ESET ENDPOINT SECURITY

Guía del usuario

Microsoft® Windows® 8 / 7 / Vista / XP / 2000 / Home Server

Haga clic aquí para descargar la versión más reciente de este documento

ESET **ENDPOINT SECURITY**

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

REV. 20. 2. 2013

Contenido

1. ESET Endpoint Security

ESET Endpoint Security representa un nuevo enfoque de la seguridad informática realmente integrada. La versión más reciente del motor de análisis ThreatSense®, combinada con el cortafuegos personal personalizado y el módulo antispam, 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 Security 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 Security está diseñado principalmente para su uso en estaciones de trabajo en empresas grandes o pequeñas. Se puede utilizar con ESET Remote Administrator, de forma que puede administrar fácilmente cualquier número de estaciones de trabajo cliente, aplicar políticas y reglas, controlar detecciones y configurar de manera remota cualquier ordenador en red.

1.1 Requisitos del sistema

Para un funcionamiento óptimo de ESET Endpoint Security, el sistema debería cumplir con los siguientes requisitos de hardware y software:

Microsoft® Windows® 2000, XP

400 MHz 32 bits (x86)/64 bits (x64)
128 MB RAM de memoria del sistema
320 MB de espacio disponible
Super VGA (800 x 600)

Microsoft® Windows® 8, 7, Vista, Home Server

1 GHz 32 bits (x86)/64 bits (x64)
512 MB RAM de memoria del sistema
320 MB de espacio disponible
Super VGA (800 x 600)

1.2 Prevención

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

Actualización regular

De acuerdo con las estadísticas de ESET Live Grid, 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 esas amenazas diariamente y preparan y publican actualizaciones para mejorar continuamente el nivel de protección para los usuarios del programa antivirus. Una actualización incorrectamente configurada reduce la eficacia del programa. 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 prefieren explotar varias vulnerabilidades del sistema para aumentar la eficacia del despliegue de códigos malintencionados. Por tanto, 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. Entre los ejemplos de estas aplicaciones se incluyen el sistema operativo Windows o el ampliamente usado navegador web Internet Explorer.

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 el daño deliberado de datos importantes. Es importante realizar copias de seguridad regulares 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

Un análisis automático y periódico del ordenador con la configuración adecuada puede eliminar las amenazas que se hayan podido perder porque las actualizaciones de firmas de virus son antiguas.

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 del ordenador. Algunas reglas útiles son:

- 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.

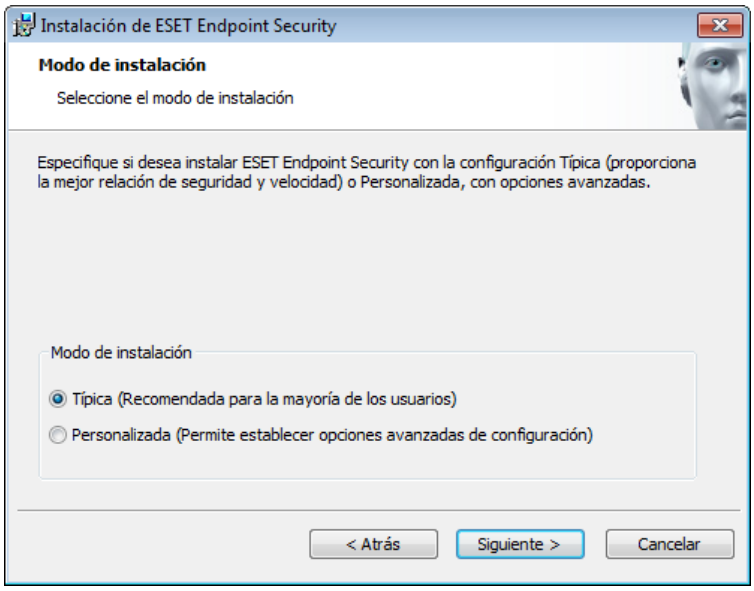
2. Instalación

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

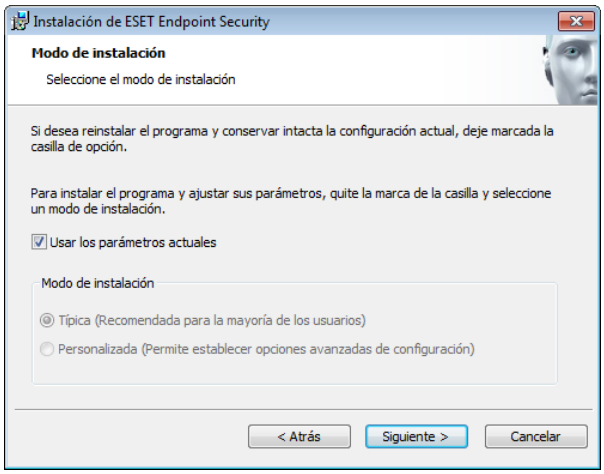
Importante: asegúrese de que no tiene instalados otros programas antivirus en el ordenador. Si instala más de dos soluciones antivirus en un solo ordenador, estas pueden entrar en conflicto. Le recomendamos que desinstale del sistema uno de los programas antivirus. Consulte nuestro artículo de la base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

Primero, el programa comprueba si hay una versión más reciente de ESET Endpoint Security y, Si se encuentra una versión más reciente, se le notificará en el primer paso del proceso de instalación. Si selecciona la opción **Descargar a instalar la nueva versión**, se descargará la nueva versión y el proceso de instalación continuará. 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. Una vez que lo haya aceptado, la instalación puede continuar de dos maneras:

1. Si va a instalar ESET Endpoint Security en un ordenador por primera vez, verá la ventana siguiente cuando acepte el **acuerdo de licencia para el usuario final**. Aquí puede elegir una instalación típica o una instalación personalizada para continuar con el proceso.



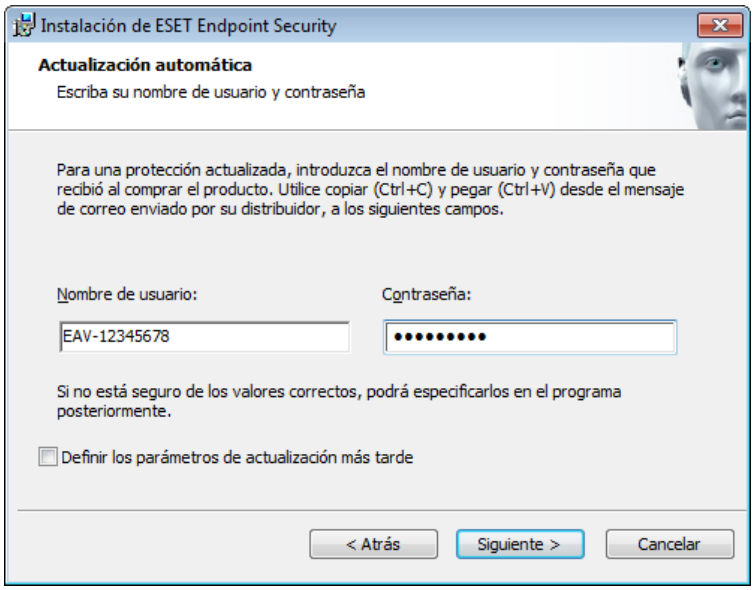
2. Si va a instalar ESET Endpoint Security sobre una versión anterior del software, la ventana que se muestra a continuación le permite elegir utilizar la configuración actual del programa para la nueva instalación o, si anula la selección de la opción **Usar los parámetros actuales**, decidirse por una de los dos modos de instalación mencionados.



2.1 Instalación típica

El modo de instalación típica incluye opciones de configuración adecuadas para la mayoría de los usuarios. Esta configuración proporciona un nivel de seguridad excelente, es fácil de usar y permite un elevado rendimiento del sistema. La instalación típica es la opción predeterminada y se recomienda cuando no es necesaria ninguna configuración específica.

Después de seleccionar el modo de instalación y hacer clic en **Siguiente**, se le solicitarán su nombre de usuario y contraseña para realizar las actualizaciones automáticas del programa. Esta tarea desempeña una función importante, ya que proporciona protección constante al sistema.

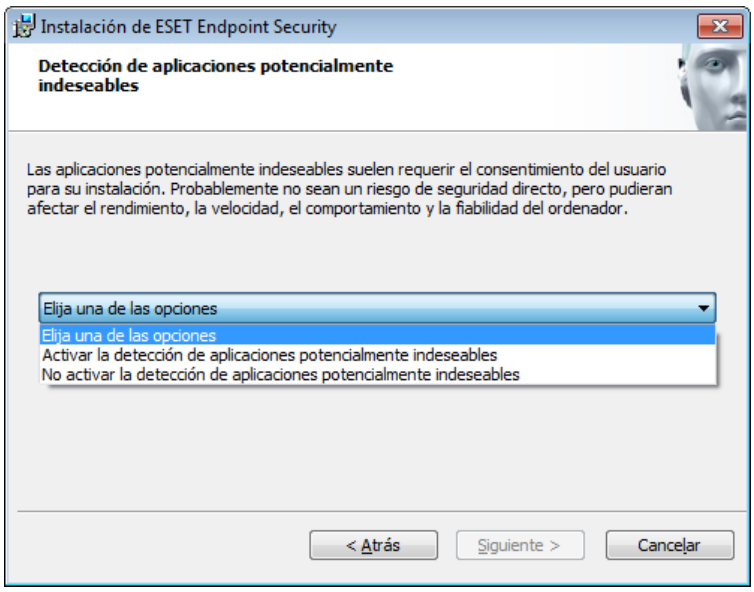


Escriba su **Nombre de usuario** y **Contraseña**, es decir, los datos de autenticación que haya recibido tras la adquisición o el registro del producto en los campos correspondientes. Si no dispone actualmente de su nombre de usuario y contraseña, seleccione la opción **Definir Usuario y Contraseña más tarde**. Puede introducir el nombre de usuario y la contraseña más adelante.

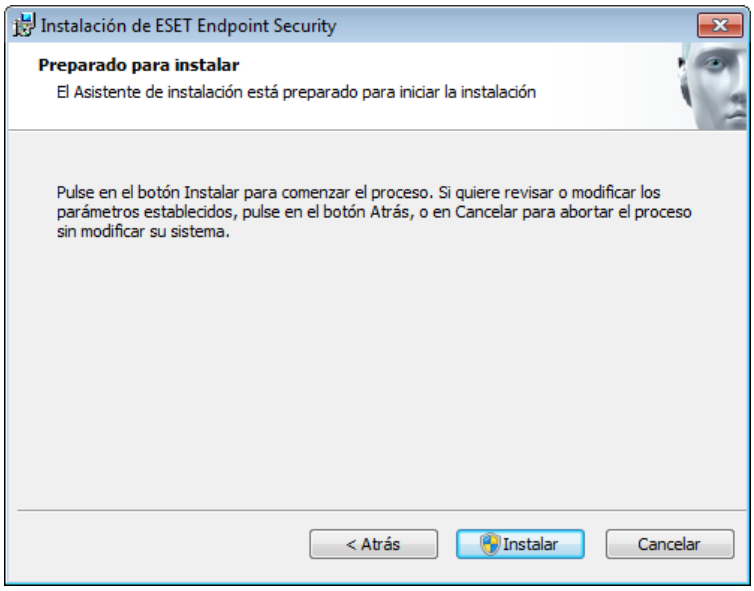
El próximo paso es la configuración de ESET Live Grid. ESET Live Grid ayuda a garantizar que ESET está informado de forma continua e inmediata de las nuevas amenazas con el fin de proteger a nuestros clientes. El sistema permite el envío de nuevas amenazas al laboratorio de virus de ESET, donde se analizan, procesan y agregan a la base de firmas de virus.

