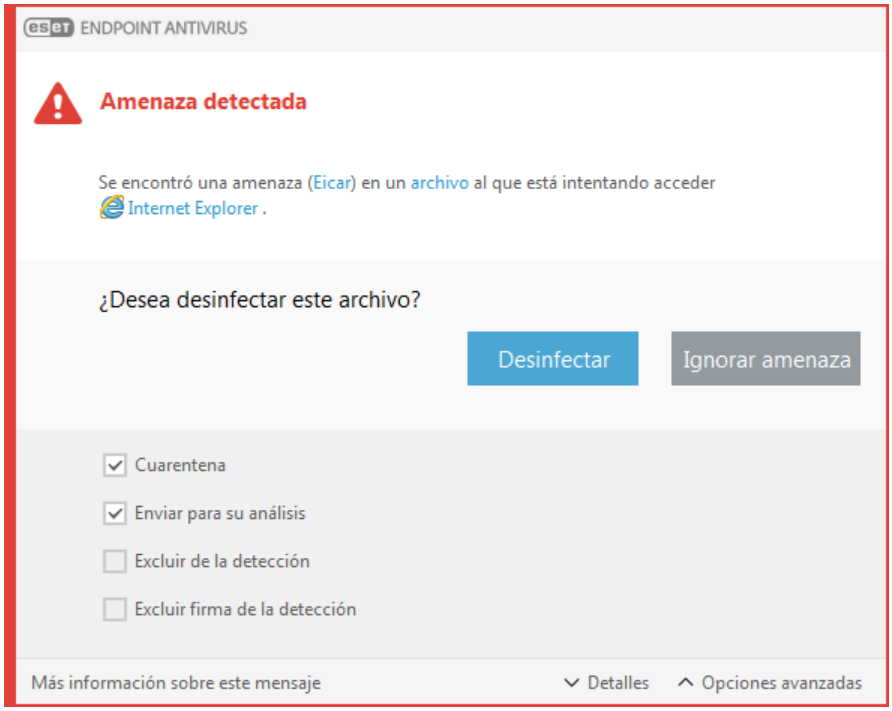
- Protección del sistema de archivos en tiempo real
- Protección del acceso a la Web
- Protección de clientes de correo electrónico
- Análisis del ordenador a petición

Cada uno de estos componentes utiliza el nivel de desinfección estándar e intentará desinfectar el archivo y moverlo a Cuarentena o finalizar la conexión. Se muestra una ventana de notificación en el área de notificación, situada en la esquina inferior derecha de la pantalla. Para obtener más información sobre los tipos de desinfección y el comportamiento, consulte la sección Desinfección.



Desinfección y eliminación

Si no hay que realizar ninguna acción predefinida para la protección en tiempo real, se le pedirá que seleccione una opción en la ventana de alerta. Normalmente, están disponibles las opciones **Desinfectar**, **Eliminar** y **Sin acciones**. No se recomienda seleccionar **Sin acciones**, ya que los archivos infectados quedarían intactos. La única excepción es cuando está seguro de que el archivo es inofensivo y se ha detectado por error.



Aplique esta opción si un archivo ha sido infectado por un virus que le ha añadido código malicioso. Si este es el caso, primero intente desinfectar el archivo infectado para restaurarlo a su estado original. Si el archivo consta exclusivamente de código malicioso, se eliminará.

Si un proceso del sistema "bloquea" o está utilizando un archivo infectado, por lo general solo se eliminará cuando se haya publicado (normalmente, tras reiniciar el sistema).

Múltiples amenazas

Si durante un análisis del ordenador no se desinfectaron algunos archivos infectados (o el Nivel de desinfección se estableció en **Sin desinfección**), aparecerá una ventana de alerta solicitándole que seleccione la acción que desea llevar a cabo en esos archivos.

Eliminar de amenazas en archivos comprimidos

En el modo de desinfección predeterminado, solo se eliminará todo el archivo comprimido si todos los archivos que contiene están infectados. En otras palabras, los archivos comprimidos no se eliminan si también contienen archivos no infectados e inofensivos. Tenga cuidado cuando realice un análisis con desinfección exhaustiva activada, ya que un archivo comprimido se eliminará si contiene al menos un archivo infectado, sin tener en cuenta el estado de los otros archivos.

Si el ordenador muestra señales de infección por código malicioso —por ejemplo, se ralentiza, se bloquea con frecuencia, etc., le recomendamos que haga lo siguiente:

- Abra ESET Endpoint Antivirus y haga clic en Análisis del ordenador.
- Haga clic en **Análisis estándar** (para obtener más información, consulte Análisis del ordenador).
- Una vez que haya finalizado el análisis, revise el registro para consultar el número de archivos analizados, infectados y desinfectados.

Si solo desea analizar una parte específica del disco, haga clic en **Análisis personalizado** y seleccione los objetos que desea incluir en el análisis de virus.

3.9.1.2 Caché local compartida

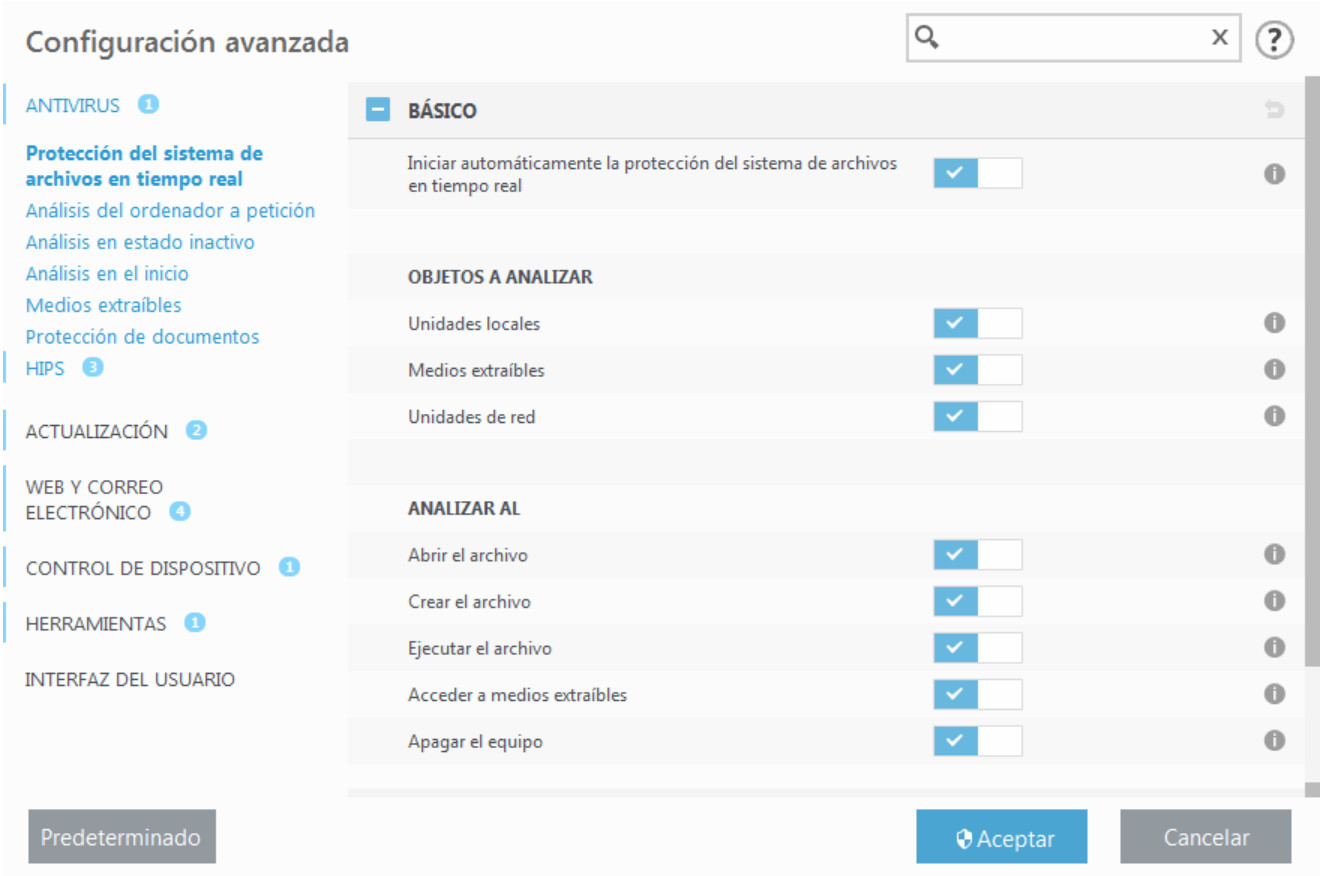
La caché local compartida mejora el rendimiento en entornos virtualizados al eliminar el análisis duplicado en la red. De esta manera se garantiza que cada archivo se analizará solo una vez y se almacenará en la caché compartida. Active el conmutador **Activar caché** para guardar en la caché local información sobre los análisis de archivos y carpetas de su red. Si realiza un análisis nuevo, ESET Endpoint Antivirus buscará los archivos analizados en la caché. Si los archivos coinciden, no se incluirán en el análisis.

La configuración de **Servidor de caché** contiene los campos siguientes**:**

- **Nombre de host**: nombre o dirección IP del ordenador donde se encuentra la caché.
- **Puerto**: número de puerto utilizado para la comunicación (el mismo que se estableció en la caché local compartida).
- **Contraseña**: especifique la contraseña de la caché local compartida de ESET, si es necesario.

3.9.1.3 Protección del sistema de archivos en tiempo real

La protección del sistema de archivos en tiempo real controla todos los sucesos relacionados con el antivirus en el sistema. Todos los archivos se analizan en busca de código malicioso en el momento de abrirlos, crearlos o ejecutarlos en el ordenador. La protección del sistema de archivos en tiempo real se inicia al arrancar el sistema.



La protección del sistema de archivos en tiempo real comienza de forma predeterminada cuando se inicia el sistema y proporciona un análisis ininterrumpido. En casos especiales (por ejemplo, si hay un conflicto con otro análisis en tiempo real), puede desactivar la protección en tiempo real anulando la selección de **Activar la protección del sistema de archivos en tiempo real**, en la sección **Configuración avanzada** de **Protección del sistema de archivos en tiempo real** > **Básico**.

Objetos a analizar

De forma predeterminada, se buscan posibles amenazas en todos los tipos de objetos:

Unidades locales: controla todas las unidades de disco duro del sistema.
Medios extraíbles: controla los discos CD y DVD, el almacenamiento USB, los dispositivos Bluetooth, etc.
Unidades de red: analiza todas las unidades asignadas.

Recomendamos que esta configuración predeterminada se modifique solo en casos específicos como, por ejemplo, cuando el control de ciertos objetos ralentiza significativamente las transferencias de datos.

Analizar al

De forma predeterminada, todos los archivos se analizan cuando se abren, crean o ejecutan. Le recomendamos que mantenga esta configuración predeterminada, ya que ofrece el máximo nivel de protección en tiempo real para su ordenador:

- **Abrir el archivo**: activa o desactiva el análisis al abrir archivos.
- **Crear el archivo**: activa o desactiva el análisis durante la creación de archivos.
- **Ejecutar el archivo**: activa o desactiva el análisis cuando se ejecutan archivos.
- **Acceso a medios extraíbles**: activa o desactiva el análisis activado por el acceso a determinados medios extraíbles con espacio de almacenamiento.

La protección del sistema de archivos en tiempo real comprueba todos los tipos de medios y se activa con varios sucesos del sistema como, por ejemplo, cuando se accede a un archivo. Si se utilizan métodos de detección con la tecnología ThreatSense (tal como se describe en la sección Configuración de parámetros del motor ThreatSense), la protección del sistema de archivos en tiempo real se puede configurar para que trate de forma diferente los archivos recién creados y los archivos existentes. Por ejemplo, puede configurar la protección del sistema de archivos en tiempo real para que supervise más detenidamente los archivos recién creados.

Con el fin de que el impacto en el sistema sea mínimo cuando se utiliza la protección en tiempo real, los archivos que ya se analizaron no se vuelven a analizar (a no ser que se hayan modificado). Los archivos se analizan de nuevo inmediatamente tras cada actualización del motor de detección. Este comportamiento se controla con la opción **Optimización inteligente**. Si la opción **Optimización inteligente** está desactivada, se analizan todos los archivos cada vez que se accede a ellos. Para modificar esta configuración, pulse **F5** para abrir Configuración avanzada y despliegue **Motor de detección** > **Protección del sistema de archivos en tiempo real**. Haga clic en **Parámetros de ThreatSense** > **Otros** y seleccione o anule la selección de **Activar optimización inteligente**.

3.9.1.3.1 Parámetros adicionales de ThreatSense

Parámetros adicionales de ThreatSense para archivos nuevos o modificados: la probabilidad de infección en archivos modificados o recién creados es superior que en los archivos existentes, por eso el programa comprueba estos archivos con parámetros de análisis adicionales. Además de los métodos de análisis basados en firmas habituales, se utiliza la heurística avanzada, que detecta amenazas nuevas antes de que se publique la actualización del motor de detección. El análisis se realiza también en archivos de autoextracción (.sfx) y empaquetadores en tiempo real (archivos ejecutables comprimidos internamente), no solo en los archivos nuevos. Los archivos se analizan, de forma predeterminada, hasta el 10º nivel de anidamiento; además, se analizan independientemente de su tamaño real. Para modificar la configuración de análisis de archivos comprimidos, desactive la opción **Configuración por defecto para archivos comprimidos**.

Para obtener más información sobre los **empaquetadores en tiempo real**, **archivos comprimidos de autoextracción** y **heurística avanzada**, consulte Configuración de parámetros del motor ThreatSense.

Parámetros adicionales de ThreatSense para los archivos ejecutados: de forma predeterminada, la heurística avanzada no se utiliza cuando se ejecutan archivos. Si esta opción está activada, se recomienda encarecidamente dejar activadas las opciones Optimización inteligente y ESET LiveGrid® con el fin de mitigar su repercusión en el rendimiento del sistema.

3.9.1.3.2 Niveles de desinfección

La protección en tiempo real tiene tres niveles de desinfección (para acceder a la configuración de niveles de desinfección, haga clic en **Configuración de los parámetros del motor ThreatSense** en la sección **Protección del sistema de archivos en tiempo real** y, a continuación, en **Desinfección**).

Sin desinfección: los archivos infectados no se desinfectan automáticamente. El programa mostrará una ventana de alerta y permitirá que el usuario seleccione una acción. Este nivel es adecuado para usuarios avanzados que conocen los pasos necesarios en caso de amenaza.

Desinfección normal: el programa intenta desinfectar o eliminar un archivo infectado de manera automática, de acuerdo con una acción predefinida (según el tipo de amenaza). La eliminación y la detección de un archivo infectado se marca mediante una notificación en la esquina inferior derecha de la pantalla. Si no es posible seleccionar la acción correcta de manera automática, el programa ofrece otras acciones que seguir. Lo mismo ocurre cuando no se puede completar una acción predefinida.

Desinfección estricta: el programa desinfecta o elimina todos los archivos infectados. Las únicas excepciones son los archivos del sistema. Si no es posible desinfectarlos, se insta al usuario a que seleccione una acción indicada en una ventana de alerta.

ADVERTENCIA

si un archivo comprimido contiene archivos infectados, se puede tratar de dos maneras: en el modo estándar (Desinfección estándar), se elimina el archivo comprimido completo si este está compuesto únicamente por código malicioso; y en el modo **Desinfección exhaustiva**, el archivo se elimina si contiene al menos una porción de código malicioso, independientemente del estado de los demás archivos.

3.9.1.3.3 Análisis de protección en tiempo real

Para verificar que la protección en tiempo real funciona y detecta virus, utilice el archivo de prueba de eicar.com., un archivo inofensivo detectable por todos los programas antivirus. El archivo fue creado por la compañía EICAR (European Institute for Computer Antivirus Research, Instituto europeo para la investigación de antivirus de ordenador) para probar la funcionalidad de los programas antivirus. Este archivo se puede descargar en http://www.eicar.org/download/eicar.com.

3.9.1.3.4 Modificación de la configuración de protección en tiempo real

La protección del sistema de archivos en tiempo real es el componente más importante para mantener un sistema seguro, por lo que debe tener cuidado cuando modifique los parámetros correspondientes. Es aconsejable que los modifique únicamente en casos concretos.

Una vez que se ha instalado ESET Endpoint Antivirus, se optimiza toda la configuración para proporcionar a los usuarios el máximo nivel de seguridad del sistema. Para restaurar la configuración predeterminada, haga clic en junto a las diferentes fichas de la ventana (**Configuración avanzada** > **Motor de detección** > **Protección del sistema de archivos en tiempo real**).

3.9.1.3.5 Qué debo hacer si la protección en tiempo real no funciona

En este capítulo, describimos los problemas que pueden surgir cuando se utiliza la protección en tiempo real y cómo resolverlos.

Protección en tiempo real desactivada

Si un usuario desactivó la protección en tiempo real sin darse cuenta, será necesario reactivarla. Para volver a activar la protección en tiempo real, vaya a **Configuración** en la ventana principal del programa y haga clic en **Protección del sistema de archivos en tiempo real**.

Si no se activa al iniciar el sistema, probablemente se deba a que la opción **Iniciar automáticamente la protección del sistema de archivos en tiempo real** no está seleccionada. Si desea activar esta opción, diríjase a **Configuración avanzada** (**F5**) y haga clic en **Motor de detección** > **Protección del sistema de archivos en tiempo real** > **Básico**.

Asegúrese de que la opción **Iniciar automáticamente la protección del sistema de archivos en tiempo real** esté activada.

Si la protección en tiempo real no detecta ni desinfecta amenazas

Asegúrese de que no tiene instalados otros programas antivirus en el ordenador. Si están activadas dos protecciones en tiempo real al mismo tiempo, estas pueden entrar en conflicto. Recomendamos que desinstale del sistema cualquier otro programa antivirus que haya en el sistema antes de instalar ESET.

La protección en tiempo real no se inicia

Si la protección en tiempo real no se activa al iniciar el sistema (y la opción **Activar la protección del sistema de archivos en tiempo real** está activada), es posible que se deba a conflictos con otros programas. Para obtener ayuda para resolver este problema, póngase en contacto con el Servicio de atención al cliente de ESET.

3.9.1.4 Análisis del ordenador

El análisis a petición es una parte importante de ESET Endpoint Antivirus. Se utiliza para realizar análisis de archivos y carpetas en su ordenador. Desde el punto de vista de la seguridad, es esencial que los análisis del ordenador no se ejecuten únicamente cuando se sospecha que existe una infección, sino que se realicen periódicamente como parte de las medidas de seguridad rutinarias. Le recomendamos que realice un análisis en profundidad de su sistema periódicamente (por ejemplo, una vez al mes) para detectar virus que la Protección del sistema de archivos en tiempo real no haya detectado. Este fallo puede deberse a que la protección del sistema de archivos en tiempo real no estaba activada en ese momento, a que el motor de detección estaba obsoleto o a que el archivo no se detectó como un virus cuando se guardó en el disco.

Están disponibles dos tipos de **Análisis del ordenador**. El **análisis estándar** analiza el sistema rápidamente, sin necesidad de realizar una configuración adicional de los parámetros de análisis. El **análisis personalizado** le permite seleccionar perfiles de análisis predefinidos y definir objetos de análisis específicos.

Consulte Progreso del análisis para obtener más información sobre el proceso de análisis.

Análisis del ordenador

El análisis estándar le permite iniciar rápidamente un análisis del ordenador y desinfectar los archivos infectados sin la intervención del usuario. La ventaja de este tipo de análisis es su sencillo funcionamiento, sin configuraciones de análisis detalladas. El análisis estándar comprueba todos los archivos de los discos locales y desinfecta o elimina automáticamente las amenazas detectadas. El nivel de desinfección se establece automáticamente en el valor predeterminado. Para obtener más información detallada sobre los tipos de desinfección, consulte Desinfección.

Análisis personalizado

El análisis personalizado es una solución óptima para especificar parámetros de análisis como, por ejemplo, objetos y métodos de análisis. La ventaja del análisis personalizado es su capacidad para configurar los parámetros detalladamente. Las diferentes configuraciones se pueden guardar en perfiles de análisis definidos por el usuario, que pueden resultar útiles si el análisis se realiza varias veces con los mismos parámetros.

Para seleccionar objetos de análisis, seleccione **Análisis del ordenador** > **Análisis personalizado** y elija una opción en el menú desplegable **Explorar objetivos**, o seleccione objetos específicos en la estructura de árbol. Los objetos de análisis también se pueden especificar introduciendo la ruta a la carpeta o los archivos que se desean incluir en el análisis. Si únicamente quiere analizar el sistema, sin realizar acciones de desinfección adicionales, seleccione **Analizar sin desinfectar**. Cuando vaya a realizar un análisis, haga clic en **Configuración...**. > **Parámetros de ThreatSense** > **Desinfección**.

Los análisis del ordenador en el modo personalizado son adecuados para usuarios avanzados que tienen experiencia previa con programas antivirus.

También puede utilizar la función **Análisis mediante arrastrar y colocar** para analizar un archivo o una carpeta manualmente al hacer clic en el archivo o la carpeta, desplazar el cursor del ratón hasta la zona marcada mientras se mantiene pulsado el botón del ratón, para después soltarlo. Después, la aplicación pasa al primer plano.

Análisis de medios extraíbles

Al igual que el análisis estándar, inicia rápidamente el análisis de medios extraíbles (como CD/DVD/USB) que están actualmente conectados al ordenador. Esto puede resultar útil cuando conecta una unidad flash USB a un ordenador y desea analizar su contenido por si contiene código malicioso u otras posibles amenazas.

Este tipo de análisis también se puede iniciar haciendo clic en **Análisis personalizado**, en **Medios extraíbles** en el menú desplegable **Explorar objetivos** y, a continuación, en **Exploración**.

Utilice el menú desplegable **Acción tras el análisis** para seleccionar la acción (Sin acciones, Apagar y Reiniciar) que desea realizar tras el análisis.

Activar apagado tras el análisis: activa el apagado programado para cuando termine el análisis del ordenador a petición. Se mostrará un cuadro de diálogo de confirmación de apagado con una cuenta atrás de 60 segundos. Haga clic en **Cancelar** para desactivar el apagado solicitado.

NOTA
Le recomendamos que ejecute un análisis del ordenador una vez al mes como mínimo. El análisis se puede configurar como una tarea programada en **Herramientas** > **Planificador de tareas**.

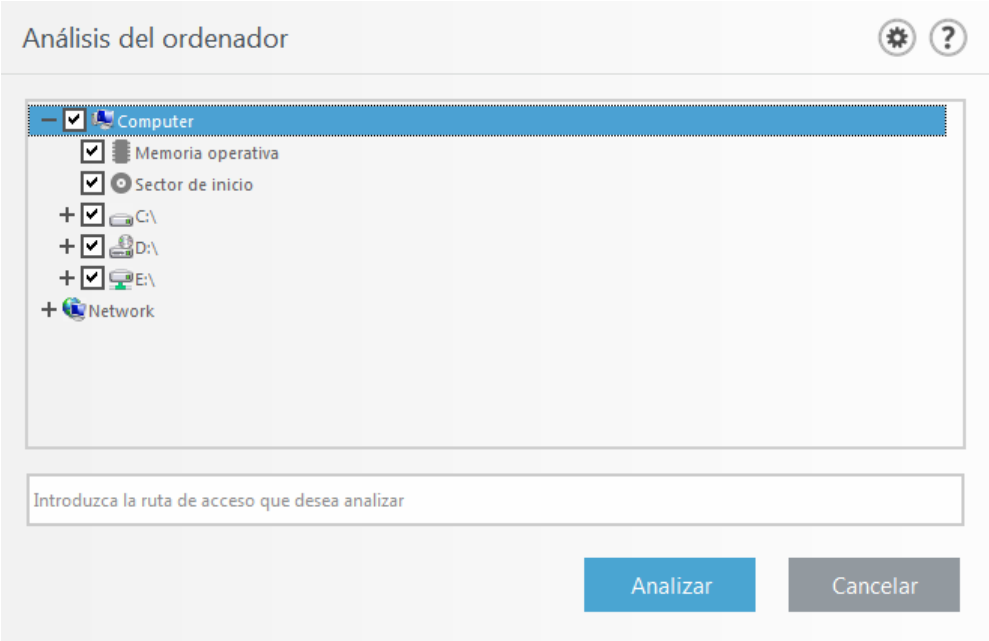
3.9.1.4.1 Iniciador del análisis personalizado

Si solo desea analizar un objeto determinado, puede usar la herramienta de análisis personalizado haciendo clic en **Análisis del ordenador** > **Análisis personalizado** y seleccionando una opción en el menú desplegable **Explorar objetivos** o seleccionando objetos específicos en la estructura de carpetas (árbol).

En la ventana de objetos de análisis puede definir los objetos (memoria, unidades, sectores, archivos y carpetas) que se deben analizar para buscar amenazas. Seleccione los objetos en la estructura de árbol, que incluye todos los dispositivos disponibles en el ordenador. En el menú desplegable **Objetos de análisis**, puede seleccionar objetos predefinidos para el análisis.

- **Por configuración de perfil**: selecciona los objetos definidos en el perfil de análisis seleccionado.
- **Medios extraíbles**: selecciona los disquetes, dispositivos de almacenamiento USB, CD y DVD.
- **Unidades locales**: selecciona todas las unidades de disco del sistema.
- **Unidades de red**: selecciona todas las unidades de red asignadas.
- **Sin selección**: cancela todas las selecciones.

Para acceder rápidamente a un objeto de análisis o agregar directamente carpetas o archivos, introdúzcalos en el campo en blanco disponible debajo de la lista de carpetas. Esto solo es posible si no se ha seleccionado ningún objeto en la estructura de árbol y el menú **Objetos de análisis** está definido en **Sin selección**.



Los elementos infectados no se desinfectan automáticamente. El análisis sin desinfección sirve para obtener una vista general del estado de protección actual. Además, puede seleccionar uno de los tres niveles de desinfección haciendo clic en **Configuración avanzada** > **Motor de detección** > **Análisis a petición** > **Parámetros de ThreatSense** > **Desinfección**. Si únicamente quiere analizar el sistema, sin realizar acciones de desinfección adicionales, seleccione **Analizar sin desinfectar**. El historial de análisis se guarda en el registro de análisis.

Cuando se selecciona **Ignorar exclusiones**, se analizan sin excepciones los archivos con extensiones excluidas anteriormente del análisis.

Puede elegir un perfil en el menú desplegable **Perfil de análisis** que se utilizará para analizar los objetos seleccionados. El perfil predeterminado es **Análisis estándar**. Hay otros dos perfiles de análisis predefinidos llamados **Análisis en profundidad** y **Análisis del menú contextual**. Estos perfiles de análisis estándar utilizan distintos parámetros de ThreatSense. Las opciones disponibles se describen en **Configuración avanzada** > **Motor de detección** > **Análisis de malware** > **Análisis a petición** > Parámetros de ThreatSense.

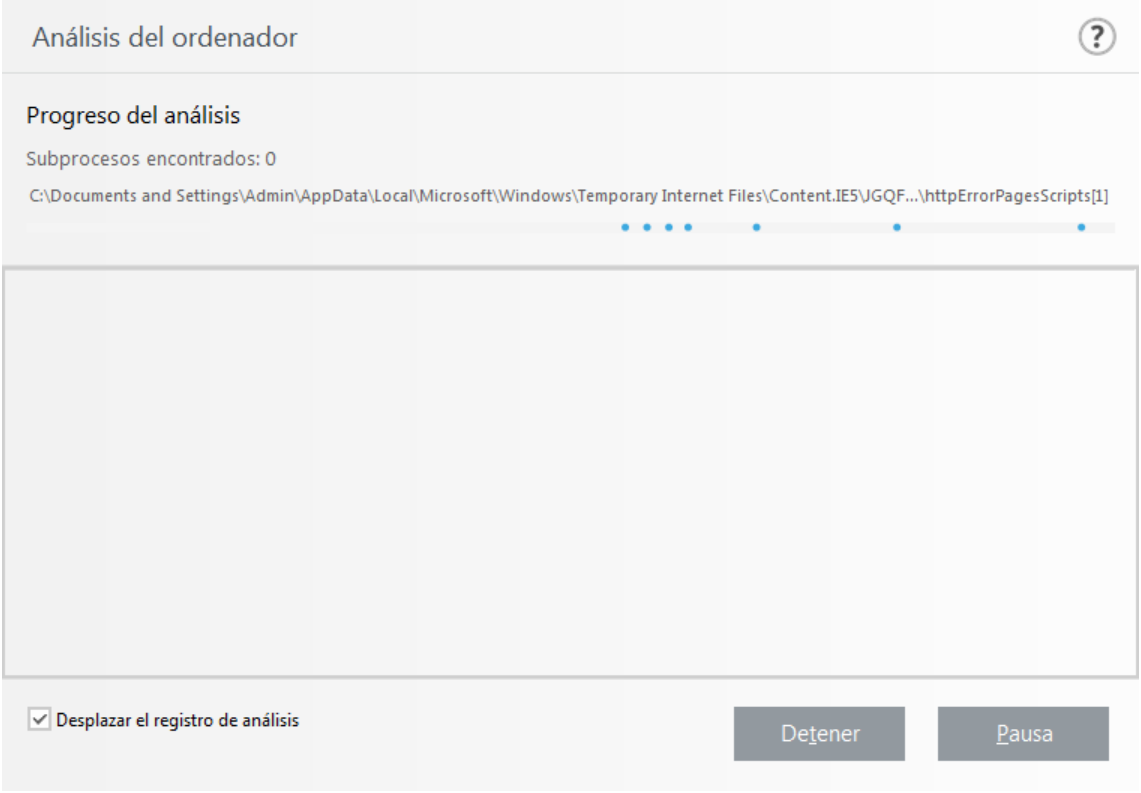
Haga clic en **Analizar** para ejecutar el análisis con los parámetros personalizados que ha definido.

Analizar como administrador le permite ejecutar el análisis con la cuenta de administrador. Haga clic en esta opción si el usuario actual no tiene privilegios para acceder a los archivos que se deben analizar. Observe que este botón no está disponible si el usuario actual no puede realizar operaciones de UAC como administrador.

NOTA
Si hace clic en **Mostrar registro**, se mostrará el registro de análisis del ordenador cuando dicho análisis concluya.

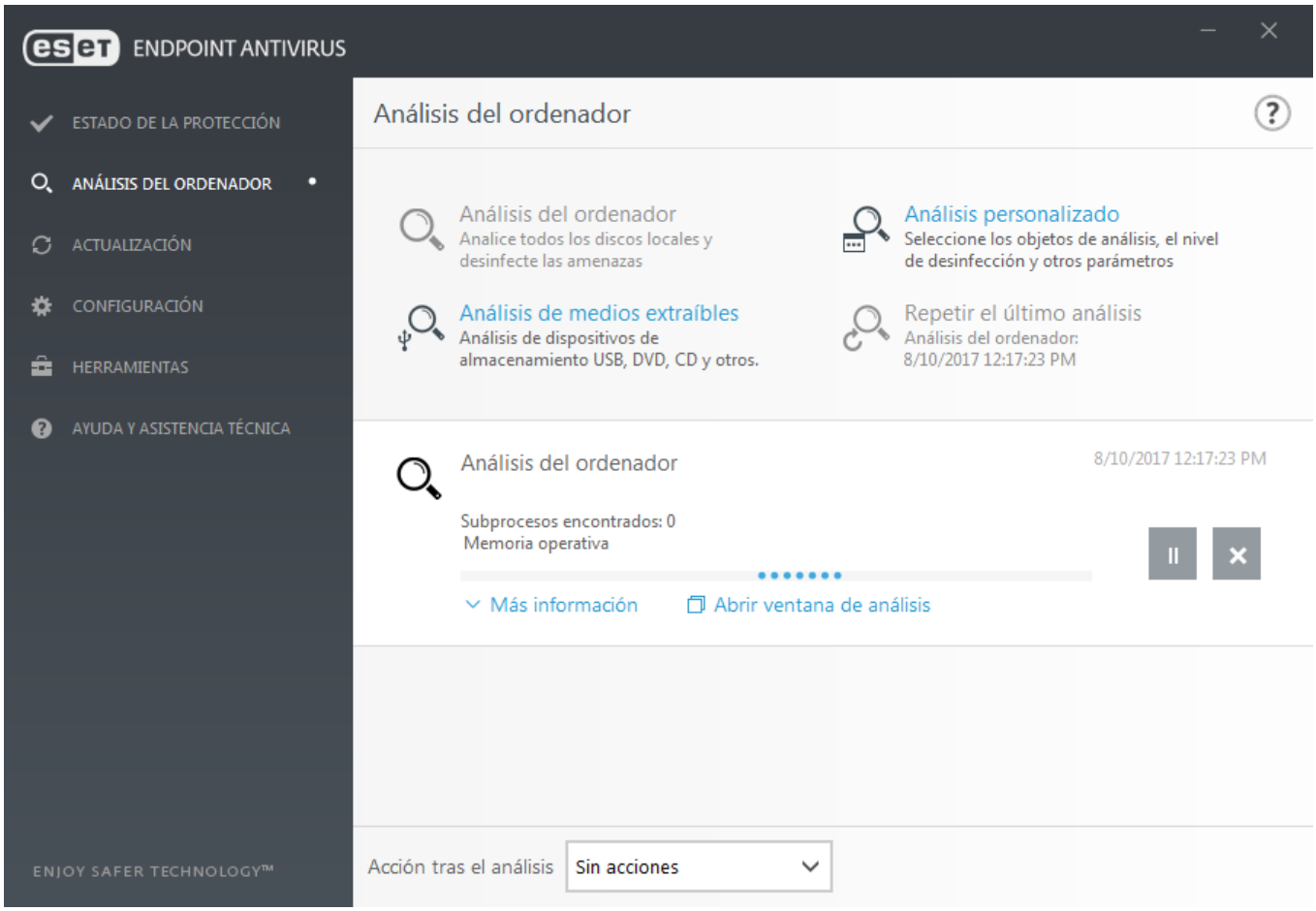
3.9.1.4.2 Progreso del análisis

En la ventana de progreso del análisis se muestra el estado actual del análisis e información sobre el número de archivos en los que se ha detectado código malicioso.



NOTA
Es normal que algunos archivos, como los archivos protegidos con contraseña o que solo utiliza el sistema (por lo general, archivos *pagefile.sys* y determinados archivos de registro), no se puedan analizar.

Progreso del análisis: la barra de progreso muestra el estado de objetos ya analizados en comparación con el porcentaje de objetos pendientes. El estado de progreso del análisis se calcula a partir del número total de objetos incluidos en el análisis.
Objeto: el nombre y la ubicación del objeto que se está analizando.
Amenazas detectadas: muestra el número total de amenazas detectadas durante un análisis.
Pausa: pone el análisis en pausa.
Reanudar: esta opción está visible cuando el progreso del análisis está en pausa. Haga clic en **Continuar** para proseguir con el análisis.
Detener: termina el análisis.
Desplazarse por el registro de exploración: si esta opción está activada, el registro de análisis se desplaza automáticamente a medida que se añaden entradas nuevas, de modo que se visualizan las entradas más recientes.



3.9.1.4.3 Registro de análisis del ordenador

El registro de análisis del ordenador contiene información general sobre el análisis, como la siguiente:

- Versión del motor de detección
- Fecha y hora del análisis
- Discos, carpetas y archivos analizados
- Número de objetos analizados
- Número de amenazas detectadas
- Hora de finalización
- Tiempo total de análisis

3.9.1.5 Control de dispositivos

ESET Endpoint Antivirus permite controlar los dispositivos automáticamente (CD, DVD, USB, etc.). Este módulo le permite bloquear o ajustar los filtros y permisos ampliados, así como establecer los permisos de un usuario para acceder a un dispositivo dado y trabajar en él. Esto puede ser útil cuando el administrador del ordenador quiere impedir que los usuarios utilicen dispositivos con contenido no solicitado.

Dispositivos externos admitidos:

- Almacenamiento en disco (unidad de disco duro, disco USB extraíble)
- CD/DVD
- Impresora USB
- Almacenamiento FireWire
- Dispositivo Bluetooth
- Lector de tarjetas inteligentes
- Dispositivo de imagen
- Módem
- Puerto LPT/COM
- Dispositivo portátil
- Todos los tipos de dispositivos

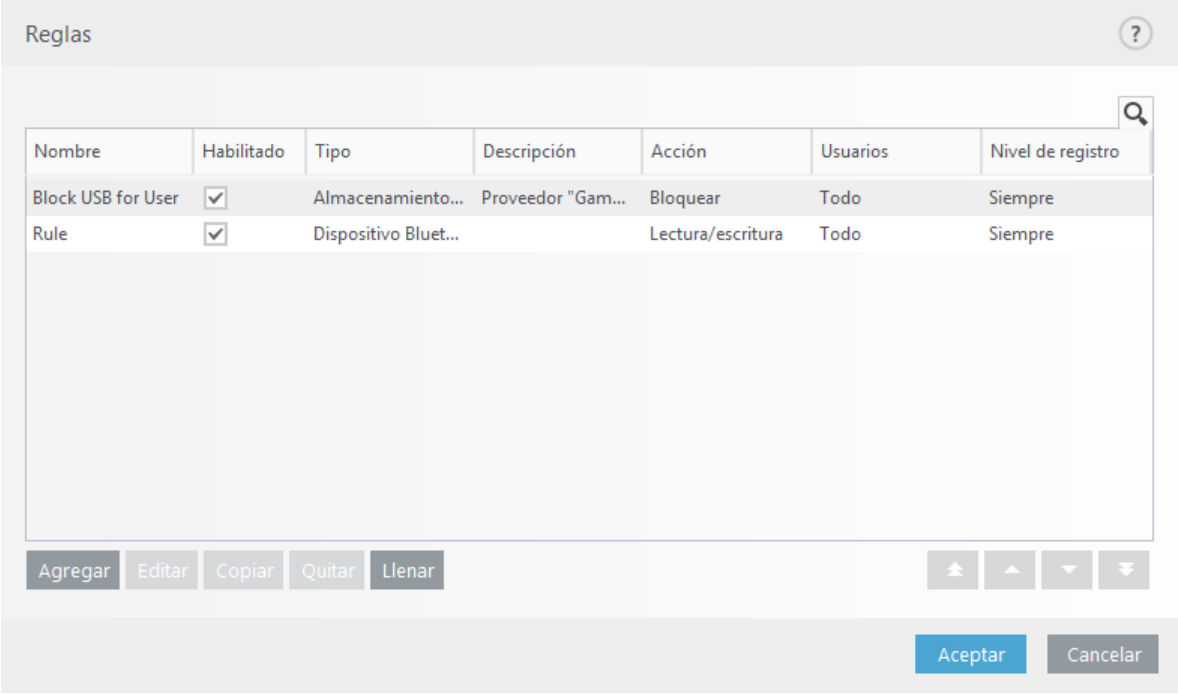
Las opciones de configuración del control del dispositivo se pueden modificar en **Configuración avanzada** (F5) > **Control del dispositivo**.

Al activar el conmutador situado junto a **Integrar en el sistema** se activa la característica de Control del dispositivo en ESET Endpoint Antivirus; deberá reiniciar el ordenador para que se aplique este cambio. Una vez que Control del dispositivo esté activado, se activarán las **Reglas**, lo que le permitirá abrir la ventana Editor de reglas.

Si se inserta un dispositivo que está bloqueado por una regla, se muestra una ventana de notificación y se prohíbe el acceso a dicho dispositivo.

3.9.1.5.1 Editor de reglas de control del dispositivo

La ventana **Editor de reglas de control de dispositivos** muestra las reglas existentes para dispositivos externos que los usuarios conectan al ordenador y permite controlarlos de forma precisa.



Determinados dispositivos se pueden permitir o bloquear según el usuario, el grupo de usuarios o según varios parámetros adicionales que se pueden especificar en la configuración de las reglas. La lista de reglas contiene varias descripciones de una regla, como el nombre, el tipo de dispositivo externo, la acción que debe realizarse tras conectar un dispositivo externo al ordenador y la gravedad del registro.

Haga clic en **Agregar** o en **Modificar** para administrar una regla. Desactive la casilla **Activado** que aparece junto a la regla para desactivarla hasta que la quiera usar en el futuro. Seleccione una o más reglas y haga clic en **Eliminar** para eliminar las reglas de forma permanente.

Copiar: crea una nueva regla con opciones predefinidas utilizadas para otra regla seleccionada.

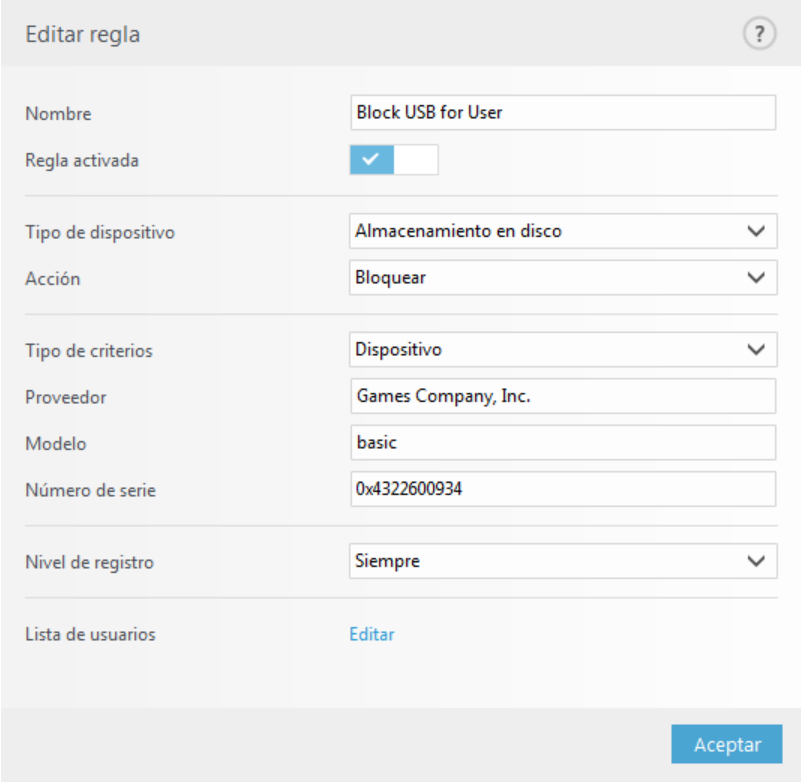
Haga clic en **Llenar** para rellenar automáticamente los parámetros del medio extraíble conectado a su ordenador.

Las reglas se muestran en orden de prioridad; las que tienen más prioridad se muestran más arriba en la lista. Las reglas pueden moverse haciendo clic en  **Superior/Arriba/Abajo/Inferior** tanto por separado como en grupo.

El Registro de control de dispositivos anota todas las ocasiones en las que se activa el Control de dispositivos. Las entradas de registro se pueden ver desde la ventana principal del programa de ESET Endpoint Antivirus en **Herramientas** > **Archivos de registro**.

3.9.1.5.2 Adición de reglas de control de dispositivos

Una regla de control de dispositivos define la acción que se realizará al conectar al ordenador un dispositivo que cumple los criterios de la regla.



Introduzca una descripción de la regla en el campo **Nombre** para mejorar la identificación. Haga clic en el conmutador situado junto a **Regla activada** para activar o desactivar esta regla, lo cual puede ser de utilidad cuando no se quiere eliminar una regla de forma permanente.

Aplicar durante: le permite aplicar la regla creada durante determinado tiempo. En el menú desplegable, seleccione el intervalo de tiempo creado. Si desea obtener más información, haga clic aquí.

Tipo de dispositivo

Elija el tipo de dispositivo externo en el menú desplegable (Almacenamiento en disco, Dispositivo portátil, Bluetooth, FireWire…). La información sobre el tipo de dispositivo se recopila del sistema operativo y se puede ver en el administrador de dispositivos del sistema cada vez que se conecta un dispositivo al ordenador. Los dispositivos de almacenamiento abarcan discos externos o lectores de tarjetas de memoria convencionales conectados mediante USB o FireWire. Los lectores de tarjetas inteligentes abarcan todos los lectores que tienen incrustado un circuito integrado, como las tarjetas SIM o las tarjetas de autenticación. Ejemplos de dispositivos de imagen son escáneres o cámaras. Como estos dispositivos solo proporcionan información sobre sus acciones y no sobre los usuarios, solo pueden bloquearse a nivel global.

NOTA
la función de la lista de usuarios no está disponible para tipos de dispositivos modernos. La regla se aplicará a todos los usuarios, y se eliminará la lista de usuarios actual.

Acción

El acceso a dispositivos que no son de almacenamiento se puede permitir o bloquear. En cambio, las reglas para los dispositivos de almacenamiento permiten seleccionar una de las siguientes configuraciones de derechos:

- **Lectura/Escritura**: se permitirá el acceso completo al dispositivo.
- **Bloquear**: se bloqueará el acceso al dispositivo.
- **Solo lectura**: solo se permitirá el acceso de lectura al dispositivo.

- **Advertir**: cada vez que se conecte un dispositivo se informará al usuario de si está permitido o bloqueado, y se efectuará una entrada de registro. Los dispositivos no se recuerdan, se seguirá mostrando una notificación en las siguientes conexiones del mismo dispositivo.

Tenga en cuenta que no todas las acciones (permisos) están disponibles para todos los tipos de dispositivos. Si se trata de un dispositivo de tipo almacenamiento, las cuatro acciones estarán disponibles. En el caso de los dispositivos que no son de almacenamiento solo hay tres disponibles (por ejemplo, **Solo lectura** no está disponible para Bluetooth, lo que significa que los dispositivos Bluetooth solo se pueden permitir, bloquear o emitirse una advertencia sobre ellos).

Tipo de criterios – Seleccione **Grupo de dispositivos** o **Dispositivo**.

Debajo se muestran otros parámetros que se pueden usar para ajustar las reglas y adaptarlas a dispositivos. Todos los parámetros distinguen entre mayúsculas y minúsculas:

- **Fabricante**: filtrado por nombre o identificador del fabricante.
- **Modelo**: el nombre del dispositivo.
- **Número de serie**: normalmente, los dispositivos externos tienen su propio número de serie. En el caso de los CD y DVD, el número de serie está en el medio, no en la unidad de CD.

NOTA
si estos parámetros están sin definir, la regla ignorará estos cambios a la hora de establecer la coincidencia. Los parámetros de filtrado de todos los campos de texto no distinguen entre mayúsculas y minúsculas, y no admiten caracteres comodín (*, ?).

CONSEJO
si desea ver información sobre un dispositivo, cree una regla para ese tipo de dispositivo, conecte el dispositivo al ordenador y, a continuación, consulte los detalles del dispositivo en el Registro de control de dispositivos.

Nivel de registro

- **Siempre**: registra todos los sucesos.
- **Diagnóstico**: registra la información necesaria para ajustar el programa.
- **Información**: registra los mensajes informativos, incluidos los mensajes de las actualizaciones realizadas con éxito y todos los registros anteriores.
- **Alerta**: registra errores graves y mensajes de alerta y los envía a ERA Server.
- **Ninguno**: no se registra nada.

Las reglas se pueden limitar a determinados usuarios o grupos de usuarios agregándolos a la **Lista de usuarios**:

- **Agregar**: abre el cuadro de diálogo **Tipos de objeto: Usuarios o grupos**, que le permite seleccionar los usuarios que desee.
- **Quitar**: elimina del filtro al usuario seleccionado.

NOTA
no todos los dispositivos se pueden filtrar mediante reglas de usuario (por ejemplo, los dispositivos de imagen no proporcionan información sobre los usuarios, sino únicamente sobre las acciones).

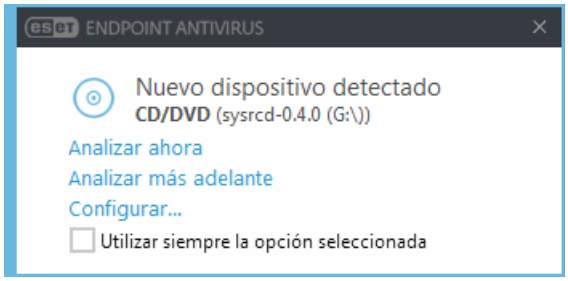
3.9.1.6 Medios extraíbles

ESET Endpoint Antivirus permite analizar los medios extraíbles (CD, DVD, USB, etc.) de forma automática. Este módulo le permite analizar un medio insertado. Esto puede ser útil cuando el administrador del ordenador quiere impedir que los usuarios utilicen medios extraíbles con contenido no solicitado.