La opción **Acepto mi participación en ESET Live Grid** está seleccionada de forma predeterminada, por lo que esta característica se activará.

El paso siguiente del proceso de instalación consiste en configurar la detección de aplicaciones potencialmente indeseables. Las aplicaciones potencialmente indeseables no tienen por qué ser maliciosas, pero pueden influir negativamente en el comportamiento del sistema operativo. Consulte el capítulo Aplicaciones potencialmente indeseables para ver más detalles.



El último paso de la instalación típica es la confirmación de la instalación, para lo que debe hacer clic en el botón **Instalar** .



2.2 Instalación personalizada

El modo de instalación personalizada está diseñado para usuarios que tienen experiencia en el ajuste de programas y que desean modificar opciones avanzadas durante la instalación.

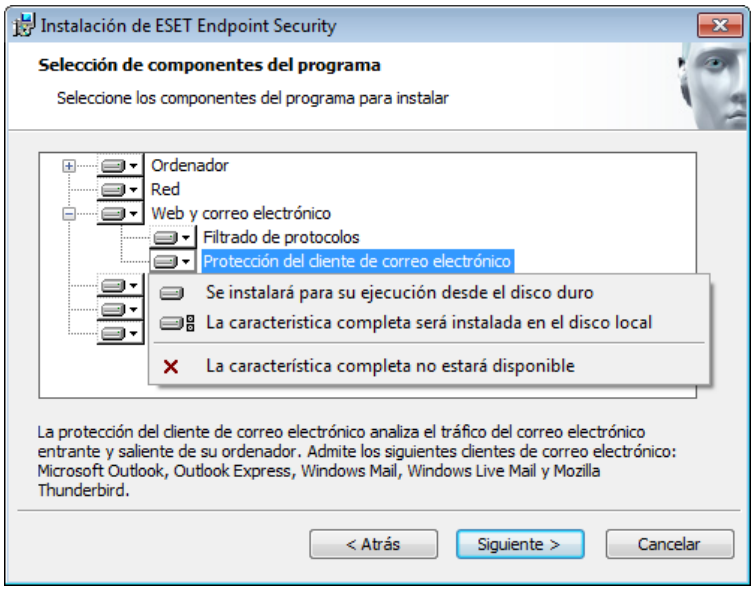
Después de seleccionar el modo de instalación y hacer clic en **Siguiente**, se le solicitará que seleccione una ubicación de destino para la instalación. De forma predeterminada, el programa se instala el el directorio siguiente:

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

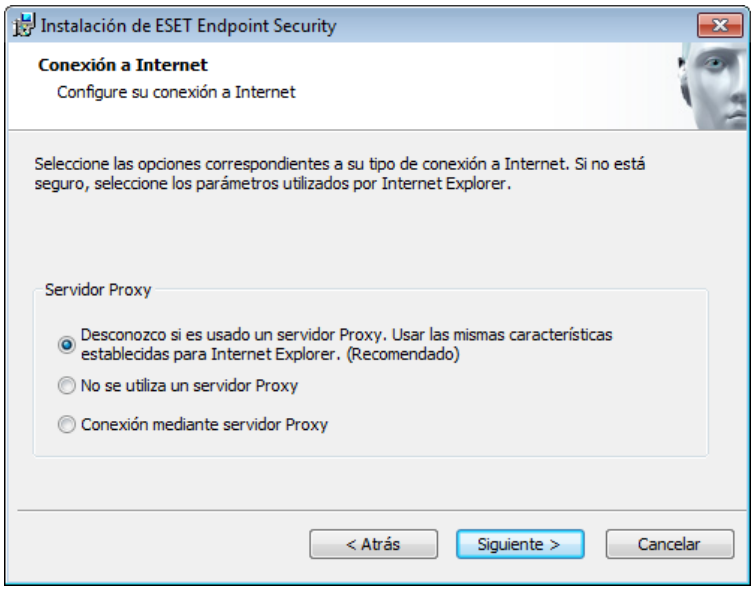
Haga clic en **Examinar** para cambiar esta ubicación (no recomendado).

A continuación, escriba su **nombre de usuario** y **contraseña**. Este paso es igual que en la instalación típica (consulte "Instalación típica").

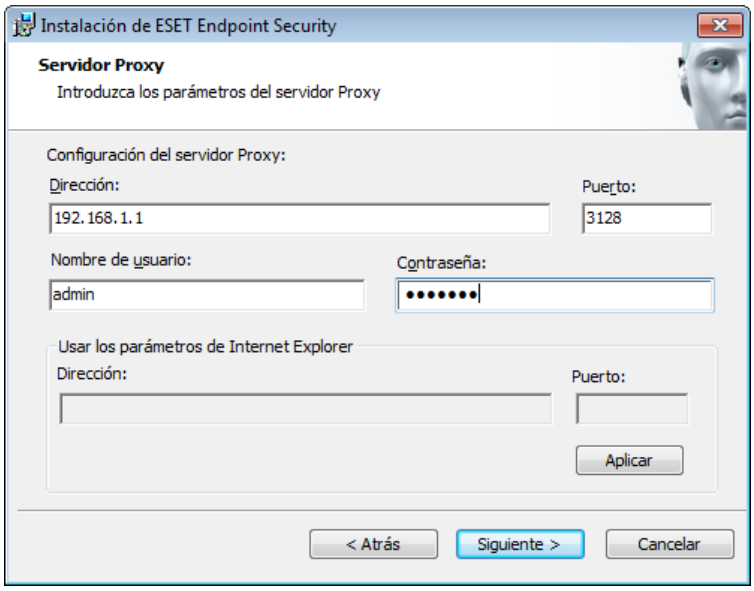
El paso siguiente en el proceso de instalación es seleccionar los componentes del programa que se instalarán. Si expande el árbol de componentes y selecciona una función, verá tres opciones de instalación. La opción **Se instalará para su ejecución desde el disco duro** aparece seleccionada de forma predeterminada. Si selecciona **La característica completa será instalada en el disco local**, todas las características se instalarán bajo el árbol seleccionado. Si no desea utilizar una característica o un componente, seleccione **La característica completa no estará disponible**.



Haga clic en **Siguiente** y continúe con la configuración de la conexión a Internet. Si utiliza un servidor Proxy, este debe estar configurado correctamente para que las actualizaciones de la base de firmas de virus funcionen correctamente. Si no está seguro de si utiliza un servidor Proxy para conectarse a Internet, seleccione **Desconozco si es usado un servidor Proxy. Usar las mismas características establecidas para Internet Explorer (recomendado)** y haga clic en **Siguiente**. Si no utiliza un servidor Proxy, seleccione la opción **No se utiliza un servidor Proxy**.

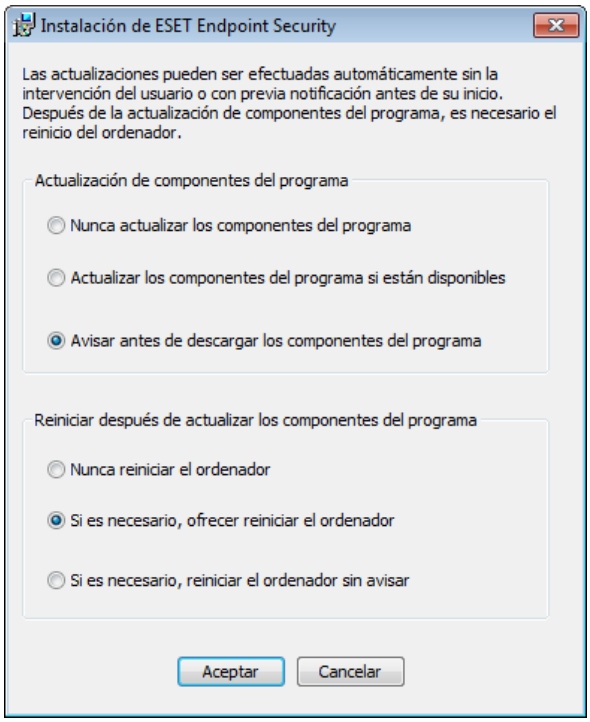


Para configurar el servidor Proxy, seleccione **Conexión mediante servidor Proxy** y haga clic en **Siguiente**. Introduzca la dirección IP o URL de su servidor Proxy en el campo **Dirección**. En el campo **Puerto**, especifique el puerto donde el servidor Proxy acepta conexiones (3128 de forma predeterminada). En el caso de que el servidor Proxy requiera autenticación, debe introducir un **nombre de usuario** y una **contraseña** válidos que permitan acceder al servidor Proxy. La configuración del servidor Proxy también se puede copiar de Internet Explorer, si se desea Para ello, haga clic en **Aplicar** y confirme la selección.



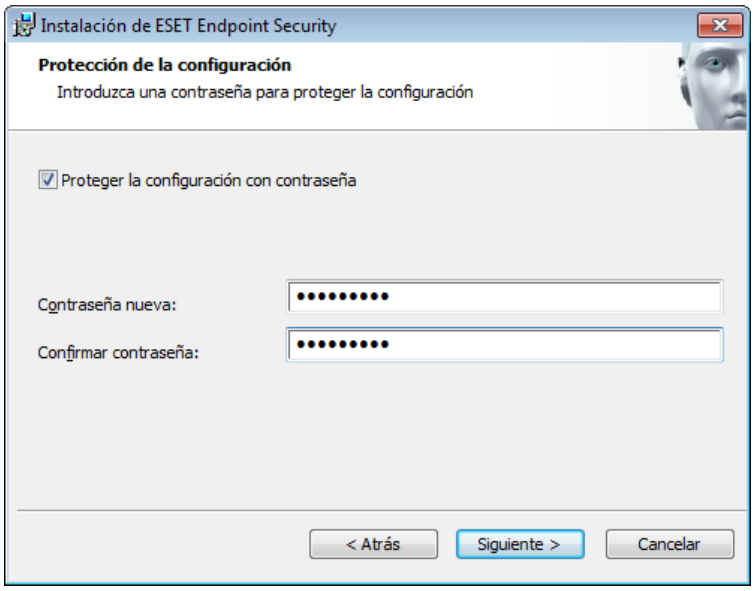
Este paso de instalación le permite diseñar la gestión de las actualizaciones automáticas del programa en el sistema. Haga clic en **Cambiar** para acceder a la configuración avanzada.

Si no desea que se actualicen los componentes del programa, seleccione la opción **Nunca actualizar los componentes del programa**. Seleccione la opción **Avisar 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 la opción **Actualizar siempre los componentes del programa**.



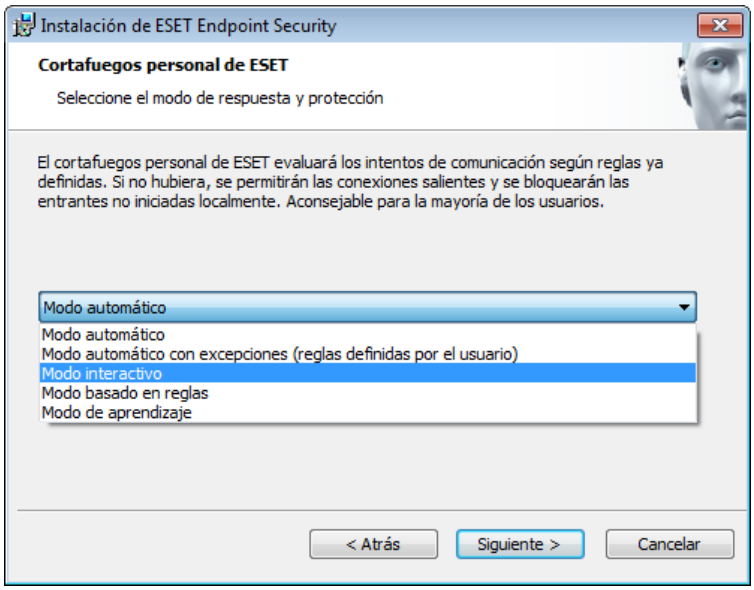
NOTA: normalmente, después de actualizar componentes del programa, es necesario reiniciar el ordenador. Le recomendamos que seleccione la opción **Si es necesario, reiniciar el ordenador sin avisar**.

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



Los pasos de instalación siguientes, **Actualización automática**, **ESET Live Grid** y **Detección de aplicaciones potencialmente indeseables**, son iguales que en la instalación típica (consulte "Instalación típica").

A continuación, seleccione un modo de filtrado para el cortafuegos personal de ESET. Están disponibles cinco modos de filtrado para el cortafuegos personal de ESET Endpoint Security. El comportamiento del cortafuegos cambia en función del modo seleccionado. Los modos de filtrado influyen igualmente en el nivel de interacción del usuario.



Haga clic en **Instalar**, en la ventana **Preparado para instalar**, para completar la instalación. Cuando haya finalizado la instalación, se le solicitará que active el producto. Consulte Instalación típica para obtener más información sobre la activación del producto.

2.3 Introducción del nombre de usuario y la contraseña

Para optimizar la funcionalidad, es importante que el programa se actualice automáticamente. Esto solo es posible si se introducen el nombre de usuario y la contraseña correctos en la **Configuración de actualizaciones**.

Si no ha especificado un nombre de usuario y una contraseña durante la instalación, puede hacerlo ahora. Pulse **CTRL+U** e introduzca los datos que haya recibido con la licencia del producto de seguridad de ESET en la ventana Detalles de la licencia.

Al introducir el **Nombre de usuario** y la **Contraseña**, es importante hacerlo exactamente como se escriben:

- Los campos de nombre de usuario y contraseña distinguen mayúsculas y minúsculas, y el guión del nombre de usuario es obligatorio.
- La contraseña tiene diez caracteres, todas en minúsculas.
- No utilizamos la letra L en las contraseñas (se utiliza el número uno (1) en su lugar).
- Un carácter 'O' grande es el número cero (0) y un carácter 'o' pequeño es la letra "o" minúscula.

Se recomienda copiar y pegar los datos del correo electrónico de registro para garantizar la precisión.

2.4 Actualización a una versión más reciente

Las versiones más recientes de ESET Endpoint Security mejoran 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. Al principio de la instalación, puede marcar la casilla de verificación **Usar los parámetros actuales** para conservar la configuración actual del programa.
3. Actualización manual, a través de la implementación automática en un entorno de red mediante ESET Remote Administrator.

2.5 Análisis del ordenador

Tras la instalación de ESET Endpoint Security, realice un análisis del ordenador para comprobar si hay código malicioso. 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 la sección Análisis del ordenador.

3. Guía para principiantes

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

3.1 Introducción del diseño de la interfaz de usuario

La ventana principal del programa ESET Endpoint Security 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 Security.

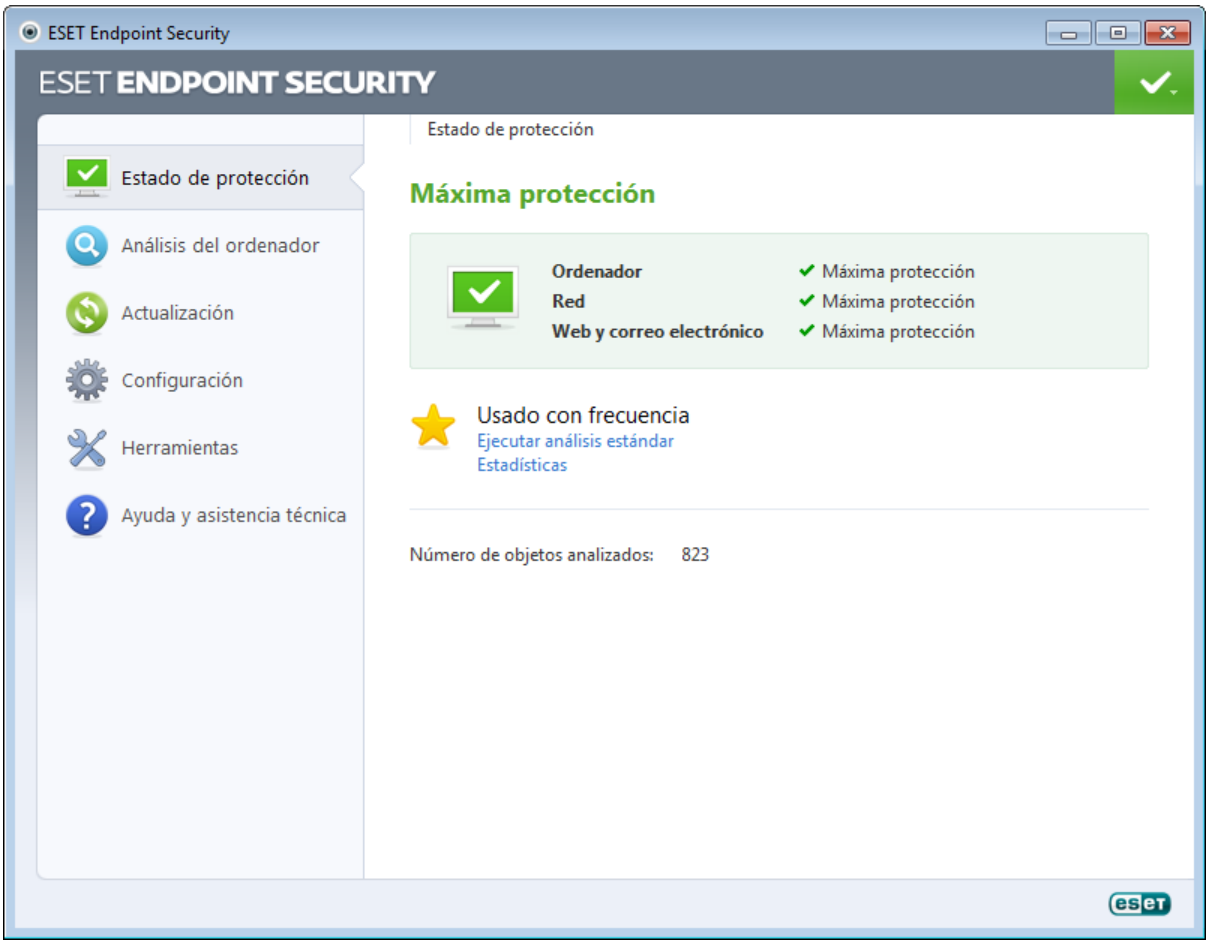
Análisis del ordenador: esta opción le permite configurar e iniciar el análisis estándar o el análisis personalizado.

Actualización: muestra información sobre las actualizaciones de la base de firmas de virus.

Configuración: seleccione esta opción para definir el nivel de seguridad de Ordenador, Web y correo electrónico, y Red .

Herramientas: proporciona acceso a Archivos de registro, Estadísticas de protección, Observar actividad, Procesos en ejecuciónConexiones de red,, Planificador de tareas, Cuarentena, ESET SysInspector y ESET SysRescue.

Ayuda y asistencia técnica: proporciona acceso a los archivos de ayuda, la Base de conocimientos de ESETy el sitio web de ESET, así como enlaces para abrir una solicitud de atención al cliente.

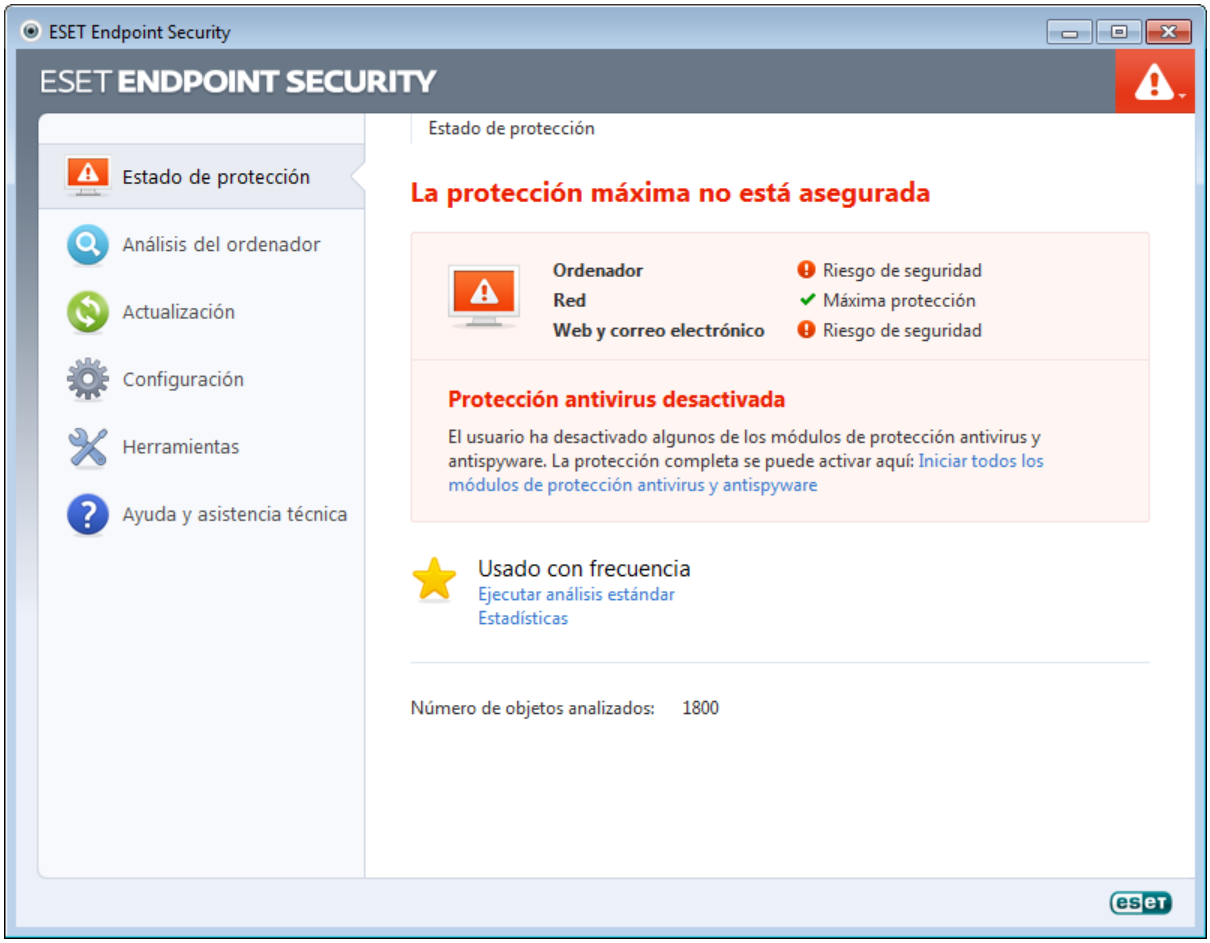


La pantalla **Estado de la protección** indica el nivel de seguridad y protección actual del ordenador. El icono de estado verde de **Máxima protección** indica que se garantiza la protección máxima.