Acción que debe efectuarse cuando se inserten medios extraíbles: seleccione la acción predeterminada que se realizará cuando se inserte un medio extraíble en el ordenador (CD, DVD o USB). Si selecciona **Mostrar las opciones de análisis**, se mostrará una ventana en la que puede seleccionar la acción deseada:

- **No analizar**: no se realizará ninguna acción y se cerrará la ventana **Nuevo dispositivo detectado**.
- **Análisis automático del dispositivo**: se realizará un análisis del ordenador a petición del medio extraíble insertado.
- **Mostrar las opciones de análisis**: abre la sección de configuración de medios extraíbles.

Cuando se inserta un medio extraíble aparece la siguiente ventana:



Analizar ahora: activa el análisis del medio extraíble.

Analizar más adelante: el análisis del medio extraíble se pospone.

Configuración: abre la configuración avanzada.

Utilizar siempre la opción seleccionada: cuando se seleccione esta opción, se realizará la misma acción la próxima vez que se introduzca un medio extraíble.

Además, ESET Endpoint Antivirus presenta funciones de control de dispositivos, lo que le permite definir reglas para el uso de dispositivos externos en un ordenador dado. Encontrará más detalles sobre el control de dispositivos en la sección Control de dispositivos.

3.9.1.7 Análisis de estado inactivo

El análisis de estado inactivo se activa en **Configuración avanzada**, en **Antivirus** > **Análisis de estado inactivo** > **Básico**. Coloque el conmutador situado junto a **Activar el análisis de estado inactivo** en la posición **Activado** para activar esta característica. Cuando el ordenador se encuentra en estado inactivo, se lleva a cabo un análisis silencioso de todos los discos locales del ordenador. Consulte Activadores de la detección del estado inactivo para ver una lista completa de condiciones que se deben cumplir para activar el análisis de estado inactivo.

De forma predeterminada, el análisis de estado inactivo no se ejecutará si el ordenador (portátil) está funcionando con batería. Puede anular este parámetro activando el conmutador situado junto a **Ejecutar aunque el ordenador esté funcionando con la batería** en Configuración avanzada.

Active **Activar el registro de sucesos** de la configuración avanzada para guardar un informe del análisis del ordenador en la sección Archivos de registro (en la ventana principal del programa, haga clic en **Herramientas** > **Archivos de registro** y seleccione **Análisis del ordenador** en el menú desplegable **Registrar**).

La detección de estado inactivo se ejecutará cuando el ordenador se encuentre en uno de los estados siguientes:

- Pantalla apagada o con protector de pantalla
- Bloqueo del ordenador
- Cierre de sesión de usuario

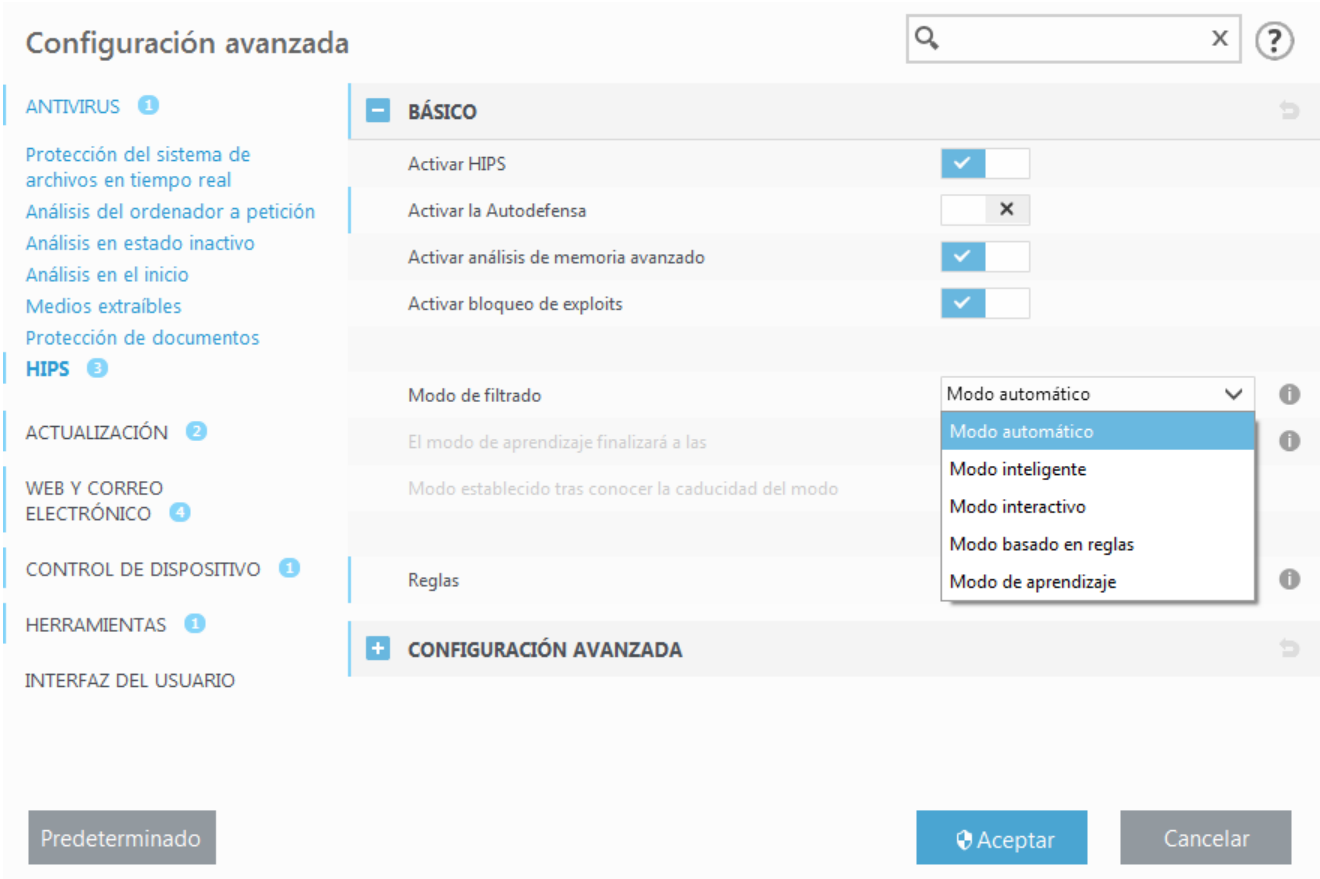
Haga clic en Configuración de parámetros del motor ThreatSense para modificar los parámetros de análisis (por ejemplo, métodos de detección) del análisis de estado inactivo.

3.9.1.8 Sistema de prevención de intrusiones del host (HIPS)

ADVERTENCIA
Solo debe modificar la configuración de HIPS si es un usuario experimentado. Una configuración incorrecta de los parámetros de HIPS puede provocar inestabilidad en el sistema.

El **Sistema de prevención de intrusiones del host** (HIPS) protege el sistema frente a código malicioso o cualquier actividad no deseada que intente menoscabar la seguridad del ordenador. Este sistema combina el análisis avanzado del comportamiento con funciones de detección del filtro de red para controlar los procesos, archivos y claves de registro. HIPS es diferente de la protección del sistema de archivos en tiempo real y no es un cortafuegos; solo supervisa los procesos que se ejecutan dentro del sistema operativo.

Los ajustes del HIPS se puede encontrar en **Configuración avanzada** (F5) > **Antivirus** > **HIPS** > **Básico**. El estado de HIPS (activado/desactivado) se muestra en la ventana principal de ESET Endpoint Antivirus, dentro de **Configuración** > **Ordenador**.



ESET Endpoint Antivirus utiliza la tecnología de **Autodefensa** integrada como parte del HIPS para impedir que el software malicioso dañe o desactive la protección antivirus y antiespía. La autodefensa evita la manipulación de procesos, claves de registro y archivos cruciales del sistema y de ESET.

Análisis avanzado de memoria: trabaja conjuntamente con el Bloqueador de exploits para aumentar la protección frente a código malicioso que utiliza los métodos de ofuscación y cifrado para evitar su detección mediante productos de protección frente a este tipo de código. El análisis avanzado de memoria está activado de forma predeterminada. Puede obtener más información sobre este tipo de protección en el glosario.

El **Bloqueador de exploits** se ha diseñado para fortificar aquellas aplicaciones que sufren más ataques, como los navegadores de Internet, los lectores de archivos pdf, los clientes de correo electrónico y los componentes de MS Office. El bloqueador de exploits está activado de forma predeterminada. Puede obtener más información sobre este tipo de protección en el glosario.

Protección contra ransomware es otra capa de protección que funciona como parte de la función HIPS. Para que la protección contra ransomware funcione, debe tener activado el sistema de reputación LiveGrid®. Puede obtener más información sobre este tipo de protección aquí.

El filtrado se puede realizar en cualquiera de los cuatro modos:

Modo automático: las operaciones están activadas, con la excepción de aquellas bloqueadas mediante reglas predefinidas que protegen el sistema.

Modo inteligente: solo se informará al usuario de los sucesos muy sospechosos.

Modo interactivo: el usuario debe confirmar las operaciones.

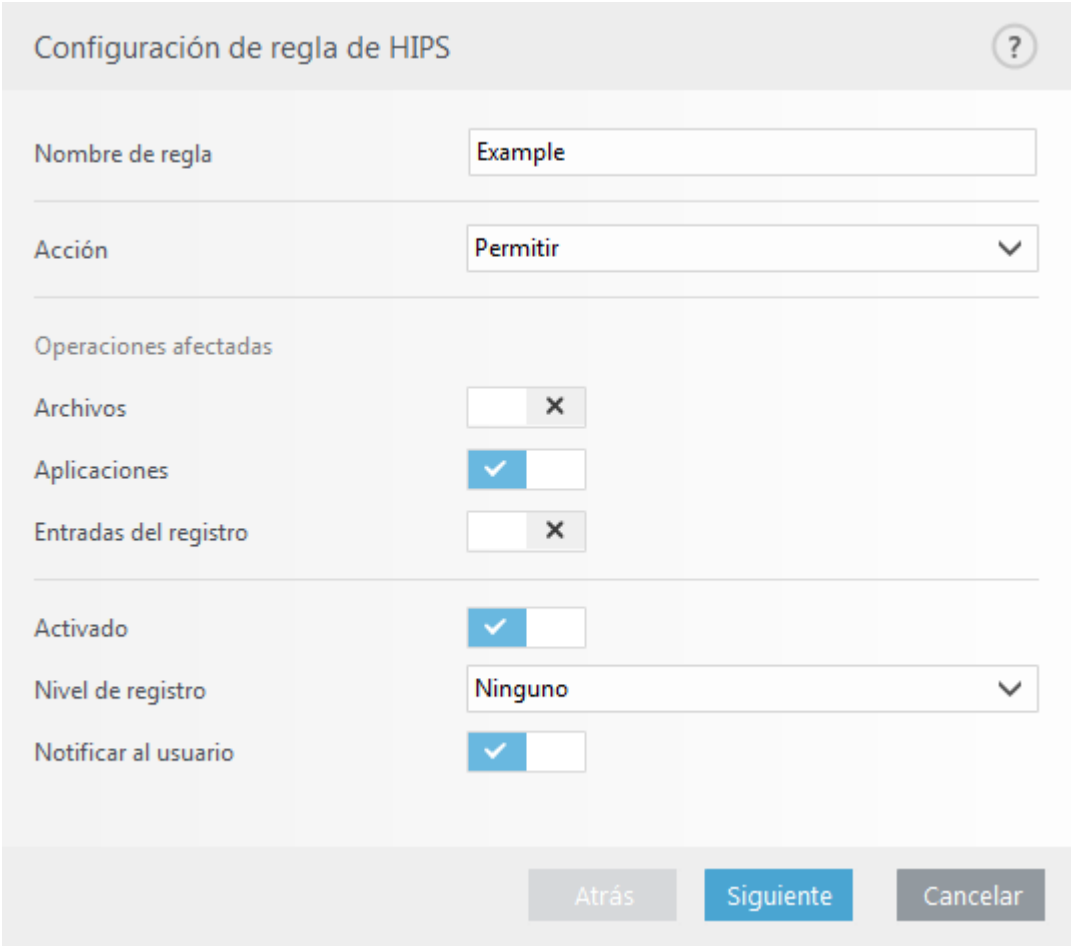
Modo basado en reglas: las operaciones están bloqueadas.

Modo de aprendizaje: las operaciones están activadas y se crea una regla después de cada operación. Las reglas creadas en este modo se pueden ver en el Editor de reglas, pero su prioridad es inferior a la de las reglas creadas manualmente o en el modo automático. Si selecciona el Modo de aprendizaje en el menú desplegable del modo de filtrado de HIPS, el ajuste **El modo de aprendizaje finalizará a las** estará disponible. Seleccione el periodo durante el que desea activar el modo de aprendizaje; la duración máxima es de 14 días. Cuando transcurra la duración especificada sele pedirá que modifique las reglas creadas por el HIPS mientras estaba en modo de aprendizaje. También puede elegir un modo de filtrado distinto o posponer la decisión y seguir usando el modo de aprendizaje.

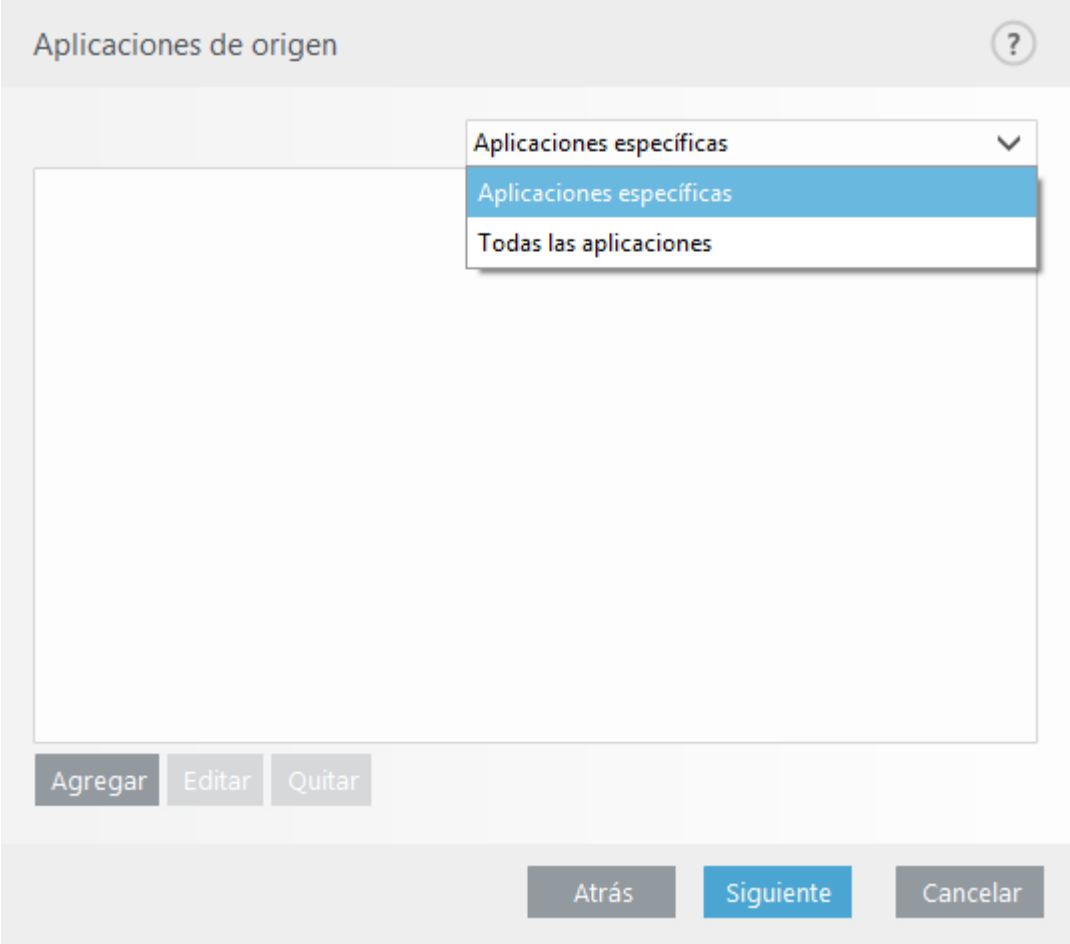
Modo establecido tras conocer la caducidad del modo: defina a qué modo de filtrado revertirá el cortafuegos de ESET Endpoint Antivirus una vez que transcurra el período de tiempo para el modo de aprendizaje.

El sistema HIPS supervisa los sucesos del sistema operativo y reacciona de acuerdo con reglas similares a las que utiliza el cortafuegos. Haga clic en **Modificar** para abrir la ventana de gestión de reglas de HIPS. Aquí puede seleccionar, crear, modificar o eliminar reglas.

En el ejemplo siguiente vamos a ver cómo restringir comportamientos no deseados de las aplicaciones:



1. Asigne un nombre a la regla y seleccione **Bloquear** en el menú desplegable **Acción**.
2. En la sección **Operaciones afectadas**, seleccione al menos una operación para la regla.
3. Seleccione el **Registro de severidad** en el menú desplegable. El administrador remoto puede recopilar los registros con detalle de Advertencia.
4. Seleccione la barra deslizante situada junto a **Notificar al usuario** para mostrar una notificación siempre que se aplique una regla. Haga clic en **Siguiente**.



5. En la ventana **Aplicaciones de origen**, seleccione **Todas las aplicaciones** en el menú desplegable para aplicar la nueva regla a todas aquellas aplicaciones que intenten realizar cualquiera de las operaciones seleccionadas. Haga clic en **Siguiente**.
6. En la siguiente ventana, seleccione la barra deslizante situada junto a **Modificar el estado de otra aplicación** y haga clic en **Siguiente** (todas las operaciones se describen en la ayuda del producto, a la que puede acceder pulsando la tecla F1).
7. Seleccione **Aplicaciones específicas** en el menú desplegable y haga clic en **Agregar** para agregar una o más aplicaciones que desee bloquear.
8. Haga clic en **Finalizar** para guardar la nueva regla.

3.9.1.8.1 Configuración avanzada

Las opciones siguientes son útiles para depurar y analizar el comportamiento de una aplicación:

Controladores con carga siempre autorizada: los controladores seleccionados pueden cargarse siempre sea cual sea el modo de filtrado configurado, a menos que la regla del usuario los bloquee de forma explícita.

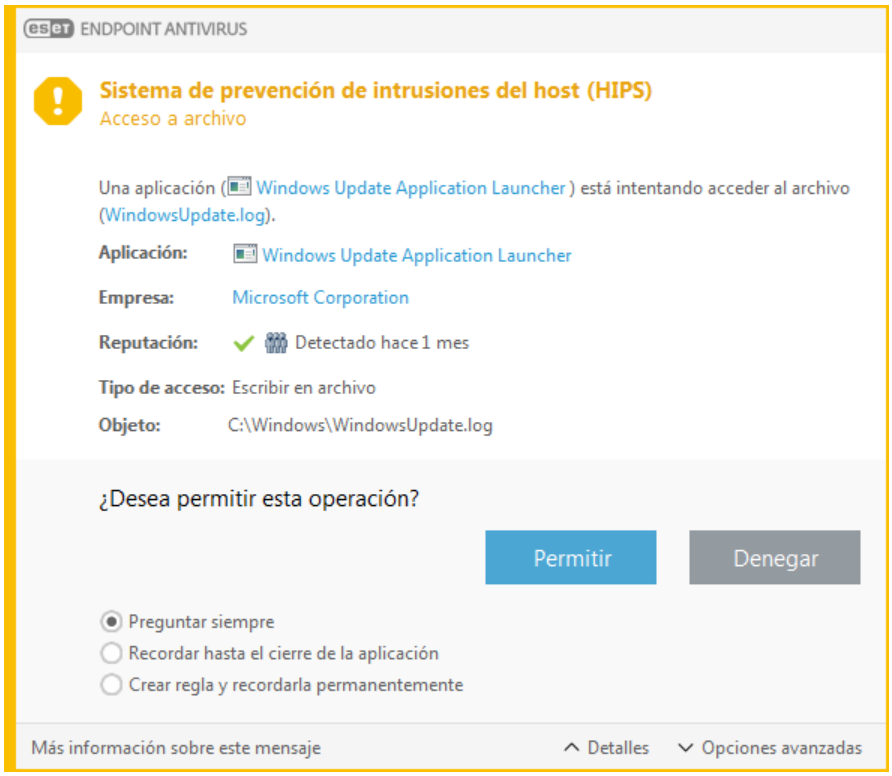
Registrar todas las operaciones bloqueadas: todas las operaciones bloqueadas se anotarán en el registro de HIPS.

Notificar cuando se produzcan cambios en las aplicaciones de inicio: muestra una notificación en el escritorio cada vez que se agrega o se elimina una aplicación del inicio del sistema.

Consulte nuestro artículo de la base de conocimiento para ver una versión actualizada de esta página de ayuda.

3.9.1.8.2 Ventana interactiva de HIPS

Si la acción predeterminada para una regla es **Preguntar**, se mostrará un cuadro de diálogo cada vez que se desencadene dicha regla. Puede seleccionar entre **Bloquear** y **Permitir** la operación. Si no selecciona una opción en el tiempo indicado, se aplican las reglas para seleccionar la nueva acción.



El cuadro de diálogo permite crear reglas de acuerdo con cualquier nueva acción que detecte HIPS y definir las condiciones en las que se permite o se rechaza dicha acción. Los parámetros exactos se pueden consultar haciendo clic en **Más información**. Las reglas creadas con este método se tratan igual que las creadas manualmente, por lo que una regla creada desde un cuadro de diálogo puede ser menos específica que la regla que activó dicho cuadro de diálogo. Esto significa que, después de crear esta regla, la misma operación puede activar la misma ventana.

Recordar temporalmente esta acción para este proceso provoca que se use la acción (**Permitir/Bloquear**) hasta que se cambien las reglas o el modo de filtrado, se actualice el módulo HIPS o se reinicie el sistema. Después de cualquiera de estas tres acciones, las reglas temporales se eliminarán.

3.9.1.8.3 Se ha detectado un comportamiento potencial de ransomware

Esta ventana interactiva aparecerá cuando se detecte un comportamiento potencial de ransomware. Puede seleccionar entre **Bloquear** y **Permitir** la operación.

El cuadro de diálogo le permite **enviar el archivo para su análisis** o **excluirlo de la detección**. Haga clic en **Detalles** para ver parámetros de detección concretos.

IMPORTANTE
Para que la protección contra ransomware funcione correctamente, ESET Live Grid debe estar activado.

3.9.1.9 Modo de presentación

El modo de presentación es una característica para usuarios que exigen un uso del software sin interrupciones y sin ventanas emergentes, así como un menor uso de la CPU. Este modo también se puede utilizar para que las presentaciones no se vean interrumpidas por la actividad del módulo antivirus. Cuando está activado, se desactivan todas las ventanas emergentes y las tareas programadas no se ejecutan. La protección del sistema sigue ejecutándose en segundo plano, pero no requiere la intervención del usuario.

Haga clic en **Configuración** > **Ordenador** y, a continuación, haga clic en el conmutador situado junto a **Modo de presentación** para activarlo de forma manual. En **Configuración avanzada** (F5), haga clic en **Herramientas** > **Modo de presentación** y, a continuación, haga clic en el conmutador situado junto a **Activar el modo de presentación automáticamente, al ejecutar aplicaciones en modo de pantalla completa** para que ESET Endpoint Antivirus active este modo automáticamente cuando se ejecuten aplicaciones a pantalla completa. Activar el modo de presentación constituye un riesgo de seguridad potencial, por lo que el icono de estado de la protección disponible en la barra de tareas se volverá naranja y mostrará un signo de alerta. Esta alerta también se puede ver en la ventana principal del programa donde verá el mensaje **El modo de presentación está activado** en naranja.

Si selecciona **Activar el modo de presentación automáticamente, al ejecutar aplicaciones en modo de pantalla completa**, el modo de presentación se activará cuando inicie una aplicación a pantalla completa y se detendrá automáticamente cuando cierre dicha aplicación. Esta función es muy útil para que el modo de presentación se inicie de inmediato al empezar un juego, abrir una aplicación a pantalla completa o iniciar una presentación.

También puede seleccionar **Desactivar el modo de presentación automáticamente después de** para definir la cantidad de tiempo, en minutos, que tardará en desactivar el modo de presentación automáticamente.

3.9.1.10 Análisis en el inicio

De forma predeterminada, la comprobación automática de los archivos en el inicio se realizará al iniciar el sistema o durante actualizaciones de los módulos. Este análisis depende de las tareas y la configuración del Planificador de tareas.

Las opciones de análisis en el inicio forman parte de la tarea **Verificación de archivos de inicio del sistema** del Planificador de tareas. Para modificar la configuración del análisis en el inicio, seleccione **Herramientas** > **Planificador de tareas**, haga clic en **Verificación automática de los archivos de inicio** y en **Modificar**. En el último paso, aparece la ventana Verificación de la ejecución de archivos en el inicio (consulte el siguiente capítulo para obtener más detalles).

Para obtener instrucciones detalladas acerca de la creación y gestión de tareas del Planificador de tareas, consulte Creación de tareas nuevas.

3.9.1.10.1 Comprobación de la ejecución de archivos en el inicio

Al crear una tarea programada de comprobación de archivos en el inicio del sistema, tiene varias opciones para ajustar los siguientes parámetros:

El menú desplegable **Analizar destinos** especifica la profundidad de análisis de los archivos ejecutados al iniciar el sistema basado en un sofisticado algoritmo secreto. Los archivos se organizan en orden descendente de acuerdo con los siguientes criterios:

- **Todos los archivos registrados** (se analiza el mayor número de archivos)
- **Archivos usados pocas veces**
- **Archivos usados ocasionalmente**
- **Archivos usados frecuentemente**
- **Solo los archivos usados con más frecuencia** (se analiza el menor número de archivos)

También se incluyen dos grupos específicos:

- **Archivos ejecutados antes del inicio de sesión del usuario**: contiene archivos de ubicaciones a las que se puede tener acceso sin que el usuario haya iniciado sesión (incluye casi todas las ubicaciones de inicio como servicios, objetos auxiliares del navegador, notificación del registro de Windows, entradas del Planificador de tareas de Windows, archivos dll conocidos, etc.).
- **Archivos en ejecución después del registro del usuario**: contiene archivos de ubicaciones a las que solo se puede tener acceso cuando el usuario se ha registrado (incluye archivos que solo ejecuta un usuario específico, generalmente los archivos de *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Las listas de los archivos que se analizan son fijas para cada grupo de los anteriores.

Prioridad de análisis: el nivel de prioridad empleado para determinar cuándo se iniciará un análisis:

- **Cuando el procesador esté desocupado**: la tarea se ejecutará solo cuando el sistema esté inactivo.
- **Muy baja**: cuando la carga del sistema es la más baja posible.
- **Baja**: con poca carga del sistema.
- **Normal**: con carga media del sistema.

3.9.1.11 Protección de documentos

La característica de protección de documentos analiza los documentos de Microsoft Office antes de que se abran y los archivos descargados automáticamente con Internet Explorer como, por ejemplo, elementos de Microsoft ActiveX. La protección de documentos proporciona un nivel de protección adicional a la protección en tiempo real del sistema de archivos y se puede desactivar para mejorar el rendimiento en sistemas que no están expuestos a un volumen elevado de documentos de Microsoft Office.

La opción **Integrar en el sistema** activa el sistema de protección. Para modificar esta opción, pulse F5 para abrir la ventana Configuración avanzada y haga clic en **Antivirus** > **Protección de documentos** en el árbol de configuración avanzada.

Esta característica se activa mediante aplicaciones que utilizan la Antivirus API de Microsoft (por ejemplo, Microsoft Office 2000 y superior, o Microsoft Internet Explorer 5.0 y superior).

3.9.1.12 Exclusiones

Las exclusiones le permiten excluir archivos y carpetas del análisis. Para garantizar que se analizan todos los objetos en busca de amenazas, le recomendamos que solo cree exclusiones cuando sea absolutamente necesario. Puede que haya situaciones en las que necesite excluir un objeto, como durante el análisis de entradas de una base de datos grande que ralentice el ordenador o software que entre en conflicto con el análisis (por ejemplo, software de copia de seguridad).

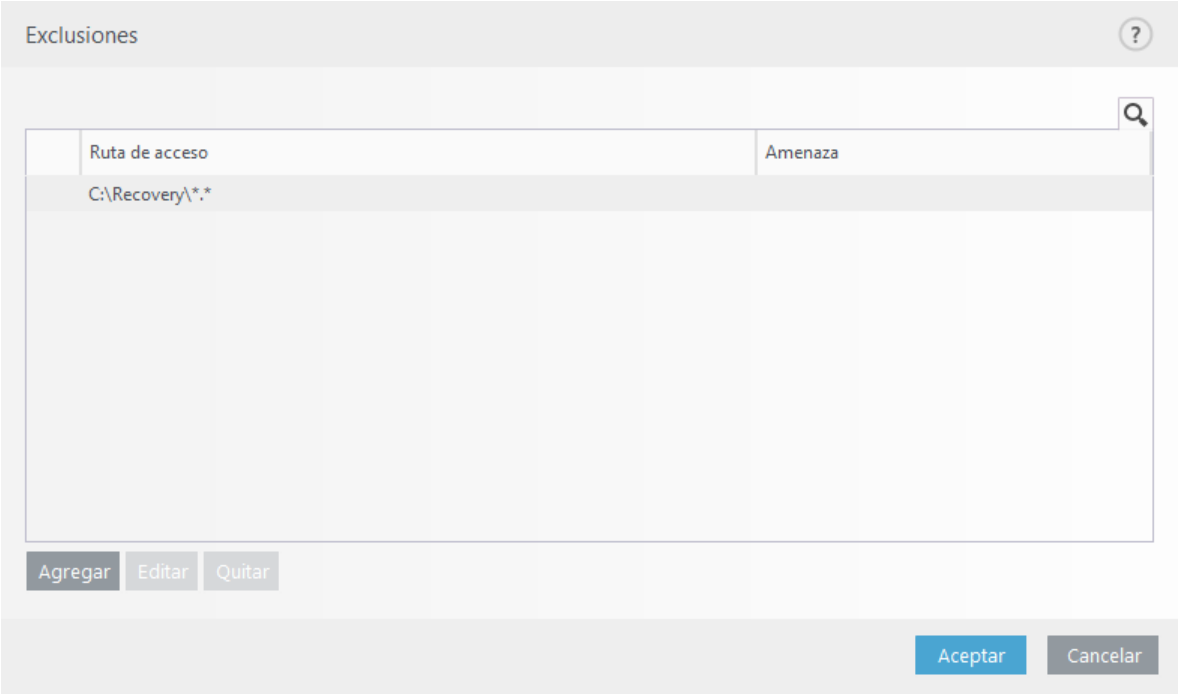
Para excluir un objeto del análisis:

1. Haga clic en **Agregar**.
2. Escriba la ruta de un objeto o selecciónelo en la estructura de árbol.

Puede utilizar comodines para abarcar un grupo de archivos. El signo de interrogación (?) representa un carácter único variable, y el asterisco (*) una cadena variable de cero o más caracteres.

Ejemplos

- Si desea excluir todos los archivos de una carpeta, escriba la ruta de acceso a la carpeta y utilice la máscara "*.*".
- Para excluir una unidad entera, incluidos archivos y subcarpetas, utilice la máscara "D:*".
- Si desea excluir únicamente los archivos .doc, utilice la máscara "*.doc".
- Si el nombre de un archivo ejecutable tiene un determinado número de caracteres (y los caracteres varían) y solo conoce con seguridad el primero (por ejemplo, "D"), utilice el siguiente formato: "D????.exe". Los símbolos de interrogación sustituyen a los caracteres que faltan (desconocidos).



NOTA
El módulo de protección del sistema de archivos en tiempo real o de análisis del ordenador no detectará las amenazas que contenga un archivo si este cumple los criterios de exclusión del análisis.

Columnas

Ruta: ruta de los archivos y carpetas excluidos.

Amenaza: si se muestra el nombre de una amenaza junto a un archivo excluido, significa que el archivo se excluye únicamente para dicha amenaza. Si este archivo se infecta más adelante con otro código malicioso, el módulo antivirus lo detectará. Este tipo de exclusión únicamente se puede utilizar para determinados tipos de amenazas, y se puede crear bien en la ventana de alerta de amenaza que informa de la amenaza (haga clic en **Mostrar opciones avanzadas** y, a continuación, seleccione **Excluir de la detección**) o bien en **Herramientas** > **Cuarentena,** haciendo clic con el botón derecho del ratón en el archivo en cuarentena y seleccionando **Restaurar y excluir de la detección** en el menú contextual.

Elementos de control

Agregar: excluye los objetos de la detección.

Modificar: le permite modificar las entradas seleccionadas.

Quitar: elimina las entradas seleccionadas.

3.9.1.13 Parámetros de ThreatSense

La tecnología ThreatSense consta de muchos métodos complejos de detección de amenazas. Esta tecnología es proactiva, lo que significa que también proporciona protección durante la fase inicial de expansión de una nueva amenaza. Utiliza una combinación de análisis de código, emulación de código, firmas genéricas y firmas de virus que funcionan de forma conjunta para mejorar en gran medida la seguridad del sistema. El motor de análisis es capaz de controlar varios flujos de datos de forma simultánea, de manera que maximiza la eficacia y la velocidad de detección. Además, la tecnología ThreatSense elimina los rootkits eficazmente.

Las opciones de configuración del motor ThreatSense permiten al usuario especificar distintos parámetros de análisis:

- los tipos de archivos y extensiones que se deben analizar;
- la combinación de diferentes métodos de detección;
- los niveles de desinfección, etc.

Para acceder a la ventana de configuración, haga clic en **Configuración de los parámetros del motor ThreatSense** en la ventana Configuración avanzada de cualquier módulo que utilice la tecnología ThreatSense (consulte más abajo). Es posible que cada escenario de seguridad requiera una configuración diferente. Con esto en mente, ThreatSense se puede configurar individualmente para los siguientes módulos de protección:

- Protección del sistema de archivos en tiempo real
- Análisis de estado inactivo
- Análisis en el inicio
- Protección de documentos
- Protección del cliente de correo electrónico
- Protección del tráfico de Internet
- Análisis del ordenador

Los parámetros de ThreatSense están altamente optimizados para cada módulo y su modificación puede afectar al funcionamiento del sistema de forma significativa. Por ejemplo, la modificación de los parámetros para que siempre analicen empaquetadores de ejecución en tiempo real o la activación de la heurística avanzada en el módulo de protección del sistema de archivos en tiempo real podrían implicar la ralentización del sistema (normalmente, solo se analizan archivos recién creados mediante estos métodos). Se recomienda que no modifique los parámetros predeterminados de ThreatSense para ninguno de los módulos, a excepción de Análisis del ordenador.

Objetos a analizar

En esta sección se pueden definir los componentes y archivos del ordenador que se analizarán en busca de amenazas.

Memoria operativa: busca amenazas que ataquen a la memoria operativa del sistema.

Sectores de inicio/UEFI: analiza los sectores de inicio y la UEFI en busca de rootkits, bootkits y demás malware. Si desea obtener más información, haga clic aquí.

Archivos de correo: el programa admite las siguientes extensiones: DBX (Outlook Express) y EML.

Archivos comprimidos: el programa admite las siguientes extensiones: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE y muchas más.

Archivos comprimidos de autoextracción: los archivos comprimidos de autoextracción (SFX) son archivos que no necesitan programas especializados (archivos comprimidos) para descomprimirse.

Empaquetadores en tiempo real: después de su ejecución, los empaquetadores de tiempo de ejecución (a diferencia de los archivos estándar) se descomprimen en la memoria. Además de los empaquetadores estáticos estándar (UPX, yoda, ASPack, FSG, etc.), el módulo de análisis permite reconocer varios tipos de empaquetadores adicionales gracias a la emulación de códigos.

Opciones de análisis

Seleccione los métodos empleados al analizar el sistema en busca de infiltraciones. Están disponibles las opciones siguientes:

Heurística: la heurística es un algoritmo que analiza la actividad (maliciosa) de los programas. La principal ventaja de esta tecnología es la habilidad para identificar software malicioso que no existía o que el motor de detección anterior no conocía. Su desventaja es la probabilidad (muy pequeña) de falsas alarmas.

Heurística avanzada/Firmas de ADN: la heurística avanzada es un algoritmo heurístico único desarrollado por ESET, y optimizado para detectar gusanos informáticos y troyanos escritos en lenguajes de programación de alto nivel. El uso de la heurística avanzada mejora en gran medida la detección de amenazas por parte de los productos de ESET. Las firmas pueden detectar e identificar virus de manera fiable. Gracias al sistema de actualización automática, las nuevas firmas están disponibles en cuestión de horas cuando se descubre una amenaza. Su desventaja es que únicamente detectan los virus que conocen (o versiones ligeramente modificadas).

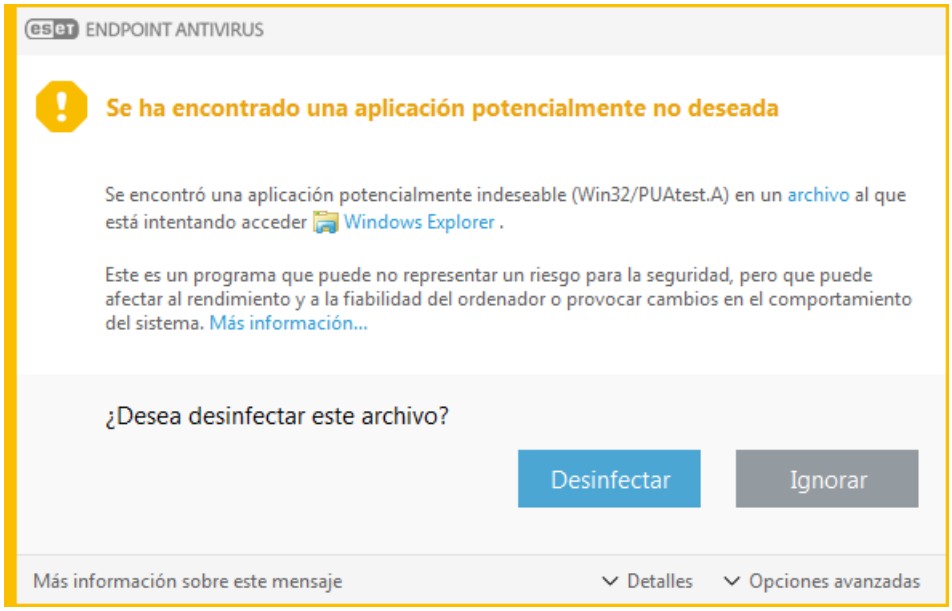
Una aplicación potencialmente indeseable es un programa que contiene software publicitario, instala barras de herramientas o tiene otros objetivos poco claros. Existen determinados casos en los que un usuario podría creer que

las ventajas de una aplicación potencialmente indeseada compensan los riesgos asociados. Este es el motivo que hace que ESET asigne a dichas aplicaciones una categoría de riesgo más baja, en comparación con otros tipos de software malicioso, como los troyanos o los gusanos.

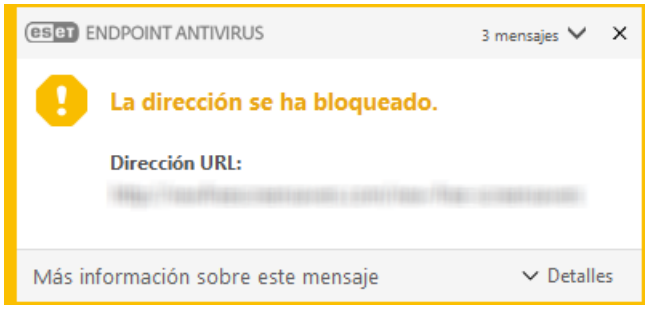
Advertencia: Amenaza potencial encontrada

Cuando se detecte una aplicación potencialmente indeseable podrá elegir qué medida desea tomar:

1. **Desinfectar/Desconectar**: esta opción finaliza la acción e impide que la amenaza potencial acceda a su sistema.
2. **Sin acciones**: esta opción permite que una amenaza potencial entre en el sistema.
3. Si desea permitir que la aplicación se ejecute en su ordenador en el futuro sin que se interrumpa, haga clic en **Más información/Mostrar opciones avanzadas** y, a continuación, active la casilla de verificación situada junto a **Excluir de la detección**.

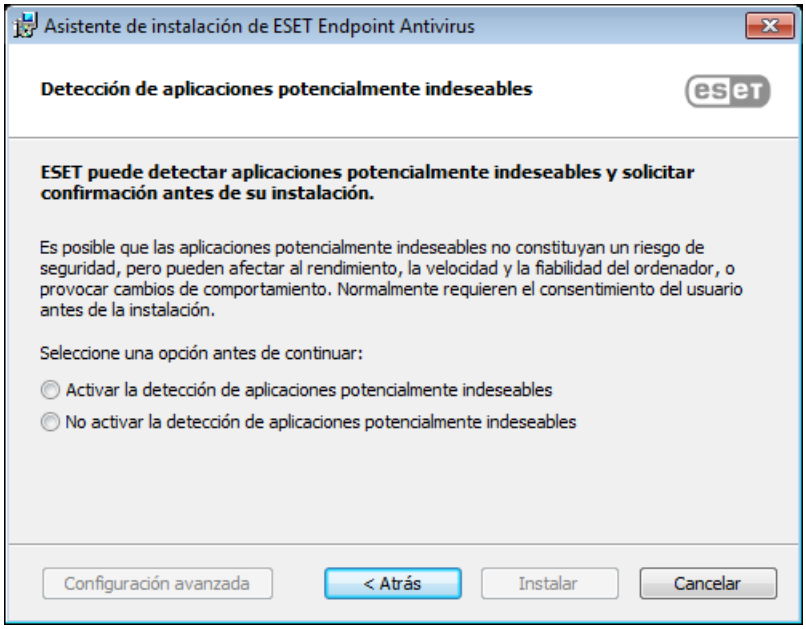


Si se detecta una aplicación potencialmente indeseable que no se puede desinfectar, aparecerá la ventana de notificación **La dirección se ha bloqueado** en la esquina inferior derecha de la pantalla. Si desea obtener más información sobre este suceso, diríjase a **Herramientas** > **Archivos de registro** > **Sitios web filtrados** desde el menú principal.



Aplicaciones potencialmente indeseables: Configuración

Durante la instalación del producto de ESET puede decidir si desea activar la detección de aplicaciones potencialmente indeseables, como se muestra a continuación:

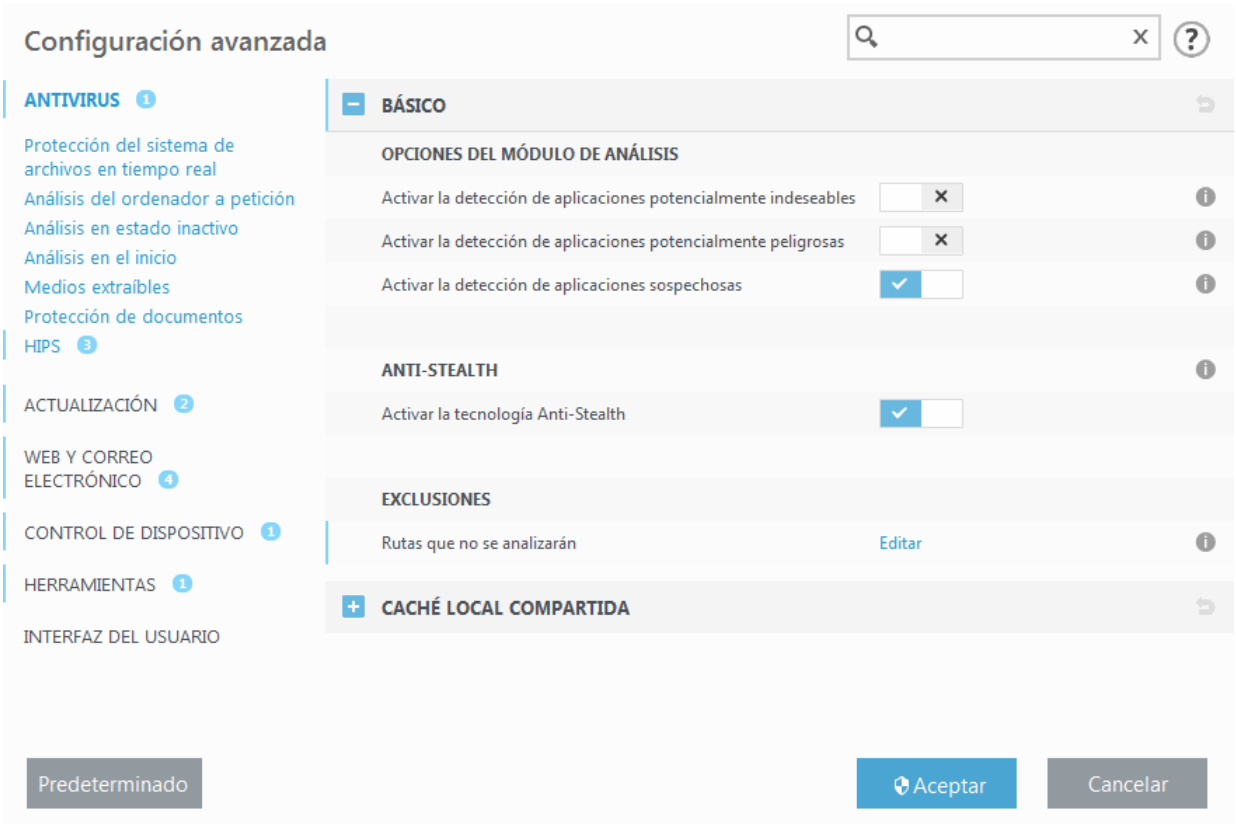


ADVERTENCIA

Las aplicaciones potencialmente indeseables podrían instalar software publicitario, barras de herramientas o contener otras características de programa no deseadas e inseguras.

Estos ajustes pueden modificarse en cualquier momento en la configuración del programa. Si desea activar o desactivar la detección de aplicaciones potencialmente indeseadas, inseguras o sospechosas, siga estas instrucciones:

1. Abra su producto de ESET. ¿Cómo abro mi producto de ESET?
2. Pulse la tecla **F5** para acceder a **Configuración avanzada**.
3. Haga clic en **Antivirus** y active o desactive las opciones **Activar la detección de aplicaciones potencialmente indeseables**, **Activar la detección de aplicaciones potencialmente peligrosas** y **Activar la detección de aplicaciones sospechosas** según sus propias preferencias. Confirme haciendo clic en **Aceptar**.



Aplicaciones potencialmente indeseables: Software encubierto

El software encubierto es un tipo de modificación de aplicación especial que utilizan algunos sitios web de alojamiento de archivos. Se trata de una herramienta de terceros que instala el programa que quería descargar pero que incorpora software adicional, como barras de herramientas o software publicitario. El software adicional podría, además, cambiar la página de inicio de su navegador web y la configuración de búsqueda. Igualmente, los sitios web de alojamiento de archivos no suelen informar al proveedor del software ni al usuario que realiza la descarga de que se han efectuado dichas modificaciones, ni tampoco facilitan la tarea de rechazar la modificación. Por estos motivos, ESET clasifica el software encubierto como un tipo de aplicación potencialmente indeseable, con el fin de permitir al usuario aceptar o rechazar la descarga.

Consulte el siguiente artículo de la base de conocimiento de ESET para ver una versión actualizada de esta página de ayuda.

Si desea obtener más información, haga clic aquí.

Aplicaciones potencialmente peligrosas: Aplicaciones potencialmente peligrosas es la clasificación utilizada para programas comerciales legítimos, como herramientas de acceso remoto, aplicaciones para detectar contraseñas y registradores de pulsaciones (programas que registran todas las teclas que pulsa un usuario). Esta opción está desactivada de manera predeterminada.

Desinfección

Las opciones de desinfección determinan el comportamiento del análisis durante la desinfección de archivos infectados. Hay 3 niveles de desinfección:

Sin desinfección: los archivos infectados no se desinfectan automáticamente. El programa mostrará una ventana de alerta y permitirá que el usuario seleccione una acción. Este nivel es adecuado para usuarios avanzados que conocen los pasos necesarios en caso de amenaza.

Desinfección normal: el programa intenta desinfectar o eliminar un archivo infectado de manera automática, de acuerdo con una acción predefinida (según el tipo de amenaza). La eliminación y la detección de un archivo infectado se marca mediante una notificación en la esquina inferior derecha de la pantalla. Si no es posible seleccionar la acción correcta de manera automática, el programa ofrece otras acciones que seguir. Lo mismo ocurre cuando no se puede completar una acción predefinida.

Desinfección estricta: el programa desinfecta o elimina todos los archivos infectados. Las únicas excepciones son los

archivos del sistema. Si no es posible desinfectarlos, se insta al usuario a que seleccione una acción indicada en una ventana de alerta.