En la ventana de estado también se muestran las características más habituales de ESET Endpoint Security. Aquí también se indica la fecha de expiración del programa.

3.2 Qué hacer si el programa no funciona correctamente

Si los módulos activados funcionan correctamente, se les asigna una marca verde. En caso contrario, se muestra un signo de exclamación rojo o un icono de notificación naranja, además de información adicional acerca del módulo en la parte superior de la ventana. También se muestra una sugerencia de solución para reparar el módulo. Para cambiar el estado de los módulos individuales, haga clic en **Configuración** en el menú principal y, a continuación, en el módulo deseado.



El icono rojo de estado indica problemas graves; no se garantiza la protección máxima del ordenador. Los posibles motivos son:

- Protección del sistema de archivos en tiempo real desactivada
- Cortafuegos personal desactivado
- La base de firmas de virus está desactualizada
- El producto no está activado
- La licencia del producto ha expirado

El icono naranja indica que la protección del cliente de correo electrónico o del tráfico de Internet está desactivada, que hay un problema con la actualización del programa (base de firmas de virus obsoleta, no se puede actualizar) o que se acerca la fecha de vencimiento de la licencia.

Protección antivirus y antiespía está desactivada: este problema se indica mediante un icono rojo y una notificación de seguridad junto al elemento **Ordenador**. Si desea activar la protección antivirus y antispyware de nuevo, haga clic en **Iniciar todos los módulos de protección antivirus y antispyware**.

Protección del tráfico de Internet desactivada - Este problema se indica mediante un icono naranja con una "i" y el estado **Notificación de seguridad**. Si desea activar de nuevo la protección del tráfico de Internet haga clic en la notificación de seguridad y, a continuación, en **Activar la protección del tráfico de Internet**.

Cortafuegos personal de ESET desactivado: este problema se indica mediante un icono rojo y una notificación de seguridad junto al elemento **Red**. Si desea activar de nuevo la protección de red, haga clic en **Activar modo de filtrado**.

Su licencia expirará 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.

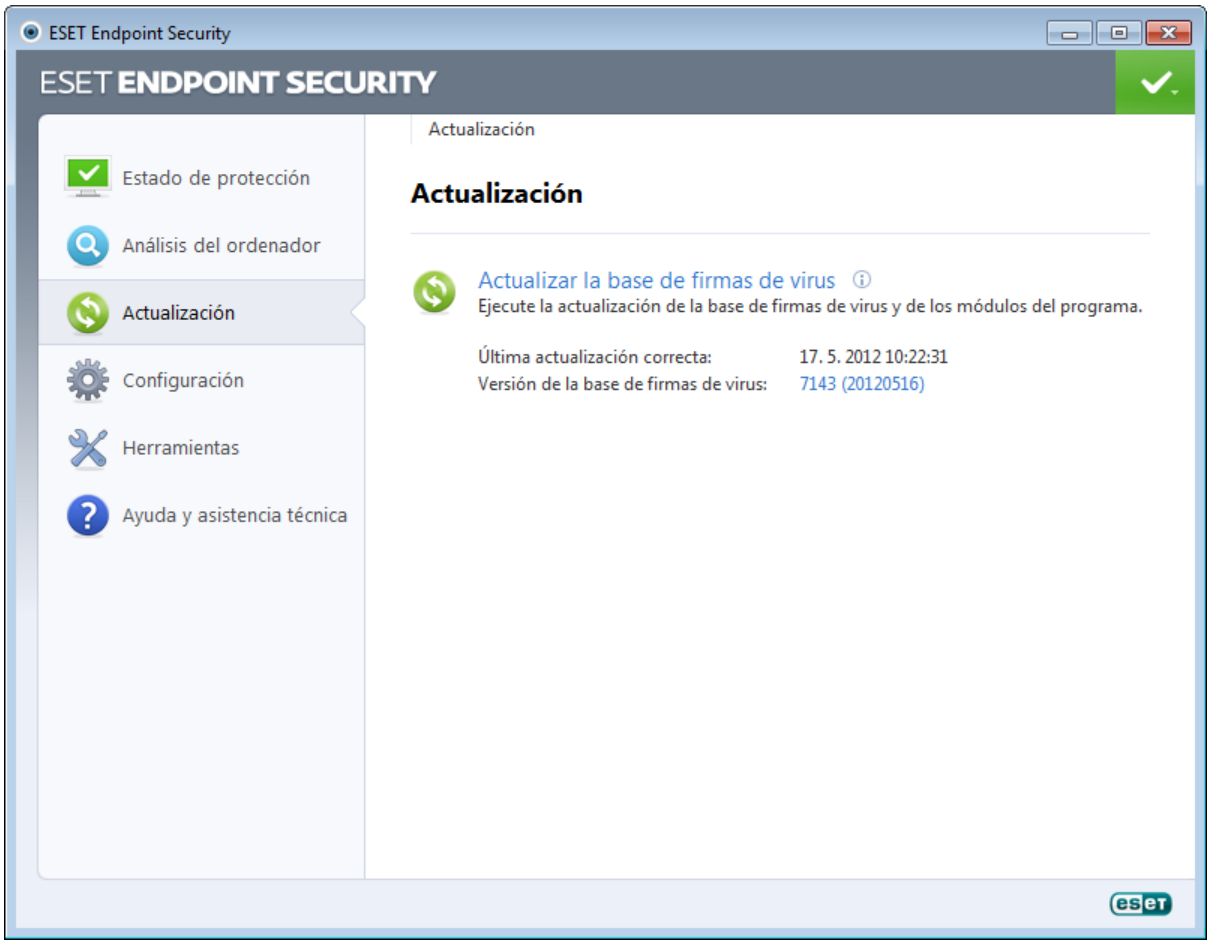
La licencia ha expirado: esto se indica mediante el icono de estado de la protección, que se vuelve rojo. Una vez que expire la licencia, el programa no se puede actualizar. Le recomendamos que siga las instrucciones de la ventana de alerta para renovar la licencia.

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 conocimientos 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.

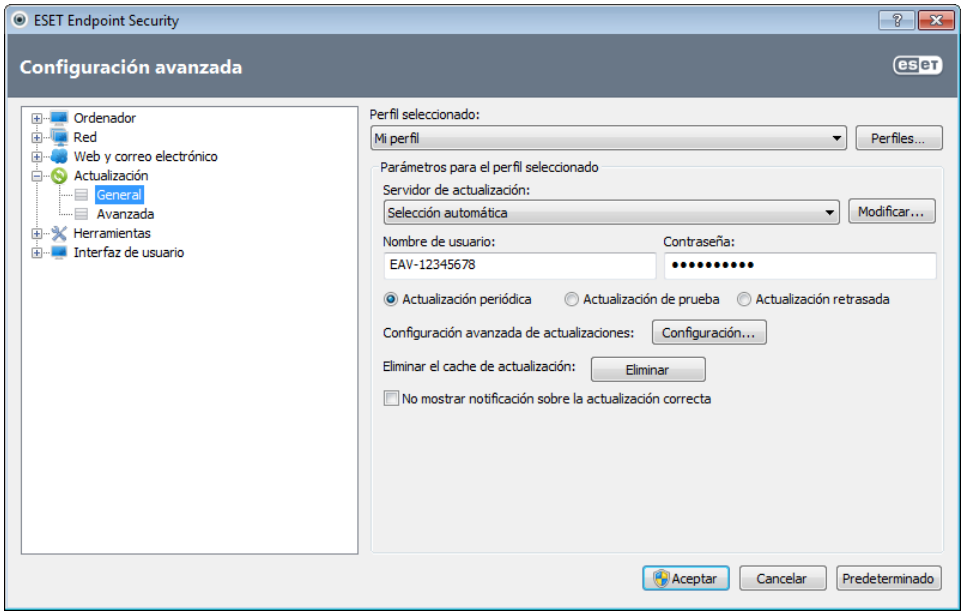
3.3 Configuración de actualizaciones

La actualización de la base de firmas de virus y la actualización de componentes del programa son partes importantes a la hora de proporcionar protección total frente a código malicioso. Preste especial atención a su configuración y funcionamiento. En el menú principal, seleccione **Actualizar** y, a continuación, haga clic en **Actualizar base de firmas de virus** para comprobar si hay alguna actualización más reciente.

Si no ha especificado un nombre de usuario y una contraseña durante el proceso de instalación de ESET Endpoint Security, se le solicitará que los especifique en este momento.

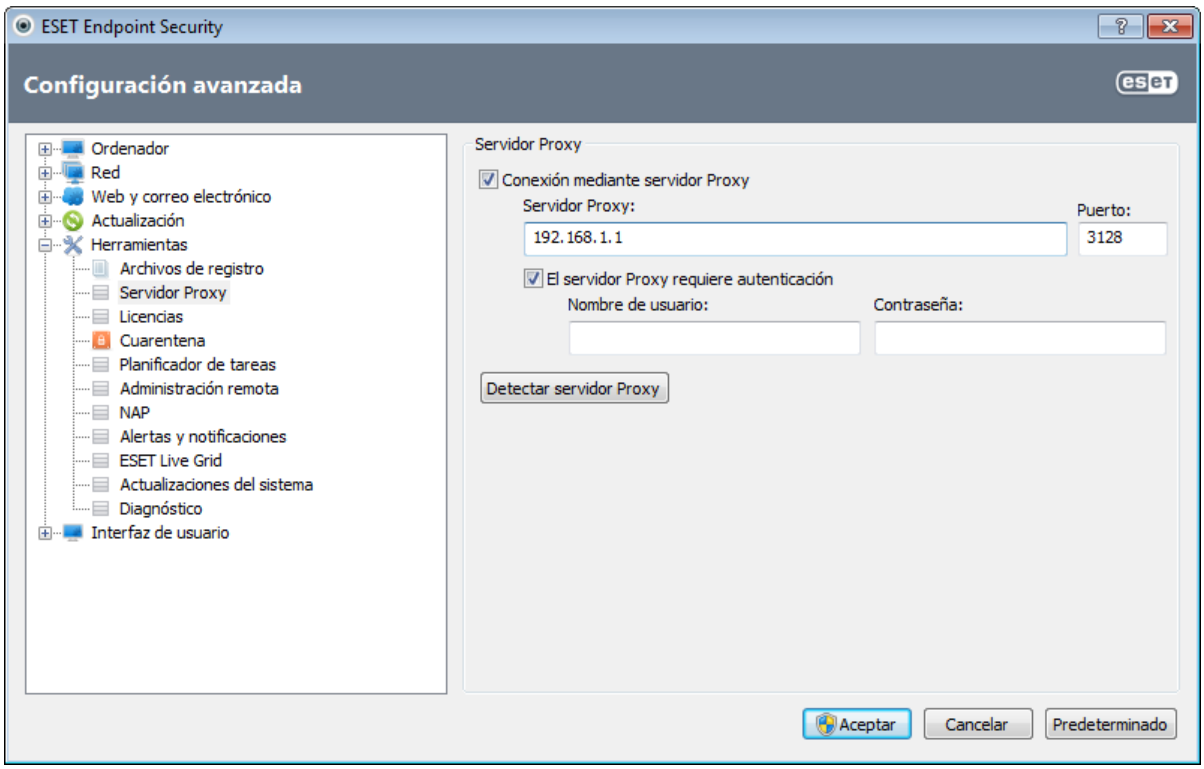


La ventana Configuración avanzada (haga clic en **Configuración** en el menú principal y, a continuación, en **Especificar configuración avanzada**, o pulse F5 en el teclado) ofrece opciones de actualización adicionales. Haga clic en **Actualizar** en el árbol de configuración avanzada disponible a la izquierda. El menú desplegable **Servidor de actualización** está establecido de forma predeterminada en **Selección automática**. 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 de firmas de virus, haga clic en el botón **Configuración**.



3.4 Servidor Proxy

Si utiliza un servidor Proxy para controlar las conexiones a Internet de un sistema que utiliza ESET Endpoint Security, este debe estar especificado en la configuración avanzada. Para acceder a la ventana de configuración del servidor Proxy, pulse F5 para abrir la ventana Configuración avanzada y haga clic en **Herramientas** > **Servidor Proxy** en el árbol de configuración avanzada. Seleccione la opción **Conexión mediante servidor Proxy** y, a continuación, cumpliméntelos campos **Servidor Proxy** (dirección IP) y **Puerto**. Si procede, seleccione la opción **El servidor Proxy requiere autenticación** y, a continuación, introduzca el **nombre de usuario** y la **contraseña**.

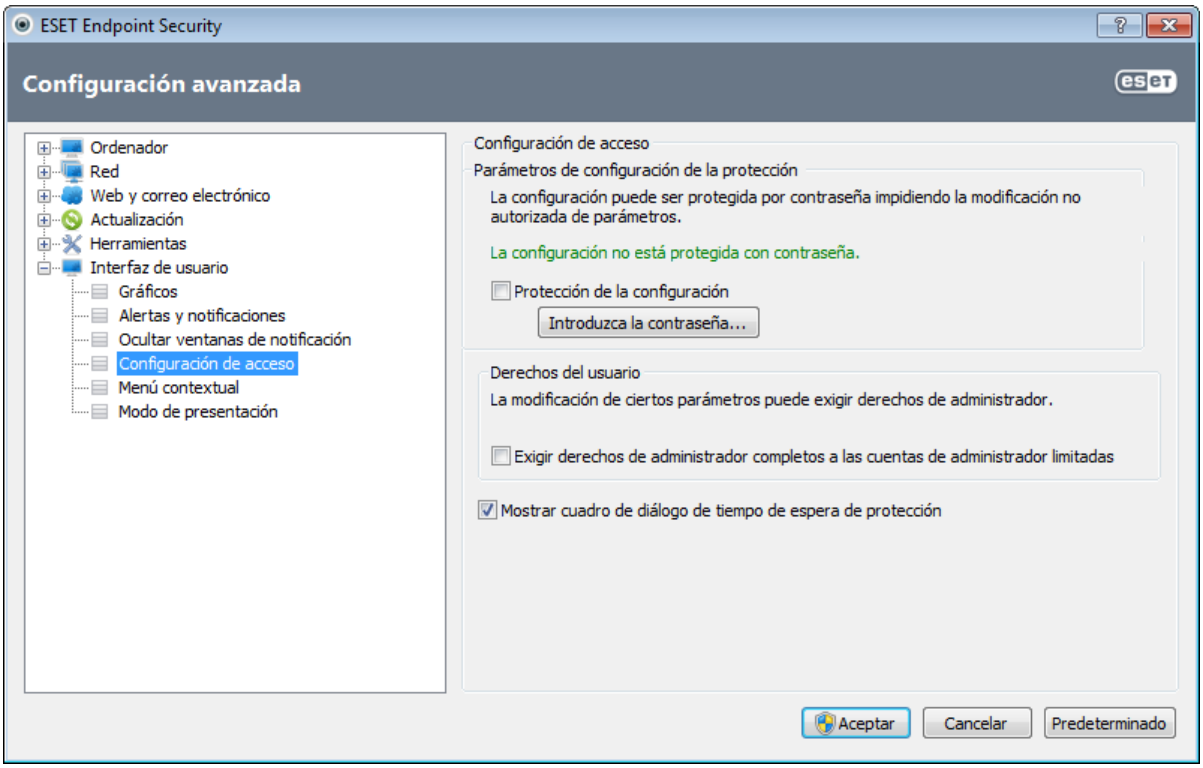


Si no dispone de esta información, haga clic en el botón **Detectar servidor Proxy** para intentar detectar automáticamente la configuración del servidor Proxy.

NOTA: las opciones del servidor Proxy pueden ser diferentes para los distintos perfiles de actualización. Si este es el caso, haga clic en **Actualizar** en el árbol de configuración avanzada para configurar los diferentes perfiles de actualización en Configuración avanzada.

3.5 Protección de la configuración

La configuración de ESET Endpoint Security puede ser muy importante para la directiva de seguridad. Las modificaciones no autorizadas pueden poner en peligro la estabilidad y la protección del sistema. Para proteger mediante contraseña los parámetros de configuración, haga clic en **Configuración** > **Especificar configuración avanzada** en el menú principal. > **Interfaz de usuario** > **Configuración de acceso** en el menú principal, seleccione la opción **Protección de la configuración** y haga clic en el botón **Introduzca la contraseña**.

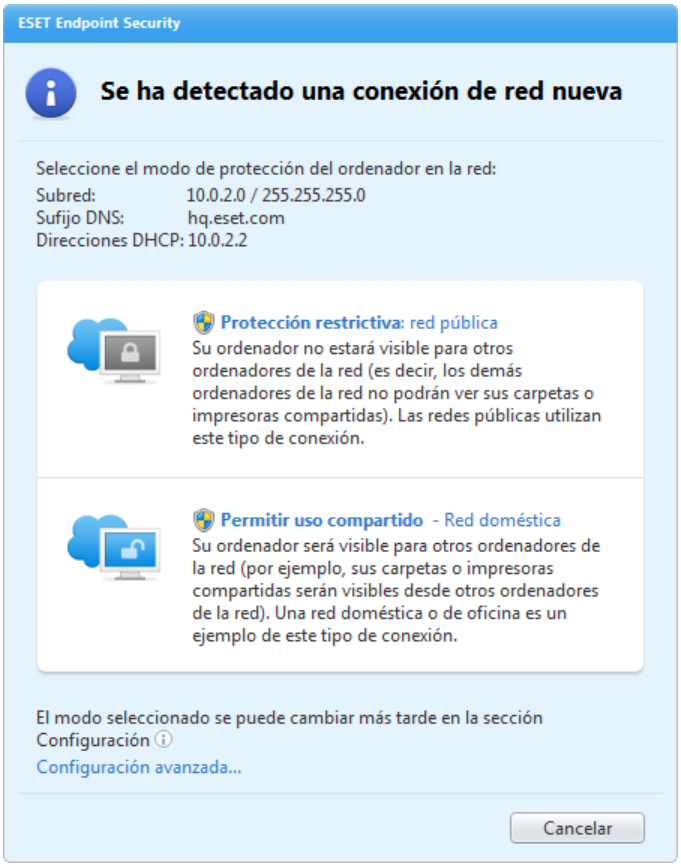


Escriba una contraseña en los campos **Contraseña nueva** y **Confirmar contraseña** y, a continuación, haga clic en **Aceptar**. Esta contraseña es necesaria para realizar modificaciones en la configuración de ESET Endpoint Security.

3.6 Configuración de la zona de confianza

Es necesario configurar la zona de confianza con el fin de proteger el ordenador en entornos de red. Puede permitir que otros usuarios accedan a su ordenador mediante la activación del uso compartido al configurar la zona de confianza. Haga clic en **Configuración** > **Red** > **Cambiar el modo de protección de su ordenador en la red**. Se abrirá una ventana con opciones para elegir el modo de protección que aplicar al ordenador en la red.

La zona de confianza se detecta después de instalar ESET Endpoint Security y cada vez que el ordenador se conecta a una red nueva, por lo que normalmente no es necesario definirla. De forma predeterminada, cuando se detecta una nueva zona se muestra un cuadro de diálogo en el que puede establecer el nivel de protección de dicha zona.



Alerta: la configuración incorrecta de una zona de confianza puede exponer su ordenador a ciertos riesgos.

NOTA: de forma predeterminada, se concede acceso a las estaciones de trabajo de una zona de confianza para compartir archivos e impresoras, tener activada la comunicación RPC entrante y disfrutar del uso compartido de escritorio remoto.

4. Uso de ESET Endpoint Security

Las opciones de configuración de ESET Endpoint Security le permiten ajustar los niveles de protección del ordenador y la red.

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

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

Haga clic en cualquier componente para ajustar la configuración avanzada del correspondiente módulo de protección.

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

- **Protección en tiempo real del sistema de archivos**: 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 por ejemplo elementos de Microsoft ActiveX.
- **Control de dispositivos**: Este módulo le permite analizar, bloquear o ajustar los filtros y permisos ampliados, así como seleccionar el modo de acceso y trabajo de un usuario en un dispositivo dado (CD/DVD/USB...).
- **HIPS**: el sistema HIPS controla los sucesos del sistema operativo y reacciona según un conjunto de reglas personalizado.
- **Modo de presentación**: activa o desactiva el modo de presentación. Recibirá un mensaje de alerta (riesgo de seguridad potencial) y la ventana principal se volverá naranja cuando se active el modo de presentación.
- **Protección Anti-Stealth**: proporciona la detección de programas peligrosos (como los rootkits) que pueden ocultarse del sistema operativo. Esto implica que no es posible detectarlos mediante las técnicas habituales.

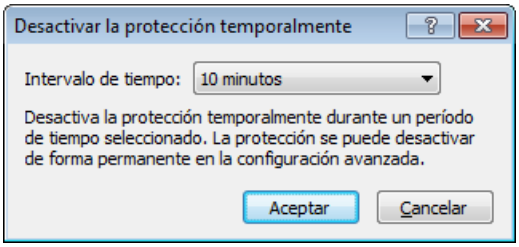
En la sección **Red** puede activar o desactivar el **cortafuegos personal**.

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

- **Protección del tráfico de Internet**: si se activa esta opción, todo el tráfico que pasa a través del protocolo HTTP o HTTPS se analiza en busca de software malicioso.
- **Protección del cliente de correo electrónico**: controla comunicaciones recibidas a través de los protocolos POP3 e IMAP.
- **Protección Antispam**: analizar el correo electrónico no solicitado (spam).
- **Control de acceso web**: le permite bloquear las páginas web que puedan contener material que podría resultar ofensivo. Además, los jefes o los administradores del sistema pueden prohibir el acceso a 27 categorías predefinidas de sitios web.

NOTA: La protección de documentos se muestra al activar la opción **Especificar configuración avanzada** (F5) > **Ordenador** > **Antivirus y antiespía** > **Protección de documentos** > **Integrar en el sistema**.

Al hacer clic en **Activado**, se abre el cuadro de diálogo **Desactivar la protección temporalmente**. Haga clic en **Aceptar** para desactivar el componente de seguridad seleccionado. En el menú desplegable **Intervalo de tiempo** se indica el período de tiempo durante el que estará desactivado el componente seleccionado.



Para volver a activar la protección del componente de seguridad desactivado, haga clic en **Desactivado**.

NOTA: si desactiva la protección con este método, todas las partes desactivadas de la protección se activarán al reiniciar el ordenador.

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 y exportar configuración**.