ADVERTENCIA

si un archivo comprimido contiene archivos infectados, se puede tratar de dos maneras: en el modo estándar (Desinfección estándar), se elimina el archivo comprimido completo si este está compuesto únicamente por código malicioso; y en el modo **Desinfección exhaustiva**, el archivo se elimina si contiene al menos una porción de código malicioso, independientemente del estado de los demás archivos.

Exclusiones

Una extensión es una parte del nombre de archivo delimitada por un punto que define el tipo y el contenido del archivo. En esta sección de la configuración de parámetros de ThreatSense, es posible definir los tipos de archivos que se desean analizar.

Otros

Al configurar parámetros del motor ThreatSense para un análisis del ordenador a petición, dispone también de las siguientes opciones en la sección **Otros**:

Analizar secuencias de datos alternativas (ADS): las secuencias de datos alternativos utilizadas por el sistema de archivos NTFS son asociaciones de carpetas y archivos que no se detectan con técnicas de análisis ordinarias. Muchas amenazas intentan evitar los sistemas de detección haciéndose pasar por flujos de datos alternativos.

Realizar análisis en segundo plano con baja prioridad: cada secuencia de análisis consume una cantidad determinada de recursos del sistema. Si se trabaja con programas cuyo consumo de recursos constituye una carga importante para el sistema, es posible activar el análisis en segundo plano con baja prioridad y reservar los recursos para las aplicaciones.

Registrar todos los objetos: si se selecciona esta opción, el archivo de registro mostrará todos los archivos analizados, incluso los que no están infectados. Por ejemplo, si se detecta una amenaza en un archivo comprimido, en el registro se incluirán también los archivos sin infectar del archivo comprimido.

Activar optimización inteligente: si la opción Optimización inteligente está activada, se utiliza la configuración más óptima para garantizar el nivel de análisis más eficaz y, al mismo tiempo, mantener la máxima velocidad de análisis posible. Los diferentes módulos de protección analizan de forma inteligente, con métodos de análisis distintos y aplicados a tipos de archivo específicos. Si la optimización inteligente está desactivada, solamente se aplica la configuración definida por el usuario en el núcleo ThreatSense de los módulos donde se realiza el análisis.

Preservar el último acceso con su fecha y hora: seleccione esta opción para guardar la hora de acceso original de los archivos analizados, en lugar de actualizarlos (por ejemplo, para utilizar con sistemas de copia de seguridad de datos).

Límites

En la sección Límites se puede especificar el tamaño máximo de los objetos y los niveles de archivos anidados que se analizarán:

Configuración de los objetos

Tamaño máximo del objeto: define el tamaño máximo de los objetos que se analizarán. El módulo antivirus analizará solo los objetos que tengan un tamaño menor que el especificado. Esta opción solo deben cambiarla usuarios avanzados que tengan motivos específicos para excluir del análisis objetos más grandes. Valor predeterminado: *ilimitado*.

Tiempo máximo de análisis para el objeto (seg.): define el tiempo máximo asignado para analizar un objeto. Si se especifica un valor definido por el usuario, el módulo antivirus detendrá el análisis de un objeto cuando se haya agotado el tiempo, independientemente de si el análisis ha finalizado o no. Valor predeterminado: *ilimitado*.

Configuración del análisis de archivos comprimidos

Nivel de anidamiento de archivos: especifica el nivel máximo de análisis de archivos. Valor predeterminado: *10*.

Tamaño máx. de archivo en el archivo comprimido: esta opción permite especificar el tamaño máximo de archivo de los archivos contenidos en archivos comprimidos (una vez extraídos) que se van a analizar. Valor predeterminado: *ilimitado*.

NOTA
No se recomienda cambiar los valores predeterminados; en circunstancias normales, no debería haber motivo para hacerlo.

3.9.1.13.1 Exclusiones

Una extensión es una parte del nombre de archivo delimitada por un punto que define el tipo y el contenido del archivo. En esta sección de la configuración de parámetros de ThreatSense, es posible definir los tipos de archivos que se desean analizar.

De forma predeterminada, se analizan todos los archivos. Se puede agregar cualquier extensión a la lista de archivos excluidos del análisis.

A veces es necesario excluir archivos del análisis si, por ejemplo, el análisis de determinados tipos de archivo impide la correcta ejecución del programa que utiliza determinadas extensiones. Por ejemplo, quizás sea aconsejable excluir las extensiones .edb, .eml y .tmp cuando se utilizan servidores Microsoft Exchange.

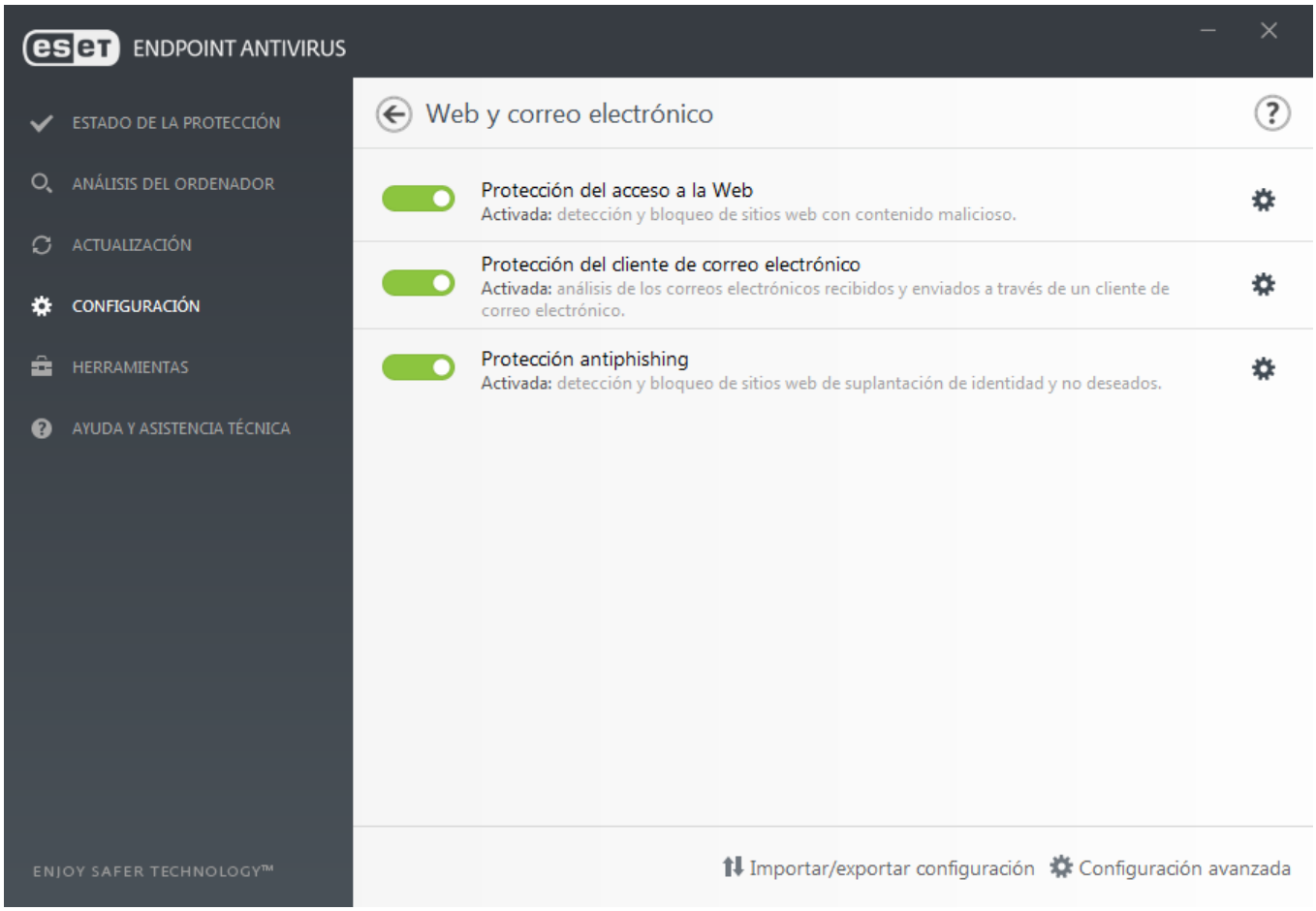
Con los botones **Agregar** y **Quitar**, puede activar o prohibir el análisis de extensiones de archivo específicas. Para añadir una extensión nueva a la lista, haga clic en **Agregar**, escriba la extensión en el campo en blanco y, a continuación, haga clic en **Aceptar**. Seleccione **Introduzca múltiples valores** para añadir varias extensiones de archivos delimitadas por líneas, comas o punto y coma. Si está activada la selección múltiple, las extensiones se mostrarán en la lista. Seleccione una extensión en la lista y haga clic en **Quitar** para eliminarla de la lista. Si desea modificar una extensión seleccionada, haga clic en **Modificar**.

Se pueden usar los símbolos especiales ? (signo de interrogación). El signo de interrogación representa cualquier símbolo.

NOTA
para mostrar la extensión (el tipo de archivo) de todos los archivos de un sistema operativo Windows, desmarque la casilla **Ocultar las extensiones de archivo para tipos de archivo conocidos** en **Panel de control** > **Opciones de carpeta** > **Ver**.

3.9.2 Web y correo electrónico

Las opciones de configuración de la Web y el correo electrónico se encuentra en **Configuración** > **Web y correo electrónico**. Desde aquí puede acceder a configuraciones más detalladas del programa.



La conectividad de Internet es una característica estándar de cualquier ordenador personal. Lamentablemente también se ha convertido en el principal medio de transferencia de código malicioso, por eso es fundamental prestar la debida atención a la **protección del tráfico de Internet**.

La opción **Protección del cliente de correo electrónico** proporciona control de las comunicaciones por correo electrónico recibidas a través de los protocolos POP3 e IMAP. Con el programa de complemento para su cliente de correo electrónico, ESET Endpoint Antivirus ofrece control de todas las comunicaciones realizadas desde el cliente de correo electrónico (POP3, IMAP, HTTP y MAPI).

La **Protección antiphishing** es otra capa de protección que aumenta la defensa frente a sitios web ilegítimos que intentan adquirir contraseñas y otra información confidencial. La protección antiphishing se puede activar en el panel **Configuración** disponible en **Web y correo electrónico**. Consulte Protección antiphishing para obtener más información.

Desactivar: haga clic en el conmutador para desconectar la protección de la Web o el correo electrónico para navegadores Web y clientes de correo electrónico  .

3.9.2.1 Filtrado de protocolos

El motor de análisis ThreatSense, que integra a la perfección todas las técnicas avanzadas de análisis de código malicioso, proporciona la protección antivirus para los protocolos de aplicación. El filtrado de protocolos funciona de manera automática, independientemente del navegador de Internet o el cliente de correo electrónico utilizados. Para editar la configuración cifrada (SSL), vaya a **Web y correo electrónico** > **SSL**.

Activar el filtrado del contenido de los protocolos de aplicación: se puede utilizar para desactivar el filtrado de protocolos. Tenga en cuenta que muchos componentes de ESET Endpoint Antivirus (Protección del tráfico de Internet, Protección de protocolos de correo electrónico, Anti-Phishing, Control de acceso web) dependen de esto para funcionar.

Aplicaciones excluidas: le permite excluir determinadas aplicaciones del filtrado de protocolos. Esta opción es útil cuando el filtrado de protocolos provoca problemas de compatibilidad.

Direcciones IP excluidas: le permite excluir determinadas direcciones remotas del filtrado de protocolos. Esta opción es útil cuando el filtrado de protocolos provoca problemas de compatibilidad.

Clientes de correo electrónico y web: solo se utiliza en sistemas operativos Windows XP, y le permite seleccionar las aplicaciones para las que se filtra todo el tráfico con el filtrado de protocolos, independientemente de los puertos utilizados.

3.9.2.1.1 Clientes de correo electrónico y web

NOTA
la arquitectura Plataforma de filtrado de Windows (WFP) se empezó a aplicar en Windows Vista Service Pack 1 y Windows Server 2008, y se utiliza para comprobar la comunicación de red. La sección **Clientes de correo electrónico y web** no se encuentra disponible porque la tecnología WFP utiliza técnicas de supervisión especiales.

Dada la ingente cantidad de código malicioso que circula en Internet, la navegación segura es un aspecto crucial para la protección de los ordenadores. Las vulnerabilidades de los navegadores web y los vínculos fraudulentos sirven de ayuda a este tipo de código para introducirse en el sistema de incógnito; por este motivo, ESET Endpoint Antivirus se centra en la seguridad de los navegadores web. Cada aplicación que acceda a la red se puede marcar como un navegador de Internet. Las aplicaciones que ya utilicen protocolos para la comunicación o procedentes de la ruta seleccionada se pueden añadir a la lista de clientes web y de correo electrónico.

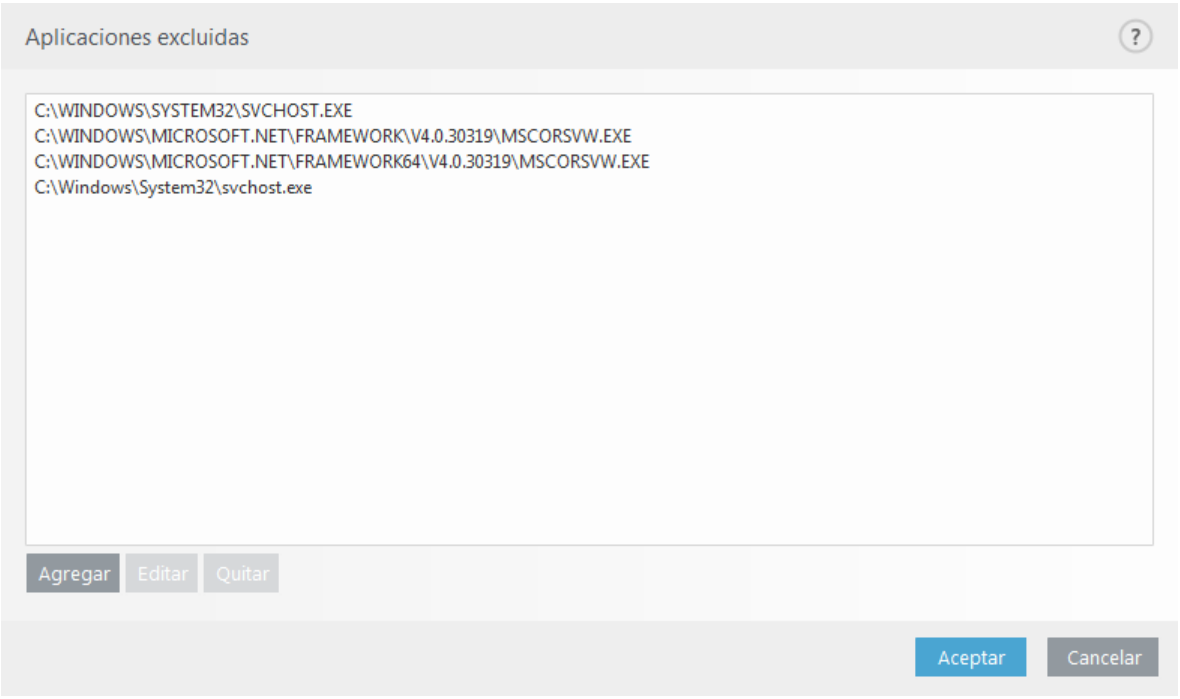
3.9.2.1.2 Aplicaciones excluidas

Para excluir del filtrado de protocolos la comunicación de aplicaciones de red específicas, añádalas a esta lista. No se comprobará la presencia de amenazas en la comunicación HTTP, POP3 e IMAP de las aplicaciones seleccionadas. Solo recomendamos utilizar esta técnica cuando las aplicaciones no funcionen correctamente con el filtrado de protocolos activado.

Las aplicaciones y los servicios que ya se hayan visto afectados por el filtrado de protocolos se mostrarán automáticamente al hacer clic en **Agregar**.

Modificar: modifique las entradas seleccionadas de la lista.

Quitar: elimina las entradas seleccionadas de la lista.



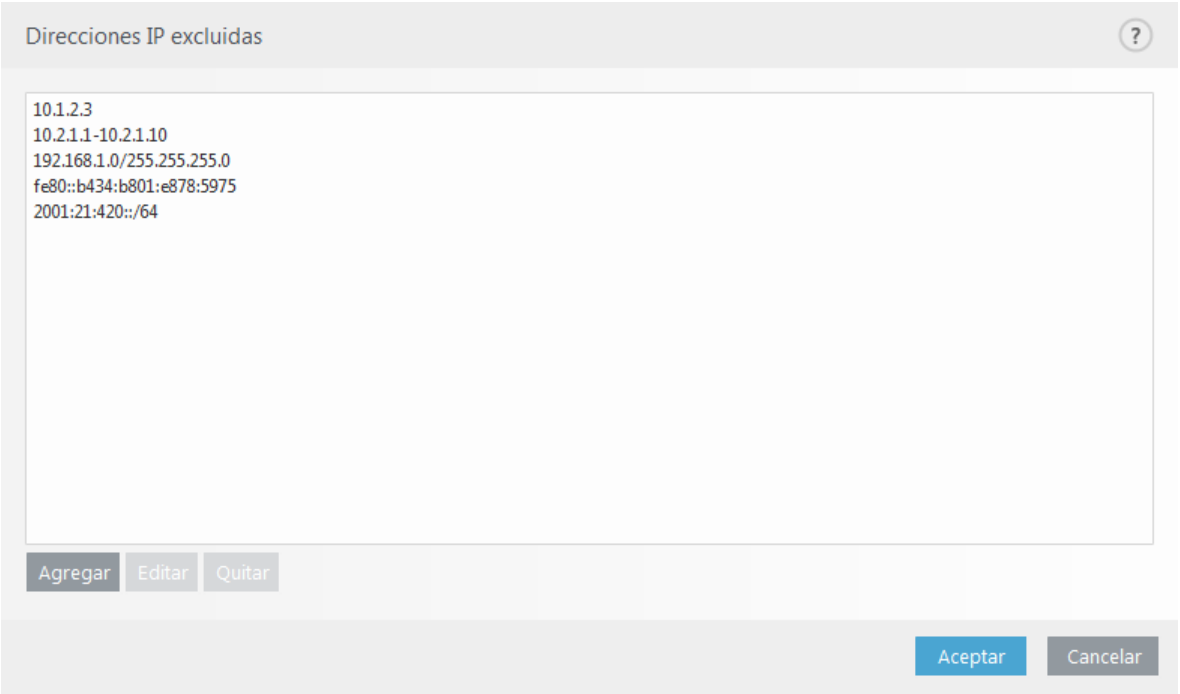
3.9.2.1.3 Direcciones IP excluidas

Las direcciones IP de esta lista no se incluirán en el filtrado de contenidos del protocolo. No se comprobará la presencia de amenazas en las comunicaciones HTTP/POP3/IMAP entrantes y salientes de las direcciones seleccionadas. Esta opción se recomienda únicamente para direcciones que se sabe que son de confianza.

Agregar: haga clic para agregar una dirección IP, un intervalo de direcciones o una subred de un punto remoto al que se aplicará una regla.

Modificar: modifique las entradas seleccionadas de la lista.

Quitar: elimina las entradas seleccionadas de la lista.



3.9.2.1.4 SSL/TLS

ESET Endpoint Antivirus puede buscar amenazas en las comunicaciones que utilizan el protocolo SSL. Puede utilizar varios modos de análisis para examinar las comunicaciones protegidas mediante el protocolo SSL: certificados de confianza, certificados desconocidos o certificados excluidos del análisis de comunicaciones protegidas mediante el protocolo SSL.

Activar el filtrado del protocolo SSL/TLS: si está desactivado el filtrado de protocolos, el programa no analizará las comunicaciones realizadas a través de SSL.

El **modo de filtrado del protocolo SSL/TLS** ofrece las opciones siguientes:

Modo automático: seleccione esta opción para analizar todas las comunicaciones protegidas mediante el protocolo SSL, excepto las protegidas por certificados excluidos del análisis. Si se establece una comunicación nueva que utiliza un certificado firmado desconocido, no se le informará y la comunicación se filtrará automáticamente. Si accede a un servidor con un certificado que no sea de confianza pero que usted ha marcado como de confianza (se encuentra en la lista de certificados de confianza), se permite la comunicación con el servidor y se filtra el contenido del canal de comunicación.

Modo interactivo: si introduce un sitio nuevo protegido mediante SSL (con un certificado desconocido), se muestra un cuadro de diálogo con las acciones posibles. Este modo le permite crear una lista de certificados SSL que se excluirán del análisis.

La **Lista de aplicaciones con filtrado SSL/TLS** permite personalizar el comportamiento de ESET Endpoint Antivirus para aplicaciones específicas

Lista de certificados conocidos le permite personalizar el comportamiento de ESET Endpoint Antivirus para certificados SSL específicos.

Excluir la comunicación con los dominios de confianza: la confianza en los dominios se determina mediante la lista blanca integrada.

Bloquear la comunicación cifrada utilizando el protocolo obsoleto SSL v2: la comunicación establecida con la versión anterior del protocolo SSL se bloqueará automáticamente.

Certificado raíz

Certificado raíz: para que la comunicación SSL funcione correctamente en los navegadores y clientes de correo electrónico, es fundamental que el certificado raíz de ESET se agregue a la lista de certificados raíz conocidos (editores). **Agregar el certificado raíz a los navegadores conocidos** debe estar activada. Seleccione esta opción para agregar el certificado raíz de ESET a los navegadores conocidos (por ejemplo, Opera y Firefox) de forma automática. En los navegadores que utilicen el almacén de certificados del sistema, el certificado se agregará automáticamente (por ejemplo, en Internet Explorer).

Para aplicar el certificado en navegadores no admitidos, haga clic en **Ver certificado** > **Detalles** > **Copiar en archivo** y, a continuación, impórtelo manualmente en el navegador.

Validez del certificado

Si el certificado no se puede verificar mediante el almacén de certificados TRCA: a veces no es posible verificar el certificado de un sitio web con el almacén de autoridades certificadoras de confianza (TRCA). Esto significa que el certificado ha sido firmado por algún usuario (por ejemplo, el administrador de un servidor web o una pequeña empresa) y que el hecho de confiar en él no siempre representa un riesgo. La mayoría de las empresas grandes (como los bancos) utilizan certificados firmados por TRCA. Si se ha seleccionado **Preguntar sobre la validez del certificado** (predeterminada), se le pedirá al usuario que seleccione la acción que desea realizar cuando se establezca la comunicación cifrada. Puede seleccionar **Bloquear las comunicaciones que usan el certificado** para finalizar siempre las conexiones cifradas a sitios que tienen certificados sin verificar.

Si el certificado no es válido o está dañado: significa que el certificado ha caducado o que la firma no es correcta. En este caso, se recomienda dejar seleccionada la opción **Bloquear las comunicaciones que usan el certificado**.

3.9.2.1.4.1 Conexión SSL crifrada

Si su sistema está configurado para utilizar el análisis del protocolo SSL, se mostrará un cuadro de diálogo para solicitarle que seleccione una acción en dos situaciones diferentes:

En primer lugar, si un sitio web utiliza un certificado no válido o que no se puede verificar y ESET Endpoint Antivirus está configurado para preguntar al usuario en estos casos (la opción predeterminada es sí para los certificados que no se pueden verificar y no para los que no son válidos), se abre un cuadro de diálogo para preguntarle si desea **Permitir** o **Bloquear** la conexión.

En segundo lugar, si el **Modo de filtrado del protocolo SSL** está establecido en **Modo interactivo**, se mostrará un cuadro de diálogo para cada sitio web para preguntarle si desea **Analizar** o **Ignorar** el tráfico. Algunas aplicaciones comprueban que nadie haya modificado ni inspeccionado su tráfico SSL en estos casos, ESET Endpoint Antivirus debe **Ignorar** el tráfico para que la aplicación siga funcionando.

En ambos casos, el usuario tiene la opción de recordar la acción seleccionada. Las acciones guardadas se almacenan en la **Lista de certificados conocidos**.

3.9.2.1.4.2 Lista de certificados conocidos

La **Lista de certificados conocidos** se puede utilizar para personalizar el comportamiento de ESET Endpoint Antivirus para determinados certificados SSL, así como para recordar las acciones elegidas al seleccionar el **Modo interactivo** en el **Modo de filtrado de protocolos SSL/TLS**. La lista se puede ver y modificar en **Configuración avanzada** (F5) > **Web y correo electrónico** > **SSL/TLS** > **Lista de certificados conocidos**.

La ventana **Lista de certificados conocidos** consta de estos elementos:

Columnas

Nombre: nombre del certificado.

Emisor del certificado: nombre del creador del certificado.

Sujeto del certificado: en este campo se identifica a la entidad asociada a la clave pública almacenada en el campo de clave pública del asunto.

Acceso: seleccione **Permitir** o **Bloquear** como **Acción del acceso** para permitir o bloquear la comunicación que protege este certificado, independientemente de su fiabilidad. Seleccione **Auto** para permitir los certificados de confianza y preguntar cuando uno no sea de confianza. Seleccione **Preguntar** para que el sistema siempre pregunte al usuario qué debe hacer.

Analizar: seleccione **Analizar** o **Ignorar** como **Acción de análisis** para analizar o ignorar la comunicación que protege este certificado. Seleccione **Auto** para que el sistema realice el análisis en el modo automático y pregunte en el modo interactivo. Seleccione **Preguntar** para que el sistema siempre pregunte al usuario qué debe hacer.

Elementos de control

Agregar: puede cargarse un certificado manualmente como un archivo con la extensión *.cer*, *.crt* o *.pem*. Haga clic en **Archivo** para cargar un certificado local, o haga clic en **URL** para especificar la ubicación de un certificado en línea.

Editar: seleccione el certificado que desea configurar y haga clic en **Editar**.

Quitar: seleccione el certificado que desea eliminar y haga clic en **Quitar**.

Aceptar/Cancelar: haga clic en **Aceptar** para guardar los cambios o en **Cancelar** para salir sin guardarlos.

3.9.2.1.4.3 Lista de aplicaciones con filtrado SSL/TLS

La **Lista de aplicaciones con filtrado SSL/TLS** se puede utilizar para personalizar el comportamiento de ESET Endpoint Antivirus para determinadas aplicaciones, así como para recordar las acciones elegidas al seleccionar el **Modo interactivo** en el **Modo de filtrado de protocolos SSL/TLS**. La lista se puede ver y modificar en **Configuración avanzada** (F5) > **Web y correo electrónico** > **SSL/TLS** > **Lista de aplicaciones con filtrado SSL/TLS**.

La ventana **Lista de aplicaciones con filtrado SSL/TLS** consta de estos elementos:

Columnas

Aplicación: nombre de la aplicación.

Acción de análisis: seleccione **Analizar** o **Ignorar** para analizar o ignorar la comunicación. Seleccione **Auto** para que el sistema realice el análisis en el modo automático y pregunte en el modo interactivo. Seleccione **Preguntar** para que el sistema siempre pregunte al usuario qué debe hacer.

Elementos de control

Agregar: agregue la aplicación filtrada.

Editar: seleccione el certificado que desea configurar y haga clic en **Editar**.

Eliminar: seleccione el certificado que desea eliminar y haga clic en **Quitar**.

Aceptar/Cancelar: haga clic en **Aceptar** para guardar los cambios o en **Cancelar** para salir sin guardarlos.

3.9.2.2 Protección del cliente de correo electrónico

3.9.2.2.1 Clientes de correo electrónico

La integración de ESET Endpoint Antivirus con clientes de correo electrónico aumenta el nivel de protección activa frente a código malicioso en los mensajes de correo electrónico. Si su cliente de correo electrónico es compatible, la integración se puede activar en ESET Endpoint Antivirus. Al activar la integración, la barra de herramientas de ESET Endpoint Antivirus se inserta directamente en el cliente de correo electrónico (la barra de herramientas de las versiones más recientes de Windows Live Mail no se inserta), aumentando así la eficacia de la protección de correo electrónico. Las opciones de integración están disponibles en **Configuración** > **Configuración avanzada** > **Web y correo electrónico** > **Protección del cliente de correo electrónico** > **Clientes de correo electrónico**.

Integración con el cliente de correo electrónico

Actualmente se admiten los siguientes clientes de correo electrónico: Microsoft Outlook, Outlook Express, Windows Mail y Windows Live Mail. La protección de correo electrónico funciona como un complemento para estos programas. La principal ventaja del complemento es el hecho de que es independiente del protocolo utilizado. Cuando el cliente de correo electrónico recibe un mensaje cifrado, este se descifra y se envía para el análisis de virus. Para ver una lista de clientes de correo electrónico compatibles y sus versiones, consulte el siguiente artículo de la base de conocimientos de ESET.

Aunque la integración no esté activada, la comunicación por correo electrónico sigue estando protegida por el módulo de protección del cliente de correo electrónico (POP3, IMAP).

Active **Deshabilitar la verificación en caso de cambios en el contenido del buzón de entrada** si el sistema se ralentiza cuando trabaja con su cliente de correo electrónico (solo MS Outlook). Esto puede suceder cuando recupera correo electrónico de Kerio Outlook Connector Store.

Correo electrónico a analizar

Activar protección del cliente de correo electrónico mediante complementos del cliente: cuando la protección del cliente de correo electrónico mediante el cliente de correo electrónico se encuentra desactivada, la comprobación del cliente de correo electrónico por medio del filtrado de protocolos seguirá estando activa.
Correo electrónico recibido: activa el análisis de los mensajes recibidos.
Correo electrónico enviado: activa el análisis de los mensajes enviados.
Correo electrónico leído: activa el análisis de los mensajes leídos.

Acción para realizar en correos electrónicos infectados

Sin acciones: si esta opción está activada, el programa identificará los archivos adjuntos infectados, pero dejará los mensajes sin realizar ninguna acción.
Eliminar mensajes: el programa informará al usuario sobre las amenazas y eliminará el mensaje.
Mover el correo electrónico a la carpeta de elementos eliminados: los mensajes infectados se moverán automáticamente a la carpeta Elementos eliminados.
Mover mensajes a la carpeta: los mensajes infectados se moverán automáticamente a la carpeta especificada.

Carpeta: especifique la carpeta personalizada a la que desea mover el correo infectado que se detecte.

Repetir análisis después de actualizar: activa el nuevo análisis tras una actualización del motor de detección.

Aceptar los resultados de los análisis realizados por otros módulos: al seleccionar esta opción, el módulo de protección de correo electrónico acepta los resultados del análisis de otros módulos de protección (análisis de los protocolos POP3 e IMAP).

NOTA
Le recomendamos que active las opciones **Activar protección del correo electrónico mediante complementos del cliente** y **Activar la protección del correo electrónico mediante el filtrado de protocolos** (Configuración avanzada (F5) > Web y correo electrónico > Protección de clientes de correo electrónico > Protocolos de correo electrónico).

3.9.2.2.2 Protocolos de correo electrónico

Los protocolos IMAP y POP3 son los más utilizados para recibir comunicaciones por correo electrónico en una aplicación de cliente de correo. ESET Endpoint Antivirus proporciona protección para estos protocolos, independientemente del cliente de correo electrónico utilizado, y sin necesidad de volver a configurar el cliente de correo electrónico.

La verificación de los protocolos IMAP/IMAPS y POP3/POP3S se puede configurar en Configuración avanzada. Para acceder a esta configuración, despliegue **Web y correo electrónico** > **Protección del cliente de correo electrónico** > **Protocolos de correo electrónico**.

Activar la protección de los protocolos de correo electrónico: permite la comprobación de protocolos de correo electrónico.

En Windows Vista y versiones posteriores, los protocolos IMAP y POP3 se detectan automáticamente y se analizan en todos los puertos. En Windows XP solo se analizan para todas las aplicaciones los **Puertos usados por el protocolo IMAP/POP3**, y se analizan todos los puertos en busca de aplicaciones marcadas como Clientes de correo electrónico y web.

ESET Endpoint Antivirus también admite el análisis de los protocolos IMAPS y POP3S, que utilizan un canal cifrado para transferir información entre el servidor y el cliente. ESET Endpoint Antivirus comprueba la comunicación con los protocolos SSL (capa de sockets seguros) y TLS (seguridad de la capa de transporte). El programa solo analizará el tráfico de los puertos definidos en **Puertos usados por el protocolo IMAPS/POP3S**, independientemente de la versión del sistema operativo.

Las comunicaciones cifradas no se analizarán cuando se utilice la configuración predeterminada. Para activar el análisis de la comunicación cifrada, vaya a SSL/TLS en Configuración avanzada, haga clic en **Web y correo electrónico** > **SSL/TLS** y seleccione **Activar el filtrado del protocolo SSL/TLS**.

3.9.2.2.3 Alertas y notificaciones

La protección de correo electrónico proporciona control de las comunicaciones por correo electrónico recibidas a través de los protocolos POP3 e IMAP. Con el complemento para Microsoft Outlook y otros clientes de correo electrónico, ESET Endpoint Antivirus ofrece control de todas las comunicaciones desde el cliente de correo electrónico (POP3, MAPI, IMAP, HTTP). Al examinar los mensajes entrantes, el programa utiliza todos los métodos de análisis avanzados incluidos en el motor de análisis ThreatSense. Esto significa que la detección de programas maliciosos tiene lugar incluso antes de que se compare con el motor de detección. El análisis de las comunicaciones de los protocolos POP3 e IMAP es independiente del cliente de correo electrónico utilizado.

Las opciones de esta función están disponibles en **Configuración avanzada**, en **Web y correo electrónico** > **Protección del cliente de correo electrónico** > **Alertas y notificaciones**.

Configuración de parámetros del motor ThreatSense: la configuración avanzada del análisis de virus le permite configurar objetos de análisis, métodos de detección, etc. Haga clic aquí para ver la ventana de configuración detallada del análisis de virus.

Después de analizar un mensaje de correo electrónico, se puede adjuntar al mensaje una notificación del análisis. Puede elegir entre las opciones **Notificar en los mensajes recibidos y leídos, Agregar una nota al asunto de los correos electrónicos infectados que fueron recibidos y leídos** o **Notificar en los mensajes enviados**. Tenga en cuenta que en ocasiones puntuales es posible que los mensajes con etiqueta se omitan en mensajes HTML problemáticos o que hayan sido falsificados por código malicioso. Los mensajes con etiqueta se pueden agregar a los mensajes recibidos y leídos, a los mensajes enviados o a ambos. Las opciones disponibles son:

- **Nunca**: no se agregará ningún mensaje con etiqueta.
- **Solo a mensajes infectados**: únicamente se marcarán como analizados los mensajes que contengan software malicioso (opción predeterminada).
- **A todos los mensajes analizados**: el programa agregará un mensaje a todo el correo analizado.

Agregar una nota al asunto de los correos electrónicos infectados enviados: desactive esta casilla de verificación si no desea que la protección de correo electrónico incluya una alerta de virus en el asunto de los mensajes infectados. Esta función permite el filtrado sencillo y por asunto de los mensajes infectados (si su programa de

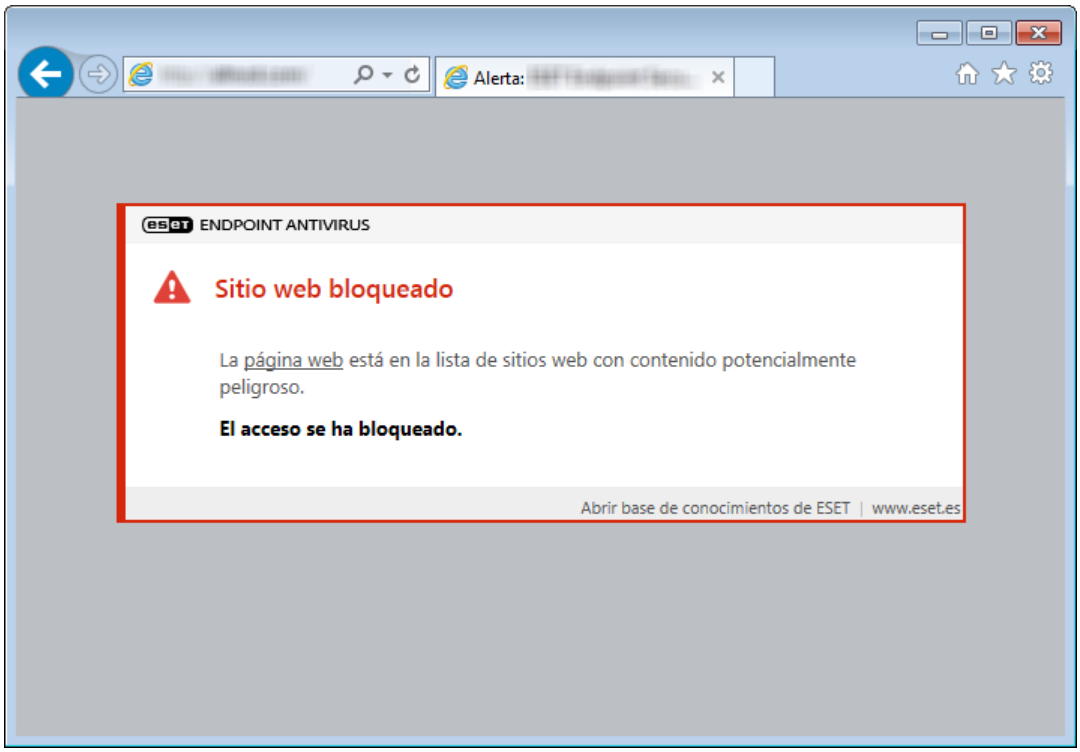
correo electrónico lo admite). Además, aumenta la credibilidad ante el destinatario y, si se detecta una amenaza, proporciona información valiosa sobre el nivel de amenaza de un correo electrónico o remitente determinado.

En mensajes infectados, agregar en el Asunto la siguiente etiqueta: modifique esta plantilla si desea modificar el formato de prefijo del asunto de un mensaje infectado. Esta función sustituye el asunto del mensaje *"Hello"* con un valor de prefijo especificado *"[virus]"* por el formato siguiente: *"[virus] Hello"*. La variable *%VIRUSNAME%* hace referencia a la amenaza detectada.

3.9.2.3 Protección del acceso a Internet

La conectividad de Internet es una característica estándar de la mayoría de los ordenadores personales. Lamentablemente, también se ha convertido en el principal medio de transferencia de código malicioso. La protección del tráfico de Internet funciona supervisando la comunicación entre navegadores web y servidores remotos, y cumple con las reglas HTTP (Protocolo de transferencia de hipertexto) y HTTPS (comunicación cifrada).

El acceso a las páginas web que se sabe que contienen código malicioso se bloquea antes de descargar contenido. El motor de análisis ThreatSense analiza todas las demás páginas web cuando se cargan y bloquean en caso de detección de contenido malicioso. La protección del tráfico de Internet ofrece dos niveles de protección: bloqueo por lista negra y bloqueo por contenido.



Le recomendamos encarecidamente que deje activada la opción de protección del tráfico de Internet. Se puede acceder a esta opción desde la ventana principal del programa de ESET Endpoint Antivirus, en **Configuración** > **Web y correo electrónico** > **Protección del tráfico de Internet**.

Las opciones siguientes están disponibles en **Configuración avanzada** (F5) > **Web y correo electrónico** > **Protección del tráfico de Internet**:

- **Protocolos web**: le permite configurar la supervisión de estos protocolos estándar que utilizan la mayoría de los navegadores de Internet.
- **Gestión de direcciones URL**: aquí puede especificar las direcciones HTTP que desea bloquear, permitir o excluir del análisis.
- **Configuración de parámetros del motor ThreatSense**: la configuración avanzada del análisis de virus le permite configurar opciones como los tipos de objetos que desea analizar (mensajes de correo electrónico, archivos comprimidos, etc.), los métodos de detección para la protección del tráfico de Internet, etc.

3.9.2.3.1 Protocolos web

De forma predeterminada, ESET Endpoint Antivirus está configurado para supervisar el protocolo HTTP que utilizan la mayoría de los navegadores de Internet.

En Windows Vista y versiones posteriores, el tráfico HTTP se supervisa siempre en todos los puertos y para todas las aplicaciones. En Windows XP se puede modificar la opción **Puertos utilizados por el protocolo HTTP** en **Configuración avanzada** (F5) > **Web y correo electrónico** > **Protección del tráfico de Internet** > **Protocolos web** > **Configuración del análisis HTTP**. El tráfico HTTP se supervisa en los puertos especificados para todas las aplicaciones, y en todos los puertos de las aplicaciones marcadas como Clientes de correo electrónico y web.

ESET Endpoint Antivirus admite también la comprobación del protocolo HTTPS. La comunicación HTTPS utiliza un canal cifrado para transferir información entre el servidor y el cliente. ESET Endpoint Antivirus comprueba la comunicación mediante los protocolos SSL (capa de sockets seguros) y TLS (seguridad de la capa de transporte). El programa solo analizará el tráfico de los puertos definidos en **Puertos utilizados por el protocolo HTTPS**, independientemente de la versión del sistema operativo.

La comunicación cifrada no se analizará cuando se utilice la configuración predeterminada. Para activar el análisis de la comunicación cifrada, vaya a SSL/TLS en Configuración avanzada, haga clic en **Web y correo electrónico** > **SSL/TLS** y seleccione **Activar el filtrado del protocolo SSL/TLS**.

3.9.2.3.2 Gestión de direcciones URL

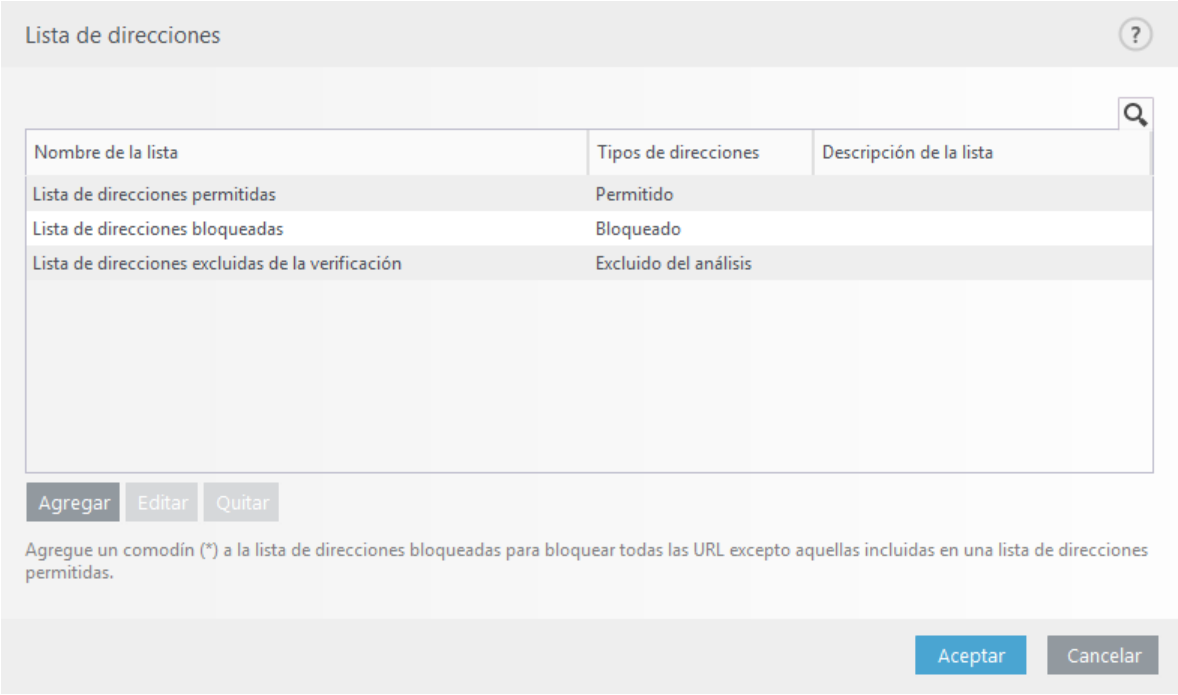
En esta sección puede especificar las direcciones HTTP que desea bloquear, permitir o excluir del análisis.

No podrá acceder a los sitios web de **Lista de direcciones bloqueadas**, a menos que también se incluyan en **Lista de direcciones permitidas**. Cuando acceda a sitios web que se encuentran en **Lista de direcciones excluidas de la verificación**, no se buscará código malicioso en ellos.

Debe seleccionar **Activar el filtrado del protocolo SSL** si desea filtrar las direcciones HTTPS, además de las páginas web HTTP. Si no lo hace, solo se agregarán los dominios de los sitios HTTP que haya visitado, pero no la URL completa.

En todas las listas, pueden utilizarse los símbolos especiales * (asterisco) y ? (signo de interrogación). El asterisco sustituye a cualquier número o carácter y el signo de interrogación, cualquier carácter. Tenga especial cuidado al especificar direcciones excluidas, ya que la lista solo debe contener direcciones seguras y de confianza. Del mismo modo, es necesario asegurarse de que los símbolos * y ? se utilizan correctamente en esta lista. Consulte Agregar dirección HTTP/máscara de dominio para obtener información sobre cómo detectar un dominio completo con todos sus subdominios de forma segura. Para activar una lista, active la opción **Lista activa**. Si desea recibir una notificación cuando se introduzca una dirección de la lista actual, active **Notificar al aplicar**.

Si desea bloquear todas las direcciones HTTP menos las incluidas en la **Lista de direcciones permitidas** activa, agregue el símbolo * a la **Lista de direcciones bloqueadas** activa.



Agregar: crea una lista nueva, que se suma a las predefinidas. Esta opción puede ser útil si se desea dividir varios grupos de direcciones de forma lógica. Por ejemplo, una lista de direcciones bloqueadas puede contener direcciones de algunas listas negras públicas externas, mientras que otra contiene su propia lista negra. Esto facilita la actualización de la lista externa sin que la suya se vea afectada.

Modificar: modifica las listas existentes. Utilice esta opción para agregar o quitar direcciones en las listas.

Quitar: elimina la lista existente. Esta opción solo se puede usar en listas creadas con **Agregar**, no en las predeterminadas.

3.9.2.4 Protección Anti-Phishing

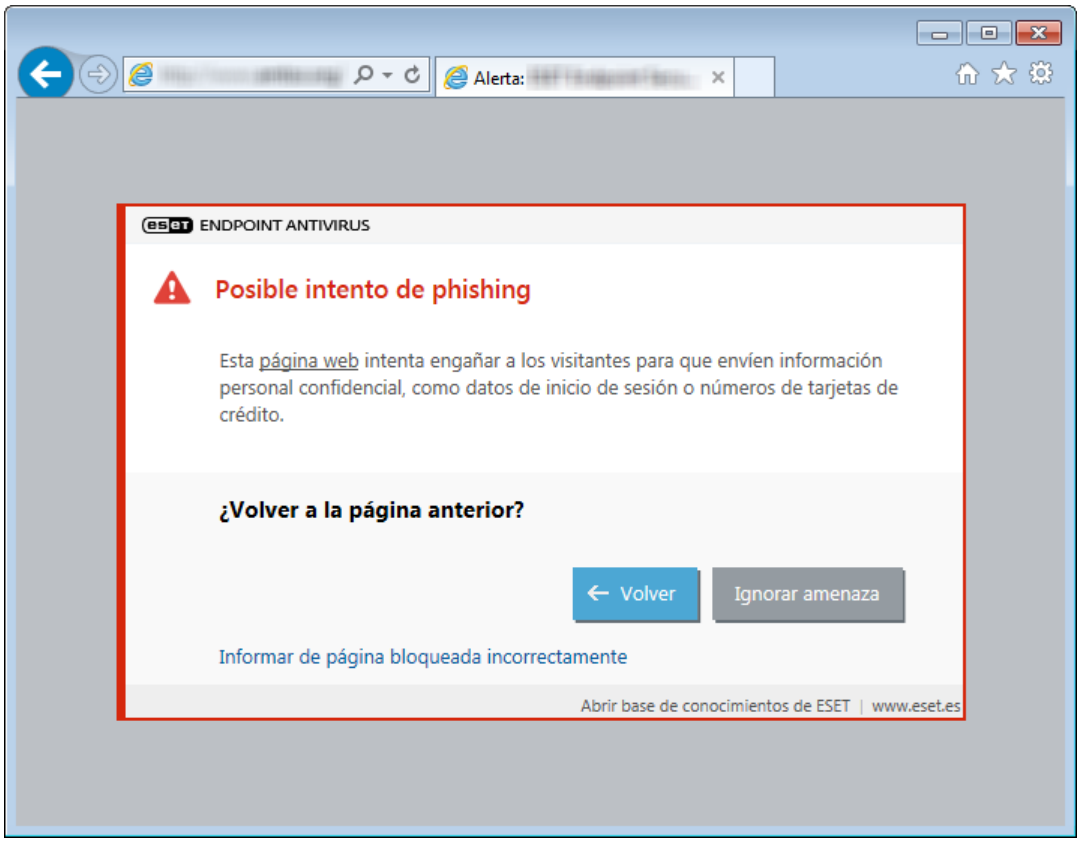
El término phishing, o suplantación de la identidad, define una actividad delictiva que usa técnicas de ingeniería social (manipulación de los usuarios para obtener información confidencial). Su objetivo con frecuencia es acceder a datos confidenciales como, por ejemplo, números de cuentas bancarias, códigos PIN, etc. Puede obtener más información sobre esta actividad en el glosario. ESET Endpoint Antivirus incluye protección frente al phishing que bloquea páginas web conocidas por distribuir este tipo de contenido.