4.1 Ordenador

Puede consultar el módulo **Ordenador** en el panel **Configuración** haciendo clic en el título **Ordenador**. Se mostrará una descripción de todos los módulos de protección. Para desactivar los módulos individuales temporalmente, haga clic en **Desactivar** debajo del módulo que desee. Tenga en cuenta que esto puede disminuir la protección del ordenador. Para acceder a la configuración detallada de cada módulo, haga clic en **Configurar**.

Haga clic en **Modificar exclusiones...** para abrir la ventana de configuración de exclusiones, en la que puede excluir archivos y carpetas del análisis antivirus.

Desactivar temporalmente la protección antivirus y antiespía: desactiva todos los módulos de protección antivirus y antispyware. Se mostrará el cuadro de diálogo **Desactivar la protección temporalmente** con el menú desplegable **Intervalo de tiempo**. En el menú desplegable **Intervalo de tiempo** se indica el período de tiempo durante el que estará desactivada la protección. Haga clic en **Aceptar** para confirmar.

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

4.1.1 Protección antivirus y antispyware

La opción Protección antivirus y antispyware 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 con código malicioso, el módulo antivirus puede bloquearlo para después desinfectarlo, eliminarlo o ponerlo en cuarentena.

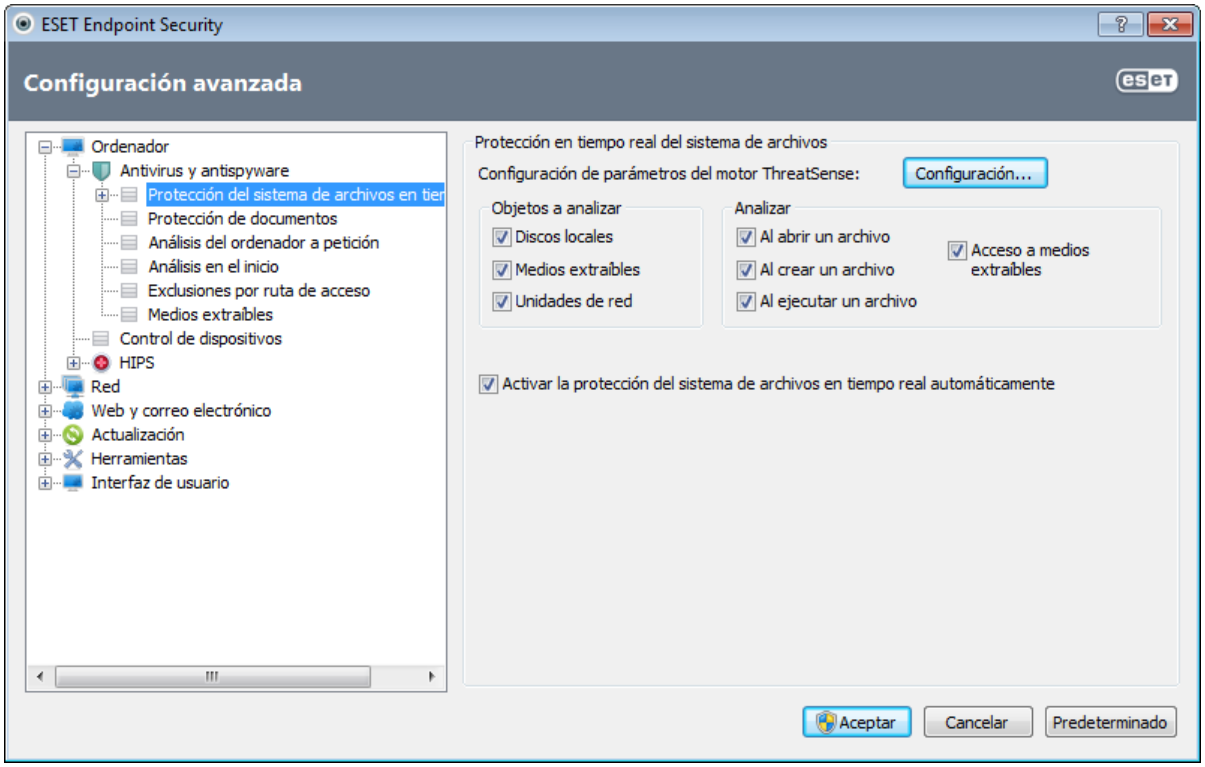
4.1.1.1 Protección del sistema de archivos en tiempo real

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 en que se abren, crean o ejecutan 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 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 de ThreatSense), la protección del sistema de archivos en tiempo real puede ser diferente para los archivos recién creados y los archivos ya existentes. Para los archivos nuevos, se puede aplicar un nivel de control más exhaustivo.

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 vuelven a analizar inmediatamente después de cada actualización de la base de firmas de virus. Este comportamiento se configura con la opción **Optimización inteligente**. Si está desactivada, todos los archivos se analizarán cada vez que se acceda a ellos. Para modificar esta opción, pulse F5 para abrir la ventana Configuración avanzada y haga clic en **Ordenador** > **Antivirus y antiespía** > **Protección del sistema de archivos en tiempo real** en el árbol de configuración avanzada. A continuación, haga clic en el botón **Configuración** situado junto a **Configuración de parámetros del motor ThreatSense**, haga clic en **Otros** y marque o desmarque la opción **Activar optimización inteligente**.

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 interrumpir la protección en tiempo real anulando la selección de la opción **Activar la protección del sistema de archivos en tiempo real automáticamente**.



4.1.1.1.1 Objetos a analizar

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

Discos locales: controla todas las unidades de disco duro del sistema.

Medios extraíbles: disquetes, discos CD y DVD, dispositivos de almacenamiento USB, 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.

4.1.1.1.2 Analizar (análisis cuando se cumpla la condición)

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

Al abrir un archivo: activa o desactiva el análisis de los archivos abiertos.

Al crear un archivo: activa o desactiva el análisis de los archivos creados o modificados recientemente.

Al ejecutar un archivo: activa o desactiva el análisis de los archivos ejecutados.

Acceso a medios extraíbles: activa o desactiva el análisis activado por el acceso a determinados medios extraíbles con espacio de almacenamiento.

4.1.1.1.3 Opciones avanzadas de análisis

Encontrará opciones de configuración más detalladas en **Ordenador** > **Antivirus y antispyware** > **Protección del sistema de archivos en tiempo real** > **Configuración avanzada**.

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 mejora en gran medida los índices de detección gracias a la detección de amenazas nuevas antes de que se publique la actualización de la base de firmas de virus. Además de los archivos nuevos, el análisis se realiza también en archivos de autoextracción (.sfx) y empaquetadores en tiempo real (archivos ejecutables comprimidos internamente). 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, anule la selección de la opción **Configuración por defecto para archivos comprimidos**.

Parámetros adicionales de ThreatSense para archivos ejecutados: de forma predeterminada, la heurística avanzada no se utiliza cuando se ejecutan archivos. Sin embargo, en algunos casos, es aconsejable activar esta opción (seleccionando **Heurística avanzada al ejecutar un archivo**). Tenga en cuenta que esta herramienta puede ralentizar la ejecución de algunos programas debido a los mayores requisitos del sistema. Cuando la opción **Heurística avanzada en la ejecución de archivos desde dispositivos externos** está activada, si desea excluir algunos puertos de medios extraíbles (USB) del análisis mediante la heurística avanzada al ejecutar un archivo, haga clic en **Excepciones** para abrir la ventana de exclusión de unidades de medios extraíbles. Aquí puede personalizar los ajustes mediante las casillas de verificación correspondientes a los diferentes puertos.

4.1.1.1.4 Niveles de desinfección

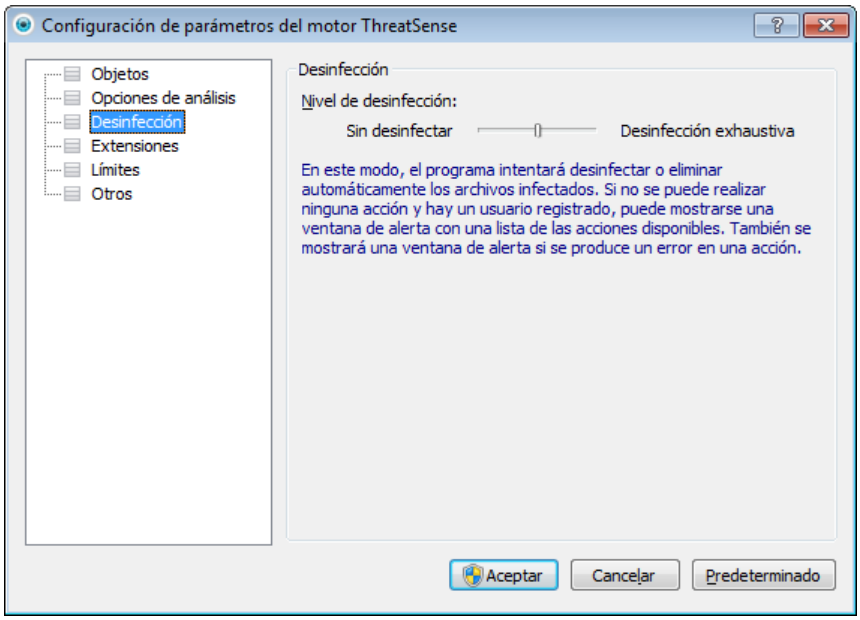
La protección en tiempo real tiene tres niveles de desinfección (para acceder, haga clic en el botón **Configuración** de la sección **Protección del sistema de archivos en tiempo real** y, a continuación, en **Desinfección**).

Sin desinfectar: 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 estándar: el programa intenta desinfectar o eliminar un archivo infectado de manera automática, de acuerdo con una acción predefinida (dependiendo del tipo de amenaza). La eliminación y la detección de un archivo infectado se marca mediante un mensaje de información localizado en la esquina inferior derecha de la pantalla. Si no es posible seleccionar la acción correcta de manera automática, el programa ofrece una selección de acciones a seguir. Lo mismo ocurre cuando no se puede completar una acción predefinida.

Desinfección exhaustiva: 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.

Alerta: 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.



4.1.1.1.5 Modificación de la configuración de protección en tiempo real

La protección 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. Por ejemplo, si se produce un conflicto con una aplicación determinada o durante el análisis en tiempo real de otro programa antivirus.

Una vez instalado ESET Endpoint Security, se optimizará toda la configuración para proporcionar a los usuarios el nivel máximo de seguridad del sistema. Para restaurar la configuración predeterminada, haga clic en el botón **Predeterminado** disponible en la esquina inferior derecha de la ventana **Protección del sistema de archivos en tiempo real** (**Configuración avanzada** > **Ordenador** > **Antivirus y antiespía** > **Protección del sistema de archivos en tiempo real**).

4.1.1.1.6 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 especial 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. El archivo eicar.com se puede descargar en http://www.eicar.org/download/eicar.com

NOTA: antes de realizar un análisis de protección en tiempo real, es necesario desactivar el cortafuegos. Si está activado, detectará el archivo y no dejará que los archivos de prueba se descarguen.

4.1.1.1.7 ¿Qué debo hacer si la protección en tiempo real no funciona?

En este capítulo, describimos las situaciones en las que puede surgir un problema cuando se utiliza la protección en tiempo real y cómo resolverlas.

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 **Activar la protección del sistema de archivos en tiempo real automáticamente** no está seleccionada. Para activar esta opción, vaya a Configuración avanzada (F5) y haga clic en **Ordenador** > **Antivirus y antiespía** > **Protección del sistema de archivos en tiempo real** en el árbol de configuración avanzada. En la sección **Configuración avanzada** situada en la parte inferior de la ventana, asegúrese de que la casilla de verificación **Activar la protección del sistema de archivos en tiempo real automáticamente** está seleccionada.

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 uno de

los programas antivirus.

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 automáticamente** está activada), es posible que se deba a conflictos con otros programas. Si este es el caso, póngase en contacto con el servicio de atención al cliente de ESET.

4.1.1.2 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 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 **Ordenador** > **Antivirus y antiespía** > **Protección de documentos** en el árbol de configuración avanzada. Si está activada, la protección de documentos se puede ver en la ventana principal del programa de ESET Endpoint Security, en **Configuración** > **Ordenador**.

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).

4.1.1.3 Análisis del ordenador

El análisis a petición es una parte importante de su solución 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 para detectar virus que la Protección del sistema de archivos en tiempo real no haya encontrado cuando se registraron en el disco, por ejemplo, si la protección del sistema de archivos en tiempo real no estaba activada en ese momento, la base de firmas de virus estaba obsoleta o 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 elegir objetos de análisis específicos.

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

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**.

4.1.1.3.1 Tipo de análisis

4.1.1.3.1.1 Análisis estándar

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 de forma automática en el valor predeterminado. Para obtener más información detallada sobre los tipos de desinfección, consulte la sección Desinfección.

4.1.1.3.1.2 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 **Objetos de análisis**, 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 la opción **Analizar sin desinfectar**. Además, puede seleccionar uno de los tres niveles de desinfección haciendo clic en **Configuración**. > **Desinfección**.

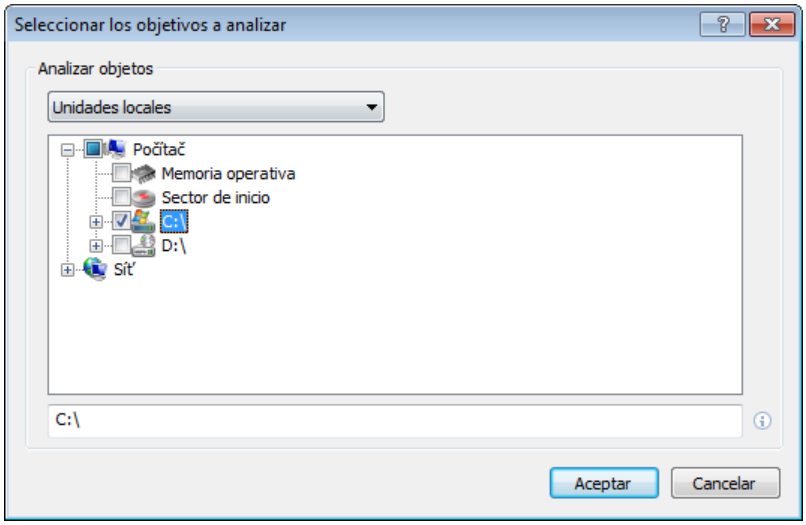
Los análisis del ordenador en el modo personalizado es adecuado para usuarios avanzados con experiencia previa en la utilización de programas antivirus.

4.1.1.3.2 Objetos de análisis

En la ventana de objetos de análisis puede definir los objetos (memoria, unidades, sectores, archivos y carpetas) que se deben analizar para buscar amenazas. En el menú desplegable **Objetos de análisis**, puede seleccionar objetos predefinidos para el análisis.

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

Los objetos de análisis también se pueden especificar introduciendo la ruta a la carpeta o los archivos que se desean incluir en el análisis. Seleccione los objetos en la estructura de árbol, que incluye todos los dispositivos disponibles en el ordenador.



Para acceder rápidamente a un objeto de análisis o agregar directamente un objeto deseado, introdúzcalo en el campo en blanco disponible debajo de la lista de carpetas. Si no se ha seleccionado ningún objeto en la estructura de árbol y el menú **Objetos de análisis** está definido en **Sin selección**, no podrá hacerlo.

4.1.1.3.3 Perfiles de análisis

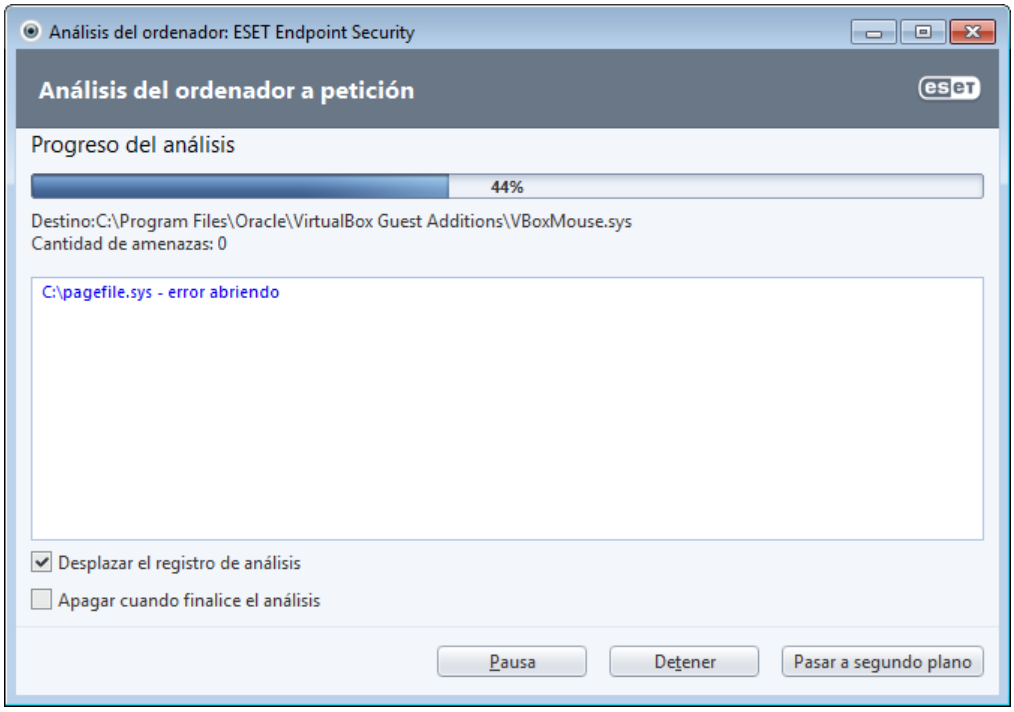
Puede guardar sus parámetros de análisis preferidos para próximas sesiones de análisis. Le recomendamos que cree un perfil diferente (con varios objetos de análisis, métodos de análisis y otros parámetros) para cada uno de los análisis que realice con frecuencia.

Para crear un perfil nuevo, abra la ventana Configuración avanzada (F5) y haga clic en **Ordenador** > **Antivirus y antiespía** > **Análisis del ordenador** > **Perfiles...**. En la ventana **Perfiles de configuración** encontrará el menú desplegable **Perfil seleccionado** con los perfiles de análisis existentes y la opción para crear uno nuevo. Si necesita ayuda para crear un perfil de análisis que se adecúe a sus necesidades, consulte la sección Configuración de parámetros del motor de 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 exhaustiva**. En la ventana **Perfiles de configuración**, haga clic en el botón **Agregar...**. Escriba el nombre del nuevo perfil en el campo **Nombre del perfil** y seleccione **Análisis estándar** en el menú desplegable **Copiar parámetros desde el perfil** A continuación, ajuste los demás parámetros de acuerdo con sus requisitos.

4.1.1.3.4 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 son utilizados exclusivamente por 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 porcentaje de objetos ya analizados en comparación con el porcentaje de objetos pendientes. El valor se calcular a partir del número total de objetos incluidos en el análisis.

Objeto: el nombre y la ubicación del objeto que se está analizando.

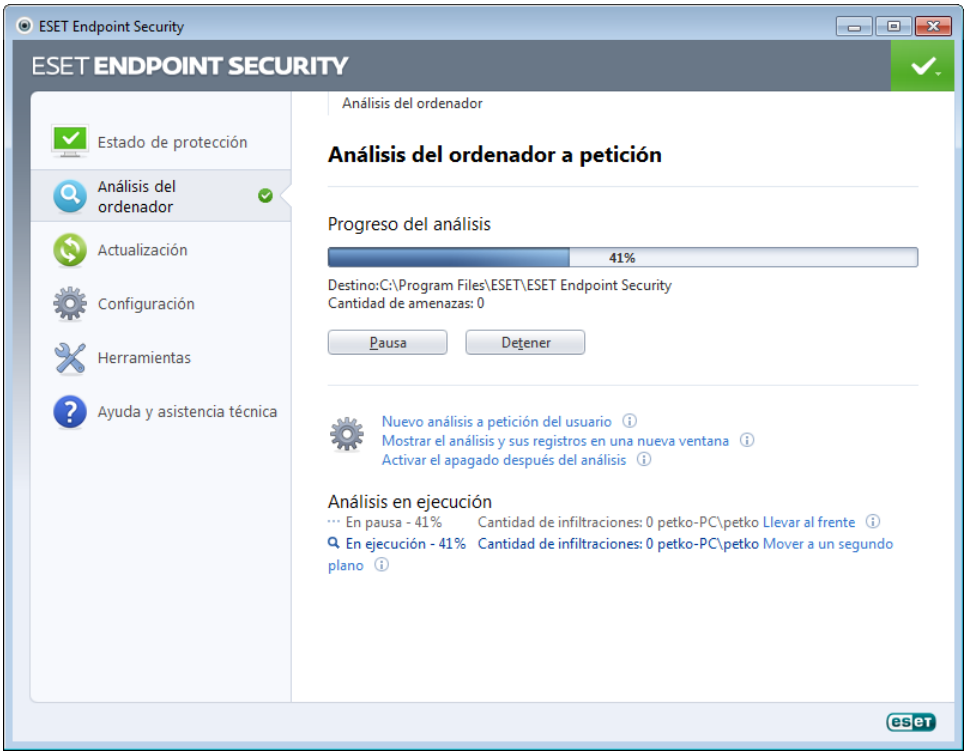
Cantidad de amenazas: muestra el número total de amenazas detectadas durante el análisis.

Pausa: pone el análisis en pausa.

Continuar: 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.

Pasar a segundo plano: le permite ejecutar otro análisis en paralelo. El análisis en ejecución se pasará a segundo plano.



Haga clic en **Cambiar a primer plano** para ejecutar el análisis en primer plano y volver al proceso de análisis.

Desplazar el registro de análisis: 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.

Activar el apagado después del análisis: activa el apagado programado para cuando termine el análisis del ordenador a petición. Se abrirá un cuadro de diálogo de confirmación de apagado con un tiempo de espera de 60 segundos. Haga clic en **Cancelar** si desea desactivar el apagado solicitado.

4.1.1.4 Análisis en el inicio

La comprobación automática de los archivos en el inicio se realizará al iniciar el sistema o actualizar la base de firmas de virus. 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 en el inicio del sistema** del Planificador de tareas. Para modificar la configuración, seleccione **Herramientas** > **Planificador de tareas**, haga clic en **Verificación de la ejecución de archivos en el inicio** y en el botón **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.