Recomendamos encarecidamente que active la protección Anti-Phishing en ESET Endpoint Antivirus. Para ello, abra **Configuración avanzada** (F5) y acceda a **Web y correo electrónico** > **Protección Anti-Phishing**.

Visite nuestro artículo de la base de conocimiento para obtener más información sobre la protección Anti-Phishing de ESET Endpoint Antivirus.

Acceso a un sitio web de phishing

Cuando entre en un sitio web de phishing reconocido se mostrará el siguiente cuadro de diálogo en su navegador web. Si aun así quiere acceder al sitio web, haga clic en **Ir al sitio** (no recomendado).



NOTA
los posibles sitios de phishing que se han incluido en la lista blanca expirarán de forma predeterminada después de unas horas. Para permitir un sitio web permanentemente, use la herramienta Gestión de direcciones URL. En **Configuración avanzada** (F5), despliegue **Web y correo electrónico** > **Protección del tráfico de Internet** > **Gestión de direcciones URL**> **Lista de direcciones**, haga clic en **Modificar** y agregue a la lista el sitio web que desee modificar.

Cómo informar de sitios de phishing

El enlace Informar le permite informar de un sitio web de phishing o malicioso para que ESET lo analice.

NOTA
antes de enviar un sitio web a ESET, asegúrese de que cumple uno o más de los siguientes criterios:

- El sitio web no se detecta en absoluto.
- El sitio web se detecta como una amenaza, pero no lo es. En este caso, puede informar de un falso positivo de phishing.

También puede enviar el sitio web por correo electrónico. Envíe su correo electrónico a samples@eset.com. Utilice un asunto descriptivo y adjunte toda la información posible sobre el sitio web (por ejemplo, el sitio web que le refirió a este, cómo tuvo constancia de su existencia, etc.).

3.9.3 Actualización del programa

La mejora manera de disfrutar del máximo nivel de seguridad en el ordenador es actualizar ESET Endpoint Antivirus de forma periódica. El módulo Actualización garantiza que el programa está siempre actualizado de dos maneras: actualizando el motor de detección y los componentes del sistema.

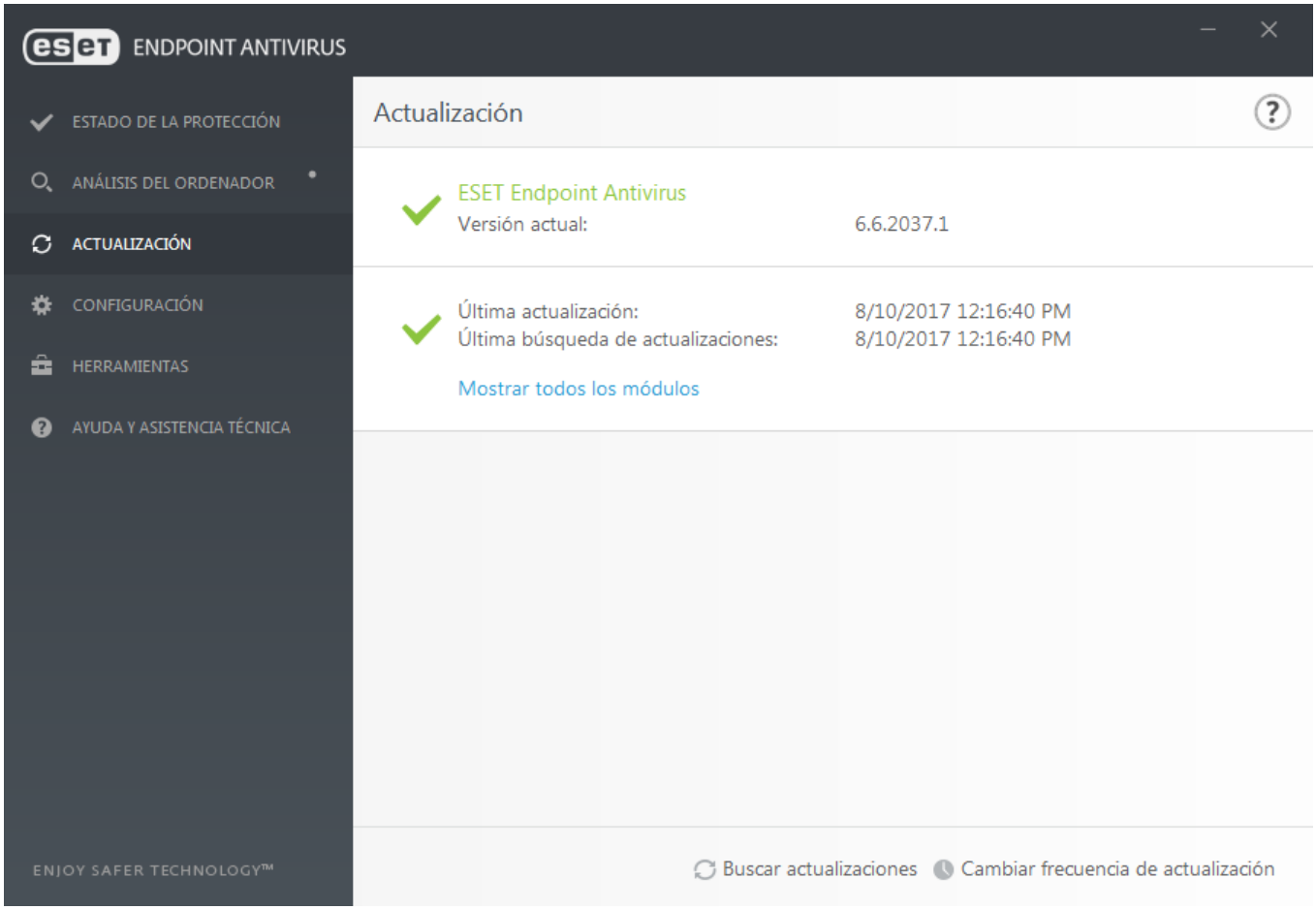
Haga clic en **Actualizar** en la ventana principal del programa para comprobar el estado de la actualización, la fecha y la hora de la última actualización, y si es necesario actualizar el programa. También puede hacer clic en el vínculo **Mostrar todos los módulos** para abrir la lista de módulos instalados y comprobar tanto la versión como la última actualización de un módulo.

También tiene a su disposición la opción **Buscar actualizaciones** para iniciar el proceso de actualización de forma manual. La actualización del motor de detección de virus y la actualización de los componentes del programa son

partes importantes a la hora de mantener una protección completa frente a código malicioso. Preste especial atención a su configuración y funcionamiento. Si no especificó los datos de la licencia durante la instalación, puede introducir la clave de licencia haciendo clic en **Activar producto** cuando realice la actualización para acceder a los servidores de actualización de ESET.

Si activa ESET Endpoint Antivirus archivo de licencia sin conexión sin nombre de usuario y contraseña e intenta actualizar, la información en rojo **La actualización del Motor de detección ha concluido con un error** le indica que solo puede descargar actualizaciones desde el mirror.

NOTA
ESET le facilita la clave de licencia tras la compra de ESET Endpoint Antivirus.



Versión actual: el número de compilación de ESET Endpoint Antivirus.

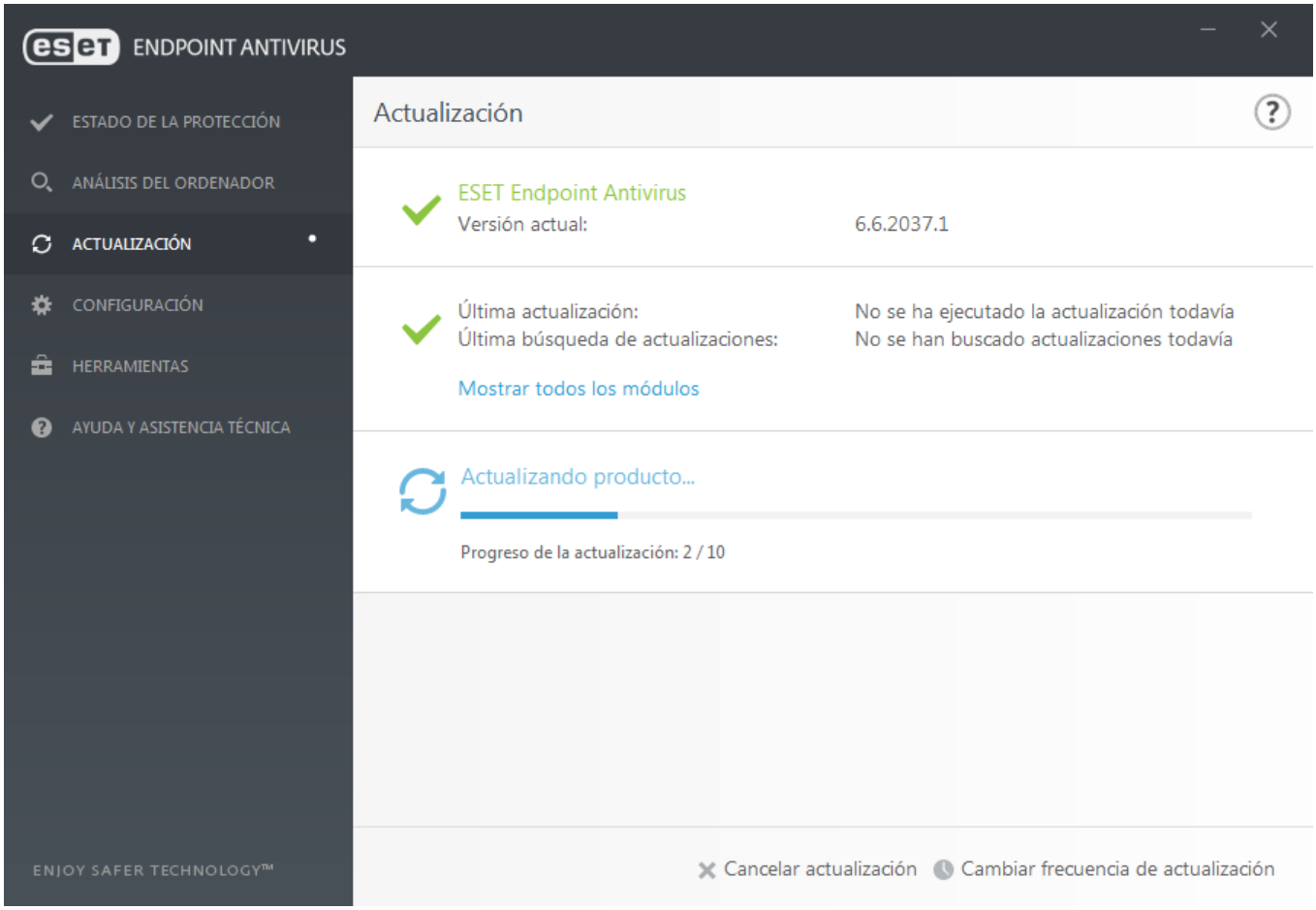
Última actualización: fecha y hora de la última actualización. Asegúrese de que hace referencia a una fecha reciente, lo que significa que el motor de detección está actualizado.

Última búsqueda de actualizaciones: la fecha y hora del último intento de búsqueda de actualizaciones.

Mostrar todos los módulos: haga clic en este enlace para abrir la lista de módulos instalados y comprobar tanto la versión como la última actualización de un módulo.

Proceso de actualización

El proceso comienza tras hacer clic en **Buscar actualizaciones**. Se muestran una barra de progreso de la descarga y el tiempo que falta para que finalice la descarga. Para interrumpir la actualización, haga clic en **Cancelar actualización**.

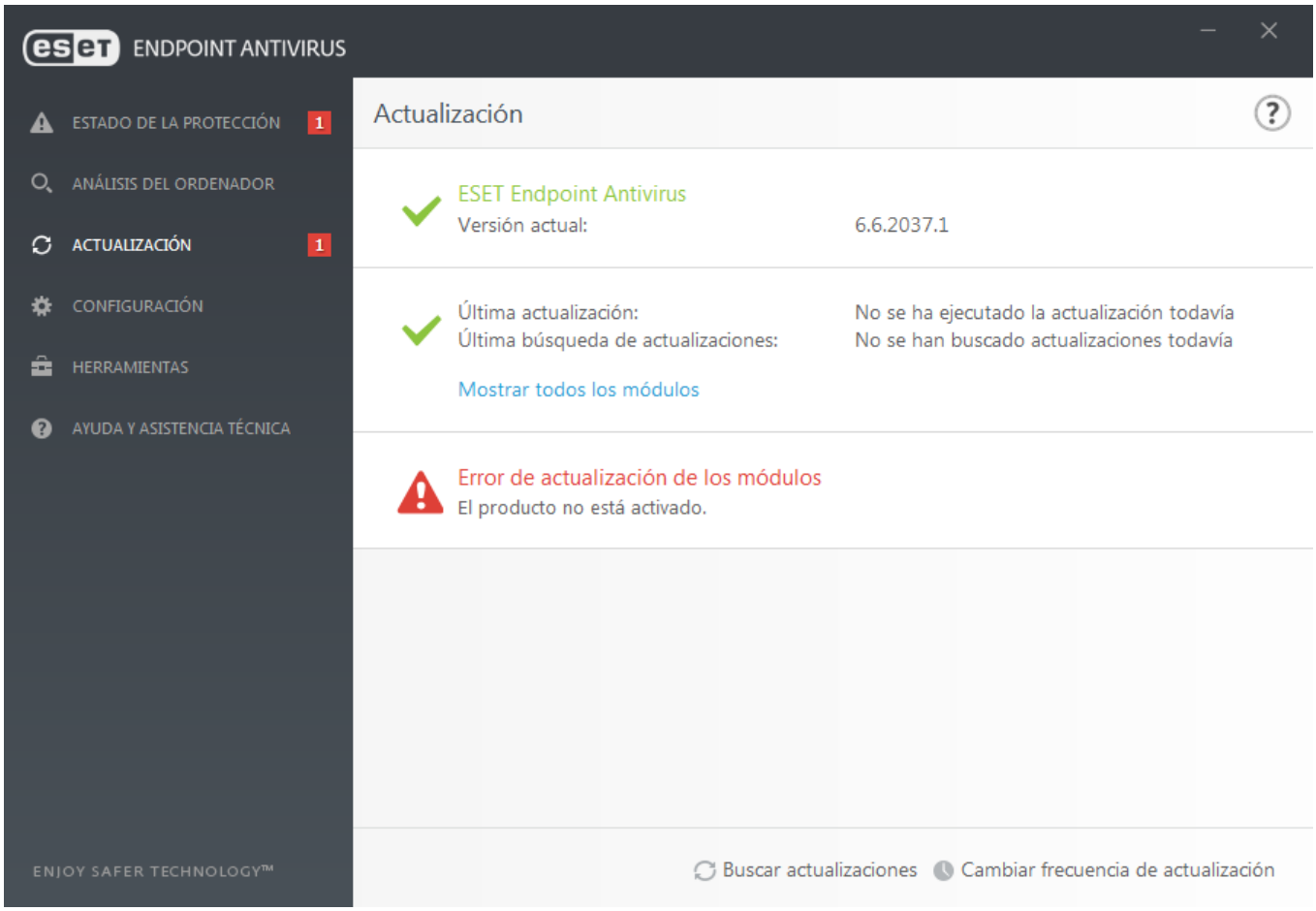


IMPORTANTE
En circunstancias normales, el motor de detección se actualiza varias veces al día. En caso contrario, el programa no estará actualizado y es más vulnerable a la infección. Actualice el motor de detección a la mayor brevedad posible.

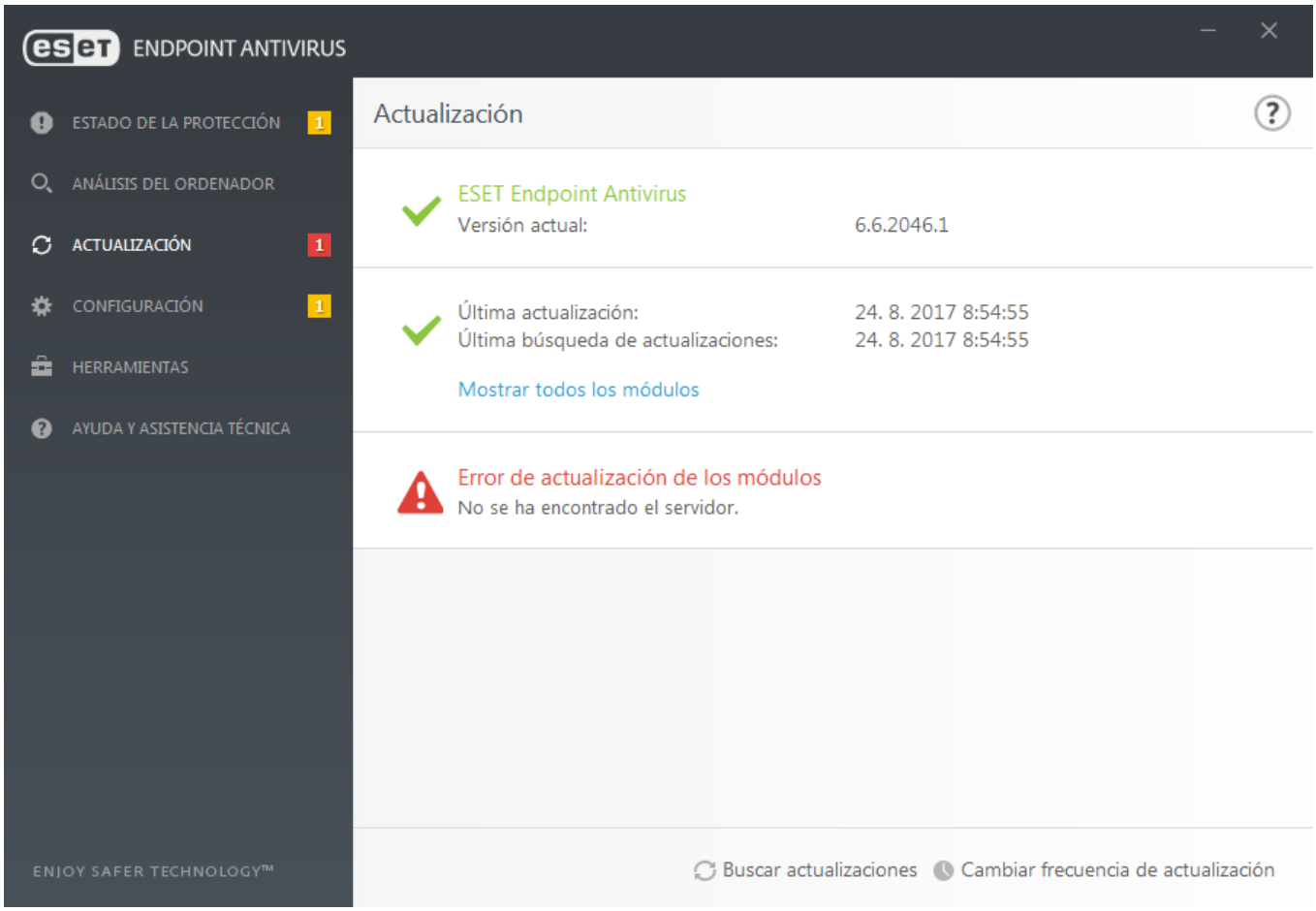
El Motor de detección está obsoleto: este error aparecerá tras varios intentos sin éxito de actualizar el motor de detección. Le recomendamos que compruebe la configuración de actualización. La causa más frecuente de este error es la introducción incorrecta de los datos de autenticación o una mala configuración de la conexión.

La notificación anterior está relacionada con los dos mensajes **La actualización del Motor de detección ha fallado** siguientes sobre actualizaciones incorrectas:

1. **Licencia no válida**: la clave de licencia se ha introducido en la configuración de actualización de forma incorrecta. Recomendamos que compruebe sus datos de autenticación. La ventana Configuración avanzada (haga clic en **Configuración** en el menú principal y, a continuación, en **Configuración avanzada**, o pulse F5 en el teclado) ofrece más opciones de actualización. Haga clic en **Ayuda y soporte** > **Administrar licencia** en el menú principal para introducir una nueva clave de licencia.



2. **Ha ocurrido un error mientras se descargaban los archivos de actualización**: el error puede deberse a una configuración de la conexión a Internet. Es recomendable que compruebe la conectividad a Internet (por ejemplo, abriendo un sitio web en el navegador web). Si el sitio web no se abre, es probable que no se haya establecido ninguna conexión a Internet o que haya problemas de conectividad con el ordenador. Consulte a su proveedor de servicios de Internet (ISP) si no tiene una conexión activa a Internet.



NOTA
consulte este artículo de la base de conocimiento de ESET para obtener más información.

3.9.3.1 Configuración de actualizaciones

Las opciones de configuración de actualizaciones están disponibles en el árbol **Configuración avanzada** (F5), en **Actualización**. En esta sección se especifica la información del origen de la actualización, como los servidores de actualización utilizados y sus datos de autenticación.

General

El perfil de actualización que se está utilizando se muestra en el menú desplegable **Perfil de actualización**. Para crear un perfil nuevo, vaya a la ficha **Perfiles** y haga clic en **Editar** junto a **Lista de perfiles**, introduzca su propio **Nombre de perfil** y, a continuación, haga clic en **Agregar**.

Si está experimentando problemas a la hora de descargar actualizaciones de los módulos, haga clic en **Borrar** para eliminar los archivos de actualización temporales/la caché.

Alertas de Motor de detección obsoleto

Establecer una antigüedad máxima para la base de datos automáticamente: permite establecer el tiempo (en días) máximo tras el cual el motor de detección se considerará desactualizado. El valor predeterminado es 7.

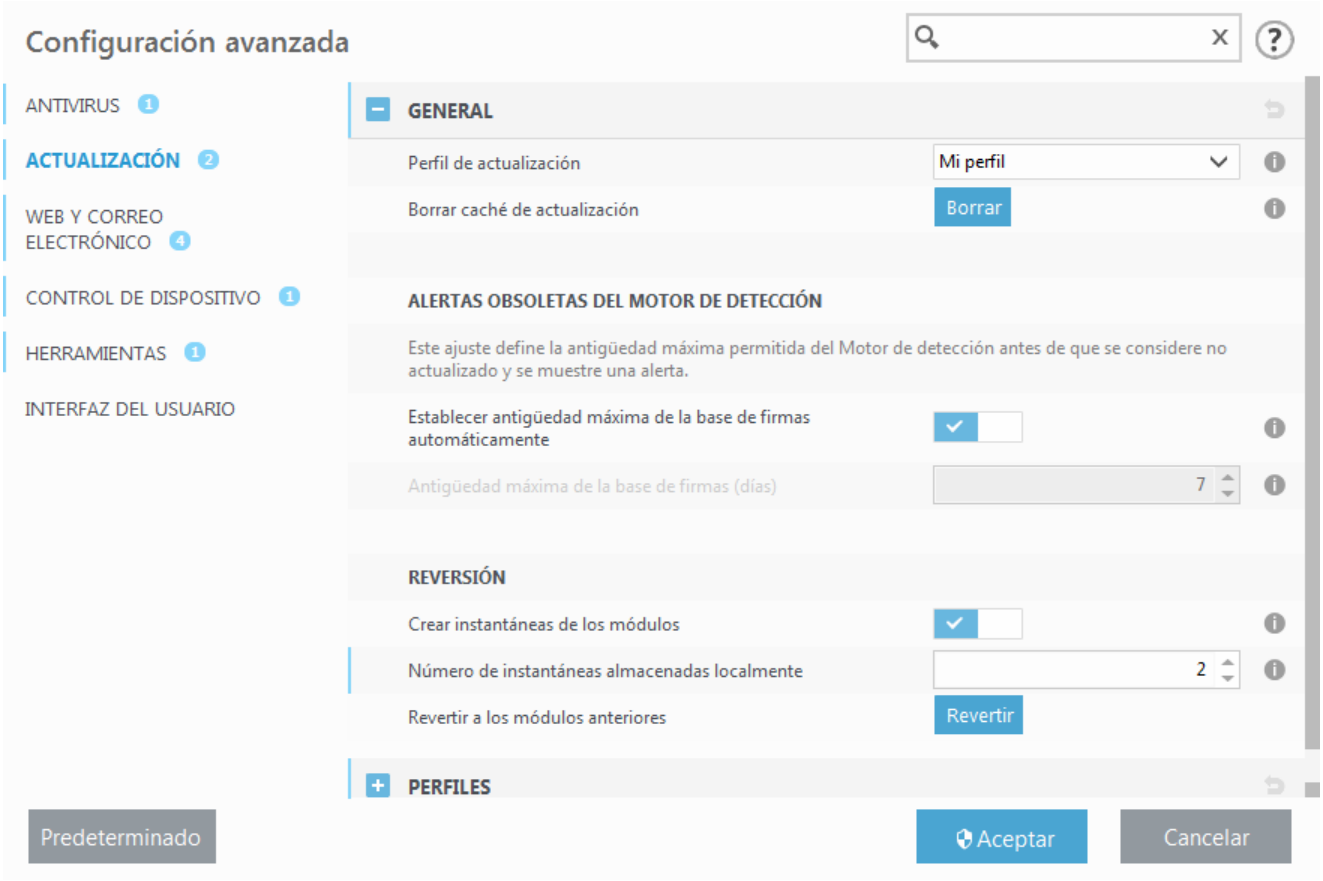
Revertir

Si sospecha que una nueva actualización del motor de detección o de los módulos del programa puede ser inestable o estar dañada, puede revertir a la versión anterior y desactivar las actualizaciones durante un periodo de tiempo

definido. También puede activar actualizaciones desactivadas con anterioridad si las había pospuesto indefinidamente.

ESET Endpoint Antivirus registra instantáneas del motor de detección y los módulos del programa para usarlas con la función de *reversión*. Para crear instantáneas de la base de firmas de virus, deje activado el conmutador **Crear instantáneas de archivos de actualización**. El campo **Número de instantáneas almacenadas localmente** define el número de instantáneas de la base de firmas de virus anteriores que se guardan.

Si hace clic en **Revertir** (**Configuración avanzada** (F5) > **Actualización** > **General**), deberá seleccionar un intervalo de tiempo en el menú desplegable que representa el periodo de tiempo durante el que estarán interrumpidas las actualizaciones del motor de detección y del módulo del programa.



Para que las actualizaciones se descarguen correctamente, es esencial cumplimentar correctamente todos los parámetros de actualización. Si utiliza un cortafuegos, asegúrese de que su programa de ESET goza de permiso para comunicarse con Internet (por ejemplo, comunicación HTTP).

Perfiles

Para crear un perfil nuevo, haga clic en **Modificar** junto a **Lista de perfiles**, introduzca su **Nombre de perfil** y, a continuación, haga clic en **Agregar**. Para editar el perfil creado, seleccione el perfil creado y haga clic en **Editar** junto a **Lista de perfiles**.

Básico

De forma predeterminada, el menú **Tipo de actualización** está definido en **Actualización normal** para garantizar que todos los archivos de actualización se descarguen automáticamente del servidor de ESET cuando la carga de red sea menor. Las actualizaciones de prueba (opción **Actualización de prueba**) son actualizaciones que han superado rigurosas pruebas internas y estarán pronto disponibles. Puede beneficiarse de activar las actualizaciones de prueba mediante el acceso a los métodos y soluciones de detección más recientes. No obstante, la actualización de prueba no siempre es estable, por lo que NO debe utilizarse en servidores de producción y estaciones de trabajo que requieran un elevado nivel de disponibilidad y estabilidad. **Actualización retrasada** permite actualizar desde servidores de actualización especiales que ofrecen nuevas versiones de bases de firmas de virus con un retraso de al menos X horas (es decir, de bases de firmas comprobadas en un entorno real y que, por lo tanto, se consideran estables).

Desactivar la notificación de actualización correcta: desactiva la notificación de la bandeja del sistema en la esquina inferior derecha de la pantalla. Selecciónela si está ejecutando un juego o una aplicación a pantalla completa. Tenga en cuenta que el modo de presentación desactiva todas las notificaciones.

Actualizar desde soporte extraíble: le permite actualizar desde un medio extraíble si contiene el servidor mirror creado. Cuando se selecciona la opción **Automático**, la actualización se ejecutará en segundo plano. Si quiere mostrar los cuadros de diálogo de actualización, seleccione **Preguntar siempre**.

El menú **Servidor de actualización** está establecido en **Elegir automáticamente** de forma predeterminada. El servidor de actualización es la ubicación donde se almacenan las actualizaciones. Si utiliza un servidor ESET, le recomendamos que deje seleccionada la opción predeterminada.

Cuando se utiliza un servidor local HTTP, también conocido como Mirror, el servidor de actualización debe configurarse de la forma siguiente:
http://nombre_del_ordenador_o_su_dirección_IP:2221

Cuando se utiliza un servidor local HTTP con SSL, el servidor de actualización debe configurarse de la forma siguiente:
https://nombre_del_ordenador_o_su_dirección_IP:2221

Cuando se utiliza una carpeta local compartida, el servidor de actualización debe configurarse de la forma siguiente:
\\nombre_o_dirección_IP_ordenador\carpeta_compartida

Actualización desde el servidor Mirror

La autenticación de los servidores de actualización se basa en la **clave de licencia** generada y enviada tras la compra. Si utiliza un servidor Repositorio local, puede definir credenciales para que los clientes inicien sesión en dicho servidor antes de recibir actualizaciones. De forma predeterminada, no se requiere ningún tipo de verificación y los campos **Nombre de usuario** y **Contraseña** se dejan en blanco.

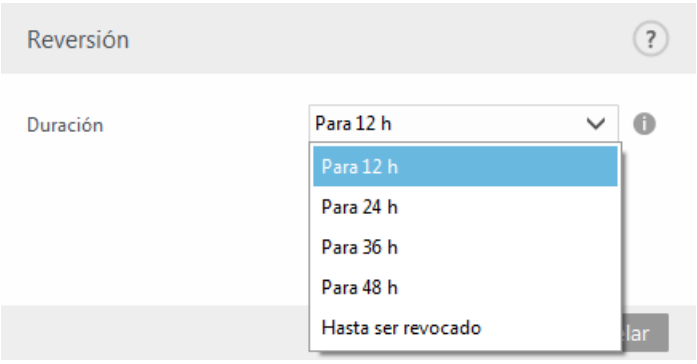
3.9.3.1.1 Perfiles de actualización

Se pueden crear perfiles de actualización para diferentes tareas y configuraciones de actualización. Estos perfiles son especialmente útiles para los usuarios móviles, que necesitan un perfil alternativo para las propiedades de conexión a Internet que cambian periódicamente.

El menú desplegable **Perfil de actualización** muestra el perfil seleccionado actualmente y está definido como **Mi perfil** de forma predeterminada. Para crear un perfil nuevo, haga clic en **Modificar** junto a **Lista de perfiles**, introduzca su **Nombre de perfil** y, a continuación, haga clic en **Agregar**.

3.9.3.1.2 Reversión de actualización

Si hace clic en **Revertir** (**Configuración avanzada** (F5) > **Actualización** > **Perfil**), deberá seleccionar un intervalo de tiempo en el menú desplegable que representa el periodo de tiempo durante el que estarán interrumpidas las actualizaciones del motor de detección y del módulo del programa.



Seleccione **Hasta que se revoque** si desea posponer las actualizaciones periódicas indefinidamente hasta que restaure la funcionalidad manualmente. Como esto representa un riesgo de seguridad potencial, no recomendamos que se seleccione esta opción.

La versión del motor de detección se degrada a la más antigua disponible y se almacena como instantánea en el sistema de archivos del ordenador local.

NOTA
Supongamos que el número 10646 es la versión más reciente del motor de detección. Se almacenan 10645 y 10643 como instantáneas del motor de detección. Observe que 10644 no está disponible porque, por ejemplo, el ordenador estuvo apagado y había disponible una actualización más reciente antes de que se descargara 10644. Si se ha definido 2 en el campo **Número de instantáneas almacenadas localmente** y hace clic en **Revertir**, el motor de detección (incluidos los módulos del programa) se restaurará a la versión número 10643. Este proceso puede tardar un tiempo. Compruebe si la versión del motor de detección se ha degradado en la ventana principal del programa de ESET Endpoint Antivirus en la sección Actualización.

3.9.3.1.3 Tipo de actualización

La pestaña **Tipo de actualización** contiene las opciones relacionadas con la actualización de componentes del programa. Este programa le permite predefinir su comportamiento cuando está disponible una nueva actualización de componentes del programa.

Las actualizaciones de componentes del programa presentan nuevas características, o realizan cambios en las características que ya existen de versiones anteriores. La actualización se puede realizar de manera automática, sin la intervención del usuario, o configurar de modo que este reciba una notificación. Después de instalar una actualización de componentes del programa, puede que sea necesario reiniciar el ordenador. En la sección **Actualización de componentes del programa** hay tres opciones disponibles:

- **Avisar antes de descargar los componentes del programa**: esta es la opción predeterminada. Se le solicitará que confirme o rechace las actualizaciones de componentes del programa cuando estén disponibles.
- **Actualizar siempre los componentes del programa**: se descargará e instalará una actualización de componentes del programa de manera automática. Recuerde que es posible que tenga que reiniciar el ordenador.
- **Nunca actualizar los componentes del programa**: las actualizaciones de componentes del programa no se realizarán. Esta opción es adecuada para las instalaciones de servidores, dado que normalmente los servidores solo se pueden reiniciar cuando realizan tareas de mantenimiento.

NOTA
La selección de la opción más adecuada depende de la estación de trabajo donde se vaya a aplicar la configuración. Tenga en cuenta que existen ciertas diferencias entre estaciones de trabajo y servidores; por ejemplo, el reinicio automático del servidor tras una actualización del programa podría causar daños graves.

Activar actualización manual de componentes del programa: está desactivado de forma predeterminada. Cuando está activado y tiene a su disposición una versión más reciente de ESET Endpoint Antivirus, podrá buscar actualizaciones en el panel **Actualización** e **instalar** la versión más actualizada.

Si está activada la opción **Preguntar antes de descargar actualizaciones**, se mostrará una notificación cuando esté disponible una nueva actualización.

Si el tamaño del archivo de actualización es superior al valor especificado en el campo **Preguntar si un archivo de actualización es mayor de (KB)**, el programa mostrará una notificación.

3.9.3.1.4 Servidor HTTP

Puerto de servidor: el puerto de servidor predeterminado es el 2221.

Autenticación: define el método de autenticación utilizado para acceder a los archivos de actualización. Están disponibles las opciones siguientes: **Ninguna**, **Básica** y **NTLM**. Seleccione **Básica** para utilizar la codificación base64 con la autenticación básica de nombre de usuario y contraseña. La opción **NTLM** proporciona la codificación a través de un método seguro. Para la autenticación, se utilizará el usuario creado en la estación de trabajo que comparte los archivos actualizados. La configuración predeterminada es **Ninguna** y concede acceso a los archivos de actualización sin necesidad de autenticación.

Si desea ejecutar el servidor HTTP con compatibilidad HTTPS (SSL), agregue el **archivo de cadena de certificados** o genere un certificado autofirmado. Están disponibles los siguientes **tipos de certificado**: ASN, PEM y PFX. Para una

mayor seguridad, puede utilizar el protocolo HTTPS para descargar los archivos de actualización. Resulta casi imposible hacer un seguimiento de las transferencias de datos y credenciales de inicio de sesión utilizando este protocolo. La opción **Tipo de clave privada** está establecida de forma predeterminada en **Integrada** (y, por lo tanto, la opción **Archivo de clave privada** está desactivada de forma predeterminada). Esto significa que la clave privada forma parte del archivo de cadena de certificados seleccionado.

NOTA
los datos de autenticación, como el **nombre de usuario** y la **contraseña** sirven para acceder al servidor Proxy. Rellene estos campos únicamente si es necesario introducir un nombre de usuario y una contraseña. Tenga en cuenta que en estos campos no debe introducir su contraseña y nombre de usuario de ESET Endpoint Antivirus, que únicamente debe proporcionar si sabe que es necesaria una contraseña para acceder a Internet a través de un servidor Proxy.

3.9.3.1.5 Opciones de conexión

Para realizar una actualización desde un servidor local con una versión del sistema operativo Windows NT, es necesario autenticar todas las conexiones de red de forma predeterminada.

Para configurar una cuenta de este tipo, seleccione en el menú desplegable **Conectarse a la LAN como**:

- **Cuenta del sistema (predeterminado)**.
- **Usuario actual**.
- **Usuario especificado**.

Seleccione **Cuenta de sistema (predeterminado)** para utilizar la cuenta del sistema para la autenticación. Normalmente, no se realiza ningún proceso de autenticación si no se proporcionan datos en la sección de configuración de actualizaciones.

Para garantizar que el programa se autentique con la cuenta de un usuario registrado actualmente, seleccione **Usuario actual**. El inconveniente de esta solución es que el programa no se puede conectar al servidor de actualizaciones si no hay ningún usuario registrado.

Seleccione **Especificar usuario** si desea que el programa utilice una cuenta de usuario específica para la autenticación. Utilice este método cuando falle la conexión predeterminada con la cuenta del sistema. Recuerde que la cuenta del usuario especificado debe tener acceso al directorio de archivos actualizados del servidor local. De lo contrario, el programa no podrá establecer ninguna conexión ni descargar las actualizaciones.

Los campos **Nombre de usuario** y **Contraseña** son opcionales.

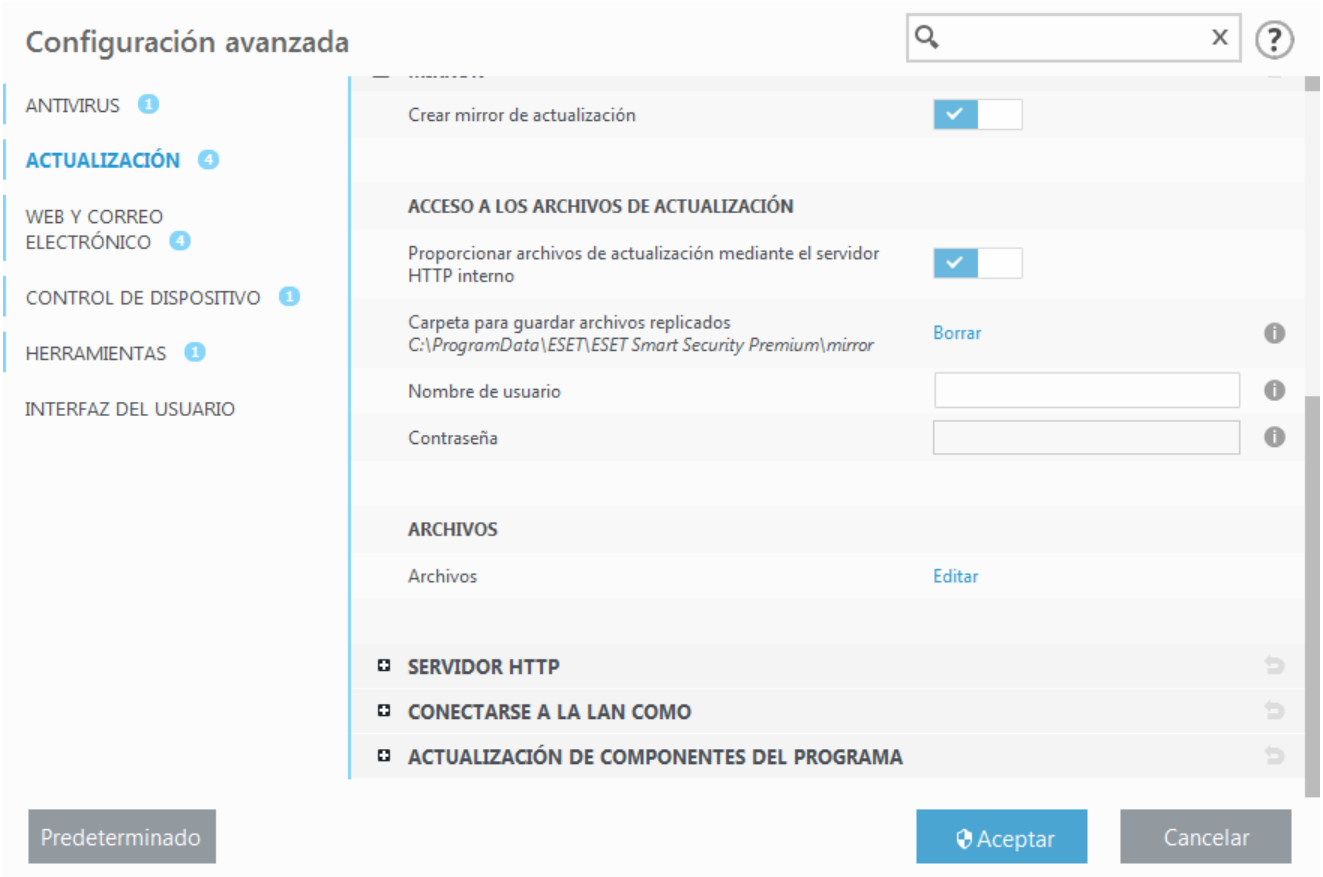
ADVERTENCIA
Cuando se selecciona **Usuario actual** o **Especificar usuario**, puede producirse un error al cambiar la identidad del programa para el usuario deseado. Por este motivo, se recomienda que introduzca los datos de autenticación de la red local en la sección principal de configuración de actualizaciones, donde los datos de autenticación se deben introducir de la forma siguiente: *nombre_dominio\usuario* (si es un grupo de trabajo, escriba *nombre_grupo de trabajo\nombre*) y la contraseña. Cuando se actualiza desde la versión HTTP del servidor local, no es necesaria ninguna autenticación.

Seleccione **Desconectar del servidor tras la actualización** para forzar la desconexión si una conexión al servidor permanece activa incluso después de descargar las actualizaciones.

3.9.3.1.6 Mirror de actualización

ESET Endpoint Antivirus le permite crear copias de los archivos de actualización, que puede utilizar para actualizar otras estaciones de trabajo de la red. El uso de un *"mirror"*: es conveniente realizar una copia de los archivos de actualización del entorno de red local, dado que no necesitan descargarse del servidor de actualización del proveedor varias veces ni que los descarguen todas las estaciones de trabajo. Las actualizaciones se descargan de manera centralizada en el servidor Repositorio local y, después, se distribuyen a todas las estaciones de trabajo para así evitar el riesgo de sobrecargar el tráfico de red. La actualización de estaciones de trabajo cliente desde un servidor Mirror optimiza el equilibrio de carga de la red y ahorra ancho de banda de la conexión a Internet.

Las opciones de configuración del servidor Repositorio local están disponibles en la sección Configuración avanzada, dentro de **Actualización**. Para acceder a esta sección pulse **F5** para acceder a Configuración avanzada, haga clic en **Actualización** > **Perfiles** y seleccione la ficha **Mirror**.



Si desea crear un mirror en una estación de trabajo cliente, active la opción **Crear mirror de actualización**. Al activar dicha opción se activan otras opciones de configuración del Mirror, como la forma de acceder a los archivos actualizados y la ruta de actualización de los archivos replicados.

Acceso a los archivos de actualización

Proporcionar archivos de actualización mediante el servidor HTTP interno: si se activa esta opción, es posible acceder a los archivos de actualización a través de HTTP sin necesidad de credenciales.

> **NOTA**
> para usar el servidor HTTP en Windows XP se necesita el Service Pack 2 o superior.

En la sección Actualización desde el servidor Mirror se describen exhaustivamente los métodos de acceso al servidor Mirror. Existen dos métodos básicos para acceder al servidor Mirror: la carpeta que contiene los archivos de actualización se puede presentar como una carpeta de red compartida o los clientes pueden acceder al Mirror situado en un servidor HTTP.

La carpeta destinada a almacenar los archivos de actualización para el servidor Mirror se define en la sección **Carpeta para guardar archivos replicados**. Para elegir una carpeta diferente, haga clic en **Borrar** para eliminar la carpeta predefinida *C:\ProgramData\ESET\ESET Endpoint Antivirus\mirror* y haga clic en **Editar** para buscar una carpeta en el

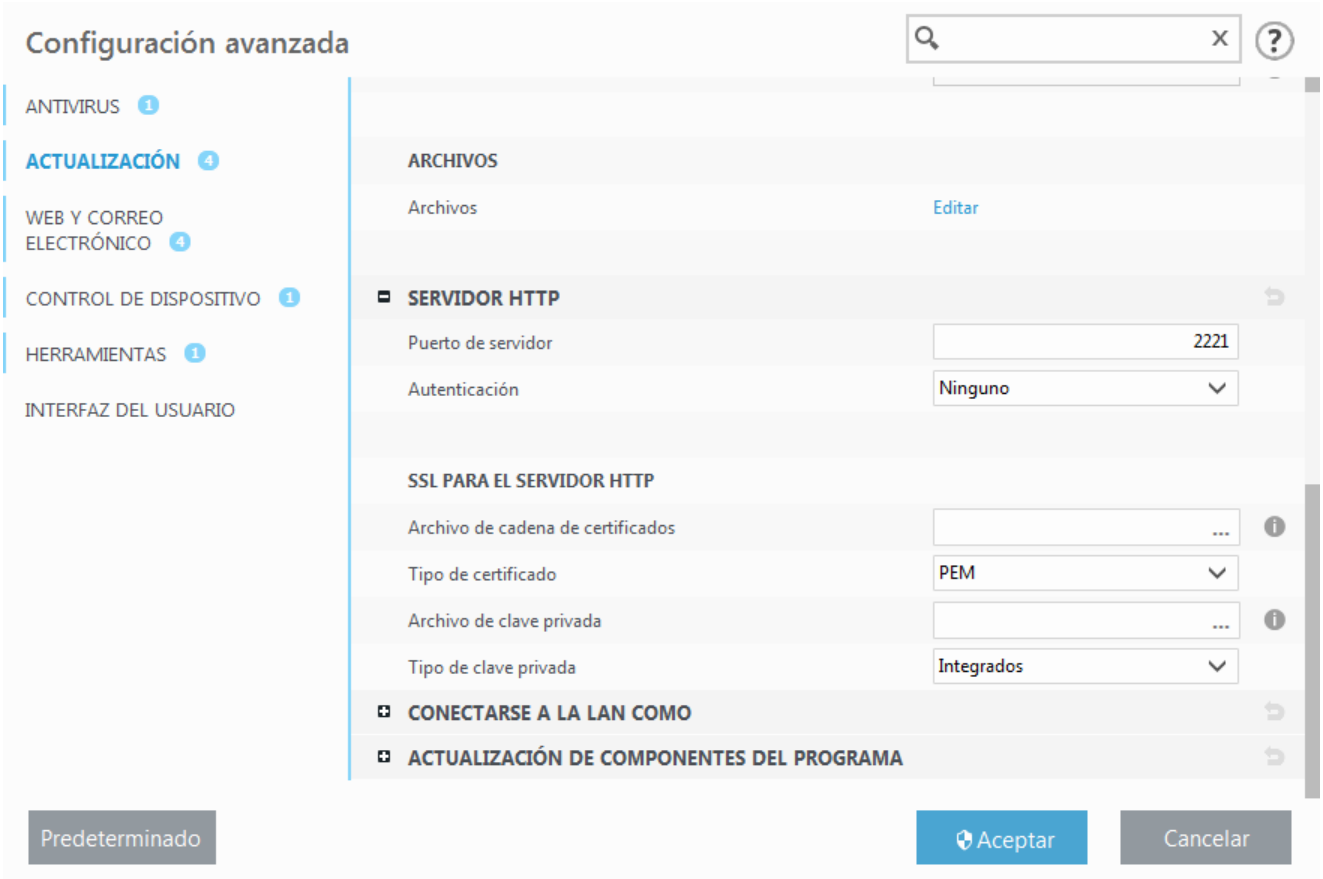
ordenador local o en la carpeta de red compartida. Si es necesaria una autorización para la carpeta especificada, deberá especificar los datos de autenticación en los campos **Nombre de usuario** y **Contraseña**. Si la carpeta de destino seleccionada se encuentra en un disco de red que ejecuta los sistemas operativos Windows NT, 2000 o XP, el nombre de usuario y la contraseña especificados deben contar con privilegios de escritura para la carpeta seleccionada. El nombre de usuario y la contraseña deben introducirse con el formato *Dominio/Usuario* o *Grupo de trabajo/Usuario*. No olvide que debe introducir las contraseñas correspondientes.

Archivos: durante la configuración del servidor Mirror puede especificar las versiones de idioma de las actualizaciones que desea descargar. Los idiomas seleccionados deben ser compatibles con el servidor Mirror configurado por el usuario.

Actualización de componentes del programa

Actualizar componentes automáticamente: permite instalar características nuevas y actualizaciones de las características existentes. La actualización se puede realizar de manera automática, sin la intervención del usuario, o configurar de modo que este reciba una notificación. Después de instalar una actualización de componentes del programa, puede que sea necesario reiniciar el ordenador.

Actualizar componentes ahora: actualiza los componentes del programa a la versión más reciente.



3.9.3.1.6.1 Actualización desde el servidor Mirror

El servidor Mirror es básicamente un repositorio en el que los clientes pueden descargar los archivos de actualización. Existen dos métodos de configuración básicos de este tipo de servidor. La carpeta que contiene los archivos de actualización puede presentarse como una carpeta de red compartida o como un servidor HTTP.

Acceso al servidor Mirror mediante un servidor HTTP interno

Esta es la configuración predeterminada, especificada en la configuración predefinida del programa. Para permitir el acceso al Mirror mediante el servidor HTTP, vaya a **Configuración avanzada** > **Actualización** > **Perfiles** > **Mirror** y seleccione **Crear mirror de actualización**.

En la sección **Servidor HTTP** de la ficha **Mirror**, puede especificar el **Puerto del servidor** donde el servidor HTTP estará a la escucha, así como el tipo de **autenticación** que utiliza el servidor HTTP. El valor predeterminado del puerto del servidor es **2221**. La opción **Autenticación** define el método de autenticación utilizado para acceder a los

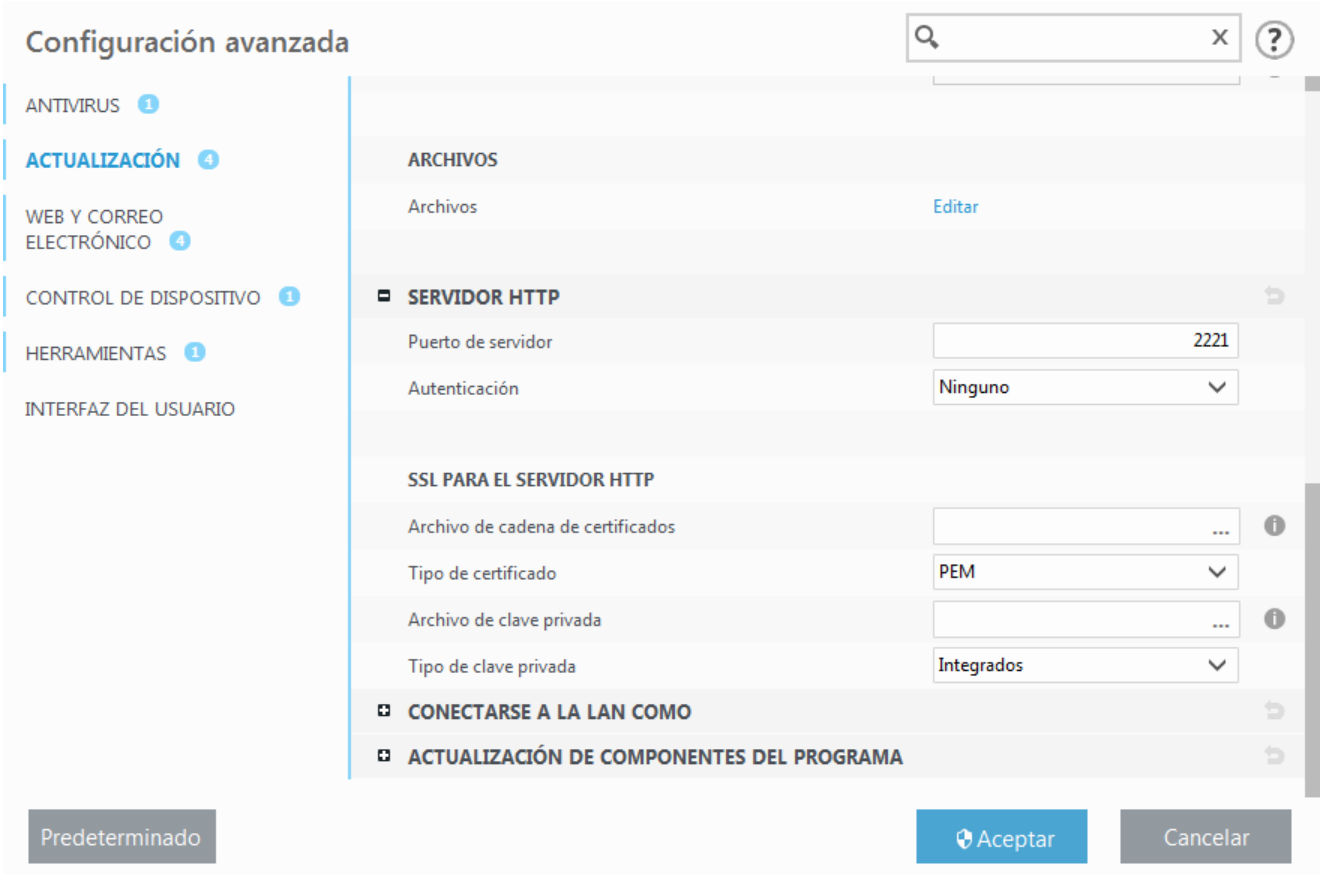
archivos de actualización. Están disponibles las opciones siguientes: **Ninguna**, **Básica** y **NTLM**. Seleccione **Básica** para utilizar la codificación base64 con la autenticación básica de nombre de usuario y contraseña. La opción **NTLM** proporciona la codificación a través de un método seguro. Para la autenticación, se utilizará el usuario creado en la estación de trabajo que comparte los archivos actualizados. La configuración predeterminada es **Ninguna** y concede acceso a los archivos de actualización sin necesidad de autenticación.

ADVERTENCIA
Si desea permitir el acceso a los archivos de actualización a través del servidor HTTP, la carpeta Mirror debe encontrarse en el mismo ordenador que la instancia de ESET Endpoint Antivirus que vaya a crearla.

SSL para el servidor HTTP

Si desea ejecutar el servidor HTTP con compatibilidad HTTPS (SSL), agregue el **archivo de cadena de certificados** o genere un certificado autofirmado. Están disponibles los siguientes tipos de certificado: **PEM, PFX** y **ASN**. Para una mayor seguridad, puede utilizar el protocolo HTTPS para descargar los archivos de actualización. Resulta casi imposible hacer un seguimiento de las transferencias de datos y credenciales de inicio de sesión utilizando este protocolo. La opción **Tipo de clave privada** está establecida en **Integrada** de forma predeterminada, lo que significa que la clave privada forma parte del archivo de cadena de certificados seleccionado.

NOTA
Si se realizan varios intentos sin éxito de actualizar el motor de detección desde el servidor Mirror, en el panel Actualización del menú principal aparecerá el error **Nombre de usuario o contraseña no válidos.**. Le recomendamos que acceda a **Configuración avanzada** > **Actualización** > **Perfiles** > **Mirror** y compruebe el nombre de usuario y la contraseña. Este error suele estar provocado por la introducción incorrecta de los datos de autenticación.



Una vez que haya configurado su servidor Mirror, debe agregar el nuevo servidor de actualización a las estaciones de trabajo cliente. Para hacerlo, siga estos pasos:

- Acceda a **Configuración avanzada** (F5) y haga clic en **Actualización** > **Perfiles** > **Básico**.
- Desactive **Elegir automáticamente** y agregue un servidor nuevo al campo **Servidor de actualización** con uno de los siguientes formatos:

http://dirección_IP_de_su_servidor:2221
https://dirección_IP_de_su_servidor:2221 (si se utiliza SSL)

Acceso al servidor Mirror mediante el uso compartido del sistema

En primer lugar, es necesario crear una carpeta compartida en un dispositivo local o de red. A la hora de crear la carpeta para el servidor mirror, es necesario proporcionar acceso de *"escritura"* al usuario que va a guardar los archivos en la carpeta y acceso de *"lectura"* a todos los usuarios que vayan a actualizar ESET Endpoint Antivirus desde la carpeta Mirror.

A continuación, configure el acceso al servidor Mirror en la sección **Configuración avanzada** > **Actualización** > **Perfiles** > ficha **Mirror** desactivando **Proporcionar archivos de actualización mediante el servidor HTTP interno**. Esta opción se activa, de forma predeterminada, en el paquete de instalación del programa.

Si la carpeta compartida se encuentra en otro ordenador de la red, debe especificar los datos de autenticación para acceder al otro ordenador. Para especificar los datos de autenticación, abra la ESET Endpoint Antivirus **Configuración avanzada** (F5) y haga clic en **Actualización** > **Perfiles** > **Conectarse a la LAN como**. Esta configuración es la misma que se aplica a las actualizaciones, tal como se describe en la sección Conectarse a la LAN como.

Cuando haya terminado de configurar el servidor Mirror, en las estaciones de trabajo cliente, siga los pasos que se indican a continuación para establecer *UNC**RUTA* como servidor de actualización:

1. Abra la ESET Endpoint Antivirus **Configuración avanzada** y haga clic en **Actualización** > **Perfiles** > **Básico**.
2. Desactive **Elegir automáticamente** y un nuevo servidor en el campo **Servidor de actualización** utilizando el formato *UNC**PATH*.

NOTA
Para que las actualizaciones funcionen correctamente, es necesario especificar la ruta a la carpeta Mirror como una ruta UNC. Es posible que las actualizaciones de las unidades asignadas no funcionen.

La última sección controla los componentes del programa (PCU). De forma predeterminada, los componentes del programa descargados se preparan para copiarse en el Repositorio local. Si la opción **Actualización de componentes del programa** está activada, no es necesario hacer clic en **Actualizar** porque los archivos se copian en el servidor Repositorio local automáticamente cuando se encuentran disponibles. Consulte Tipo de actualización para obtener más información acerca de las actualizaciones de los componentes del programa.

3.9.3.1.6.2 Resolución de problemas de actualización del Mirror

En la mayoría de los casos, los problemas durante la actualización desde un servidor Mirror se deben a una de estas causas: la especificación incorrecta de las opciones de la carpeta Mirror, la introducción de datos de autenticación no válidos para la carpeta Mirror, la configuración incorrecta de las estaciones de trabajo que intentan descargar archivos de actualización del Mirror o una combinación de los motivos anteriores. A continuación, se ofrece información general acerca de los problemas más frecuentes durante la actualización desde el Mirror:

ESET Endpoint Antivirus notifica un error al conectarse al servidor de imagen: suele deberse a la especificación incorrecta del servidor de actualización (ruta de red a la carpeta Mirror) desde el que se actualizan las descargas de las estaciones de trabajo locales. Para verificar la carpeta, haga clic en el menú **Inicio** de Windows y en **Ejecutar**, introduzca el nombre de la carpeta y haga clic en **Aceptar**. A continuación, debe mostrarse el contenido de la carpeta.

ESET Endpoint Antivirus requiere un nombre de usuario y una contraseña: probablemente se deba a la presencia de datos de autenticación incorrectos (nombre de usuario y contraseña) en la sección de actualización. El nombre de usuario y la contraseña se utilizan para conceder acceso al servidor de actualización desde el que se actualiza el programa. Asegúrese de que los datos de autenticación son correctos y se introducen en el formato adecuado. Por ejemplo, *Dominio/Nombre de usuario* o *Grupo de trabajo/Nombre de usuario*, más las contraseñas correspondientes. Si "Todos" pueden acceder al servidor Mirror, debe ser consciente de que esto no quiere decir que cualquier usuario tenga acceso. "Todos" no hace referencia a cualquier usuario no autorizado, tan solo significa que todos los usuarios del dominio pueden acceder a la carpeta. Por ello, si "Todos" pueden acceder a la carpeta, será igualmente necesario introducir un nombre de usuario y una contraseña en la sección de configuración de actualizaciones.

ESET Endpoint Antivirus notifica un error al conectarse al servidor de imagen: la comunicación del puerto definida para acceder a la versión HTTP del Mirror está bloqueada.

3.9.3.2 Cómo crear tareas de actualización

Las actualizaciones se pueden activar manualmente al hacer clic en **Buscar actualizaciones** de la ventana principal que se muestra al hacer clic en **Actualización** en el menú principal.

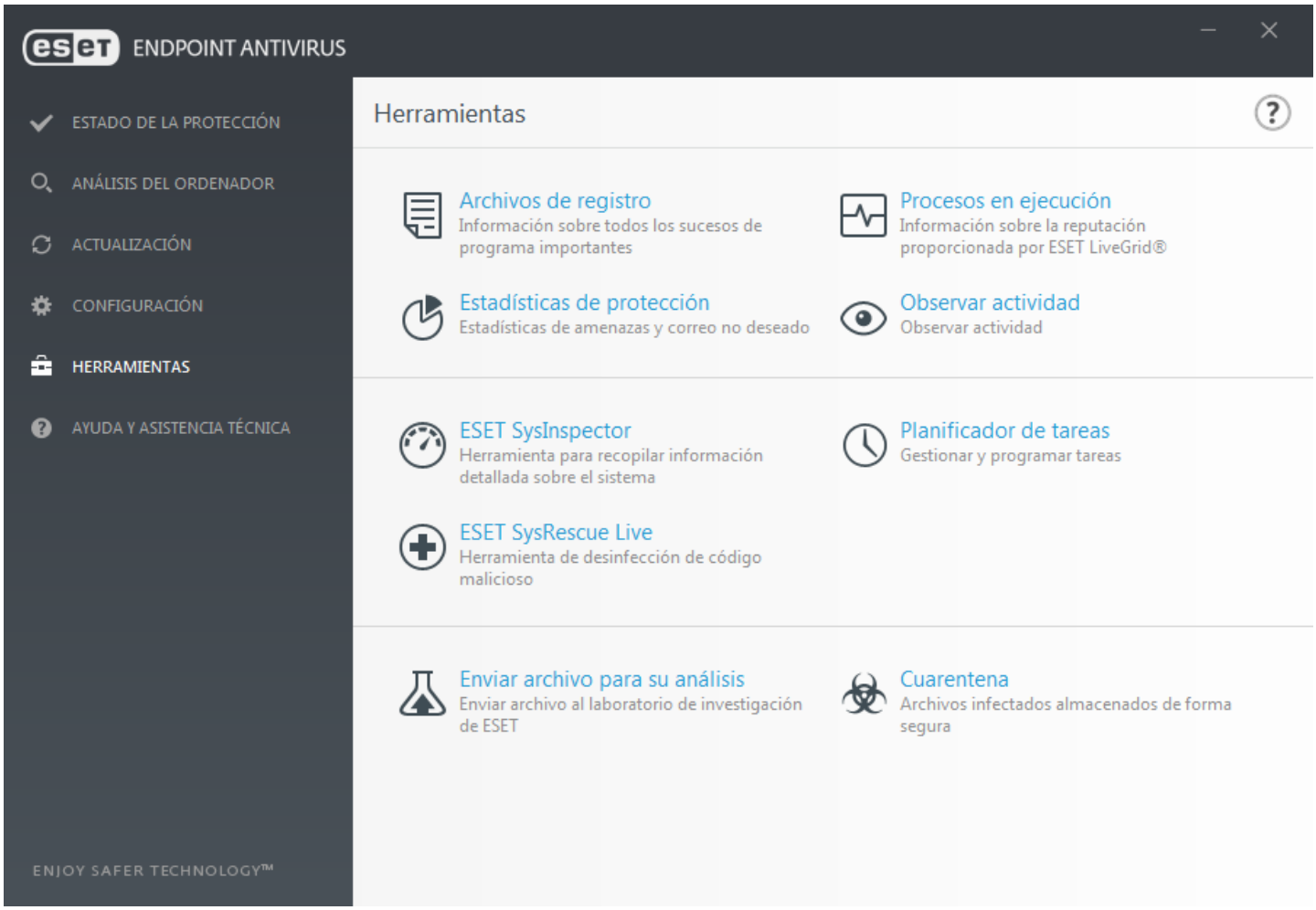
Las actualizaciones también se pueden ejecutar como tareas programadas. Para configurar una tarea programada, haga clic en **Herramientas** > **Tareas programadas**. Las siguientes tareas están activadas de forma predeterminada en ESET Endpoint Antivirus:

- **Actualización automática de rutina**
- **Actualización automática al detectar la conexión por módem**
- **Actualización automática después del registro del usuario**

Todas las tareas de actualización se pueden modificar en función de sus necesidades. Además de las tareas de actualización predeterminadas, se pueden crear nuevas tareas de actualización con una configuración definida por el usuario. Para obtener más información acerca de la creación y la configuración de tareas de actualización, consulte Planificador de tareas.

3.9.4 Herramientas

El menú **Herramientas** incluye módulos que ayudan a simplificar la administración del programa y ofrece opciones adicionales para usuarios avanzados.



Este menú incluye las herramientas siguientes:

- Archivos de registro
- Estadísticas de protección
- Observar actividad
- Procesos en ejecución (si ESET LiveGrid® se ha activado en ESET Endpoint Antivirus)
- Tareas programadas
- Cuarentena
- ESET SysInspector

Enviar muestra para su análisis: le permite enviar un archivo sospechoso para que lo analicen en el laboratorio de investigación de ESET. La ventana de diálogo mostrada al hacer clic en esta opción se describe en la sección Envío de muestras para el análisis.

ESET SysRescue: la redirige a la página de ESET SysRescue Live, desde la que puede descargar la imagen de ESET SysRescue Live o Live CD/USB Creator para sistemas operativos Microsoft Windows.

3.9.4.1 Archivos de registro

Los archivos de registro contienen información relacionada con todos los sucesos importantes del programa y proporcionan información general acerca de las amenazas detectadas. Los registros constituyen una herramienta esencial en el análisis del sistema, la detección de amenazas y la resolución de problemas. Se lleva a cabo de forma activa en segundo plano, sin necesidad de que intervenga el usuario. La información se registra según el nivel de detalle de los registros. Los mensajes de texto y los registros se pueden ver directamente desde el entorno de ESET Endpoint Antivirus. También es posible comprimir los archivos de registro.

Se puede acceder a los archivos de registro desde ventana principal del programa de haciendo clic en **Herramientas** > **Archivos de registro**. Seleccione el tipo de registro que desee en el menú desplegable **Registro**, Están disponibles los siguientes registros:

- **Amenazas detectadas**: el registro de amenazas contiene información detallada acerca de las amenazas detectadas por los módulos de ESET Endpoint Antivirus. La información incluye el momento de la detección, el nombre de la amenaza, la ubicación, la acción ejecutada y el nombre del usuario registrado en el momento en que se detectó la amenaza. Haga doble clic en la entrada del registro para ver los detalles en una ventana independiente.
- **Sucesos**: todas las acciones importantes realizadas por ESET Endpoint Antivirus se registran en el registro de sucesos. El registro de sucesos contiene información sobre sucesos y errores que se produjeron en el programa. Esta opción se ha diseñado para ayudar a los administradores del sistema y los usuarios con la solución de problemas. Con frecuencia, la información aquí disponible puede ayudarle a encontrar una solución para un problema del programa.
- **Análisis del ordenador**: en esta ventana se muestran todos los resultados del análisis. Cada línea se corresponde con un control informático individual. Haga doble clic en cualquier entrada para ver los detalles del análisis correspondiente.
- **Archivos bloqueados**: contiene registros de los archivos que estaban bloqueados y a los que no fue posible acceder. El protocolo muestra el motivo y el módulo de origen que bloqueó el archivo, así como la aplicación y el usuario que ejecutaron el archivo.
- **HIPS**: contiene registros de reglas específicas que se marcaron para su registro. El protocolo muestra la aplicación que invocó la operación, el resultado (si la regla se admitió o no) y el nombre de la regla creada.
- **Sitios web filtrados**: esta lista es útil si desea ver una lista de sitios web que la Protección del tráfico de Internet ha bloqueado. En estos registros puede ver la hora, la URL, el usuario y la aplicación que estableció una conexión con el sitio web determinado.
- **Control de dispositivos**: contiene registros de los dispositivos o medios extraíbles conectados al ordenador. Solo los dispositivos con una regla de control de dispositivos se registran en el archivo de registro. Si la regla no coincide con un dispositivo conectado, no se creará una entrada de registro para un dispositivo conectado. Aquí puede ver también detalles como el tipo de dispositivo, número de serie, nombre del fabricante y tamaño del medio (si está disponible).

La información mostrada en las diferentes secciones se puede copiar en el portapapeles seleccionando la entrada y haciendo clic en **Copiar** (o con el acceso directo **Ctrl + C**). Utilice las teclas **Ctrl** y **Mayús** para seleccionar varias entradas.

Haga clic en **Filtrado** para abrir la ventana **Filtrado de registros**, donde puede definir los criterios de filtrado.

Haga clic con el botón derecho del ratón en un registro determinado para abrir el menú contextual. En este menú contextual, están disponibles las opciones siguientes:

- **Mostrar**: muestra información detallada sobre el registro seleccionado en una ventana nueva.
- **Filtrar los mismos registros**: tras activar este filtro, solo verá registros del mismo tipo (diagnósticos, advertencias, etc.).
- **Filtrar/Buscar**: después de hacer clic en esta opción, en la ventana Buscar en el registro podrá definir los criterios de filtrado para entradas de registro específicas.
- **Activar filtro**: activa la configuración del filtro.
- **Desactivar filtro**: borra todos los ajustes del filtro (tal como se describe arriba).
- **Copiar/Copiar todo**: copia información sobre todos los registros de la ventana.
- **Eliminar/Eliminar todos**: elimina los registros seleccionados, o todos los registros mostrados. Se necesitan privilegios de administrador para poder realizar esta acción.
- **Exportar**: exporta información acerca de los registros en formato XML.
- **Exportar todo...**: exportar información acerca de todos los registros en formato XML.
- **Desplazar registro**: deje esta opción activada para desplazarse automáticamente por los registros antiguos y ver los registros activos en la ventana **Archivos de registro**.

3.9.4.1.1 Buscar en el registro

Los registros guardan información sobre sucesos importantes del sistema. La característica de filtrado de registros permite ver los registros de un tipo de suceso determinado.

Escriba la palabra clave de búsqueda en el campo **Buscar texto**. Si desea buscar la palabra clave en columnas específicas, cambie el filtro en el menú desplegable **Buscar en columnas**.

Tipos de registro: seleccione uno o varios tipos de registro en el menú desplegable:

- **Diagnóstico**: registra la información necesaria para ajustar el programa y todos los registros anteriores.
- **Informativo**: registra los mensajes informativos, incluidos los mensajes de las actualizaciones realizadas con éxito y todos los registros anteriores.
- **Alertas**: registra errores graves y mensajes de alerta.
- **Errores**: se registran los errores graves y errores del tipo "Error al descargar el archivo".
- **Críticos**: registra únicamente los errores graves (errores al iniciar la protección antivirus, etc.).

Período de tiempo: define el período de tiempo para el que desea visualizar los resultados.

Solo palabras completas: seleccione esta casilla de verificación si desea buscar palabras completas específicas para obtener resultados más precisos.

Distinguir mayúsculas y minúsculas: active esta opción si considera que es importante distinguir mayúsculas y minúsculas durante el filtrado.

Buscar hacia arriba: los resultados de la búsqueda que aparecen antes en el documento se muestran en primer lugar.

3.9.4.2 Servidor Proxy

En las redes LAN de gran tamaño, un servidor proxy puede mediar en la comunicación entre el ordenador e Internet. Si se usa esta configuración se deberán definir los siguientes parámetros. De lo contrario, el programa no se podrá actualizar de manera automática. En ESET Endpoint Antivirus, el servidor proxy se puede configurar en dos secciones diferentes del árbol de Configuración avanzada.

En primer lugar, se puede configurar en **Configuración avanzada**, bajo **Herramientas** > **Servidor Proxy**. Al especificar el servidor Proxy en este nivel, se define la configuración global del servidor Proxy para ESET Endpoint Antivirus. Todos los módulos que requieran conexión a Internet utilizarán estos parámetros.

Para especificar la configuración del servidor proxy en este nivel, seleccione **Usar servidor proxy** y especifique la dirección del servidor proxy en el campo **Servidor proxy** y su número de **Puerto**.

Si la comunicación con el servidor proxy requiere autenticación, seleccione **El servidor proxy requiere autenticación** e introduzca un **nombre de usuario** y una **contraseña** válidos en los campos correspondientes. Haga clic en **Detectar** para detectar y cumplimentar la configuración del servidor proxy de forma automática. Se copiarán los parámetros especificados en Internet Explorer.

NOTA
debe especificar el nombre de usuario y la contraseña manualmente en la configuración del **Servidor proxy**.

Usar conexión directa si el proxy no está disponible: si un producto está configurado para utilizar un proxy HTTP y el proxy está inaccesible, el producto ignorará el proxy y se comunicará directamente con los servidores de ESET.

La configuración del servidor proxy también se puede definir en Configuración avanzada de actualizaciones (**Configuración avanzada** > **Actualización** > **Perfiles** > **Actualizaciones** > **Opciones de conexión**; para ello, seleccione **Conexión a través de un servidor proxy** en el menú desplegable **Modo proxy**). Esta configuración se aplica al perfil de actualización dado y se recomienda para ordenadores portátiles que suelen recibir actualizaciones del motor de detección de ubicaciones remotas. Para obtener más información sobre este ajuste, consulte Configuración avanzada de actualizaciones.

3.9.4.3 Planificador de tareas

El planificador de tareas administra e inicia las tareas programadas con la configuración y las propiedades predefinidas.

Se puede acceder al Planificador de tareas desde la ventana principal del programa de ESET Endpoint Antivirus haciendo clic en **Herramientas** > **Planificador de tareas**. El **Planificador de tareas** contiene una lista de todas las tareas programadas y sus propiedades de configuración, como la fecha, la hora y el perfil de análisis predefinidos utilizados.

El Planificador de tareas sirve para programar las siguientes tareas: actualización del motor de detección, tarea de análisis, verificación de archivos en el inicio del sistema y mantenimiento de registros. Puede agregar o eliminar tareas directamente desde la ventana Planificador de tareas (haga clic en **Agregar tarea** o **Eliminar** en la parte inferior). Haga clic con el botón derecho en cualquier parte de la ventana Planificador de tareas para realizar las siguientes acciones: mostrar detalles de la tarea, ejecutar la tarea inmediatamente, agregar una tarea nueva y eliminar una tarea existente. Utilice las casillas de verificación disponibles al comienzo de cada entrada para activar o desactivar las tareas.

De forma predeterminada, en el **Planificador de tareas** se muestran las siguientes tareas programadas:

- **Mantenimiento de registros**
- **Actualización automática de rutina**
- **Actualización automática al detectar la conexión por módem**
- **Actualización automática después del registro del usuario**
- **Verificación automática de archivos en el inicio** (tras inicio de sesión del usuario)
- **Comprobación de la ejecución de archivos en el inicio** (tras una actualización correcta del módulo)

Para modificar la configuración de una tarea programada existente (tanto predeterminada como definida por el usuario), haga clic con el botón derecho del ratón en la tarea y, a continuación, haga clic en **Modificar**, o seleccione la tarea que desea modificar y haga clic en el botón **Modificar**.

Agregar una nueva tarea

1. Haga clic en **Agregar tarea**, en la parte inferior de la ventana.
2. Introduzca un nombre para la tarea.
3. Seleccione la tarea deseada en el menú desplegable:

- **Ejecutar aplicación externa**: programa la ejecución de una aplicación externa.
- **Mantenimiento de registros**: los archivos de registro también contienen restos de los registros eliminados. Esta tarea optimiza periódicamente los registros incluidos en los archivos para aumentar su eficacia.
- **Verificación de archivos en el inicio del sistema**: comprueba los archivos que se pueden ejecutar al encender o iniciar el sistema.
- **Crear un análisis del ordenador**: crea una instantánea del ordenador de ESET SysInspector recopila información detallada sobre los componentes del sistema (por ejemplo, controladores y aplicaciones) y evalúa el nivel de riesgo de cada componente.
- **Análisis del ordenador a petición**: analiza los archivos y las carpetas del ordenador.
- **Actualización**: programa una tarea de actualización mediante la actualización del motor de detección y los módulos del programa.

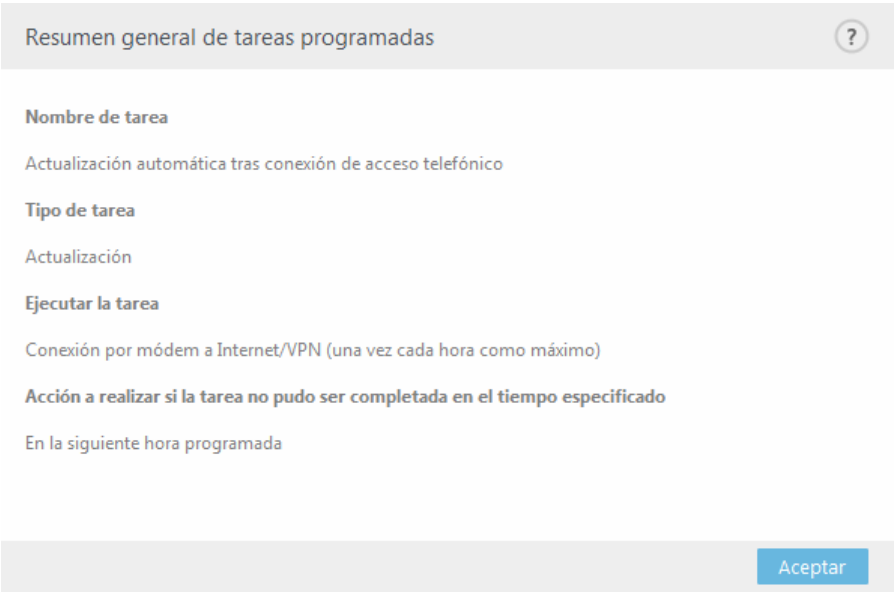
4. Active la opción **Activado** si desea activar la tarea (puede hacerlo más adelante mediante la casilla de verificación situada en la lista de tareas programas), haga clic en **Siguiente** y seleccione una de las opciones de programación:

- **Una vez**: la tarea se ejecutará en la fecha y a la hora predefinidas.
- **Reiteradamente**: la tarea se realizará con el intervalo de tiempo especificado.
- **Diariamente**: la tarea se ejecutará todos los días a la hora especificada.
- **Semanalmente**: la tarea se ejecutará el día y a la hora seleccionados.
- **Cuando se cumpla la condición**: la tarea se ejecutará tras un suceso especificado.

5. Seleccione **No ejecutar la tarea si está funcionando con batería** para minimizar los recursos del sistema mientras un ordenador portátil esté funcionando con batería. La tarea se ejecutará en la fecha y hora especificadas en el campo **Ejecución de la tarea**. Si la tarea no se pudo ejecutar en el tiempo predefinido, puede especificar cuándo se ejecutará de nuevo:

- **En la siguiente hora programada**
- **Lo antes posible**
- **Inmediatamente, si la hora desde la última ejecución excede un valor especificado** (el intervalo se puede definir con el cuadro **Tiempo desde la última ejecución**)

Si desea revisar la tarea programada, haga clic con el botón derecho del ratón y, después, haga clic en **Mostrar detalles de la tarea**.



3.9.4.4 Estadísticas de protección

Para ver un gráfico de datos estadísticos relacionados con los módulos de protección de ESET Endpoint Antivirus, haga clic en **Herramientas** > **Estadísticas de protección**. Seleccione el módulo de protección deseado en el menú desplegable **Estadísticas** para ver el gráfico y la leyenda correspondientes. Si pasa el ratón por encima de un elemento de la leyenda, solo aparecerán en el gráfico los datos de ese elemento.

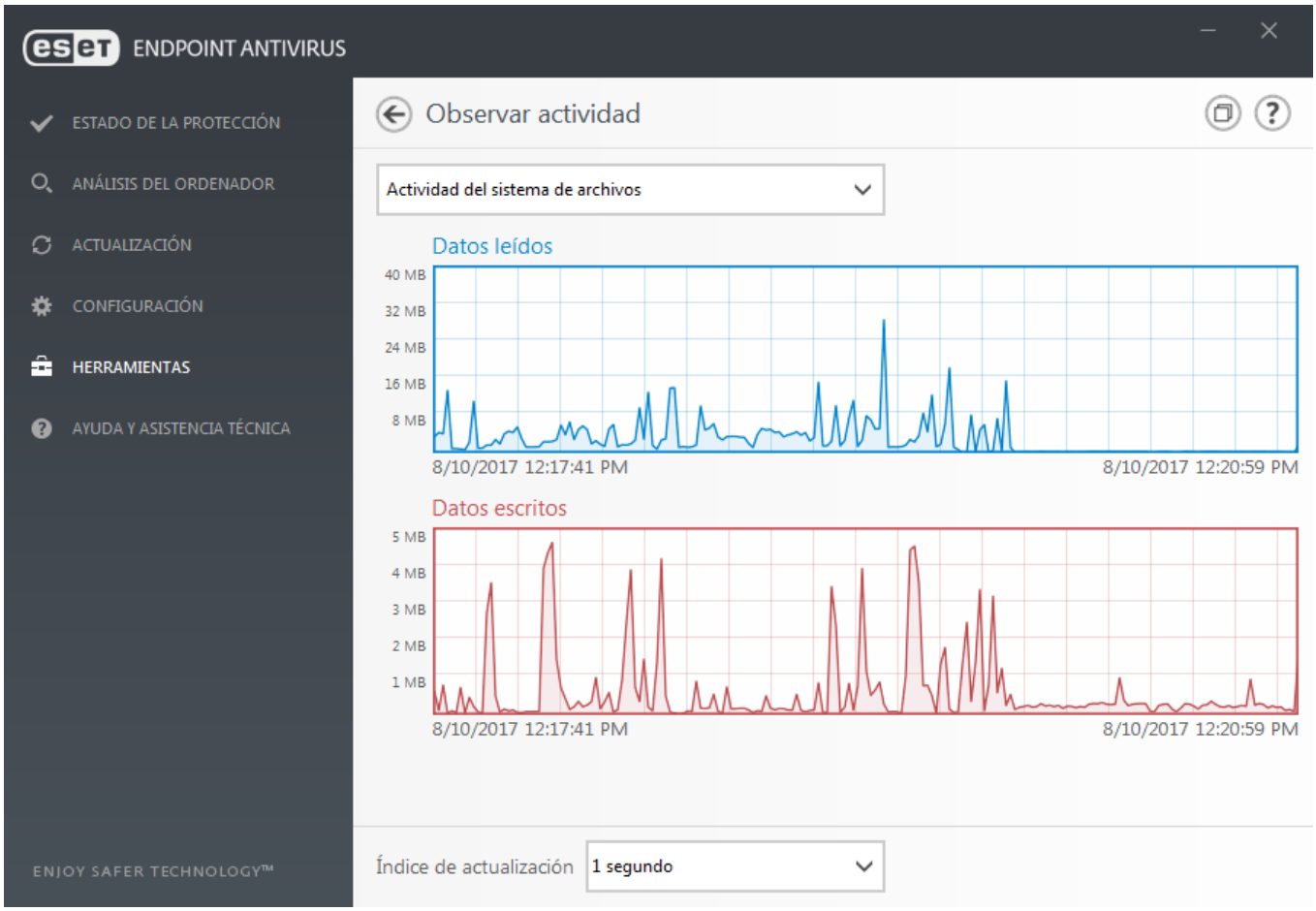
Están disponibles los siguientes gráficos de estadísticas:

- **Protección antivirus y antiespía**: muestra el número de objetos infectados y no infectados
- **Protección del sistema de archivos**: solo muestra objetos que se leyeron o escribieron en el sistema de archivos.
- **Protección del cliente de correo electrónico**: solo muestra objetos que fueron enviados o recibidos por clientes de correo electrónico.
- **Protección del tráfico de Internet y Anti-Phishing**: solo muestra objetos descargados por los navegadores web.

Junto a los gráficos de estadísticas, se muestra el número de objetos analizados, de objetos infectados, de objetos desinfectados y de objetos limpios. Haga clic **Restablecer** para borrar los datos estadísticos o haga clic en **Restablecer todo** para borrar y eliminar todos los datos disponibles.

3.9.4.5 Observar actividad

Para ver la **Actividad del sistema de archivos** actual en un gráfico, haga clic en **Herramientas** > **Observar actividad**. En la parte inferior del gráfico hay una línea cronológica que registra la actividad del sistema de archivos en tiempo real en el intervalo de tiempo seleccionado. Si desea cambiar el intervalo de tiempo, realice la selección en el menú desplegable **Índice de actualización**.



Están disponibles las opciones siguientes:

- **Pasar 1 segundo**: el gráfico se actualiza cada segundo y la línea cronológica abarca los últimos 10 minutos.
- **Pasar 1 minuto (últimas 24 horas)**: el gráfico se actualiza cada minuto y la línea cronológica abarca las últimas 24 horas.
- **Pasar 1 hora (último mes)**: el gráfico se actualiza cada hora y la línea cronológica abarca el último mes.
- **Pasar 1 hora (mes seleccionado)**: el gráfico se actualiza cada hora y la línea cronológica abarca los últimos X meses seleccionados.

El eje vertical del **Gráfico de actividad del sistema de** archivos representa la cantidad de datos leídos (azul) y escritos (rojo). Ambos valores se ofrecen en KB (kilobytes), MB o GB. Si pasa el ratón por encima de los datos leídos o escritos en la leyenda disponible debajo del gráfico, el gráfico solo mostrará los datos de ese tipo de actividad.

3.9.4.6 ESET SysInspector

ESET SysInspector es una aplicación que inspecciona a fondo el ordenador, recopila información detallada sobre los componentes del sistema (como los controladores y aplicaciones instalados, las conexiones de red o las entradas importantes del registro) y evalúa el nivel de riesgo de cada componente. Esta información puede ayudar a determinar la causa de un comportamiento sospechoso del sistema, que puede deberse a una incompatibilidad de software o hardware o a una infección de código malicioso.

En la ventana de SysInspector se muestra la siguiente información de los registros creados:

- **Fecha y hora**: fecha y hora de creación del registro.
- **Comentario**: breve comentario.
- **Usuario**: nombre del usuario que creó el registro.
- **Estado**: estado de la creación del registro.

Están disponibles las siguientes acciones:

- **Abrir**: abre el registro creado. También puede hacer clic con el botón derecho del ratón sobre un archivo de registro determinado y seleccionar **Mostrar** en el menú contextual.
- **Comparar**: compara dos registros existentes.
- **Crear...**: crea un registro nuevo. Espere hasta que ESET SysInspector finalice (el estado del registro se mostrará como Creado) antes de intentar acceder al registro.
- **Eliminar**: elimina de la lista los archivos de registro seleccionados.

El menú contextual ofrece las siguientes opciones al seleccionar uno o más archivos de registro:

- **Mostrar**: abre el registro seleccionado en ESET SysInspector (igual que al hacer doble clic en un registro).
- **Comparar**: compara dos registros existentes.
- **Crear...**: crea un registro nuevo. Espere hasta que ESET SysInspector finalice (el estado del registro se mostrará como Creado) antes de intentar acceder al registro.
- **Eliminar todos**: elimina todos los registros.
- **Exportar**: exporta el registro a un archivo *.xml* o *.xml* comprimido.

3.9.4.7 ESET LiveGrid®

ESET LiveGrid® es un sistema avanzado de alerta temprana compuesto por varias tecnologías basadas en la nube. Ayuda a detectar las amenazas emergentes según su reputación, y mejora el rendimiento de análisis mediante la creación de listas blancas. La nueva información sobre la amenaza se transmite en tiempo real a la nube, lo que permite que el laboratorio de investigación de software malicioso de ESET responda a tiempo y mantenga una protección constante en todo momento. Los usuarios pueden consultar la reputación de los archivos y procesos en ejecución directamente en la interfaz del programa o en el menú contextual; además, disponen de información adicional en ESET LiveGrid®. Seleccione una de las siguientes opciones durante la instalación de ESET Endpoint Antivirus:

1. La activación de ESET LiveGrid® no es obligatoria. El software no perderá funcionalidad, pero puede que ESET Endpoint Antivirus responda más lento a las nuevas amenazas que la actualización del motor de detección.
2. Puede configurar ESET LiveGrid® para enviar información anónima acerca de nuevas amenazas y sobre la ubicación del nuevo código malicioso detectado. Este archivo se puede enviar a ESET para que realice un análisis detallado. El estudio de estas amenazas ayudará a ESET a actualizar sus funciones de detección de amenazas.

ESET LiveGrid® recopilará información anónima del ordenador relacionada con las amenazas detectadas recientemente. Esta información puede incluir una muestra o copia del archivo donde haya aparecido la amenaza, la ruta a ese archivo, el nombre de archivo, la fecha y la hora, el proceso por el que apareció la amenaza en el ordenador e información sobre el sistema operativo del ordenador.

De forma predeterminada, ESET Endpoint Antivirus está configurado para enviar archivos sospechosos para su análisis detallado en el laboratorio de virus de ESET. Los archivos con determinadas extensiones, como *.doc* o *.xls*, se excluyen siempre. También puede agregar otras extensiones para excluir los archivos que usted o su empresa no deseen enviar.

El sistema de reputación de ESET LiveGrid® ofrece listas blancas y negras basadas en la nube. Si desea acceder a la configuración de ESET LiveGrid®, pulse **F5** para ir a Configuración avanzada y expanda **Herramientas** > **ESET LiveGrid®**.

Activar el sistema de reputación ESET LiveGrid® (recomendado): el sistema de reputación ESET LiveGrid® mejora la eficiencia de las soluciones contra software malicioso de ESET mediante la comparación de los archivos analizados con una base de datos de elementos incluidos en listas blancas y negras disponibles en la nube.

Enviar estadísticas anónimas: permita a ESET recopilar información sobre nuevas amenazas detectadas, como el nombre de la amenaza, información sobre la fecha y hora en la que se detectó, el método de detección y los metadatos asociados y la versión y la configuración del producto la versión del producto, incluida información sobre su sistema.

Enviar archivos: los archivos sospechosos que por su comportamiento inusual o características recuerdan a amenazas se envían a ESET para su análisis.

Seleccione **Activar el registro de sucesos** para crear un registro de sucesos en el que anotar los envíos de archivos e información estadística. Permitirá agregar anotaciones al registro de sucesos cuando se envíen archivos o información estadística.

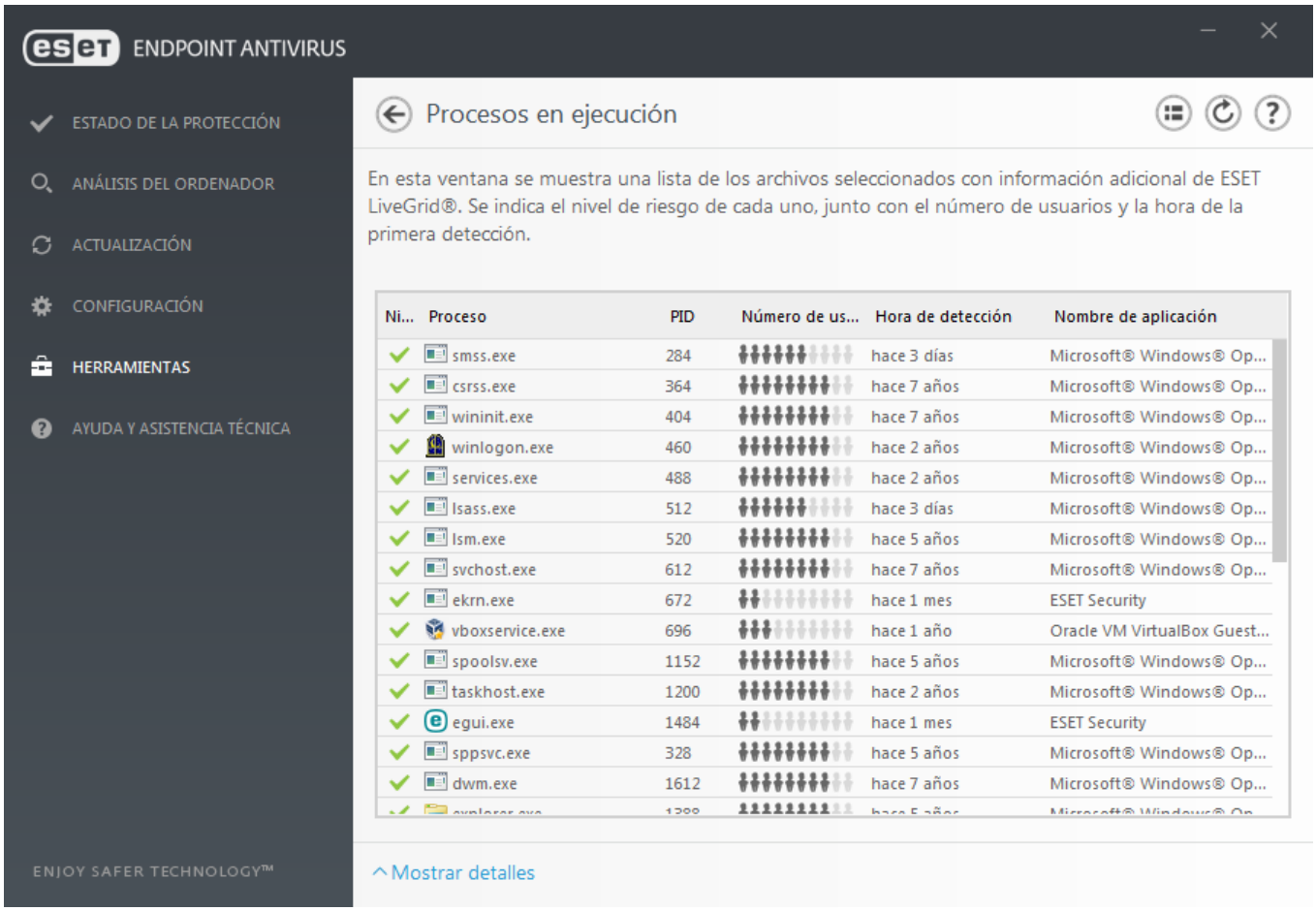
Correo electrónico de contacto (opcional): su correo electrónico de contacto se puede enviar con cualquier archivo sospechoso y puede servir para localizarle si se necesita más información para el análisis. Tenga en cuenta que no recibirá una respuesta de ESET, a no ser que sea necesaria más información.

Exclusión: esta opción le permite excluir del envío determinados archivos o carpetas (por ejemplo, puede ser útil para excluir archivos que puedan contener información confidencial, como documentos u hojas de cálculo). Los archivos mostrados en la lista nunca se enviarán al laboratorio de ESET para su análisis, aunque contengan código sospechoso. Los tipos de archivos más comunes se excluyen de manera predeterminada (.doc, etc.). Si lo desea, puede añadir elementos a la lista de archivos excluidos.

Si utilizó ESET LiveGrid® anteriormente pero lo desactivó, es posible que aún haya paquetes de datos pendientes de envío. Estos paquetes se enviarán a ESET incluso después de la desactivación. Una vez que se haya enviado toda la información actual, no se crearán más paquetes.

3.9.4.8 Procesos en ejecución

En Procesos en ejecución se indican los programas o procesos que se están ejecutando en el ordenador y se informa a ESET de forma inmediata y continua de las nuevas amenazas. ESET Endpoint Antivirus proporciona información detallada sobre los procesos en ejecución para proteger a los usuarios con la tecnología ESET LiveGrid® activada.



Nivel de riesgo: generalmente, ESET Endpoint Antivirus y la tecnología ESET LiveGrid® asignan un nivel de riesgo a los objetos (archivos, procesos, claves del registro, etc.). Para ello, utilizan una serie de reglas heurísticas que examinan las características de cada objeto y, después, ponderan el potencial de actividad maliciosa. Según estas heurísticas, a los objetos se les asignará un nivel de riesgo desde el valor "1: seguro" (en color verde) hasta "9: peligroso" (en color rojo).

Proceso: nombre de la imagen del programa o proceso que se está ejecutando en el ordenador. También puede utilizar el Administrador de tareas de Windows para ver todos los procesos que están en ejecución en el ordenador. Para abrir el Administrador de tareas, haga clic con el botón derecho del ratón sobre un área vacía de la barra de tareas y, a continuación, haga clic en Administrador de tareas o pulse la combinación **Ctrl** + **Mayús** + **Esc** en el teclado.

PID: se trata de un identificador de los procesos que se ejecutan en sistemas operativos Windows.

NOTA
Las aplicaciones conocidas marcadas con un Correcto (verde) son totalmente seguras (incluidas en lista blanca) y no se analizan; esto aumenta la velocidad del análisis a petición del ordenador o la protección del sistema de archivos en tiempo real.

Número de usuarios: el número de usuarios que utilizan una aplicación determinada. La tecnología ESET LiveGrid® se encarga de recopilar esta información.

Hora de la detección: tiempo transcurrido desde que la tecnología ESET LiveGrid® detectó la aplicación.

NOTA

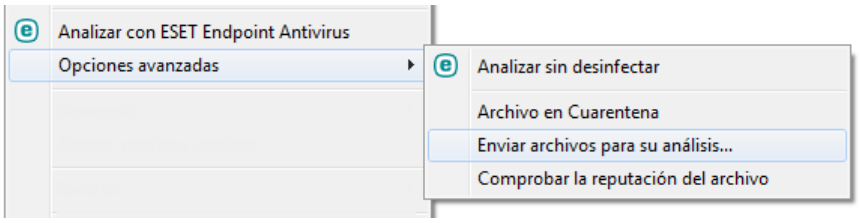
Cuando una aplicación se marca con el nivel de seguridad Desconocido (naranja), no siempre se trata de software malicioso. Normalmente, se trata de una aplicación reciente. Si el archivo le plantea dudas, utilice la característica enviarlo para su análisis para enviarlo al laboratorio de virus de ESET. Si resulta que el archivo es una aplicación maliciosa, su detección se agregará a una de las siguientes actualizaciones del motor de detección.

Nombre de aplicación: nombre de un programa o un proceso.

Al hacer clic en una aplicación en la parte inferior, se mostrará la siguiente información en la parte inferior de la ventana:

- **Ruta**: ubicación de una aplicación en el ordenador.
- **Tamaño**: tamaño del archivo en KB (kilobytes) o MB (megabytes).
- **Descripción**: características del archivo de acuerdo con la descripción del sistema operativo.
- **Empresa**: nombre del proveedor o el proceso de la aplicación.
- **Versión**: información sobre el editor de la aplicación.
- **Producto**: nombre de la aplicación o nombre comercial.
- **Fecha de creación**: fecha y hora en que se creó una aplicación.
- **Fecha de modificación**: última fecha y hora en que se modificó una aplicación.

NOTA
La reputación también se puede comprobar en los archivos que no actúan como programas o procesos en ejecución. Para ejecutarla, seleccione los archivos que desea comprobar, haga clic con el botón derecho del ratón en ellos y, en el menú contextual, seleccione **Opciones avanzadas** > **Comprobar la reputación del archivo con ESET LiveGrid®**.



3.9.4.9 Envío de muestras para el análisis

El cuadro de diálogo de envío de muestras le permite enviar un archivo o un sitio a ESET para que lo analice; esta opción está disponible en **Herramientas** > **Enviar muestra para su análisis**. Si encuentra un archivo en su ordenador que se comporta de manera sospechosa o un sitio sospechoso en Internet, puede enviarlo al laboratorio de virus de ESET para su análisis. Si resulta que el archivo es una aplicación o un sitio web malicioso, su detección se agregará a una actualización futura.

También puede enviar el archivo por correo electrónico. Si prefiere esta opción, comprima los archivos con WinRAR/ZIP, proteja el archivo comprimido con la contraseña "infected" y envíelo a samples@eset.com. Utilice un asunto descriptivo y adjunte toda la información posible sobre el archivo (por ejemplo, el sitio web del que lo descargó).

NOTA
Antes de enviar una muestra a ESET, asegúrese de que cumple uno o más de los siguientes criterios:

- El archivo o sitio web no se detecta en absoluto.
- El archivo o sitio web se detecta como una amenaza, pero no lo es.

No recibirá ninguna respuesta a menos que se requiera información adicional para poder realizar el análisis.

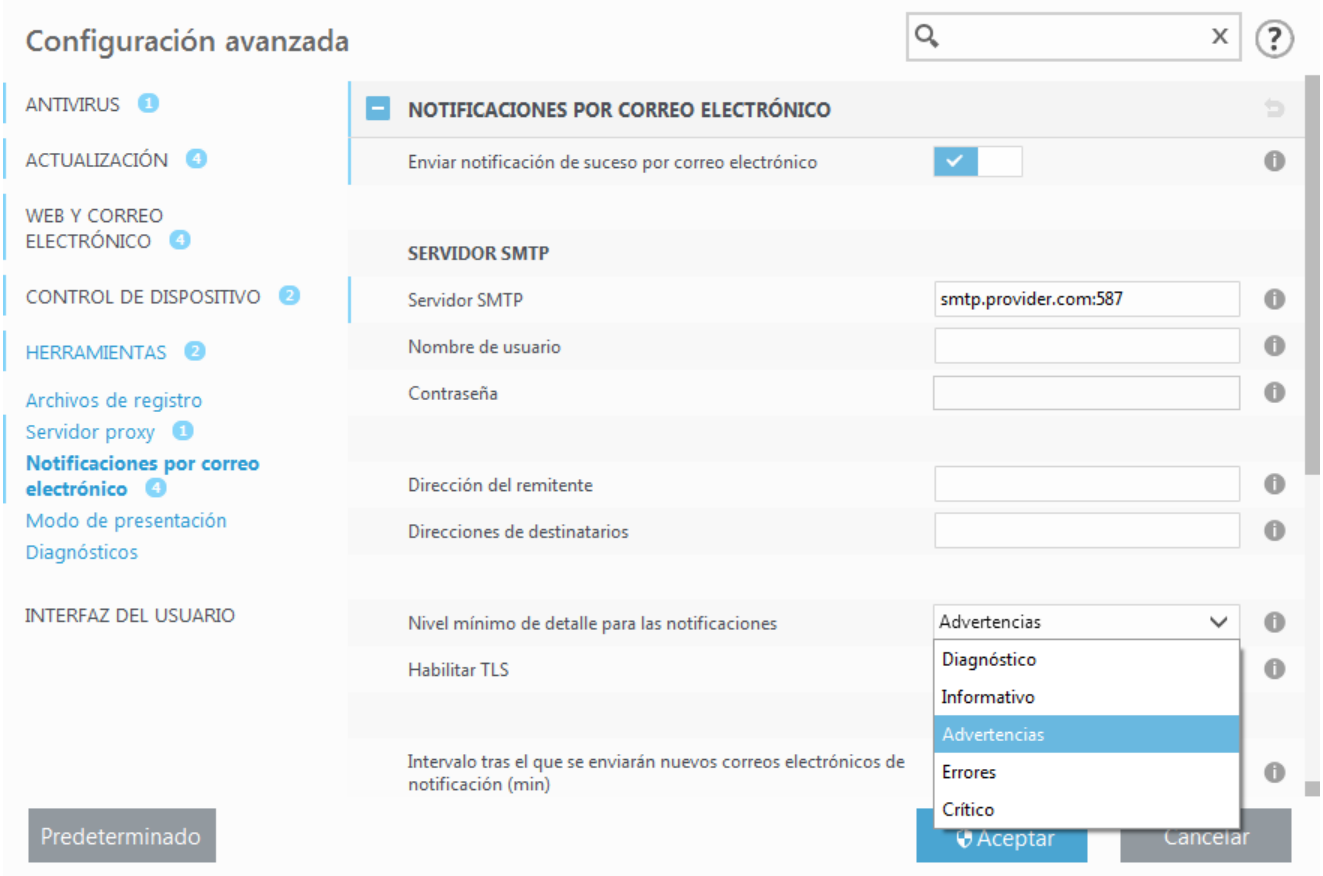
Seleccione la descripción en el menú desplegable **Motivo de envío de la muestra** que mejor se ajuste a su mensaje:
- **Archivo sospechoso**
- **Sitio web sospechoso** (sitio web que está infectado por código malicioso)
- **Archivo de falso positivo** (archivo que se detecta como amenaza pero no está infectado)
- **Sitio de falso positivo**
- **Otros**

Archivo/Sitio: la ruta del archivo o sitio web que quiere enviar.

Correo electrónico de contacto: la dirección de correo de contacto se envía a ESET junto con los archivos sospechosos y se puede utilizar para el contacto con usted en caso de que sea necesario enviar más información para poder realizar el análisis. No es obligatorio introducir una dirección de correo electrónico de contacto. No obtendrá ninguna respuesta de ESET a menos que sea necesario enviar información adicional, ya que cada día nuestros servidores reciben decenas de miles de archivos, lo que hace imposible responder a todos los envíos.

3.9.4.10 Notificaciones por correo electrónico

ESET Endpoint Antivirus puede enviar correos electrónicos de forma automática si se produce un suceso con el nivel de detalle seleccionado. Active **Enviar notificaciones de sucesos por correo electrónico** para activar las notificaciones por correo electrónico.



Servidor SMTP

Servidor SMTP: el servidor SMTP que se utiliza para enviar notificaciones (por ejemplo, *smtp.provider.com:587*, el puerto predefinido es 25).

NOTA
Los servidores SMTP con cifrado TLS son compatibles con ESET Endpoint Antivirus.

Nombre de usuario y **contraseña**: si el servidor SMTP requiere autenticación, estos campos deben cumplimentarse con un nombre de usuario y una contraseña válidos que faciliten el acceso al servidor SMTP.

Dirección del remitente: este campo especifica la dirección de correo del emisor, que se mostrará en el encabezado de los mensajes de notificación.

Direcciones de destinatarios: este campo especifica la dirección de correo de los destinatarios que se mostrarán en el encabezado de los mensajes de notificación. Utilice un punto y coma ";" para separar varias direcciones de correo electrónico.

En el menú desplegable **Nivel mínimo de detalle para las notificaciones** puede seleccionar el nivel de gravedad inicial de las notificaciones que desea enviar.

- **Diagnóstico**: registra la información necesaria para ajustar el programa y todos los registros anteriores.
- **Informativo**: registra los mensajes informativos, como los sucesos de red no convencionales, incluidos los mensajes de las actualizaciones realizadas con éxito y todos los registros anteriores.
- **Alertas**: registra los errores graves y los mensajes de advertencia (la tecnología Anti-Stealth no está funcionando adecuadamente o el proceso de actualización ha fallado).
- **Errores**: se registran los errores (protección de documentos no iniciada) y los errores graves.
- **Críticos**: registra únicamente los errores graves (errores al iniciar la protección antivirus o de infección del sistema).

Habilitar TLS: active el envío de mensajes de notificación y alerta que admite el cifrado TLS.

Intervalo tras el que se enviarán nuevos correos electrónicos de notificación (min): intervalo en minutos tras el cual se enviarán nuevas notificaciones al correo electrónico. Si define este valor en 0, las notificaciones se enviarán de forma inmediata.

Enviar cada notificación en un correo electrónico distinto: si esta opción está activada, el destinatario recibirá un correo electrónico nuevo para cada notificación. Esto podría suponer la recepción de numerosos correos electrónicos en un breve periodo de tiempo.

Formato de mensajes

Las comunicaciones entre el programa y un usuario o administrador de sistemas remotos se realizan a través de mensajes de correo electrónico o mensajes de red local (mediante el servicio de mensajería de Windows). El formato predeterminado de los mensajes de alerta y las notificaciones será el óptimo para la mayoría de situaciones. En algunas circunstancias, tendrá que cambiar el formato de los mensajes de sucesos.

Para notificar la ocurrencia de sucesos: formato de los mensajes de suceso que se muestran en los ordenadores remotos.

Para alertar sobre amenazas: los mensajes de notificación y alerta de amenazas tienen un formato predefinido de forma predeterminada. Le aconsejamos que no modifique este formato. No obstante, en algunas circunstancias (por ejemplo, si tiene un sistema automatizado de procesamiento de correo electrónico), es posible que deba modificar el formato de los mensajes.

Conjunto de caracteres: convierte un mensaje de correo electrónico a la codificación de caracteres ANSI según la configuración regional de Windows (por ejemplo, windows-1250), Unicode (UTF-8), ACSII 7-bit (por ejemplo "á" se cambiará a "a" y un símbolo desconocidoa "?") o japonés (ISO-2022-JP).

Usar codificación Quoted-printable: el origen del mensaje de correo electrónico se codificará a formato Quoted-printable (QP), que utiliza caracteres ASCII y solo pude transmitir correctamente caracteres nacionales especiales por correo electrónico en formato de 8 bits (áéíóú).

Las palabras clave (cadenas separadas por signos %) se sustituyen en el mensaje por la información real especificada. Están disponibles las siguientes palabras clave:

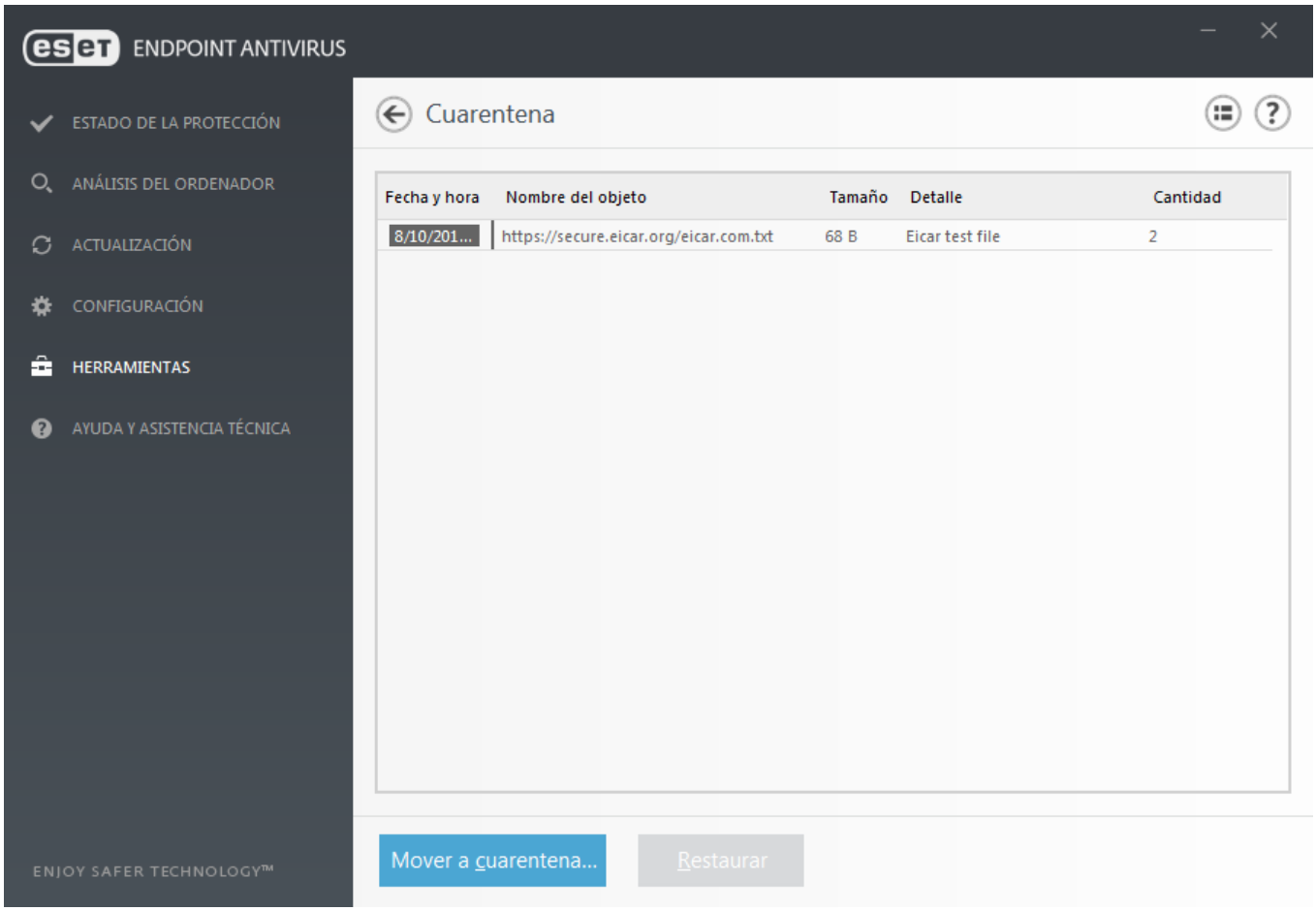
- **%ComputerName%**: nombre del equipo en el que se produjo la alerta.
- **%ProgramName%**: el programa que generó la alerta
- **%TimeStamp%**: fecha y hora del suceso.
- **%UserName%**: nombre del usuario registrado en el que se produjo la alerta.
- **%InfectedObject%**: nombre del archivo, mensaje, etc., infectado.
- **%VirusName%**: identificación de la infección.
- **%ErrorDescription%**: descripción de un suceso no causado por un virus.
- **%Scanner%**: módulo correspondiente.
- **%Action%**: acción emprendida contra la amenaza.

Las palabras clave **%InfectedObject%** y **%VirusName%** se utilizan únicamente en los mensajes de alerta de amenaza, y **%ErrorDescription%** en los mensajes de sucesos.

3.9.4.11 Cuarentena

La función principal de la cuarentena es almacenar los archivos infectados de forma segura. Los archivos deben ponerse en cuarentena si no es posible desinfectarlos, si no es seguro ni aconsejable eliminarlos o si ESET Endpoint Antivirus los detecta incorrectamente como infectados.

Es posible poner en cuarentena cualquier archivo. La cuarentena se recomienda cuando el comportamiento de un archivo es sospechoso y el análisis no lo ha detectado. Los archivos en cuarentena se pueden enviar para su análisis al laboratorio de virus de ESET.



Los archivos almacenados en la carpeta de cuarentena se pueden ver en una tabla que muestra la fecha y la hora en que se pusieron en cuarentena, la ruta de la ubicación original del archivo infectado, su tamaño en bytes, el motivo (agregado por el usuario, por ejemplo) y el número de amenazas (por ejemplo, si se trata de un archivo comprimido que contiene varias amenazas).

Puesta de archivos en cuarentena

ESET Endpoint Antivirus pone los archivos eliminados en cuarentena automáticamente (si no ha desactivado esta opción en la ventana de alerta). Si lo desea, puede poner en cuarentena cualquier archivo sospechoso de forma manual, haciendo clic en el botón **Poner en cuarentena**. El archivo original se eliminará de su ubicación original. El menú contextual también se puede utilizar con este fin: haga clic con el botón derecho en la ventana **Cuarentena** y seleccione **Poner en cuarentena**.

Restauración de archivos de cuarentena

Los archivos puestos en cuarentena se pueden restaurar a su ubicación original. Si desea restaurar un archivo puesto en cuarentena, haga clic en él con el botón derecho del ratón en la ventana Cuarentena y seleccione **Restaurar** en el menú contextual. Si el archivo está marcado como aplicación potencialmente no deseada, también estará disponible la opción **Restaurar y excluir del análisis**. El menú contextual también contiene la opción **Restaurar a...**, que le permite restaurar archivos en una ubicación distinta a la original de la cual se eliminaron.

Eliminación de la cuarentena: haga clic con el botón derecho del ratón en el elemento que desee y seleccione **Eliminar de la cuarentena**, o seleccione el elemento que desee eliminar y pulse **Suprimir** en el teclado. Es posible seleccionar varios elementos y eliminarlos al mismo tiempo.

NOTA
si el programa ha puesto en cuarentena un archivo no dañino por error, exclúyalo del análisis después de restaurarlo y enviarlo al servicio de atención al cliente de ESET.

Envío de un archivo de cuarentena

Si ha copiado en cuarentena un archivo sospechoso que el programa no ha detectado o si se ha evaluado incorrectamente un archivo como amenaza y, consecuentemente, se ha copiado a cuarentena, envíe el archivo al laboratorio de virus de ESET. Para enviar un archivo de cuarentena, haga clic con el botón derecho del ratón en el archivo y seleccione **Enviar para su análisis** en el menú contextual.

3.9.4.12 Microsoft Windows Update

La característica Windows Update es un componente importante de protección de los usuarios de software malicioso, por eso es fundamental que instale las actualizaciones de Microsoft Windows en cuanto se publiquen. ESET Endpoint Antivirus le informa sobre las actualizaciones que le faltan, según el nivel que haya especificado. Están disponibles los siguientes niveles:

- **Sin actualizaciones**: no se ofrecerá ninguna actualización del sistema para la descarga.
- **Actualizaciones opcionales**: se ofrecerán para la descarga las actualizaciones marcadas como de baja prioridad y de niveles superiores.
- **Actualizaciones recomendadas**: se ofrecerán para la descarga las actualizaciones marcadas como habituales y de niveles superiores.
- **Actualizaciones importantes**: se ofrecerán para la descarga las actualizaciones marcadas como importantes y de niveles superiores.
- **Actualizaciones críticas**: solo se ofrecerá la descarga de actualizaciones críticas.

Haga clic en **Aceptar** para guardar los cambios. La ventana de actualizaciones del sistema se mostrará después de la verificación del estado con el servidor de actualización. Por tanto, es posible que la información de actualización del sistema no esté disponible inmediatamente después de guardar los cambios.

3.9.4.13 CMD de ESET

Se trata de una función que activa comandos de ecmd avanzados. Le ofrece la posibilidad de exportar e importar la configuración utilizando la línea de comandos (ecmd.exe). Hasta ahora, solo era posible exportar e importar la configuración utilizando solo la interfaz gráfica de usuario. La configuración de ESET Endpoint Antivirus puede exportarse a un archivo *.xml*.

Si tiene activado CMD de ESET, dispone de dos métodos de autorización:

- **Ninguno**: sin autorización. No le recomendamos este método, ya que permite importar configuraciones no firmadas, lo que supone un riesgo.
- **Configuración avanzada de contraseña**: utiliza protección mediante contraseña. Al importar la configuración desde un archivo *.xml*, este archivo deberá firmarse (consulte cómo firmar un archivo de configuración *.xml* más abajo). Este método de autorización verifica la contraseña durante la importación de la configuración para garantizar que coincide con la contraseña especificada en Configuración de acceso. Si no ha activado la configuración de acceso, la contraseña no coincide o el archivo de configuración *.xml* no está firmado, la configuración no se importará.

Una vez que CMD de ESET esté activado, podrá comenzar a utilizar la línea de comandos para exportar/importar la configuración de ESET Endpoint Antivirus. Podrá hacerlo manualmente o crear un script con fines de automatización.

IMPORTANTE
Para poder utilizar comandos de ecmd avanzados, deberá ejecutarlos con privilegios de administrador, o abrir el símbolo del sistema de Windows (cmd) utilizando **Ejecutar como administrador**. De lo contrario, se mostrará el

mensaje **Error executing command.**. Asimismo, a la hora de exportar la configuración, deberá existir una carpeta de destino.

NOTA
Los comandos de ecmd avanzados solo pueden ejecutarse de forma local. La ejecución de la tarea de cliente **Ejecutar comando** utilizando ERA no funcionará correctamente.

EJEMPLO
Comando para exportar configuración:
```
ecmd /getcfg c:\config\settings.xml
```

Comando para importar configuración:
```
ecmd /setcfg c:\config\settings.xml
```

Cómo firmar un archivo de configuración *.xml*:

1. Descargue **XmlSignTool** en la página de descargas de Herramientas y utilidades de ESET y extráigalo. Esta herramienta se desarrolló específicamente para firmar archivos de configuración *.xml* de ESET.
2. Abra el símbolo del sistema de Windows (cmd) utilizando **Ejecutar como administrador**.
3. Desplácese hasta una ubicación con `XmlSignTool.exe`.
4. Ejecute un comando para firmar el archivo de configuración *.xml*, uso: `XmlSignTool <xml_file_path>`
5. Introduzca y vuelva a introducir la contraseña de Configuración avanzada como le solicita XmlSignTool. El archivo de configuración *.xml* ya estará firmado y podrá utilizarse para importarse en otra instancia de ESET Endpoint Antivirus con CMD de ESET utilizando el método de autorización mediante contraseña de Configuración avanzada.

ADVERTENCIA
No se recomienda activar el CMD de ESET sin autorización, ya que hacerlo permitirá importar configuraciones no firmadas. Configure la contraseña en **Configuración avanzada** > **Interfaz de usuario** > **Configuración de acceso** para evitar que los usuarios realicen modificaciones no autorizadas.

3.9.5 Interfaz de usuario

En la sección **Interfaz de usuario** es posible configurar el comportamiento de la interfaz gráfica de usuario (GUI) del programa.

La herramienta Elementos de la interfaz del usuario le permite ajustar el aspecto visual del programa y los efectos utilizados.

Si desea disponer del máximo nivel de seguridad del software de seguridad, utilice la herramienta Configuración de acceso para impedir los cambios no autorizados.

En la configuración de Alertas y notificaciones, puede cambiar el comportamiento de las alertas de amenaza detectadas y las notificaciones del sistema, que se pueden adaptar a las necesidades de cada uno.

Si elige la opción de no mostrar algunas notificaciones, estas se mostrarán en el área **Elementos de la interfaz del usuario** > **Estados de la aplicación**. Aquí puede comprobar su estado o, si lo desea, impedir la visualización de estas notificaciones.

La opción Integración en el menú contextual aparece al hacer clic con el botón derecho en el objeto seleccionado. Utilice esta herramienta para integrar elementos de control de ESET Endpoint Antivirus en el menú contextual.

El Modo de presentación es útil para usuarios que deseen trabajar con una aplicación sin la interrupción de ventanas emergentes, tareas programadas y cualquier componente que cargue el procesador y la memoria RAM.

3.9.5.1 Elementos de la interfaz del usuario

Las opciones de configuración de la interfaz de usuario de ESET Endpoint Antivirus le permiten ajustar el entorno de trabajo según sus necesidades. Estas opciones de configuración están disponibles en la sección **Interfaz de usuario** > **Elementos de la interfaz del usuario** del árbol de configuración avanzada de ESET Endpoint Antivirus.

En la sección **Elementos de la interfaz del usuario** puede ajustar el entorno de trabajo. Utilice el menú desplegable **Modo de inicio** para seleccionar uno de los siguientes modos de inicio de la interfaz gráfica de usuario (GUI):

Completo: se muestra la GUI completa.

Mínimo: la interfaz gráfica no está disponible y el usuario solo ve las notificaciones.

Manual: no se muestra ninguna notificación ni alerta.

Silencioso: no se muestra la interfaz gráfica de usuario, las notificaciones ni las alertas. Este modo puede resultar útil en aquellas situaciones en las que necesita conservar los recursos del sistema. El modo silencioso solo lo puede iniciar el administrador.

NOTA
cuando se seleccione el modo de inicio de GUI Mínimo y se reinicie el ordenador las notificaciones se mostrarán, pero la interfaz gráfica no. Para volver al modo de interfaz gráfica de usuario completa, ejecute la interfaz gráfica desde el menú Inicio en **Todos los programas** > **ESET** > ESET Endpoint Antivirus como administrador, o hágalo desde ESET Remote Administrator utilizando una directiva.

Si desea desactivar la pantalla inicial de ESET Endpoint Antivirus, anule la selección de **Mostrar pantalla inicial con la carga del sistema**.

Si desea que ESET Endpoint Antivirus reproduzca un sonido cuando se produzcan sucesos importantes durante un análisis, por ejemplo al detectar una amenaza o al finalizar el análisis, seleccione **Usar señal acústica**.

Integrar en el menú contextual: integra los elementos de control de ESET Endpoint Antivirus en el menú contextual.

Estados

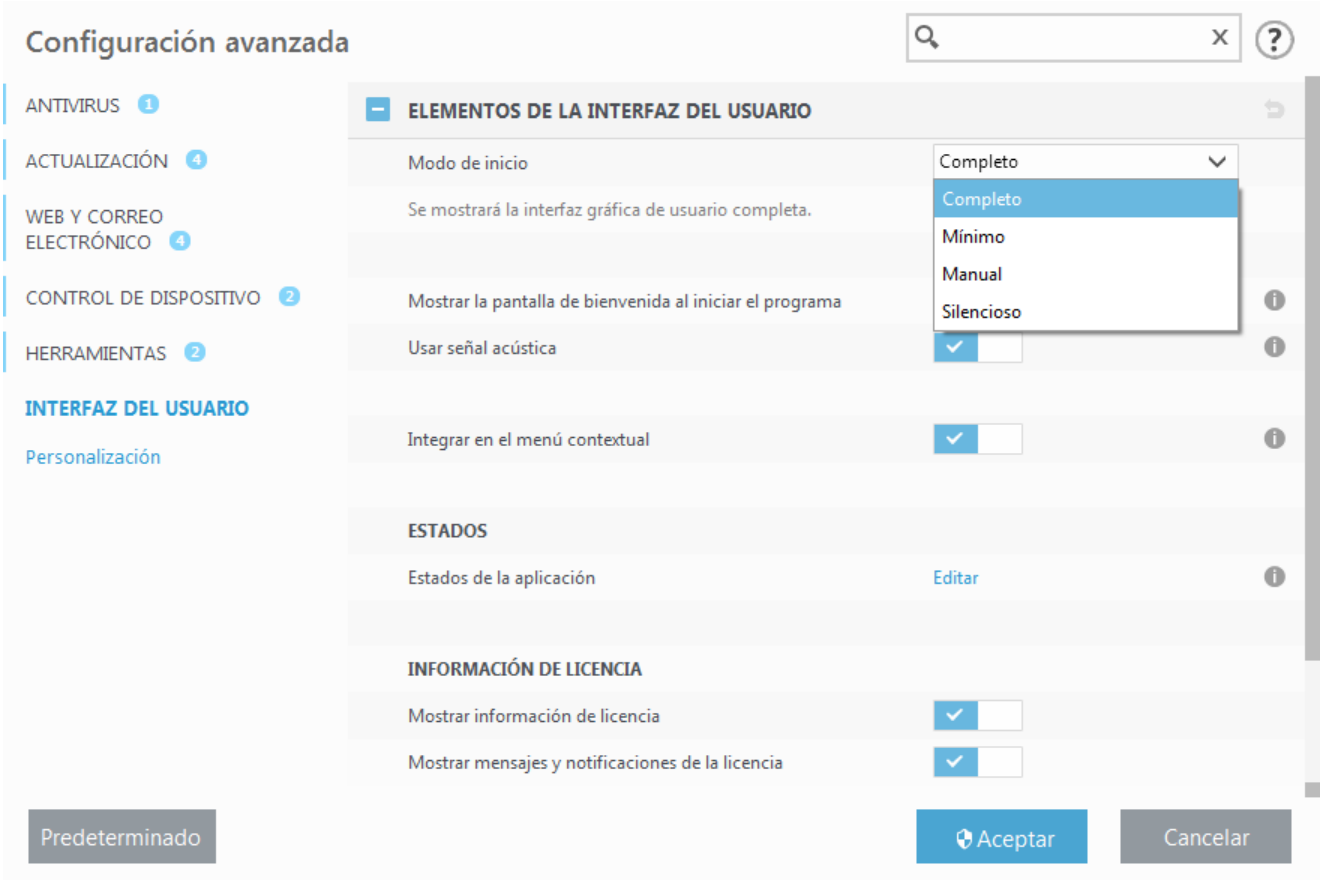
Estados de la aplicación: haga clic en el botón **Editar** para administrar (desactivar) los estados que se muestran en el menú **Estado de protección** del menú principal.

Información de licencia

Mostrar información de licencia: cuando esta opción esté desactivada, no se mostrará la información de la licencia en las pantallas **Estado de protección** y **Ayuda y asistencia técnica**.

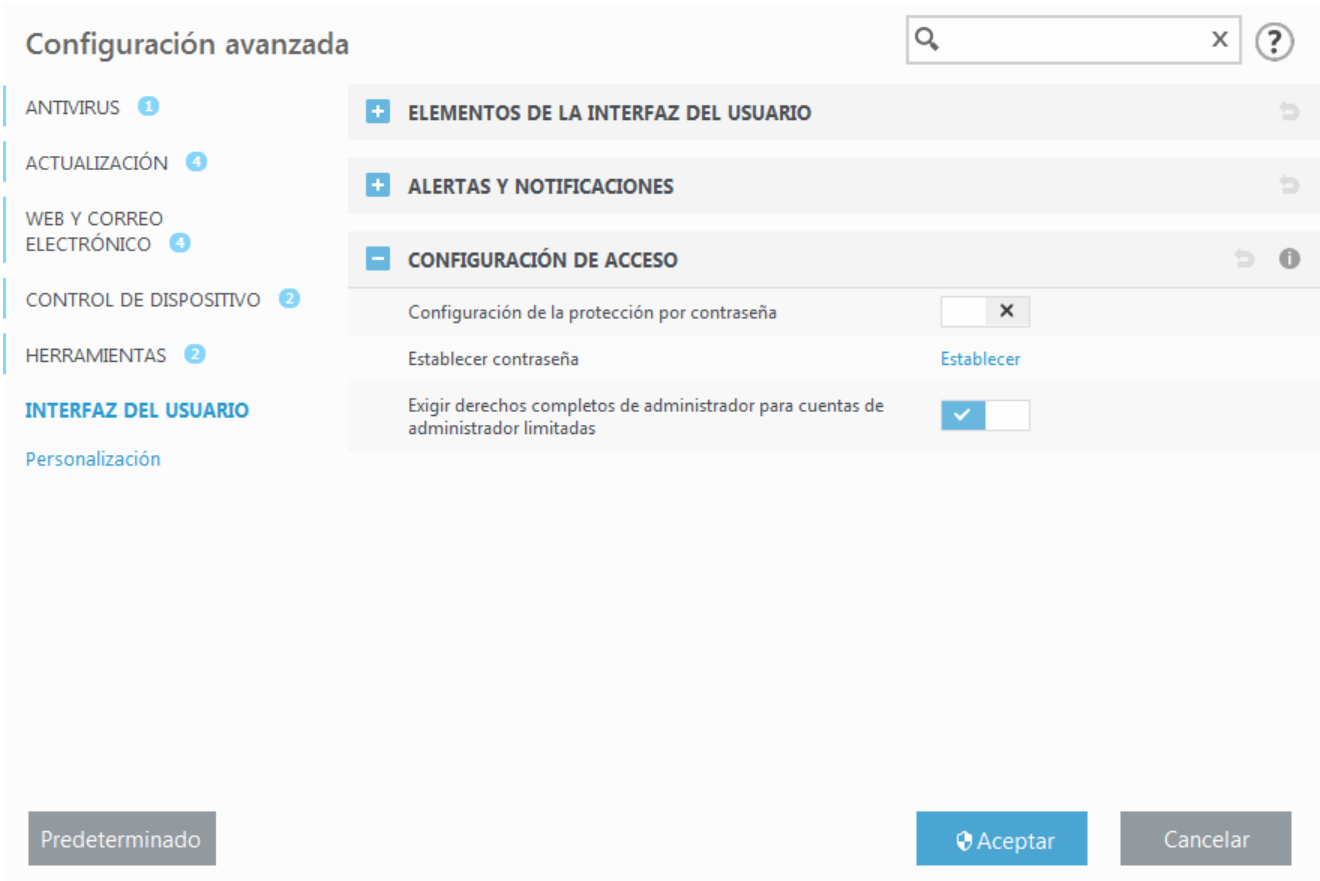
Mostrar mensajes y notificaciones de la licencia: cuando esta opción está desactivada, las notificaciones y los mensajes solo se mostrarán cuando la licencia caduque.

NOTA
en las instancias de ESET Endpoint Antivirus activadas con licencia MSP, los ajustes de información de la licencia se aplican pero no son accesibles.


Configuración avanzada
ANTIVIRUS 1
ACTUALIZACIÓN 4
WEB Y CORREO ELECTRÓNICO 4
CONTROL DE DISPOSITIVO 2
HERRAMIENTAS 2
INTERFAZ DEL USUARIO
Personalización
ELEMENTOS DE LA INTERFAZ DEL USUARIO
Modo de inicio
Completo
Completo
Mínimo
Manual
Silencioso
Se mostrará la interfaz gráfica de usuario completa.
Mostrar la pantalla de bienvenida al iniciar el programa
Usar señal acústica
Integrar en el menú contextual
ESTADOS
Estados de la aplicación
Editar
INFORMACIÓN DE LICENCIA
Mostrar información de licencia
Mostrar mensajes y notificaciones de la licencia
Predeterminado
Aceptar
Cancelar

3.9.5.2 Configuración de acceso

Para ofrecer la máxima seguridad a su sistema, es esencial que ESET Endpoint Antivirus se haya configurado correctamente. Una configuración incorrecta puede provocar la pérdida de datos importantes. Para evitar modificaciones no autorizadas, los parámetros de configuración de ESET Endpoint Antivirus se pueden proteger mediante contraseña. Los ajustes de configuración de la protección por contraseña se encuentran en **Configuración avanzada** (F5) bajo **Interfaz del usuario** > **Configuración de acceso**.



Configuración de la protección por contraseña: indique la configuración de la contraseña. Haga clic para abrir la ventana de configuración de contraseña.

Para configurar o cambiar una contraseña para proteger los parámetros de configuración, haga clic en **Definir**.

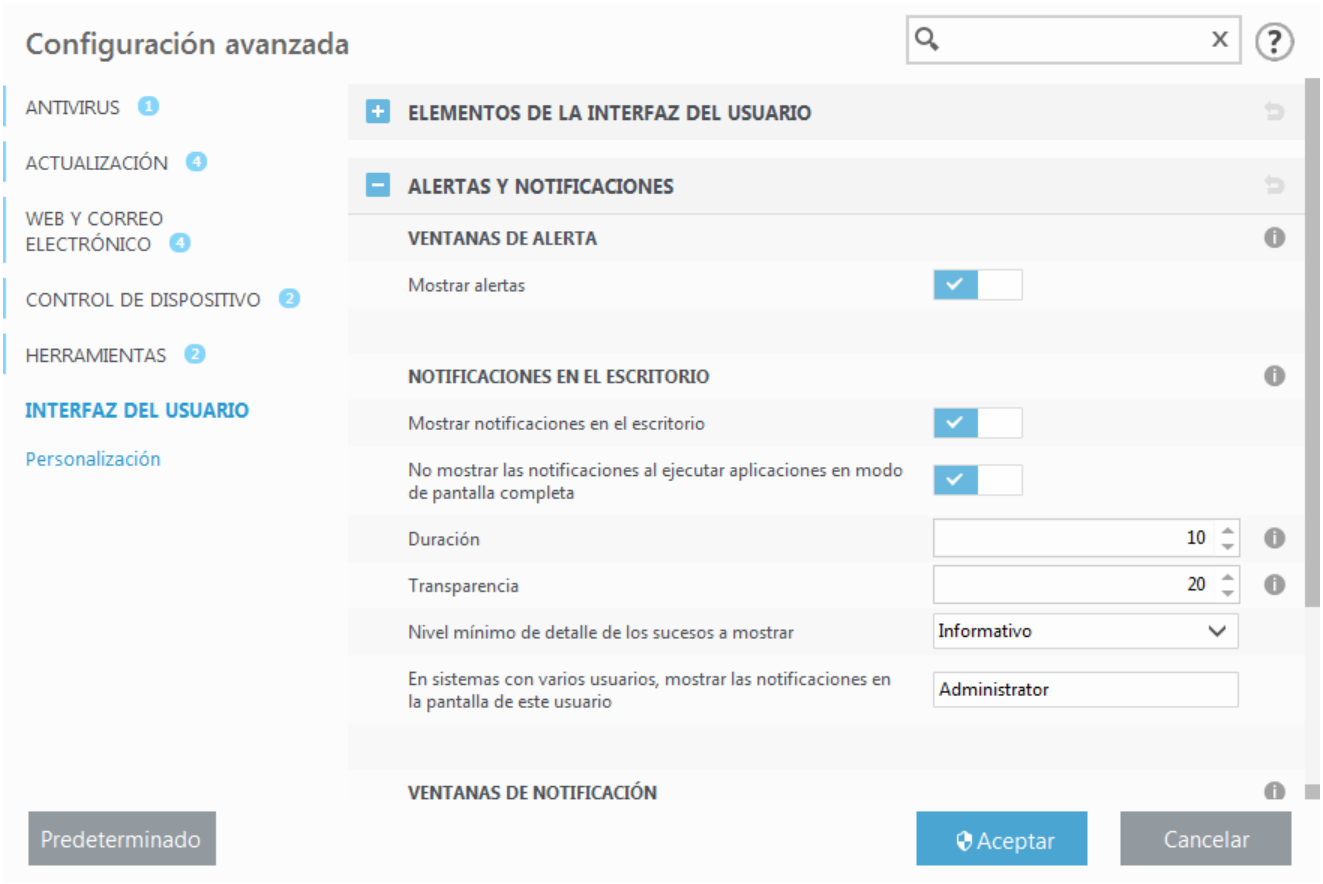
Exigir derechos completos de administrador para cuentas de administrador limitadas: mantenga esta opción activa para solicitar al usuario actual (si no tiene derechos de administrador) que introduzca el nombre de usuario y la contraseña de administrador al modificar determinados parámetros del sistema (parecido al UAC en Windows Vista). Estas modificaciones incluyen la desactivación de los módulos de protección.

Solo para Windows XP:

Exigir derechos de administrador (sistema sin soporte UAC): active esta opción para que ESET Endpoint Antivirus solicite las credenciales de administrador.

3.9.5.3 Alertas y notificaciones

La sección de **Alertas y notificaciones** de **Interfaz de usuario** le permite configurar cómo gestiona ESET Endpoint Antivirus las notificaciones del sistema (por ejemplo, mensajes de actualización correcta) y las alertas de amenaza. También puede definir si se muestra la hora y la transparencia de las notificaciones de la bandeja del sistema (esto se aplica únicamente a los sistemas que admiten notificaciones en la bandeja del sistema).



Ventanas de alerta

Si desactiva la opción **Mostrar alertas**, se cancelarán todos los mensajes de alerta. Solo resulta útil para una serie de situaciones muy específicas. Para la mayoría de los usuarios, se recomienda mantener la configuración predeterminada (activada).

Notificaciones en el escritorio

Las notificaciones del escritorio y los globos de sugerencias son medios de información que no requieren la intervención del usuario. Se muestran en el área de notificación, situada en la esquina inferior derecha de la pantalla. Para activar las notificaciones de escritorio, seleccione **Mostrar notificaciones en el escritorio**. Active el conmutador **No mostrar las notificaciones al ejecutar aplicaciones en modo de pantalla completa** para suprimir todas las notificaciones que no sean interactivas. A continuación encontrará más opciones avanzadas, como la modificación del tiempo de visualización de las notificaciones y la transparencia de las ventanas.

En el menú desplegable **Nivel mínimo de detalle de los sucesos a mostrar** se puede seleccionar el nivel de gravedad de las alertas y notificaciones que se mostrarán. Están disponibles las opciones siguientes:

- **Diagnóstico**: registra la información necesaria para ajustar el programa y todos los registros anteriores.
- **Informativo**: registra los mensajes informativos, incluidos los mensajes de las actualizaciones realizadas con éxito y todos los registros anteriores.
- **Alertas**: registra errores graves y mensajes de alerta.
- **Errores**: se registran los errores graves y errores del tipo "Error al descargar el archivo".
- **Críticos**: registra únicamente los errores graves (errores al iniciar la protección antivirus, etc.).

La última característica de esta sección le permite configurar el destino de las notificaciones en un entorno con varios usuarios. En el campo **En sistemas con varios usuarios, mostrar las notificaciones en la pantalla de este**

usuario se especifica el usuario que recibirá notificaciones del sistema y de otro tipo en sistemas que permitan la conexión de varios usuarios al mismo tiempo. Normalmente, este usuario es un administrador de sistemas o de redes. Esta opción resulta especialmente útil para servidores de terminal, siempre que todas las notificaciones del sistema se envíen al administrador.

Cuadros de mensajes

Para cerrar las ventanas emergentes automáticamente después de un período de tiempo determinado, seleccione la opción **Cerrar ventanas de notificación automáticamente**. Si no se cierran de forma manual, las ventanas de alerta se cerrarán automáticamente cuando haya transcurrido el período de tiempo especificado.

Mensajes de confirmación: muestra una lista de mensajes de confirmación que se pueden seleccionar para que se muestren o no.

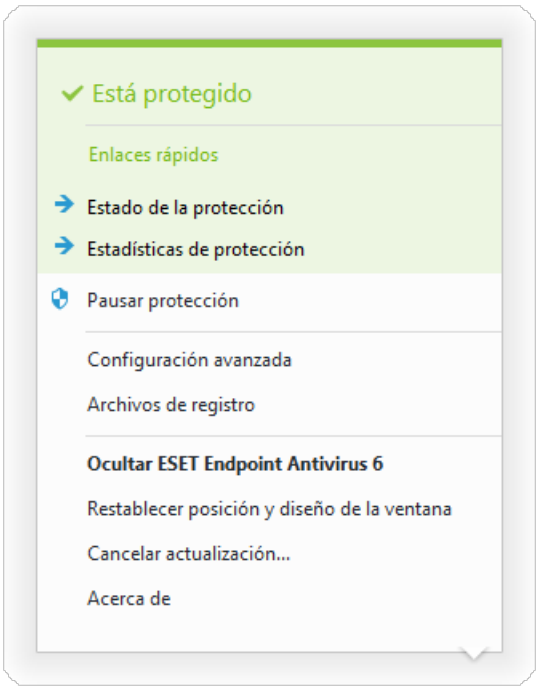
3.9.5.3.1 Error de conflicto de configuración avanzada

Este error se puede producir si algún componente (p. ej., HIPS) y el usuario crean las reglas en modo de aprendizaje o interactivo al mismo tiempo.

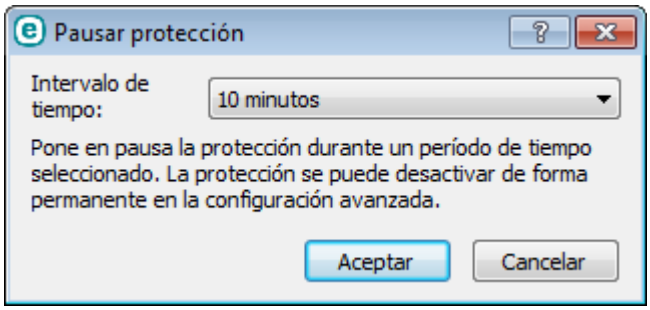
IMPORTANTE
Se recomienda cambiar el modo de filtrado al **modo automático** predeterminado si quiere crear sus propias reglas. Más información acerca de HIPS y modos de filtrado.

3.9.5.4 Icono en la bandeja del sistema

Algunas de las opciones y características de configuración más importantes están disponibles al hacer clic con el botón derecho del ratón en el icono de la bandeja del sistema.



Pausar protección: muestra el cuadro de diálogo de confirmación que desactiva la Protección antivirus y antiespía, que protege el sistema frente a ataques mediante el control de archivos, Internet y la comunicación por correo electrónico.



En el menú desplegable **Intervalo de tiempo** se indica el período de tiempo durante el que estará desactivada la protección antivirus y antiespía.

Configuración avanzada: seleccione esta opción para acceder al árbol de **Configuración avanzada**. También puede acceder a Configuración mediante la tecla F5 o desde **Configuración** > **Configuración avanzada**.

Archivos de registro: los archivos de registro contienen información acerca de todos los sucesos importantes del programa y proporcionan información general acerca de las amenazas detectadas.

Ocultar ESET Endpoint Antivirus: oculta la ventana de ESET Endpoint Antivirus de la pantalla.

Restablecer posición y diseño de la ventana: esta opción restablece el tamaño y la posición predeterminados de la ventana de ESET Endpoint Antivirus.

Buscar actualizaciones...: inicia la actualización de los módulos del programa para garantizar su nivel de protección contra el código malicioso.

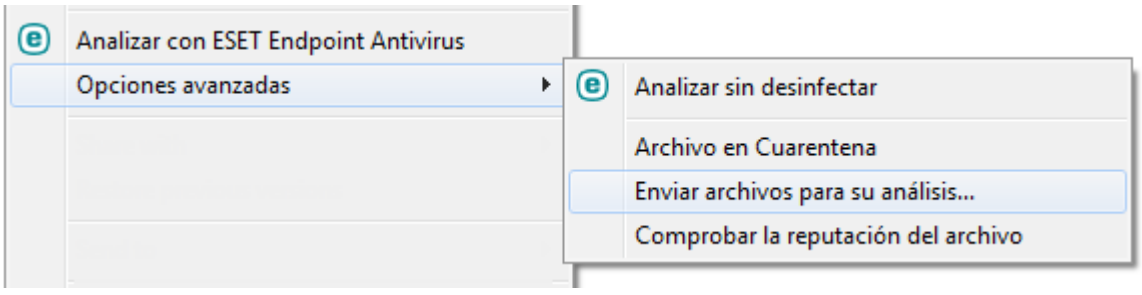
Acerca de: contiene información del sistema y detalles acerca de la versión instalada de ESET Endpoint Antivirus, así como de los módulos del programa instalados y la fecha de caducidad de la licencia. Al final de la página encontrará información sobre el sistema operativo y los recursos del sistema.

3.9.5.5 Menú contextual

El menú contextual aparece al hacer clic con el botón derecho en un objeto (archivo). En el menú se muestra una lista de todas las acciones que se pueden realizar en un objeto.

Es posible integrar elementos de control de ESET Endpoint Antivirus en el menú contextual. En el árbol de configuración avanzada se proporciona una opción de configuración para esta funcionalidad, en **Interfaz de usuario** > **Elementos de la interfaz del usuario**.

Integrar en el menú contextual: integra los elementos de control de ESET Endpoint Antivirus en el menú contextual.



3.10 Usuario avanzado

3.10.1 Administrador de perfiles

El administrador de perfiles se utiliza en dos secciones de ESET Endpoint Antivirus: en **Análisis del ordenador** y en **Actualización**.

Análisis del ordenador a petición

Puede guardar sus parámetros de análisis preferidos para próximas sesiones de análisis. Le recomendamos que cree un perfil diferente (con varios objetos de análisis, métodos de análisis y otros parámetros) para cada uno de los análisis que realice con frecuencia.

Para crear un perfil nuevo, abra la ventana Configuración avanzada (F5) y haga clic en **Antivirus** > **Análisis del ordenador a petición** y, a continuación, en **Modificar** junto a **Lista de perfiles**. En el menú desplegable **Perfil de actualización** se muestra una lista de los perfiles de análisis disponibles. Si necesita ayuda para crear un perfil de análisis que se adecúe a sus necesidades, consulte la sección Configuración de parámetros del motor ThreatSense para ver una descripción de los diferentes parámetros de la configuración del análisis.

Ejemplo: supongamos que desea crear su propio perfil de análisis y parte de la configuración del análisis estándar es adecuada; sin embargo, no desea analizar los empaquetadores en tiempo real ni las aplicaciones potencialmente peligrosas y, además, quiere aplicar la opción **Desinfección estricta**. Introduzca el nombre del nuevo perfil en la ventana **Administrador de perfiles** y haga clic en **Agregar**. Seleccione un perfil nuevo en el menú desplegable **Perfil de actualización**, ajuste los demás parámetros según sus requisitos y haga clic en **Aceptar** para guardar el nuevo perfil.

Actualización

El editor de perfil de la sección de configuración de actualizaciones permite a los usuarios crear nuevos perfiles de actualización. Cree y utilice sus propios perfiles personalizados (es decir, distintos al predeterminado **Mi perfil**) únicamente si su ordenador utiliza varios medios para conectarse a servidores de actualización.

Por ejemplo, un ordenador portátil que normalmente se conecta a un servidor local (Mirror) de la red local, pero descarga las actualizaciones directamente desde los servidores de actualización de ESET cuando se desconecta de la red local (en viajes de negocios) podría utilizar dos perfiles: el primero para conectarse al servidor local y el segundo, a los servidores de ESET. Una vez configurados estos perfiles, seleccione **Herramientas** > **Planificador de tareas** y modifique los parámetros de la tarea de actualización. Designe un perfil como principal y el otro, como secundario.

Perfil de actualización: el perfil de actualización utilizado actualmente. Para cambiarlo, seleccione un perfil en el menú desplegable.

Lista de perfiles: cree perfiles de actualización nuevos o quite los actuales.

3.10.2 Diagnóstico

El diagnóstico proporciona volcados de memoria de los procesos de ESET (por ejemplo, *ekrn*). Cuando una aplicación se bloquea, se genera un volcado de memoria que puede ayudar a los desarrolladores a depurar y arreglar varios problemas de ESET Endpoint Antivirus. Haga clic en el menú desplegable situado junto a **Tipo de volcado** y seleccione una de las tres opciones disponibles:

- Seleccione **Desactivar** (predeterminada) para desactivar esta característica.
- **Mini**: registra la información mínima necesaria para identificar el motivo del bloqueo inesperado de la aplicación. Este tipo de archivo de volcado puede resultar útil cuando el espacio es limitado, pero dada la poca información que contiene, es posible que el análisis de este archivo no detecte los errores que no estén relacionados directamente con el subproceso que se estaba ejecutando cuando se produjo el problema.
- **Completo**: registra todo el contenido de la memoria del sistema cuando la aplicación se detiene de forma inesperada. Los volcados de memoria completos pueden contener datos de procesos que se estaban ejecutando cuando se generó el volcado.

Activar el registro avanzado del filtrado de protocolos: registrar los datos que pasan a través del motor de filtrado de protocolos en formato PCAP. Esto puede ayudar a los desarrolladores a diagnosticar y corregir problemas relacionados con el filtrado de protocolos.

Activar registro avanzado del motor de actualización: registrar todos los eventos que se producen durante el proceso de actualización. Esto puede ayudar a los desarrolladores a diagnosticar y corregir los problemas relacionados con el motor de actualización.

Activar registro avanzado de las licencias: registrar toda la comunicación del producto con el servidor de licencias.

Activar registro avanzado del motor antispam: registrar todos los sucesos que tienen lugar durante el análisis antispam. Esto puede ayudar a los desarrolladores a diagnosticar y corregir problemas relacionados con el motor antispam de ESET.

Activar registro avanzado del sistema operativo: se recopilará información adicional sobre el sistema operativo, tal como los procesos en ejecución, la actividad de la CPU, las operaciones del disco, etc. Estos datos pueden ayudar a los desarrolladores a diagnosticar y corregir problemas relacionados con el producto de ESET que se ejecuta en su sistema operativo.

Los archivos de registro se pueden encontrar en:
C:\ProgramData\ESET\ESET Security\Diagnostics en Windows Vista y versiones posteriores o en *C:\Documents and Settings\All Users\...* en versiones anteriores de Windows.

Directorio de destino: directorio en el que se genera el volcado durante el bloqueo.

Abrir la carpeta de diagnóstico: haga clic en **Abrir** para abrir este directorio en una ventana nueva del *Explorador de Windows*.

Crear volcado de diagnóstico: haga clic en **Crear** para crear archivos de volcado de diagnóstico en el **Directorio de destino**.

3.10.3 Importar y exportar configuración

Puede importar o exportar el archivo de configuración .xml de ESET Endpoint Antivirus del menú **Configuración**.

La importación y la exportación de un archivo de configuración son útiles cuando necesita realizar una copia de seguridad de la configuración actual de ESET Endpoint Antivirus para utilizarla en otro momento. La opción de exportación de configuración también es de utilidad para los usuarios que desean utilizar su configuración preferida en varios sistemas, ya que les permite importar fácilmente el archivo *.xml* para transferir estos ajustes.

Importar la configuración es muy fácil. En la ventana principal del programa, haga clic en **Configuración** > **Importar/exportar configuración** y, a continuación, seleccione la opción **Importar configuración**. Introduzca el nombre del archivo de configuración o haga clic en el botón **...** para buscar el archivo de configuración que desea importar.

Los pasos para exportar una configuración son muy similares. En la ventana principal del programa, haga clic en **Configuración** > **Importar/exportar configuración**. Seleccione **Exportar configuración** e introduzca el nombre del archivo de configuración (por ejemplo, *export.xml*). Utilice el navegador para seleccionar la ubicación del ordenador donde desee guardar el archivo de configuración.

NOTA
Puede encontrarse con un error al exportar la configuración si no dispone de derechos suficientes para escribir el archivo exportado en el directorio especificado.

3.10.4 Línea de comandos

El módulo antivirus de ESET Endpoint Antivirus se puede iniciar manualmente a través de la línea de comandos, con el comando "ecls" o con un archivo por lotes ("bat"). Uso del análisis de línea de comandos ESET:

```
ecls [OPTIONS..] FILES..
```

Los siguientes parámetros y modificadores se pueden utilizar al ejecutar el análisis a petición desde la línea de comandos:

Opciones

/base-dir=CARPETA	cargar módulos desde una CARPETA
/quar-dir=CARPETA	CARPETA de cuarentena
/exclude=MÁSCARA	excluir del análisis los archivos que cumplan MÁSCARA
/subdir	analizar subcarpetas (predeterminado)
/no-subdir	no analizar subcarpetas
/max-subdir-level=NIVEL	máximo nivel de anidamiento para subcarpetas a analizar
/symlink	seguir enlaces simbólicos (predeterminado)
/no-symlink	omitir enlaces simbólicos
/ads	analizar ADS (predeterminado)
/no-ads	no analizar ADS
/log-file=ARCHIVO	registrar salida en ARCHIVO
/log-rewrite	sobrescribir el archivo de salida (predeterminado – agregar)
/log-console	enviar registro a la consola (predeterminado)
/no-log-console	no enviar registro a la consola
/log-all	registrar también los archivos sin infectar

/no-log-all	no registrar archivos sin infectar (predeterminado)
/aind	mostrar indicador de actividad
/auto	analizar y desinfectar automáticamente todos los discos locales

Opciones de análisis

/files	analizar archivos (predeterminado)
/no-files	no analizar archivos
/memory	analizar memoria
/boots	analizar sectores de inicio
/no-boots	no analizar sectores de inicio (predeterminado)
/arch	analizar archivos comprimidos (predeterminado)
/no-arch	no analizar archivos
/max-obj-size=TAMAÑO	analizar solo archivos menores de TAMAÑO megabytes (predeterminado 0 = ilimitado)
/max-arch-level=NIVEL	máxima profundidad de anidamiento para archivos comprimidos (archivos anidados) a analizar
/scan-timeout=LÍMITE	analizar archivos comprimidos durante LÍMITE segundos como máximo
/max-arch-size=TAMAÑO	analizar los archivos dentro de un archivo comprimido solo si su tamaño es inferior a TAMAÑO (predeterminado 0 = ilimitado)
/max-sfx-size=TAMAÑO	analizar solo los archivos en un archivo comprimido de autoextracción si su tamaño es inferior a TAMAÑO megabytes (predeterminado 0 = ilimitado)
/mail	analizar archivos de correo (predeterminado)
/no-mail	no analizar archivos de correo
/mailbox	analizar buzones de correo (predeterminado)
/no-mailbox	no analizar buzones de correo
/sfx	analizar archivos comprimidos de autoextracción (predeterminado)
/no-sfx	no analizar archivos comprimidos de autoextracción
/rtp	analizar empaquetadores en tiempo real (predeterminado)
/no-rtp	no analizar empaquetadores en tiempo real
/unsafe	analizar en busca de aplicaciones potencialmente peligrosas
/no-unsafe	no analizar en busca de aplicaciones potencialmente peligrosas
/unwanted	analizar en busca de aplicaciones potencialmente indeseables
/no-unwanted	no analizar en busca de aplicaciones potencialmente indeseables (predeterminado)
/suspicious	analizar en busca de aplicaciones sospechosas (predeterminado)
/no-suspicious	no analizar en busca de aplicaciones sospechosas
/pattern	usar firmas (predeterminado)
/no-pattern	no usar firmas
/heur	activar heurística (predeterminado)
/no-heur	desactivar heurística
/adv-heur	activar heurística avanzada (predeterminado)
/no-adv-heur	desactivar heurística avanzada
/ext=EXTENSIONES	analizar solo EXTENSIONES separadas por dos puntos
/ext-exclude=EXTENSIONES	excluir EXTENSIONES del análisis, separándolas por el signo ":" (dos puntos)
/clean-mode=MODO	utilizar el MODO desinfección para objetos infectados

Están disponibles las opciones siguientes:

- none (ninguno): no se realiza la desinfección automática.
- standard (estándar, predeterminado): ecls.exe intenta desinfectar o eliminar automáticamente los archivos infectados.
- strict (estricto): ecls.exe intenta desinfectar o eliminar automáticamente los archivos infectados sin la intervención del usuario (no verá una notificación antes de que se eliminen los archivos).
- rigorous (riguroso): ecls.exe elimina los archivos sin intentar desinfectarlos, sea cual sea el archivo.
- delete (eliminar): ecls.exe elimina los archivos sin intentar desinfectarlos, pero no elimina archivos delicados como los archivos del sistema de Windows.

/quarantine	copiar archivos infectados (si se han desinfectado) a la carpeta Cuarentena (complementa la acción realizada durante la desinfección)
/no-quarantine	no copiar archivos infectados a cuarentena

Opciones generales

/help	mostrar ayuda y salir
/version	mostrar información sobre la versión y salir
/preserve-time	conservar hora del último acceso

Códigos de salida

0	no se ha detectado ninguna amenaza
1	amenaza detectada y eliminada
10	no se han podido analizar todos los archivos (podrían ser amenazas)
50	amenaza detectada
100	error

NOTA
los códigos de salida superiores a 100 significan que no se ha analizado el archivo y que, por lo tanto, puede estar infectado.

3.10.5 Detección de estado inactivo

La detección de estado inactivo se puede configurar en **Configuración avanzada**, bajo **Antivirus** > **Análisis de estado inactivo** > **Detección de estado inactivo**. Esta configuración especifica un activador para el Análisis de estado inactivo cuando:

- el salvapantallas se está ejecutando,
- el ordenador está bloqueado,
- un usuario cierra sesión.

Utilice los conmutadores de cada estado correspondiente para activar o desactivar los distintos activadores de la detección del estado inactivo.

3.10.6 ESET SysInspector

3.10.6.1 Introducción a ESET SysInspector

ESET SysInspector es una aplicación que examina el ordenador a fondo y muestra los datos recopilados de forma exhaustiva. La información sobre los controladores y aplicaciones instalados, las conexiones de red o las entradas de registro importantes, por ejemplo, puede ayudarle en la investigación de un comportamiento sospechoso del sistema, ya sea debido a incompatibilidades del software o hardware o a una infección por malware.

Puede acceder a ESET SysInspector de dos formas: desde la versión integrada en las soluciones de ESET Security o descargando la versión independiente (SysInspector.exe) de forma gratuita desde el sitio web de ESET. Ambas versiones funcionan igual y tienen los mismos controles del programa. La única diferencia es cómo se administran los resultados. Las versiones independiente e integrada le permiten exportar instantáneas del sistema a un archivo *.xml* y guardarlas en el disco. Sin embargo, la versión integrada también permite almacenar las instantáneas del sistema directamente en **Herramientas** > **ESET SysInspector** (excepto ESET Remote Administrator). Para obtener más información, consulte la sección ESET SysInspector como parte de ESET Endpoint Antivirus.

Espere lo necesario mientras ESET SysInspector analiza el ordenador. Puede tardar entre 10 segundos y unos minutos en función de la configuración del hardware, el sistema operativo y el número de aplicaciones instaladas en el ordenador.

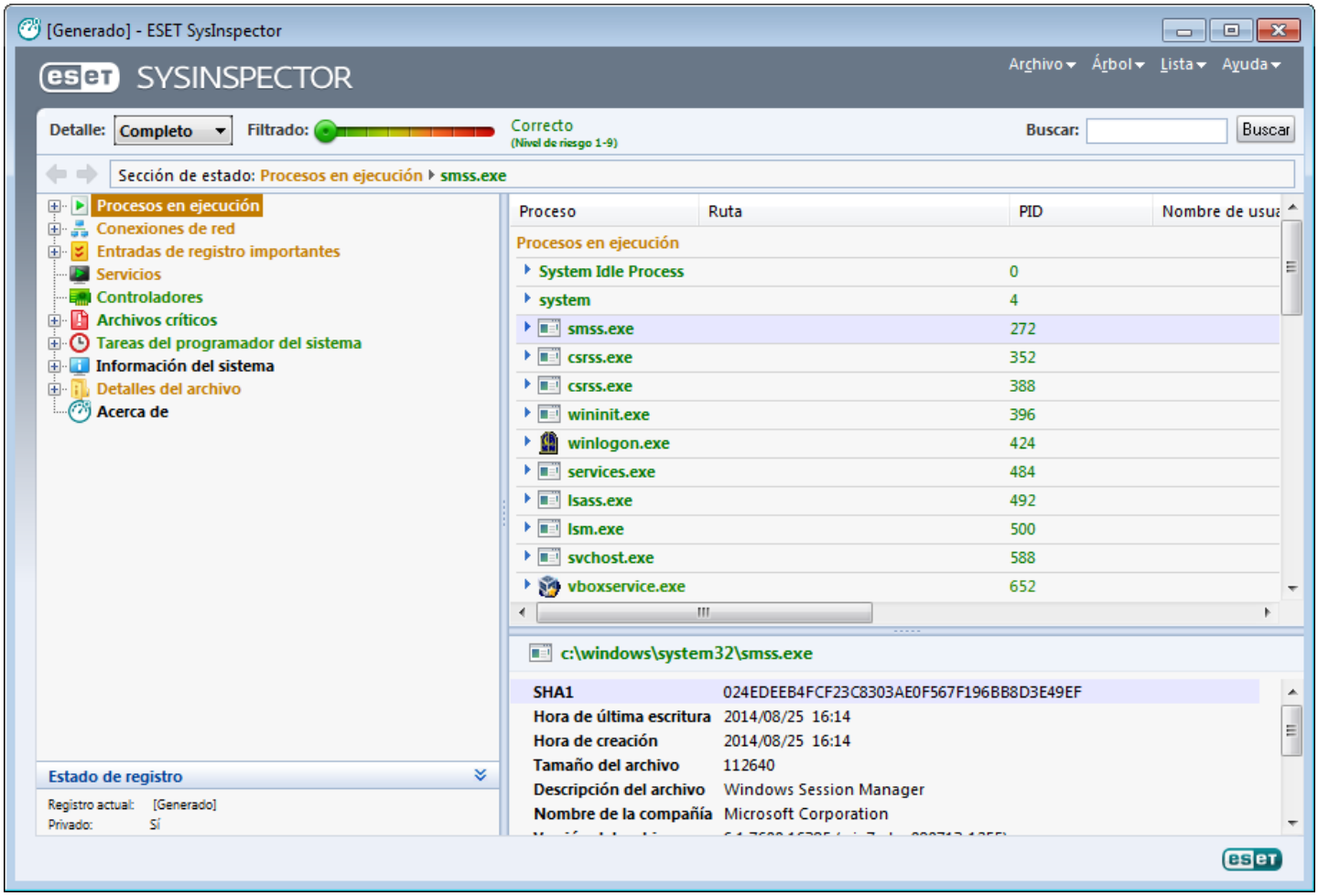
3.10.6.1.1 Inicio de ESET SysInspector

Para iniciar ESET SysInspector simplemente tiene que ejecutar el archivo *SysInspector.exe* que descargó del sitio web de ESET. Si ya tiene instalada alguna de las soluciones de ESET Security, puede ejecutar ESET SysInspector directamente desde el menú Inicio (haga clic en **Programas** > **ESET** > **ESET Endpoint Antivirus**).

Espere mientras la aplicación examina el sistema. El proceso de inspección puede tardar varios minutos.

3.10.6.2 Interfaz de usuario y uso de la aplicación

Para un uso sencillo, la ventana principal del programa se divide en cuatro secciones: Controles de programa, en la parte superior de la ventana principal del programa; la ventana de navegación, situada a la izquierda; la ventana Descripción, situada a la derecha; y la ventana Detalles, situada en la parte inferior de la ventana principal. La sección Estado del registro incluye los parámetros básicos de un registro (filtro utilizado, tipo de filtro, etc.) e indica si el registro es el resultado de una comparación.



3.10.6.2.1 Controles de programa

Esta sección contiene la descripción de todos los controles de programa disponibles en ESET SysInspector.

Archivo

Al hacer clic en **Archivo**, puede guardar el estado actual del sistema para examinarlo más tarde o abrir un registro guardado anteriormente. Para la publicación, es recomendable que genere un registro **Adecuado para su envío**. De esta forma, el registro omite la información confidencial (nombre del usuario actual, nombre del ordenador, nombre del dominio, privilegios del usuario actual, variables de entorno, etc.).

NOTA

los informes previamente almacenados de ESET SysInspector se pueden abrir arrastrándolos y colocándolos en la ventana principal del programa. Esta funcionalidad no está disponible en el sistema operativo Windows Vista por motivos de seguridad.

Árbol

Le permite expandir o cerrar todos los nodos, y exportar las secciones seleccionadas al script de servicio.

Lista

Contiene funciones para una navegación más sencilla por el programa y otras funciones como, por ejemplo, la búsqueda de información en línea.

Ayuda

Contiene información sobre la aplicación y sus funciones.

Detalle

Este ajuste modifica la información mostrada en la ventana principal del programa para que pueda trabajar con ella más fácilmente. En el modo "Básico", tiene acceso a información utilizada para buscar soluciones a problemas comunes de su sistema. En el modo "Medio", el programa muestra información menos utilizada. En el modo "Completo", ESET SysInspector muestra toda la información necesaria para solucionar problemas muy específicos.

Filtrado

Es la mejor opción para buscar entradas de registro o archivos sospechosos en el sistema. Mediante el ajuste del control deslizante, puede filtrar elementos por su nivel de riesgo. Si el control deslizante se coloca en el extremo izquierdo (nivel de riesgo 1), se muestran todos los elementos. Al mover el control deslizante a la derecha, el programa filtra todos los elementos que tienen un nivel de riesgo inferior al actual y muestra solo los elementos con un nivel de sospecha superior al mostrado. Si el control deslizante se encuentra en el extremo derecho, el programa muestra únicamente los elementos dañinos conocidos.

Todos los elementos que tengan un nivel de riesgo entre 6 y 9 pueden constituir un riesgo de seguridad. Si no está utilizando una solución de seguridad de ESET, le recomendamos que analice su sistema con ESET Online Scanner cuando ESET SysInspector encuentre un elemento de este tipo. ESET Online Scanner es un servicio gratuito.

NOTA
el nivel de riesgo de un elemento se puede determinar rápidamente comparando el color del elemento con el color del control deslizante del nivel de riesgo.

Comparar

Cuando se comparan dos registros, puede elegir que se visualicen todos los elementos, solo los elementos agregados, solo los elementos eliminados y solo los elementos sustituidos.

Buscar

Esta opción se puede utilizar para buscar rápidamente un elemento específico por su nombre o parte del nombre. Los resultados de la solicitud de búsqueda aparecerán en la ventana de descripción.

Retorno

Al hacer clic en las flechas hacia atrás o hacia delante, puede volver a la información mostrada previamente en la ventana Descripción. Puede utilizar la tecla Retroceso y la tecla de espacio, en lugar de hacer clic en las flechas atrás y adelante.

Sección de estado

Muestra el nodo actual en la ventana de navegación.

IMPORTANTE

los elementos destacados en rojo son elementos desconocidos, motivo por el que el programa los marca como potencialmente peligrosos. Que un elemento aparezca marcado en rojo no significa que deba eliminar el archivo. Antes de eliminarlo, asegúrese de que el archivo es realmente peligroso o innecesario.

3.10.6.2.2 Navegación por ESET SysInspector

ESET SysInspector divide los tipos de información en distintas secciones básicas denominadas nodos. Si está disponible, puede encontrar información adicional expandiendo los subnodos de cada nodo. Para abrir o contraer un nodo, haga doble clic en el nombre del nodo o haga clic en ⊞ o ⊟, junto al nombre del nodo. Cuando examine la estructura de árbol de nodos y subnodos en la ventana de navegación, puede encontrar información variada de cada nodo en la ventana de descripción. Si examina los elementos en la ventana de descripción, es posible que se muestre información adicional de cada uno de los elementos en la ventana de detalles.

A continuación se encuentran las descripciones de los nodos principales de la ventana de navegación e información relacionada en las ventanas de descripción y detalles.

Procesos en ejecución

Este nodo contiene información sobre aplicaciones y procesos que se ejecutan al generar el registro. En la ventana de descripción, puede encontrar información adicional de cada proceso como, por ejemplo, bibliotecas dinámicas utilizadas por el proceso y su ubicación en el sistema, el nombre del proveedor de la aplicación y el nivel de riesgo del archivo.

La ventana de detalles contiene información adicional de los elementos seleccionados en la ventana de descripción como, por ejemplo, el tamaño del archivo o su hash.

NOTA
un sistema operativo incluye varios componentes de kernel importantes que se ejecutan constantemente y proporcionan funciones básicas y esenciales para otras aplicaciones de usuario. En determinados casos, dichos procesos aparecen en la herramienta ESET SysInspector con una ruta de archivo que comienza por \??\. Estos símbolos optimizan el inicio previo de esos procesos; son seguros para el sistema.

Conexiones de red

La ventana de descripción contiene una lista de procesos y aplicaciones que se comunican a través de la red utilizando el protocolo seleccionado en la ventana de navegación (TCP o UDP), así como la dirección remota a la que se conecta la aplicación. También puede comprobar las direcciones IP de los servidores DNS.

La ventana de detalles contiene información adicional de los elementos seleccionados en la ventana de descripción como, por ejemplo, el tamaño del archivo o su hash.

Entradas de registro importantes

Contiene una lista de entradas de registro seleccionadas que suelen estar asociadas a varios problemas del sistema, como las que especifican programas de arranque, objetos auxiliares del navegador (BHO), etc.

En la ventana de descripción, puede encontrar los archivos que están relacionados con entradas de registro específicas. Puede ver información adicional en la ventana de detalles.

Servicios

La ventana de descripción contiene una lista de archivos registrados como Windows Services (Servicios de Windows). En la ventana de detalles, puede consultar la forma de inicio establecida para el servicio e información específica del archivo.

Controladores

Lista de los controladores instalados en el sistema.

Archivos críticos

En la ventana de descripción se muestra el contenido de los archivos críticos relacionados con el sistema operativo Microsoft Windows.

Tareas del programador del sistema

Contiene una lista de las tareas desencadenadas por el Programador de tareas de Windows a una hora/intervalo especificado.

Información del sistema

Contiene información detallada sobre el hardware y el software, así como información sobre las variables de entorno, los derechos de usuario y los registros de eventos del sistema establecidos.

Detalles del archivo

La lista de los archivos del sistema y los archivos de la carpeta Archivos de programa importantes. Se puede encontrar información adicional específica de los archivos en las ventanas de descripción y detalles.

Acerca de

Información acerca de la versión de ESET SysInspector y la lista de los módulos de programa.

3.10.6.2.2.1 Accesos directos del teclado

Los accesos directos que se pueden utilizar en ESET SysInspector son:

Archivo

Ctrl+O	Abrir el registro existente
Ctrl+S	Guardar los registros creados

Generar

Ctrl+G	Generar una instantánea de estado del ordenador estándar
Ctrl+H	Generar una instantánea de estado del ordenador que también puede registrar información confidencial

Filtrado de elementos

1, O	Seguro, se muestran los elementos que tienen un nivel de riesgo de 1 a 9
2	Seguro, se muestran los elementos que tienen un nivel de riesgo de 2 a 9
3	Seguro, se muestran los elementos que tienen un nivel de riesgo de 3 a 9
4, U	Desconocido, se muestran los elementos que tienen un nivel de riesgo de 4 a 9
5	Desconocido, se muestran los elementos que tienen un nivel de riesgo de 5 a 9
6	Desconocido, se muestran los elementos que tienen un nivel de riesgo de 6 a 9
7, B	Peligroso, se muestran los elementos que tienen un nivel de riesgo de 7 a 9
8	Peligroso, se muestran los elementos que tienen un nivel de riesgo de 8 a 9
9	Peligroso, se muestran los elementos que tienen un nivel de riesgo de 9
-	Disminuir el nivel de riesgo
+	Aumentar el nivel de riesgo
Ctrl+9	Modo de filtrado, mismo nivel o superior
Ctrl+0	Modo de filtrado, sólo mismo nivel

Ver

Ctrl+5	Ver por proveedor, todos los proveedores
Ctrl+6	Ver por proveedor, sólo Microsoft
Ctrl+7	Ver por proveedor, resto de proveedores
Ctrl+3	Mostrar todos los detalles
Ctrl+2	Mostrar la mitad de los detalles
Ctrl+1	Visualización básica

Retroceso	Volver un paso atrás
Espacio	Continuar con el paso siguiente
Ctrl+W	Expandir el árbol
Ctrl+Q	Contraer el árbol

Otros controles

Ctrl+T	Ir a la ubicación original del elemento tras seleccionarlo en los resultados de búsqueda
Ctrl+P	Mostrar la información básica de un elemento
Ctrl+A	Mostrar la información completa de un elemento
Ctrl+C	Copiar el árbol del elemento actual
Ctrl+X	Copiar elementos
Ctrl+B	Buscar información en Internet acerca de los archivos seleccionados
Ctrl+L	Abrir la carpeta en la que se encuentra el archivo seleccionado
Ctrl+R	Abrir la entrada correspondiente en el editor de registros
Ctrl+Z	Copiar una ruta de acceso a un archivo (si el elemento está asociado a un archivo)
Ctrl+F	Activar el campo de búsqueda
Ctrl+D	Cerrar los resultados de búsqueda
Ctrl+E	Ejecutar el script de servicio

Comparación

Ctrl+Alt+O	Abrir el registro original/comparativo
Ctrl+Alt+R	Cancelar la comparación
Ctrl+Alt+1	Mostrar todos los elementos
Ctrl+Alt+2	Mostrar sólo los elementos agregados, el registro incluirá los elementos presentes en el registro actual
Ctrl+Alt+3	Mostrar sólo los elementos eliminados, el registro incluirá los elementos presentes en el registro anterior
Ctrl+Alt+4	Mostrar sólo los elementos sustituidos (archivos incluidos)
Ctrl+Alt+5	Mostrar sólo las diferencias entre los registros
Ctrl+Alt+C	Mostrar la comparación
Ctrl+Alt+N	Mostrar el registro actual
Ctrl+Alt+P	Abrir el registro anterior

Varios

F1	Ver la Ayuda
Alt+F4	Cerrar el programa
Alt+Mayús+F4	Cerrar el programa sin preguntar
Ctrl+I	Estadísticas del registro

3.10.6.2.3 Comparar

La característica Comparar permite al usuario comparar dos registros existentes. El resultado es un conjunto de elementos no comunes a ambos registros. Esta herramienta permite realizar un seguimiento de los cambios introducidos en el sistema, una característica muy útil para la detección de código malicioso.

Una vez iniciada, la aplicación crea un nuevo registro, que aparecerá en una ventana nueva. Haga clic en **Archivo** > **Guardar registro** para guardar un registro en un archivo. Los archivos de registro se pueden abrir y ver posteriormente. Para abrir un registro existente, haga clic en **Archivo** > **Abrir registro**. En la ventana principal del programa, ESET SysInspector muestra siempre un registro cada vez.

La ventaja de comparar dos registros es que puede ver un registro actualmente activo y un registro guardado en un archivo. Para comparar registros, haga clic en **Archivo** > **Comparar registros** y elija **Seleccionar archivo**. El registro seleccionado se comparará con el registro activo en las ventanas principales del programa. El registro comparativo sólo mostrará las diferencias entre estos dos registros.

NOTA

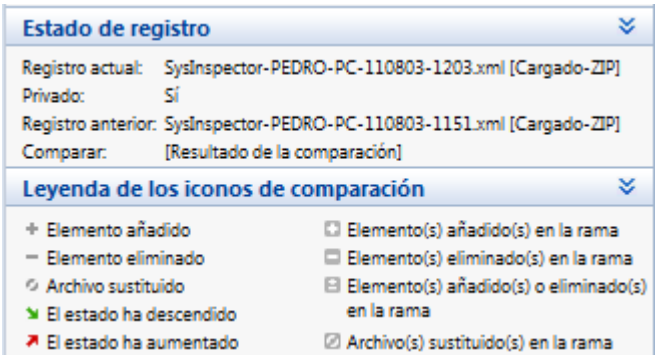
si compara dos archivos de registro, haga clic en **Archivo** > **Guardar registro** para guardarlo como archivo ZIP. Se guardarán ambos archivos. Si abre posteriormente dicho archivo, se compararán automáticamente los registros que contiene.

Junto a los elementos mostrados, ESET SysInspector muestra símbolos que identifican las diferencias entre los registros comparados.

Descripción de todos los símbolos que pueden aparecer junto a los elementos:

- + Nuevo valor que no se encuentra en el registro anterior.
- Sección de estructura de árbol contiene nuevos valores.
- – Valor eliminado que sólo se encuentra en el registro anterior.
- Sección de estructura de árbol contiene valores eliminados.
- Se ha cambiado un valor o archivo.
- Sección de estructura de árbol que contiene valores o archivos modificados.
- Ha disminuido el nivel de riesgo o era superior en el registro anterior.
- Ha aumentado el nivel de riesgo o era inferior en el registro anterior.

La explicación que aparece en la esquina inferior izquierda describe todos los símbolos y muestra los nombres de los registros que se están comparando.



Se puede guardar cualquier registro comparativo en un archivo y abrirlo posteriormente.

Ejemplo

Genere y guarde un registro, en el que se recopile información original sobre el sistema, en un archivo con el nombre previo.xml. Tras realizar los cambios en el sistema, abra ESET SysInspector y permita que genere un nuevo registro. Guárdelo en un archivo con el nombre *actual.xml*.

Para realizar un seguimiento de los cambios entre estos dos registros, haga clic en **Archivo** > **Comparar registros**. El programa creará un registro comparativo con las diferencias entre ambos registros.

Se puede lograr el mismo resultado si utiliza la siguiente opción de la línea de comandos:

SysIsnpector.exe actual.xml previo.xml

3.10.6.3 Parámetros de la línea de comandos

ESET SysInspector admite la generación de informes desde la línea de comandos con estos parámetros:

/gen	genera un registro directamente desde la línea de comandos, sin ejecutar la interfaz gráfica.
/privacy	genera un registro omitiendo la información personal.
/zip	guarda el registro obtenido en un archivo comprimido zip.
/silent	cancela la ventana de progreso cuando se genera un registro desde la línea de comandos.
/blank	inicia ESET SysInspector sin generar o cargar un registro.

Ejemplos

Uso:

```
Sysinspector.exe [load.xml] [/gen=save.xml] [/privacy] [/zip] [compareto.xml]
```

Para cargar un registro determinado directamente en el navegador, utilice: *SysInspector.exe .\clientlog.xml*
Para generar un registro desde la línea de comandos, utilice: *SysInspector.exe /gen=.\mynewlog.xml*
Para generar un registro que no incluya la información confidencial directamente como archivo comprimido, utilice: *SysInspector.exe /gen=.\mynewlog.zip /privacy /zip*
Para comparar dos archivos de registro y examinar las diferencias, utilice: *SysInspector.exe new.xml old.xml*

NOTA
si el nombre del archivo o la carpeta contiene un espacio, debe escribirse entre comillas.

3.10.6.4 Script de servicio

El script de servicio es una herramienta que ofrece ayuda a los clientes que utilizan ESET SysInspector eliminando de forma sencilla objetos no deseados del sistema.

El script de servicio permite al usuario exportar el registro completo de ESET SysInspector o únicamente las partes seleccionadas. Tras la exportación, puede marcar los objetos no deseados que desee eliminar. A continuación, puede ejecutar el registro modificado para eliminar los objetos marcados.

El script de servicio es útil para usuarios avanzados con experiencia previa en el diagnóstico de problemas del sistema. Las modificaciones realizadas por usuarios sin experiencia pueden provocar daños en el sistema operativo.

Ejemplo

Si sospecha que el ordenador está infectado por un virus que el antivirus no detecta, siga estas instrucciones:

1. Ejecute ESET SysInspector para generar una nueva instantánea del sistema.
2. Seleccione el primer elemento de la sección que se encuentra a la izquierda (en la estructura de árbol), pulse Mayús y seleccione el último elemento para marcarlos todos.
3. Haga clic con el botón secundario en los objetos seleccionados y elija la opción **Exportar las secciones seleccionadas al script de servicio**.
4. Los objetos seleccionados se exportarán a un nuevo registro.
5. Este es el paso más importante de todo el procedimiento: abra el registro nuevo y cambie el atributo - a + para todos los objetos que desee eliminar. Asegúrese de no marcar ningún archivo/objeto importante del sistema operativo.
6. Abra ESET SysInspector, haga clic en **Archivo** > **Ejecutar script de servicio** e introduzca la ruta del script.
7. Haga clic en **Aceptar** para ejecutar el script.

3.10.6.4.1 Generación de scripts de servicio

Para generar un script de servicio, haga clic con el botón derecho del ratón en cualquier elemento del árbol de menús (en el panel izquierdo) de la ventana principal de ESET SysInspector. En el menú contextual, seleccione **Exportar todas las secciones al script de servicio** o **Exportar secciones seleccionadas al script de servicio**.

NOTA
cuando se comparan dos registros, el script de servicio no se puede exportar.

3.10.6.4.2 Estructura del script de servicio

En la primera línea del encabezado del script encontrará información sobre la versión del motor (ev), la versión de la interfaz gráfica de usuario (gv) y la versión del registro (lv). Puede utilizar estos datos para realizar un seguimiento de los posibles cambios del archivo .xml que genere el script y evitar las incoherencias durante la ejecución. Esta parte del script no se debe modificar.

El resto del archivo se divide en secciones, donde los elementos se pueden modificar (indique los que procesará el script). Para marcar los elementos que desea procesar, sustituya el carácter "-" situado delante de un elemento por el carácter "+". En el script, las secciones se separan mediante una línea vacía. Cada sección tiene un número y un título.

01) Running processes (Procesos en ejecución)

En esta sección se incluye una lista de todos los procesos que se están ejecutando en el sistema. Cada proceso se identifica mediante su ruta UNC y, posteriormente, su código hash CRC16 representado mediante asteriscos (*).

Ejemplo:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

En este ejemplo se ha seleccionado (marcado con el carácter "+") el proceso module32.exe, que finalizará al ejecutar el script.

02) Loaded modules (Módulos cargados)

En esta sección se enumeran los módulos del sistema que se utilizan actualmente.

Ejemplo:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

En este ejemplo, se marcó el módulo khbekhb.dll con el signo "+". Cuando se ejecute, el script reconocerá los procesos mediante el módulo específico y los finalizará.

03) TCP connections (Conexiones TCP)

En esta sección se incluye información sobre las conexiones TCP existentes.

Ejemplo:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

Cuando se ejecute, el script localizará al propietario del socket en las conexiones TCP marcadas y detendrá el socket, liberando así recursos del sistema.

04) UDP endpoints (Puntos finales UDP)

En esta sección se incluye información sobre los puntos finales UDP existentes.

Ejemplo:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Cuando se ejecute, el script aislará al propietario del socket en los puntos finales UDP marcados y detendrá el socket.

05) DNS server entries (Entradas del servidor DNS)

En esta sección se proporciona información sobre la configuración actual del servidor DNS.

Ejemplo:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Las entradas marcadas del servidor DNS se eliminarán al ejecutar el script.

06) Important registry entries (Entradas de registro importantes)

En esta sección se proporciona información sobre las entradas de registro importantes.

Ejemplo:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

Cuando se ejecute el script, las entradas marcadas se eliminarán, se reducirán a valores de 0 bytes o se restablecerán en sus valores predeterminados. La acción realizada en cada entrada depende de su categoría y del valor de la clave en el registro específico.

07) Services (Servicios)

En esta sección se enumeran los servicios registrados en el sistema.

Ejemplo:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

Cuando se ejecute el script, los servicios marcados y los servicios dependientes se detendrán y desinstalarán.

08) Drivers (Controladores)

En esta sección se enumeran los controladores instalados.

Ejemplo:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:
\windows\system32\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Cuando se ejecuta el script, los controladores seleccionados se detendrán. Tenga en cuenta que algunos controladores no permiten su detención.

09) Critical files (Archivos críticos)

En esta sección se proporciona información sobre los archivos que son críticos para el correcto funcionamiento del sistema operativo.

Ejemplo:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Los elementos seleccionados se eliminarán o restablecerán en sus valores originales.

3.10.6.4.3 Ejecución de scripts de servicio

Seleccione todos los elementos que desee y, a continuación, guarde y cierre el script. Ejecute el script modificado directamente desde la ventana principal de ESET SysInspector, con la opción **Ejecutar script de servicio** del menú Archivo. Cuando abra un script, el programa mostrará el mensaje siguiente: **¿Está seguro de que desea ejecutar el script de servicio "%Scriptname%"?** Una vez que haya confirmado la selección, es posible que se muestre otra advertencia para informarle de que el script de servicio que intenta ejecutar no está firmado. Haga clic en **Ejecutar** para iniciar el script.

Una ventana de diálogo confirmará que el script se ha ejecutado correctamente.

Si el script no se puede procesar por completo, se mostrará una ventana de diálogo con el mensaje siguiente: **El script de servicio se ejecutó parcialmente. ¿Desea ver el informe de errores?** Seleccione **Sí** para ver un informe de errores completo con todas las operaciones que no se ejecutaron.

Si no se reconoce el script, aparece una ventana de diálogo con el mensaje siguiente: **No se ha firmado el script de servicio seleccionado. La ejecución de scripts desconocidos y sin firmar podría dañar seriamente los datos del ordenador. ¿Está seguro de que desea ejecutar el script y llevar a cabo las acciones?** Esto podría deberse a que el script presenta inconsistencias (encabezado dañado, título de sección dañado, falta línea vacía entre secciones, etc.). Vuelva a abrir el archivo del script y corrija los errores o cree un script de servicio nuevo.

3.10.6.5 Preguntas frecuentes

¿Es necesario contar con privilegios de administrador para ejecutar ESET SysInspector?

Aunque ESET SysInspector no requiere privilegios de administrador para su ejecución, sí es necesario utilizar una cuenta de administrador para acceder a parte de la información que recopila. Si lo ejecuta como usuario normal o restringido, se recopilará menor cantidad de información acerca de su entorno operativo.

¿ESET SysInspector crea archivos de registro?

ESET SysInspector puede crear un archivo de registro de la configuración de su ordenador. Para guardar uno, haga clic en **Archivo** > **Guardar registro** en la ventana principal del programa. Los registros se guardan con formato XML. De forma predeterminada, los archivos se guardan en el directorio *%USERPROFILE%\Mis documentos*\, con una convención de nomenclatura del tipo "SysInpsector-%COMPUTERNAME%-YYMMDD-HHMM.XML". Si lo desea, puede modificar tanto la ubicación como el nombre del archivo de registro antes de guardarlo.

¿Cómo puedo ver el contenido del archivo de registro de ESET SysInspector?

Para visualizar un archivo de registro creado por ESET SysInspector, ejecute la aplicación y haga clic en **Archivo** > **Abrir registro** en la ventana principal del programa. También puede arrastrar y soltar los archivos de registro en la aplicación ESET SysInspector. Si necesita ver los archivos de registro de ESET SysInspector con frecuencia, le recomendamos que cree un acceso directo al archivo SYSINSPECTOR.EXE en su escritorio. Para ver los archivos de registro, arrástrelos y suéltelos en ese acceso directo. Por razones de seguridad, es posible que Windows Vista/7 no permita la acción de arrastrar y soltar entre ventanas que cuentan con permisos de seguridad diferentes.

¿Existe alguna especificación disponible para el formato del archivo de registro? ¿Y algún conjunto de herramientas para el desarrollo de aplicaciones (SDK)?

Actualmente, no se encuentra disponible ninguna especificación para el formato del archivo de registro, ni un conjunto de herramientas para el desarrollo de aplicaciones, ya que el programa se encuentra aún en fase de desarrollo. Una vez que se haya lanzado, podremos proporcionar estos elementos en función de la demanda y los comentarios por parte de los clientes.

¿Cómo evalúa ESET SysInspector el riesgo que plantea un objeto en particular?

Generalmente, ESET SysInspector asigna un nivel de riesgo a los objetos (archivos, procesos, claves de registro, etc.). Para esto, utiliza una serie de reglas heurísticas que examinan las características de cada uno de ellos y después estima el potencial de actividad maliciosa. Según estas heurísticas, a los objetos se les asignará un nivel de riesgo desde el valor 1: seguro (en color verde) hasta 9: peligroso (en color rojo). En el panel de navegación que se encuentra a la izquierda, las secciones estarán coloreadas según el nivel máximo de peligrosidad que presente un objeto en su interior.

El nivel de riesgo "6: desconocido (en color rojo)", ¿significa que un objeto es peligroso?

Las evaluaciones de ESET SysInspector no garantizan que un objeto sea malicioso. Esta determinación deberá confirmarla un experto en seguridad informática. ESET SysInspector está diseñado para proporcionar una guía rápida a estos expertos, con la finalidad de que conozcan los objetos que deberían examinar en un sistema en busca de algún comportamiento inusual.

¿Por qué ESET SysInspector se conecta a Internet cuando se ejecuta?

Como muchas otras aplicaciones, ESET SysInspector contiene una firma digital que actúa a modo de "certificado". Esta firma sirve para garantizar que ESET ha desarrollado la aplicación y que no se ha alterado. Para comprobar la autenticidad del certificado, el sistema operativo debe contactar con la autoridad certificadora, que verificará la identidad del desarrollador de la aplicación. Este es un comportamiento normal para todos los programas firmados digitalmente que se ejecutan en Microsoft Windows.

¿En qué consiste la tecnología AntiStealth?

La tecnología AntiStealth proporciona un método efectivo de detección de rootkits.

Si el código malicioso que se comporta como un rootkit ataca al sistema, el usuario se expone a pérdidas o robo de información. Si no se dispone de una herramienta antirootkit especial, es prácticamente imposible detectar los rootkits.

¿Por qué a veces hay archivos con la marca "Firmado por MS" que, al mismo tiempo, tienen una entrada de "Nombre de compañía" diferente?

Al intentar identificar la firma digital de un archivo ejecutable, ESET SysInspector comprueba en primer lugar si el archivo contiene una firma digital integrada. Si se encuentra una firma digital, el archivo se validará utilizando dicha información. Si no se encuentra una firma digital, ESI comienza a buscar el archivo CAT correspondiente (Catálogo de seguridad: *%systemroot%\system32\catroot*) que contiene información sobre el archivo ejecutable procesado. Si se encuentra el archivo CAT relevante, la firma digital de dicho archivo CAT será la que se aplique en el proceso de validación del archivo ejecutable.

Esa es la razón por la cual a veces hay archivos marcados como "Firmado por MS", pero que tienen una entrada "Nombre de compañía" diferente.

3.10.6.6 ESET SysInspector como parte de ESET Endpoint Antivirus

Para abrir la sección ESET SysInspector en ESET Endpoint Antivirus, haga clic en **Herramientas** > **ESET SysInspector**. El sistema de administración de la ventana de ESET SysInspector es parecido al de los registros de análisis del equipo o las tareas programadas. Se puede obtener acceso a todas las operaciones con instantáneas del sistema (como crear, ver, comparar, quitar y exportar) con tan sólo un par de clics.

La ventana de ESET SysInspector contiene información básica acerca de las instantáneas creadas como, por ejemplo, la hora de creación, un breve comentario, el nombre del usuario que ha creado la captura y el estado de esta.

Para comparar, crear o eliminar instantáneas, utilice los botones correspondientes ubicados debajo de la lista de instantáneas de la ventana de ESET SysInspector. Estas opciones también están disponibles en el menú contextual. Para ver la instantánea del sistema seleccionada, seleccione **Mostrar** en el menú contextual. Para exportar la instantánea seleccionada a un archivo, haga clic con el botón derecho del ratón en ella y seleccione **Exportar...**

A continuación se muestra una descripción detallada de las opciones disponibles:

- **Comparar**: le permite comparar dos registros existentes. Esta opción es ideal para realizar un seguimiento de los cambios entre el registro actual y el anterior. Para poder aplicar esta opción, debe seleccionar dos instantáneas con el fin de compararlas.
- **Crear...**: le permite crear un nuevo registro. Antes debe introducir un breve comentario acerca del registro. Para obtener información sobre el progreso del proceso de creación de la instantánea (de la instantánea que se ha generado en ese momento), consulte la columna **Estado**. Todas las instantáneas completadas aparecen marcadas con el estado **Creado**.
- **Eliminar/Eliminar todo**: quita entradas de la lista.
- **Exportar...**: guarda la entrada seleccionada en un archivo XML (y también en una versión comprimida).

3.10.7 Supervisión y administración remotas

Remote Monitoring and Management (RMM) is the process of supervising and controlling software systems using a locally installed agent that can be accessed by a management service provider. The default ESET Endpoint Antivirus installation contains the file *ermm.exe* located in the Endpoint application within the directory *c:\Program Files\ESET\ESET Security*. *ermm.exe* is a command line utility designed to facilitate the management of endpoint products and communications with any RMM Plugin. *ermm.exe* exchanges data with the RMM Plugin, which communicates with the RMM Agent linked to an RMM Server. By default, the ESET RMM tool is disabled. For more information, see Cómo activar supervisión y administración remotas.

The default ESET Endpoint Antivirus installation contains file ermm.exe located in the Endpoint application directory (default path *c:\Program Files\ESET\ESET Security*). ermm.exe exchanges data with the RMM Plugin, which communicates with the RMM Agent that is linked to an RMM Server.

- ermm.exe – command line utility developed by ESET that allows managing of Endpoint products and communication with any RMM Plugin.

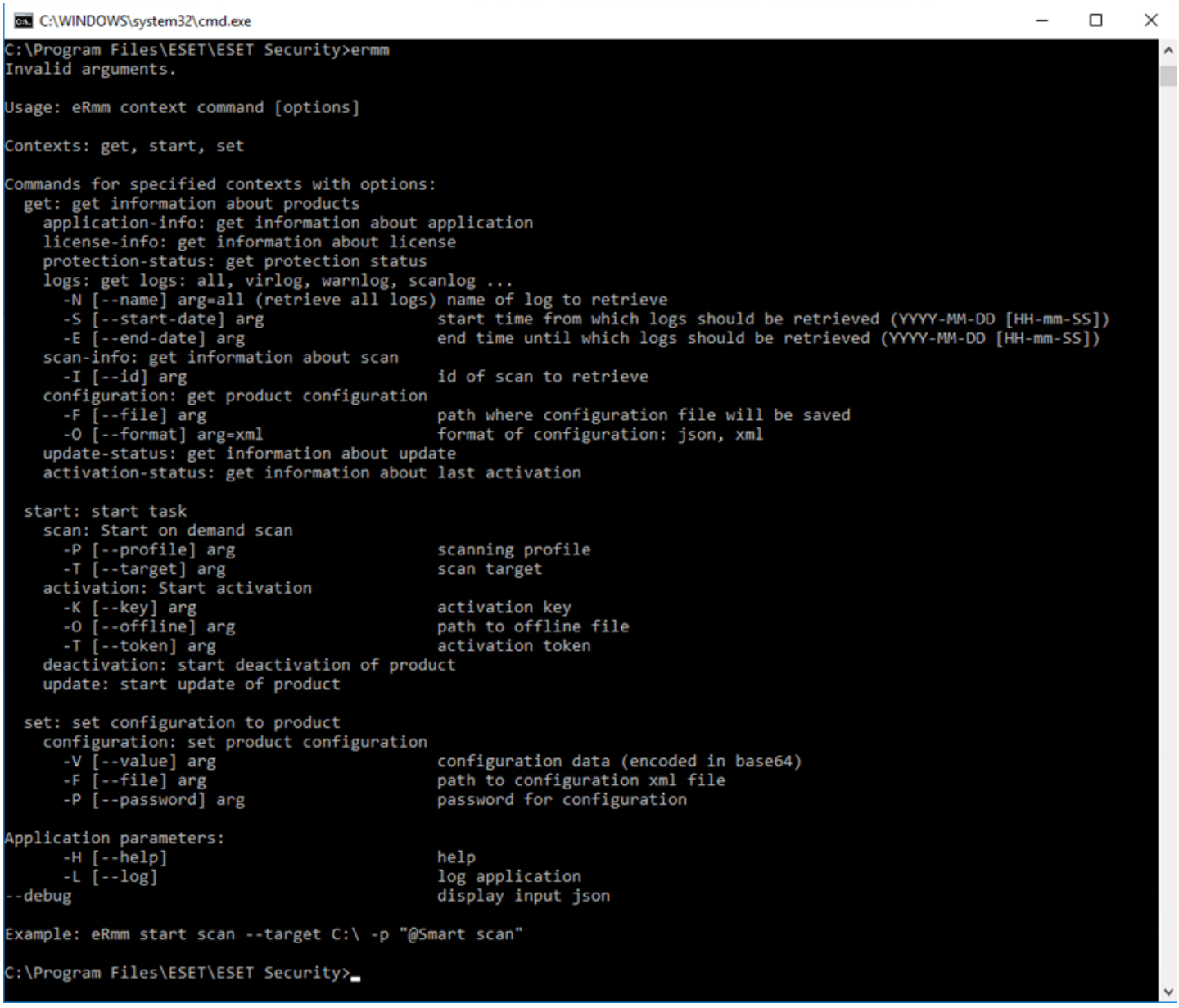
3.10.7.1 Línea de comandos RMM

Remote monitoring management is run using the command line interface. The default ESET Endpoint Antivirus installation contains the file *ermm.exe* located in the Endpoint application within the directory *c:\Program Files\ESET\ESET Security*.

Run the Command Prompt (cmd.exe) as an Administrator and navigate to the mentioned path. (To open Command Prompt, press Windows button + R on your keyboard, type a *cmd.exe* into the Run window and press Enter.)

The command syntax is: `ermm context command [options]`

Also note that the log parameters are case sensitive.



ermm.exe uses three basic contexts: Get, Start and Set. In the table below you can find examples of commands syntax. Click the link in the Command column to see the further options, parameters, and usage examples. After successful execution of command, the output part (result) will be displayed. To see an input part, add parameter `--debug` at the of the command.

Context	Command	Description
get		**Get information about products**

Context	Command	Description
	información-aplicación	Get information about product
	información-licencia	Get information about license
	estado-protección	Get protection status
	registros	Get logs
	información-análisis	Get information about running scan
	configuración	Get product configuration
	estado-actualización	Get information about update
	estado-activación	Get information about last activation
start		**Start task**
	análisis	Start on demand scan
	activación	Start activation of product
	desactivación	Start deactivation of product
	actualizar	Start update of product
set		**Set options for product**
	configuración	Set configuration to product

In the output result of every command, the first information displayed is result ID. To understand better the result information, check the table of IDs below.

Error ID	Error	Description
0	Success	
1	Command node not present	"Command" node not present in input json
2	Command not supported	Particular command is not supported
3	General error executing the command	Error during execution of command
4	Task already running	Requested task is already running and has not been started
5	Invalid parameter for command	Bad user input
6	Command not executed because it's disabled	RMM isn't enabled in advanced settings or isn't started as an administrator

3.10.7.2 Lista de comandos JSON

- obtener estado-protección
- obtener información-aplicación
- obtener información-licencia
- obtener registros
- obtener estado-activación
- obtener información-análisis
- obtener configuración
- obtener estado-actualización
- iniciar análisis
- iniciar activación
- iniciar desactivación
- iniciar actualización
- definir configuración

3.10.7.2.1 obtener estado-protección

Get the list of application statuses and the global application status

Command line

```
ermm.exe get protection-status
```

Parameters

None

Example

call

```
{
 "command":"get_protection_status",
 "id":1,
 "version":"1"
}
```

result

```
{
 "id":1,
 "result":{
  "statuses":[{
    "id":"EkrnNotActivated",
    "status":2,
    "priority":768,
    "description":"Product not activated"
   }],
  "status":2,
```

```
  "description":"Security alert"
 },
 "error":null
}
```

3.10.7.2.2 obtener información-aplicación

Get information about the installed application

Command line

```
ermm.exe get application-info
```

Parameters

None

Example

call

```
{
 "command":"get_application_info",
 "id":1,
 "version":"1"
}
```

result

```
{
  "id":1,
  "result":{
   "description":"ESET Endpoint Antivirus",
   "version":"6.6.2018.0",
   "product":"eea",
   "lang_id":1033,
   "modules":[{
    "id":"SCANNER32",
    "description":"Detection engine",
    "version":"15117",
    "date":"2017-03-20"
   },{
    "id":"PEGASUS32",
    "description":"Rapid Response module",
    "version":"9734",
    "date":"2017-03-20"
```

```
},{
 "id":"LOADER32",
 "description":"Update module",
 "version":"1009",
 "date":"2016-12-05"
},{
 "id":"PERSEUS32",
 "description":"Antivirus and antispyware scanner module",
 "version":"1513",
 "date":"2017-03-06"
},{
 "id":"ADVHEUR32",
 "description":"Advanced heuristics module",
 "version":"1176",
 "date":"2017-01-16"
},{
 "id":"ARCHIVER32",
 "description":"Archive support module",
 "version":"1261",
 "date":"2017-02-22"
},{
 "id":"CLEANER32",
 "description":"Cleaner module",
 "version":"1132",
 "date":"2017-03-15"
},{
 "id":"ANTISTEALTH32",
 "description":"Anti-Stealth support module",
 "version":"1106",
 "date":"2016-10-17"
},{
 "id":"SYSTEMSTATUS32",
 "description":"ESET SysInspector module",
 "version":"1266",
 "date":"2016-12-22"
},{
 "id":"TRANSLATOR32",
 "description":"Translation support module",
 "version":"1588B",
 "date":"2017-03-01"
},{
 "id":"HIPS32",
```

```
    "description":"HIPS support module",
    "version":"1267",
    "date":"2017-02-16"
   },{
    "id":"PROTOSCAN32",
    "description":"Internet protection module",
    "version":"1300",
    "date":"2017-03-03"
   },{
    "id":"DBLITE32",
    "description":"Database module",
    "version":"1088",
    "date":"2017-01-05"
   },{
    "id":"CONFENG32",
    "description":"Configuration module (33)",
    "version":"1496B",
    "date":"2017-03-17"
   },{
    "id":"IRIS32",
    "description":"LiveGrid communication module",
    "version":"1022",
    "date":"2016-04-01"
   },{
    "id":"SAURON32",
    "description":"Rootkit detection and cleaning module",
    "version":"1006",
    "date":"2016-07-15"
   },{
    "id":"SSL32",
    "description":"Cryptographic protocol support module",
    "version":"1009",
    "date":"2016-12-02"
   }
  },
  "error":null
 }
}
```

3.10.7.2.3 obtener información-licencia

Get information about the license of the product

Command line

```
ermm.exe get license-info
```

Parameters

None

Example

call


```
{
 "command":"get_license_info",
 "id":1,
 "version":"1"
}
```


result


```
{
 "id":1,
 "result":{
  "type":"NFR",
  "expiration_date":"2020-12-31",
  "expiration_state":"ok",
  "public_id":"3XX-7ED-7XF",
  "seat_id":"6f726793-ae95-4e04-8ac3-e6a20bc620bf",
  "seat_name":"M"
 },
 "error":null
}
```


3.10.7.2.4 obtener registros

Get logs of the product

Command line

```
ermm.exe get logs --name warnlog --start-date "2017-04-04 06-00-00" --end-date "2017-04-04 12-00-00"
```

Parameters

Name	Value

name	{ all, virlog, warnlog, scanlog, blocked, hipslog, urllog, devctrllog } : log to retrieve
start-date	start date from which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])
end-date	end time until which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])

Example

call


```
{
 "command":"get_logs",
 "id":1,
 "version":"1",
 "params":{
  "name":"warnlog",
  "start_date":"2017-04-04 06-00-00",
  "end_date":"2017-04-04 12-00-00"
 }
}
```


result


```
{
 "id":1,
 "result":{
  "warnlog":{
   "display_name":"Events",
   "logs":[{
    "Time":"2017-04-04 06-05-59",
    "Severity":"Info",
    "PluginId":"ESET Kernel",
    "Code":"Malware database was successfully updated to version 15198 (20170404).",
    "UserData":""
   },{
    "Time":"2017-04-04 11-12-59",
    "Severity":"Info",
    "PluginId":"ESET Kernel",
    "Code":"Malware database was successfully updated to version 15199 (20170404).",
    "UserData":""
   }]
  }
 },
```

```
 "error":null
}
```

3.10.7.2.5 obtener estado-activación

Get information about the last activation. Result of status can be { success, error }

Command line

```
ermm.exe get activation-status
```

Parameters

None

Example

call

```
{
 "command":"get_activation_status",
 "id":1,
 "version":"1"
}
```

result

```
{
 "id":1,
 "result":{
  "status":"success"
 },
 "error":null
}
```

3.10.7.2.6 obtener información-análisis

Get information about running scan.

Command line

```
ermm.exe get scan-info
```

Parameters

None

Example

call


```
{
 "command":"get_scan_info",
 "id":1,
 "version":"1"
}
```


result


```
{
 "id":1,
 "result":{
  "scan-info":{
 "scans":[{
  "scan_id":65536,
  "timestamp":272,
  "state":"finished",
  "pause_scheduled_allowed":false,
  "pause_time_remain":0,
  "start_time":"2017-06-20T12:20:33Z",
  "elapsed_tickcount":328,
  "exit_code":0,
  "progress_filename":"Operating memory",
  "progress_arch_filename":"",
  "total_object_count":268,
  "infected_object_count":0,
  "cleaned_object_count":0,
  "log_timestamp":268,
  "log_count":0,
  "log_path":"C:\\ProgramData\\ESET\\ESET Security\\Logs\\eScan\\ndl31494.dat",
  "username":"test-PC\\test",
  "process_id":3616,
  "thread_id":3992,
  "task_type":2
 }],
 "pause_scheduled_active":false
}
 },
```

```
 "error":null
}
```

3.10.7.2.7 obtener configuración

Get the product configuration. Result of status may be { success, error }

Command line

```
ermm.exe get configuration --file C:\tmp\conf.xml --format xml
```

Parameters

Name	Value
file	the path where the configuration file will be saved
format	format of configuration: json, xml. Default format is xml

Example

call

```
{
 "command":"get_configuration",
 "id":1,
 "version":"1",
 "params":{
  "format":"xml",
  "file":"C:\\tmp\\conf.xml"
 }
}
```

result

```
{
 "id":1,
 "result":{
  "configuration":"PD94bWwgdmVyc2lvbj0iMS4w=="
 },
 "error":null
}
```

3.10.7.2.8 obtener estado-actualización

Get information about the update. Result of status may be { success, error }

Command line

```
ermm.exe get update-status
```

Parameters

None

Example

call


```
{
 "command":"get_update_status",
 "id":1,
 "version":"1"
}
```


result


```
{
 "id":1,
 "result":{
  "last_update_time":"2017-06-20 13-21-37",
  "last_update_result":"error",
  "last_successful_update_time":"2017-06-20 11-21-45"
 },
 "error":null
}
```

3.10.7.2.9 iniciar análisis

Start scan with the product

Command line

```
ermm.exe start scan --profile "profile name" --target "path"
```

Parameters

Name	Value
profile	Profile name of On-demand computer scan defined in product
target	Path to be scanned

Example

call

```
{
 "command":"start_scan",
 "id":1,
 "version":"1",
 "params":{
  "profile":"Smart scan",
  "target":"c:\\"
 }
}
```

result

```
{
 "id":1,
 "result":{
  "task_id":458752
 },
 "error":null
}
```

3.10.7.2.10 iniciar activación

Start activation of product

Command line

```
ermm.exe start activation --key "activation key" | --offline "path to offline file" | --token "activation to
```

Parameters

Name	Value
key	Activation key
offline	Path to offline file
token	Activation token

Example

call

```
{
 "command":"start_activation",
 "id":1,
 "version":"1",
 "params":{
  "key":"XXXX-XXXX-XXXX-XXXX-XXXX"
 }
}
```

result

```
{
 "id":1,
 "result":{
 },
 "error":null
}
```

3.10.7.2.11 iniciar desactivación

Start deactivation of the product

Command line

```
ermm.exe start deactivation
```

Parameters

None

Example

call

```
{
 "command":"start_deactivation",
 "id":1,
 "version":"1"
}
```

result

```
{
 "id":1,
 "result":{
 },
 "error":null
}
```

3.10.7.2.12 iniciar actualización

Start update of the product. Only one update may be running in the product so in case the update is already running, "Task already running" error code is returned

Command line

```
ermm.exe start update
```

Parameters

None

Example

call

```
{
 "command":"start_update",
 "id":1,
```

```
 "version":"1"
}
```

result

```
{
 "id":1,
 "result":{
 },
  "error":{
   "id":4,
   "text":"Task already running."
  }
}
```

3.10.7.2.13 definir configuración

Set configuration to the product. Result of status may be { success, error }

Command line

```
ermm.exe set configuration --file C:\tmp\conf.xml --format xml --password pass
```

Parameters

Name	Value
file	the path where the configuration file will be saved
password	password for configuration
value	configuration data from the argument (encoded in base64)

Example

call

```
{
 "command":"set_configuration",
 "id":1,
 "version":"1",
 "params":{
  "format":"xml",
  "file":"C:\\tmp\\conf.xml",
  "password": "pass"
 }
}
```

result

{
"id":1,
"result":{
},
"error":null
}

3.11 Glosario

3.11.1 Tipos de amenazas

Una amenaza es un software malicioso que intenta entrar en el ordenador de un usuario y dañarlo.

3.11.1.1 Virus

Un virus informático es un código malicioso que puede agregarse al principio o al final de archivos existentes en su ordenador. Su nombre se debe a los virus biológicos, ya que usan técnicas similares para pasar de un ordenador a otro. En cuanto al término "virus", suele utilizarse de forma errónea para referirse a cualquier tipo de amenaza. Este término está desapareciendo gradualmente y se está sustituyendo por el nuevo término "malware" (software malicioso), que es más preciso.

Los virus informáticos atacan principalmente a los archivos y documentos ejecutables. En resumen, así es cómo funciona un virus informático: tras la ejecución de un archivo infectado, el código malicioso es invocado y ejecutado antes de la ejecución de la aplicación original. Un virus puede infectar cualquier archivo para el que el usuario actual tenga permisos de escritura.

Los virus informáticos pueden tener diversos fines y niveles de gravedad. Algunos son muy peligrosos, debido a su capacidad para eliminar archivos del disco duro de forma deliberada. Sin embargo, otros virus no causan daños reales, solo sirven para molestar al usuario y demostrar las capacidades técnicas de sus autores.

Si su ordenador está infectado con un virus y la desinfección no es posible, envíelo al laboratorio de ESET para su análisis. En ciertos casos, los archivos infectados se pueden modificar hasta tal punto que la desinfección no sea posible y sea necesario sustituir los archivos por una copia no infectada.

3.11.1.2 Gusanos

Un gusano informático es un programa que contiene código malicioso que ataca a los ordenadores host y se extiende a través de una red. La principal diferencia entre un virus y un gusano es que estos últimos tienen la capacidad de propagarse por sí mismos: no dependen de archivos host (ni de sectores de inicio). Los gusanos se extienden a las direcciones de correo electrónico de la lista de contactos o aprovechan las vulnerabilidades de seguridad de las aplicaciones de red.

Los gusanos son mucho más viables que los virus informáticos; dada la gran disponibilidad de Internet, se pueden extender por todo el mundo en cuestión de horas, o incluso minutos, desde su lanzamiento. Esta capacidad para reproducirse de forma independiente y rápida los hace más peligrosos que otros tipos de código malicioso.

Un gusano activado en un sistema puede causar una serie de problemas: puede eliminar archivos, degradar el rendimiento del sistema o incluso desactivar algunos programas. Además, su naturaleza le permite servir de "medio de transporte" para otros tipos de amenazas.

Si el ordenador está infectado con un gusano, es recomendable eliminar los archivos infectados, pues podrían contener código malicioso.

3.11.1.3 Troyanos

Históricamente, los troyanos informáticos (caballos de Troya) se han definido como una clase de amenaza que intenta presentarse como un programa útil, engañando así a los usuarios para que permitan su ejecución.

Dado que los troyanos forman una categoría muy amplia, con frecuencia se divide en varias subcategorías:

- **Descargador**: programas maliciosos con capacidad para descargar otras amenazas de Internet.
- **Lanzador**: programas maliciosos con la capacidad de dejar otros tipos de software malicioso en ordenadores atacados.
- **Puerta trasera**: programas maliciosos que se comunican con los atacantes remotos, permitiéndoles acceder al ordenador y controlarlo.
- **Registrador de pulsaciones** : programa que registra todas las teclas pulsadas por el usuario y envía la información a atacantes remotos.
- **Marcador** : programas maliciosos diseñados para conectarse a través de números de teléfono de tarifas con recargo en lugar a través del proveedor de servicios de Internet. Es casi imposible que un usuario note que se ha creado una conexión. Los marcadores solo pueden causar daño a los usuarios con módems de marcación, que ya casi no se utilizan.

Si se determina que un archivo es un caballo de Troya en su ordenador, es recomendable que lo elimine, ya que lo más probable es que contenga código malicioso.

3.11.1.4 Rootkits

Los rootkits son programas malintencionados que conceden a los atacantes de Internet acceso ilimitado a un sistema, al tiempo que ocultan su presencia. Una vez que han accedido al sistema (normalmente explotando alguna vulnerabilidad del mismo), usan funciones del sistema operativo para evitar su detección por parte del antivirus: ocultan procesos, archivos y datos de registro de Windows. Por este motivo, es casi imposible detectarlos con las técnicas de detección normales.

Hay dos niveles de detección disponibles para evitar los rootkits:

1. Cuando intentan acceder a un sistema: Aún no están presentes y, por tanto, están inactivos. La mayoría de los sistemas antivirus pueden eliminar rootkits en este nivel (suponiendo que realmente detectan dichos archivos como infectados).

2. Cuando se ocultan de los análisis habituales. Los usuarios de ESET Endpoint Antivirus tienen la ventaja de la tecnología Anti-Stealth que también detecta y elimina rootkits activos.

3.11.1.5 Adware

Adware es la abreviatura del término inglés utilizado para el software relacionado con publicidad. Los programas que muestran material publicitario se incluyen en esta categoría. Por lo general, las aplicaciones de adware abren automáticamente una ventana emergente nueva con anuncios en el navegador de Internet o cambian la página de inicio del mismo. La aplicación de adware suele instalarse con programas gratuitos, lo que permite a los creadores de esos programas gratuitos cubrir los costes de desarrollo de sus aplicaciones (que suelen ser útiles).

La aplicación de adware no es peligrosa en sí, pero molesta a los usuarios con publicidad. El peligro reside en el hecho de que la aplicación de adware también puede realizar funciones de seguimiento (al igual que las aplicaciones de spyware).

Si decide utilizar un producto gratuito, preste especial atención al programa de instalación. La mayoría de los instaladores le informarán sobre la instalación de un programa de adware adicional. Normalmente, podrá cancelarlo e instalar el programa sin esta aplicación de adware.

Sin embargo, algunos programas no se instalarán sin la aplicación de adware, o su funcionalidad será limitada. Esto significa que la aplicación de adware puede acceder al sistema de manera "legal" a menudo, pues los usuarios así lo han aceptado. En estos casos, es mejor prevenir que curar. Si se detecta un archivo de adware en el ordenador, es recomendable eliminarlo, pues existen muchas probabilidades de que contenga código malicioso.

3.11.1.6 Spyware

Esta categoría abarca todas las aplicaciones que envían información privada sin el consentimiento o conocimiento del usuario. El spyware usa funciones de seguimiento para enviar diversos datos estadísticos, como una lista de sitios web visitados, direcciones de correo electrónico de la lista de contactos del usuario o una lista de palabras escritas.

Los autores de spyware afirman que el objetivo de estas técnicas es averiguar más sobre las necesidades y los intereses de los usuarios, así como permitir una publicidad mejor gestionada. El problema es que no existe una distinción clara entre las aplicaciones útiles y las malintencionadas, de modo que nadie puede estar seguro de que no se hará un mal uso de la información recuperada. Los datos obtenidos por aplicaciones spyware pueden contener códigos de seguridad, códigos PIN, números de cuentas bancarias, etc. Con frecuencia, el spyware se envía junto con versiones gratuitas de programas para generar ingresos u ofrecer un incentivo para comprar el software. A menudo, se informa a los usuarios sobre la presencia de spyware durante la instalación de un programa para ofrecerles un incentivo para la adquisición de una versión de pago.

Algunos ejemplos de productos gratuitos conocidos que se envían junto con spyware son las aplicaciones cliente de redes P2P (peer to peer). Spyfalcon o Spy Sheriff (y muchos más) pertenecen a una subcategoría específica de spyware: parecen programas antispyware, pero en realidad son aplicaciones de spyware.

Si se detecta un archivo de spyware en su ordenador, es aconsejable que lo elimine, ya que es muy posible que contenga código malicioso.

3.11.1.7 Empaquetadores

Un empaquetador es un archivo ejecutable autoextraíble en tiempo de ejecución que implementa varios tipos de código malicioso en un solo paquete.

Los más comunes son UPX, PE_Compact, PKLite y ASPack. El mismo código malicioso se puede detectar de forma diferente cuando se comprime con un empaquetador diferente. Los empaquetadores también tienen la capacidad de hacer que sus "firmas" muten con el tiempo, haciendo que el código malicioso sea más difícil de detectar y eliminar.

3.11.1.8 Aplicaciones potencialmente peligrosas

Existen muchos programas legítimos que sirven para simplificar la administración de ordenadores en red. Sin embargo, si caen en las manos equivocadas, podrían utilizarse con fines maliciosos. ESET Endpoint Antivirus proporciona una opción para detectar estas amenazas.

Aplicaciones potencialmente peligrosas es la clasificación utilizada para el software comercial legítimo. Esta clasificación incluye programas como herramientas de acceso remoto, aplicaciones para detectar contraseñas y registradores de pulsaciones (programas que graban todas las teclas pulsadas por un usuario).

Si detecta la presencia de una aplicación potencialmente peligrosa que esté en ejecución en su ordenador (y no la ha instalado usted), consulte con el administrador de la red o elimine la aplicación.

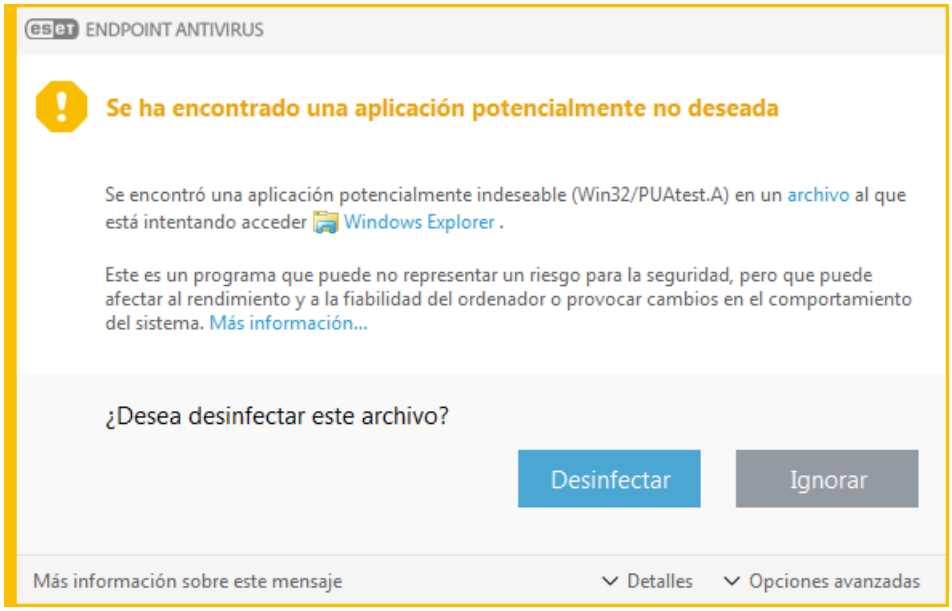
3.11.1.9 Aplicaciones potencialmente indeseables

Una aplicación potencialmente indeseable es un programa que contiene software publicitario, instala barras de herramientas o tiene otros objetivos poco claros. Existen determinados casos en los que un usuario podría creer que las ventajas de una aplicación potencialmente indeseada compensan los riesgos asociados. Este es el motivo que hace que ESET asigne a dichas aplicaciones una categoría de riesgo más baja, en comparación con otros tipos de software malicioso, como los troyanos o los gusanos.

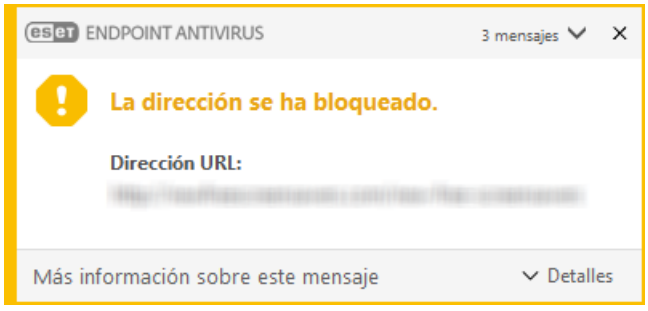
Advertencia: Amenaza potencial encontrada

Cuando se detecte una aplicación potencialmente indeseable podrá elegir qué medida desea tomar:

1. **Desinfectar/Desconectar**: esta opción finaliza la acción e impide que la amenaza potencial acceda a su sistema.
2. **Sin acciones**: esta opción permite que una amenaza potencial entre en el sistema.
3. Si desea permitir que la aplicación se ejecute en su ordenador en el futuro sin que se interrumpa, haga clic en **Más información/Mostrar opciones avanzadas** y, a continuación, active la casilla de verificación situada junto a **Excluir de la detección**.

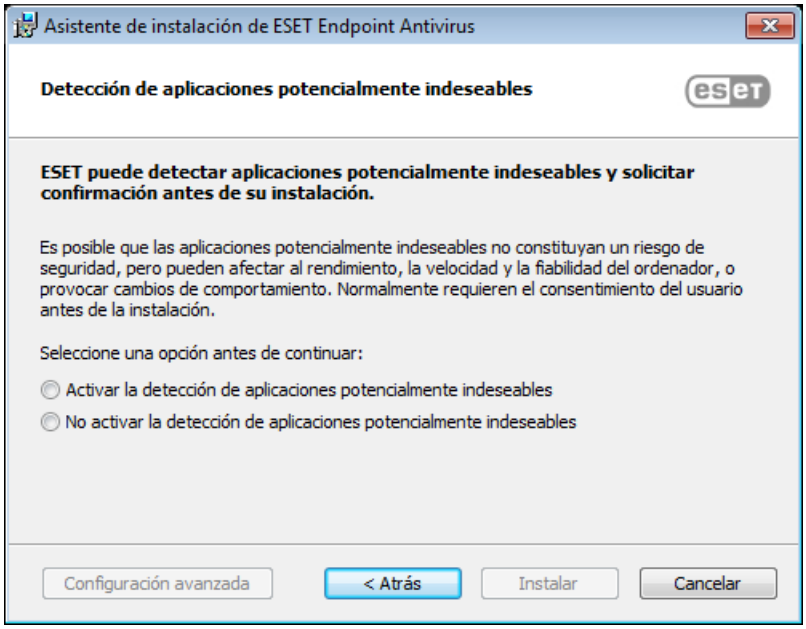


Si se detecta una aplicación potencialmente indeseable que no se puede desinfectar, aparecerá la ventana de notificación **La dirección se ha bloqueado** en la esquina inferior derecha de la pantalla. Si desea obtener más información sobre este suceso, diríjase a **Herramientas** > **Archivos de registro** > **Sitios web filtrados** desde el menú principal.



Aplicaciones potencialmente indeseables: Configuración

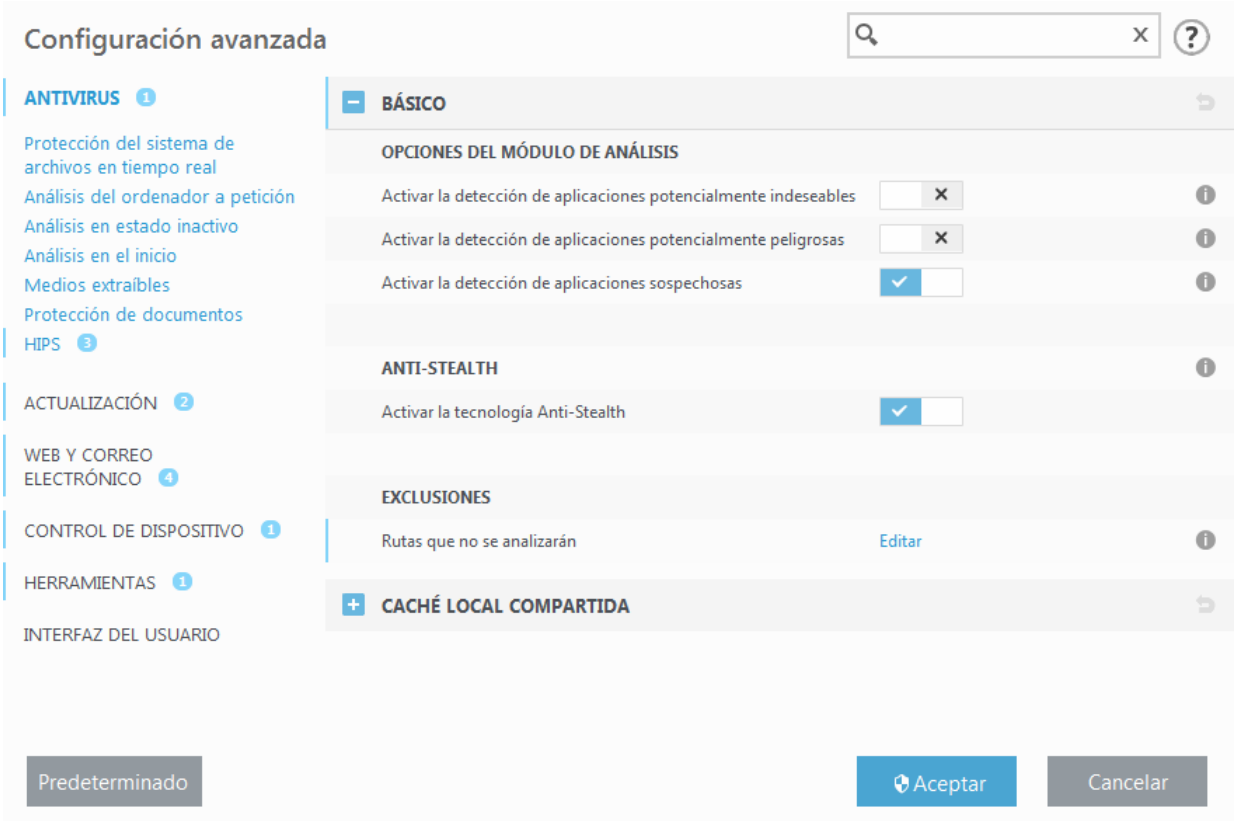
Durante la instalación del producto de ESET puede decidir si desea activar la detección de aplicaciones potencialmente indeseables, como se muestra a continuación:



ADVERTENCIA
Las aplicaciones potencialmente indeseables podrían instalar software publicitario, barras de herramientas o contener otras características de programa no deseadas e inseguras.

Estos ajustes pueden modificarse en cualquier momento en la configuración del programa. Si desea activar o desactivar la detección de aplicaciones potencialmente indeseadas, inseguras o sospechosas, siga estas instrucciones:

1. Abra su producto de ESET. ¿Cómo abro mi producto de ESET?
2. Pulse la tecla **F5** para acceder a **Configuración avanzada**.
3. Haga clic en **Antivirus** y active o desactive las opciones **Activar la detección de aplicaciones potencialmente indeseables**, **Activar la detección de aplicaciones potencialmente peligrosas** y **Activar la detección de aplicaciones sospechosas** según sus propias preferencias. Confirme haciendo clic en **Aceptar**.



Aplicaciones potencialmente indeseables: Software encubierto

El software encubierto es un tipo de modificación de aplicación especial que utilizan algunos sitios web de alojamiento de archivos. Se trata de una herramienta de terceros que instala el programa que quería descargar pero que incorpora software adicional, como barras de herramientas o software publicitario. El software adicional podría, además, cambiar la página de inicio de su navegador web y la configuración de búsqueda. Igualmente, los sitios web de alojamiento de archivos no suelen informar al proveedor del software ni al usuario que realiza la descarga de que se han efectuado dichas modificaciones, ni tampoco facilitan la tarea de rechazar la modificación. Por estos motivos, ESET clasifica el software encubierto como un tipo de aplicación potencialmente indeseable, con el fin de permitir al usuario aceptar o rechazar la descarga.

Consulte el siguiente artículo de la base de conocimiento de ESET para ver una versión actualizada de esta página de ayuda.

Si desea obtener más información, haga clic aquí.

3.11.2 Correo electrónico

El correo electrónico es una forma de comunicación moderna que ofrece muchas ventajas: es flexible, rápido y directo; y tuvo un papel fundamental en la expansión de Internet a principios de los años 90.

Lamentablemente, a causa de su alto nivel de anonimato, el correo electrónico e Internet dan cabida a actividades ilegales como la distribución de correo no deseado. El correo no deseado incluye anuncios no solicitados, información falsa y la difusión de software malicioso (código malicioso). Sus inconvenientes y peligros para el usuario son mayores porque el envío de correo no deseado tiene un coste mínimo, y los autores de este tipo de correo disponen de muchas herramientas para obtener nuevas direcciones de correo electrónico. Además, la cantidad y la variedad de correo no deseado dificulta en gran medida su regulación. Cuanto más utilice su dirección de correo electrónico, mayores serán las posibilidades de que acabe en la base de datos de un motor de correo no deseado. A continuación, le ofrecemos algunos consejos para su prevención:

- Si es posible, no publique su dirección de correo electrónico en Internet.
- Proporcione su dirección de correo electrónico únicamente a personas de confianza.
- Si es posible, no utilice alias muy comunes; cuanto más complicados sean, menor será la posibilidad de que puedan obtenerlos.
- No conteste a mensajes de correo no deseado que hayan llegado a su buzón de correo.
- Tenga cuidado cuando rellene formularios en Internet, preste especial atención a casillas como "Sí, deseo recibir información".
- Utilice direcciones de correo electrónico "especializadas"; por ejemplo, una para el trabajo, otra para comunicarse con sus amigos, etc.
- Cambie su dirección de correo electrónico periódicamente.
- Utilice una solución antispam.

3.11.2.1 Publicidad

La publicidad en Internet es una de las formas de publicidad que presentan un crecimiento más rápido. Sus principales ventajas de marketing son los costes mínimos, un contacto muy directo y, lo más importante, el hecho de que los mensajes se entregan de forma casi inmediata. Muchas empresas utilizan herramientas de marketing por correo electrónico para comunicarse eficazmente con sus clientes actuales y potenciales.

Este tipo de publicidad es legítimo, ya que es posible que el usuario esté interesado en recibir información comercial sobre algunos productos. No obstante, son muchas las empresas que envían mensajes publicitarios no deseados en serie. En estos casos, la publicidad por correo electrónico cruza la línea y se convierte en correo no deseado.

Actualmente, la enorme cantidad de correo no solicitado constituye un problema y no tiene visos de disminuir. Los autores de correos electrónicos no solicitados intentan disfrazar el correo no deseado como mensajes legítimos.

3.11.2.2 Información falsa

La información falsa se extiende a través de Internet. Normalmente, la información falsa se envía mediante herramientas de comunicación o correo electrónico como ICQ y Skype. El mensaje en sí suele ser una broma o una leyenda urbana.

La información falsa sobre virus de ordenador pretende generar miedo, incertidumbre y duda en los destinatarios, haciéndoles creer que existe un "virus indetectable" que elimina archivos y recupera contraseñas, o que realiza ciertas acciones que pueden provocar daños en el sistema.

Algunos elementos de información falsa solicitan a los destinatarios que reenvíen los mensajes a sus contactos, divulgando así dicha información. La información falsa también se transmite a través de teléfonos móviles, peticiones de ayuda, personas que se ofrecen a enviarle dinero desde países extranjeros, etc. Por lo general, es imposible averiguar la intención del creador.

Si recibe un mensaje donde se le solicita que lo reenvíe a todas las personas que conozca, es muy probable que se trate de información falsa. En Internet encontrará muchos sitios web que pueden verificar la legitimidad de un mensaje de correo electrónico. Antes de reenviarlo, realice una búsqueda en Internet sobre cualquier mensaje que sospeche que contiene información falsa.

3.11.2.3 Phishing

El término phishing define una actividad delictiva que usa técnicas de ingeniería social (manipulación de los usuarios para obtener información confidencial). Su objetivo es acceder a datos confidenciales como, por ejemplo, números de cuentas bancarias, códigos PIN, etc.

Normalmente, el acceso se consigue enviando correos electrónicos con remitentes disfrazados de personas o empresas serias (instituciones financieras, compañías de seguros, etc.). La apariencia del correo electrónico puede ser muy genuina, y contener gráficos y texto originales de la fuente por la que desean hacerse pasar. En el mensaje se le pide que escriba, con varios pretextos (verificación de datos, operaciones financieras), algunos de sus datos personales: números de cuentas bancarias o nombres de usuario y contraseñas. Dichos datos, si se envían, pueden ser fácilmente sustraídos o utilizados de forma fraudulenta.

Los bancos, las compañías de seguros y otras empresas legítimas nunca le pedirían sus nombres de usuario y contraseñas en un correo electrónico no solicitado.

3.11.2.4 Reconocimiento de correo no deseado no solicitado

Por lo general, existen pocos indicadores que puedan ayudarle a identificar el correo no deseado (spam) en su buzón de correo. Si un mensaje cumple, como mínimo, una de las siguientes condiciones, es muy probable que se trate de un mensaje de correo no deseado.

- La dirección del remitente no pertenece a ninguna persona de su lista de contactos.
- El mensaje le ofrece una gran cantidad de dinero, pero tiene que proporcionar una pequeña cantidad previamente.
- El mensaje le solicita que introduzca, con varios pretextos (verificación de datos, operaciones financieras), algunos de sus datos personales (números de cuentas bancarias, nombres de usuario y contraseñas, etc.).
- Está escrito en otro idioma.
- Le solicita que adquiera un producto en el que no está interesado. Si decide comprarlo de todos modos, compruebe que el remitente del mensajes es un proveedor fiable (consulte el fabricante del producto original).
- Algunas palabras están mal escritas para intentar engañar a su filtro de correo no deseado. Por ejemplo, "vaigra" en lugar de "viagra", entre otros.

3.11.3 Tecnología de ESET

3.11.3.1 Bloqueador de exploits

El Bloqueador de exploits controla las aplicaciones que suelen aprovechar los hackers (navegadores, lectores de documentos, clientes de correo electrónico, Flash, Java, etc.) y, en lugar de centrarse en identificadores de CVE concretos, lo hace en las técnicas de aprovechamiento de vulnerabilidades. Cuando está activado, se analiza el comportamiento del proceso y, si se considera sospechoso, la amenaza puede bloquearse inmediatamente en el ordenador.

Mientras que el motor de análisis de ESET se ocupa de exploits que aparecen en archivos de documento con formato incorrecto y Protección contra los ataques de red se centra en el nivel de la comunicación, la tecnología del Bloqueador de exploits bloquea el propio proceso de aprovechamiento de vulnerabilidades y registra los datos de la amenaza, que después se envían al sistema de nube de ESET LiveGrid®. El laboratorio de amenazas de ESET procesa estos datos y los utiliza para mejorar la protección que ofrece a los usuarios frente a amenazas desconocidas y ataques 0-day (código malicioso reciente para que el que no hay ninguna solución preconfigurada).

3.11.3.2 Análisis de memoria avanzado

El Análisis avanzado de memoria trabaja conjuntamente con el Bloqueador de exploits para mejorar la protección frente a código malicioso, que utiliza los métodos de ofuscación y cifrado para evitar su detección mediante productos de protección frente a este tipo de código. En aquellos casos en los que la emulación o la heurística normales no detectan una amenaza, el Análisis de memoria avanzado consigue identificar comportamientos sospechosos y analiza las amenazas que se presentan en la memoria del sistema. Esta solución es eficaz incluso para código malicioso muy ofuscado. A diferencia del Bloqueador de exploits, se trata de un método posterior a la ejecución, lo cual significa que existe la posibilidad de que haya habido actividad maliciosa antes de la detección de una amenaza. No obstante, ofrece una capa de seguridad adicional cuando las otras técnicas de detección fallan.

3.11.3.3 ESET LiveGrid®

ESET LiveGrid®, que se basa en el sistema avanzado de alerta temprana ThreatSense.Net®, utiliza los datos enviados por usuarios de ESET de todo el mundo y los envía al laboratorio de virus de ESET. ESET LiveGrid® proporciona metadatos y muestras sospechosas en estado salvaje, lo cual nos permite reaccionar de forma inmediata a las necesidades de nuestros clientes y hace posible la respuesta de ESET a las amenazas más recientes. Los investigadores de código malicioso de ESET utilizan la información para crear una instantánea precisa de la naturaleza y el alcance de las amenazas globales, de modo que podemos centrarnos en los objetos adecuados. Los datos de ESET LiveGrid® son fundamentales a la hora de establecer las prioridades en nuestro procesamiento automatizado.

Además implementa un sistema de reputación que contribuye a la mayor eficacia de nuestras soluciones de protección contra código malicioso. Cuando se inspecciona un archivo ejecutable en el sistema de algún usuario, primero se contrasta su etiqueta hash con una base de datos de elementos incluidos en las listas blanca y negra. Si el elemento se encuentra en la lista blanca, el archivo inspeccionado se marca para su exclusión de próximos análisis. Si está en la lista negra, se emprenden las acciones necesarias de acuerdo con la naturaleza de la amenaza. Si no se encuentra ninguna coincidencia, el archivo se analiza a fondo. Los archivos se clasifican como amenazas o no en función de los resultados de este análisis. Este enfoque tiene un gran impacto positivo en el rendimiento del análisis.

Este sistema de reputación permite detectar eficazmente muestras de código malicioso, incluso antes de que sus firmas lleguen a los usuarios mediante actualizaciones del motor de detección (lo cual sucede varias veces al día).

3.11.3.4 Bloqueador de exploits de Java

El Bloqueador de exploits de Java es una extensión de la protección actual del Bloqueador de exploits de ESET. Esta extensión busca comportamientos de tipo exploit en Java. Puede informar de las muestras bloqueadas a los analistas de código malicioso, a fin de que puedan crean firmas para bloquear intentos de exploit de Java en diferentes capas (bloqueo de URL, descarga de archivos, etc.).

3.11.3.5 Protección contra ataques basados en scripts

La Protección contra ataques basados en scripts consiste en protección contra JavaScript en los navegadores web y protección de la herramienta Interfaz de análisis contra el código malicioso (AMSI) de Microsoft contra los scripts de Powershell (wscript.exe y también cscript.exe).

ADVERTENCIA
Para que esta función esté disponible, el HIPS debe estar activado.

La protección contra ataques basados en scripts es compatible con los siguientes navegadores web:

- Mozilla Firefox
- Google Chrome
- Internet Explorer
- Microsoft Edge

NOTA
La versión mínima compatible de los navegadores web puede variar, ya que la firma del archivo de los navegadores cambia con frecuencia. La versión más reciente del navegador web es siempre compatible.

3.11.3.6 Protección contra ransomware

El ransomware es un tipo de código malicioso que impide que los usuarios accedan a su sistema bloqueando la pantalla del sistema o cifrando los archivos. La protección contra ransomware supervisa el comportamiento de las aplicaciones y los procesos que intentan modificar sus datos personales. Si se considera que el comportamiento de una aplicación es malicioso o el análisis basado en la reputación indica que una aplicación es sospechosa, la aplicación se bloqueará o se pedirá al usuario que la bloquee o la autorice.

IMPORTANTE
Para que la protección contra ransomware funcione correctamente, ESET LiveGrid® debe estar activado.

3.11.3.7 Detecciones de ADN

Los tipos de detección van de hashes muy específicos a las Detecciones de ADN de ESET, que son definiciones complejas de comportamiento malintencionado y características de malware. Los atacantes pueden modificar u ocultar fácilmente el código malicioso, pero el comportamiento de los objetos no es tan sencillo de cambiar, y Detecciones de ADN de ESET es una herramienta diseñada para aprovechar este principio.

Realizamos un análisis profundo del código, extraemos los "genes" responsables de su comportamiento y construimos Detecciones de ADN de ESET, herramienta que se usa para evaluar código que puede resultar sospechoso, tanto si se encuentra en el disco como si está en la memoria de proceso. Detecciones de ADN puede identificar muestras de malware conocido específicas, nuevas variantes de una familia de malware conocido o incluso malware no visto anteriormente o desconocido que contiene genes que indican comportamiento malintencionado.

3.11.3.8 Análisis UEFI

El análisis de la interfaz de firmware extensible unificada (UEFI) forma parte del sistema de prevención de intrusiones del host (HIPS) que protege la UEFI en su ordenador. La UEFI es un firmware que se carga en la memoria al principio del proceso de inicio. El código está en un chip de memoria flash soldado a la placa base. Al infectarlo, los atacantes pueden implementar malware que sobreviva a las reinstalaciones y los reinicios del sistema. Además, es fácil que las soluciones contra malware no lo detecten, pues la mayoría no analizan esta capa.

Análisis UEFI se activa automáticamente. También puede iniciar un análisis del ordenador manualmente desde la ventana principal del programa haciendo clic en **Análisis del ordenador** > **Análisis avanzados** > **Análisis personalizado** y seleccionando el destino **Sectores de inicio/UEFI**. Encontrará más información sobre los análisis del ordenador en la sección Análisis del ordenador.

Si su ordenador ya está infectado por malware de la UEFI, lea el siguiente artículo de la base de conocimiento de ESET:
Mi ordenador está infectado por malware de la UEFI, ¿qué debo hacer?