4.1.1.4.1 Comprobación de la ejecución de archivos en el inicio

El menú desplegable **Nivel de análisis** especifica la profundidad del análisis para los archivos que se ejecutan al iniciar el sistema. Los archivos se organizan en orden ascendente según el número de archivos que se analizarán:

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

También se incluyen dos grupos específicos de **niveles de análisis**:

- **Archivos en ejecución antes del registro del usuario**: contiene archivos de ubicaciones que permiten la ejecución de estos archivos sin que el usuario se haya registrado (incluye casi todas las ubicaciones de inicio como servicios, objetos auxiliares del navegador, entradas del Planificador de tareas de Windows, dlls conocidas, etc.).
- **Archivos en ejecución después del registro del usuario** : contiene archivos de ubicaciones que permiten la ejecución de estos archivos únicamente cuando el usuario se ha registrado (incluye archivos que solo se ejecutan para usuarios específicos, habitualmente los archivos de HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run).

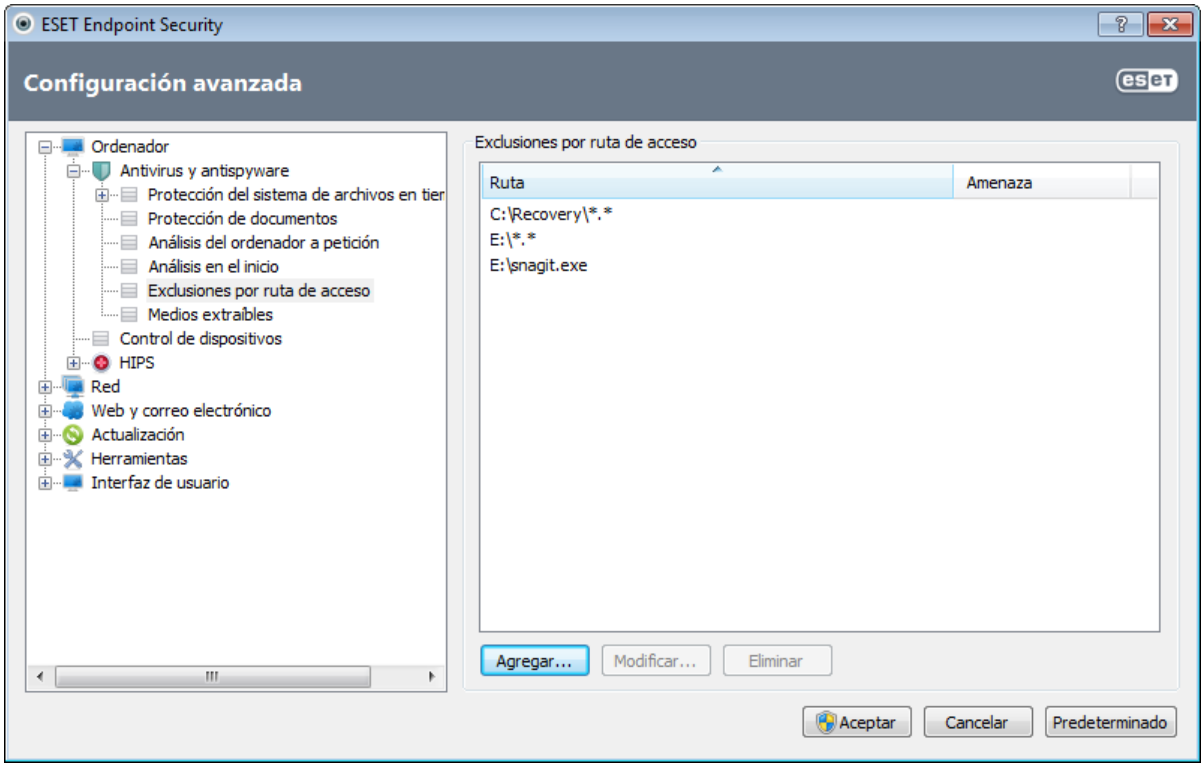
Las listas de los archivos que se analizan son fijas para cada grupo.

Prioridad del análisis: nivel de prioridad que se utilizará para el inicio de la tarea:

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

4.1.1.5 Exclusiones por ruta de acceso

Las exclusiones le permiten excluir archivos y carpetas del análisis. Es recomendable que no modifique estas opciones para así garantizar que se analizan todos los objetos en busca de amenazas. No obstante, es posible que en algunas situaciones tenga que excluir un objeto. Por ejemplo, entradas grandes de una base de datos que ralenticen el ordenador durante el análisis o software que entre en conflicto con el análisis.



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. Por lo tanto, 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 **Configuración** > **Cuarentena**, con la opción del menú contextual **Restaurar y excluir de la detección** del archivo en cuarentena.

Agregar: excluye los objetos de la detección.

Modificar: le permite modificar las entradas seleccionadas.

Quitar: elimina las entradas seleccionadas.

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 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).

4.1.1.6 Configuración de parámetros del motor 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, y utiliza una combinación de diferentes métodos (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 de la tecnología 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 el botón **Configuración** ubicado en la ventana de configuración de cualquier módulo que utilice la tecnología ThreatSense (ver 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.
- 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 ejecuten aplicaciones 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.

4.1.1.6.1 Objetos

En la sección **Objetos** 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: analiza los sectores de inicio para detectar virus en el registro de inicio principal.

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

Archivos comprimidos: el programa admite las 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 auto extracción (SFX) son archivos que no necesitan programas especializados (archivos) para descomprimirse.

Empaquetadores en tiempo real: después de su ejecución, los empaquetadores en tiempo real (a diferencia de los archivos estándar) se descomprimen en la memoria. Además de los empaquetadores estáticos estándar (UPX, yoda, ASPack, FSG, etc.), el analizador admite —gracias a la emulación de código— muchos otros tipos de empaquetadores.

4.1.1.6.2 Opciones

Utilice la sección **Opciones** para seleccionar los métodos utilizados durante el análisis del sistema en busca de amenazas. Están disponibles las opciones siguientes:

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

Heurística avanzada/DNA/Firmas inteligentes: 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. Gracias a la heurística avanzada, las capacidades de detección del programa son significativamente superiores. 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 (u operaciones ligeramente modificadas).

Las **aplicaciones potencialmente indeseables** (PUA) no tienen por qué ser maliciosas, pero pueden afectar al rendimiento del ordenador de forma negativa. Dichas aplicaciones suelen necesitar que se consienta su instalación. Si se encuentran en su ordenador, el sistema se comportará de manera diferente (en comparación con el estado en el que se encontraba antes de la instalación). Los cambios más importantes son:

- Se abren ventanas nuevas que no se habían visto anteriormente (ventanas emergentes, anuncios, etc.).
- Activación y ejecución de procesos ocultos.
- Mayor uso de los recursos del sistema.
- Cambios en los resultados de búsqueda.
- La aplicación se comunica con servidores remotos.

Aplicaciones potencialmente peligrosas: aplicaciones potencialmente peligrosas es la clasificación utilizada para el software comercial legítimo. e incluye programas como herramientas de acceso remoto, aplicaciones para detectar contraseñas y registradores de pulsaciones (programas que graban cada tecla pulsada por un usuario). Esta opción está desactivada de manera predeterminada.

ESET Live Grid: la tecnología de reputación de ESET permite comparar la información sobre los archivos analizados con los datos del sistema ESET Live Grid basado en la nube con el fin de mejorar la detección y agilizar el análisis.

4.1.1.6.3 Desinfección

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

Sin desinfectar: 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.

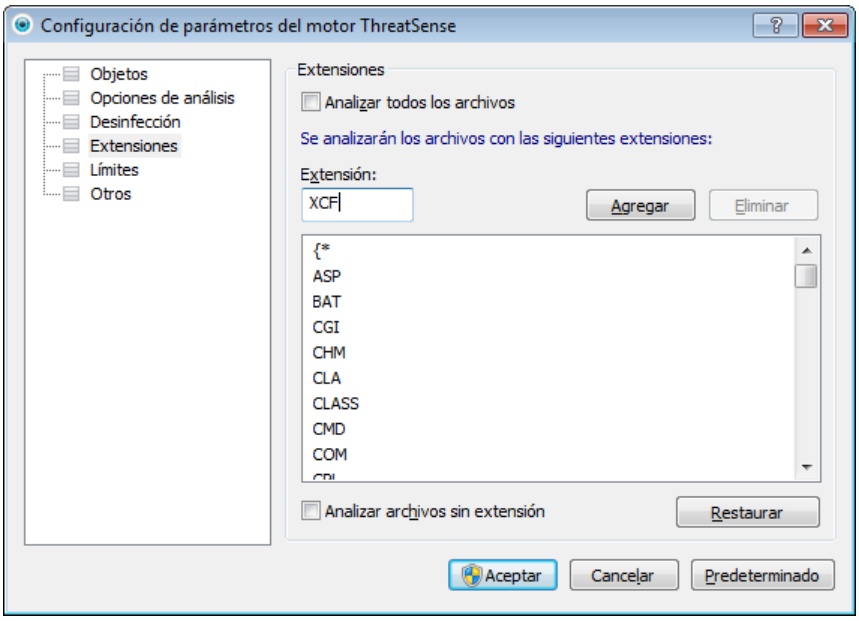
Desinfección estándar: el programa intenta desinfectar o eliminar un archivo infectado de manera automática, de acuerdo con una acción predefinida (dependiendo del tipo de amenaza). La eliminación y la detección de un archivo infectado se marca mediante un mensaje de información localizado en la esquina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

Desinfección exhaustiva: 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.

Alerta: 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.

4.1.1.6.4 Extensión

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 independientemente de su extensión. Se puede agregar cualquier extensión a la lista de archivos excluidos del análisis. Si no está seleccionada la opción **Analizar todos los archivos**, la lista cambia para mostrar todas las extensiones de archivo analizadas actualmente.

Para activar el análisis de archivos sin extensión, seleccione la opción **Analizar archivos sin extensión**. La opción **No analizar archivos sin extensión** está disponible cuando se activa la opción **Analizar todos los archivos**.

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 las 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. Al escribir una **Extensión**, se activa el botón **Agregar** para agregar la nueva extensión a la lista. Seleccione una extensión en la lista y, a continuación, en el botón **Quitar** para eliminarla de la lista.

Se pueden utilizar los símbolos especiales * (asterisco) y ? (signo de interrogación). El asterisco sustituye a cualquier cadena de caracteres y el signo de interrogación, a cualquier símbolo. 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.

Para analizar únicamente el conjunto predeterminado de extensiones, haga clic en el botón **Predeterminado** y haga clic en **Sí** cuando se le solicite para confirmarlo.

4.1.1.6.5 Límites

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

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.

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

Tamaño máx. de archivo en el archivo comprimido (bytes): 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.

Si el análisis de un archivo comprimido finaliza antes de lo previsto por estos motivos, la casilla de verificación del archivo no estará seleccionada.

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

4.1.1.6.6 Otros

En la sección **Otros** se pueden configurar las opciones siguientes:

Registrar todos los objetos: si se selecciona esta opción, el archivo de registro mostrará todos los archivos analizados, incluso los que no están infectados. Si, por ejemplo, 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 realizar el análisis.

Al configurar parámetros del motor ThreatSense para un análisis del ordenador, dispone de las siguientes opciones:

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

Ejecutar análisis en segundo plano y con baja prioridad: cada secuencia de análisis consume una cantidad determinada de recursos del sistema. Si trabaja con programas que colocan una gran carga en los recursos del sistema, puede activar el análisis en segundo plano con prioridad baja y ahorrar recursos para sus aplicaciones.

Conservar hora del último acceso: 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).

Desplazar el registro de análisis: esta opción le permite activar o desactivar el desplazamiento del registro. Si la selecciona, la información se desplaza hacia arriba dentro de la ventana de visualización.

4.1.1.7 Detección de una amenaza

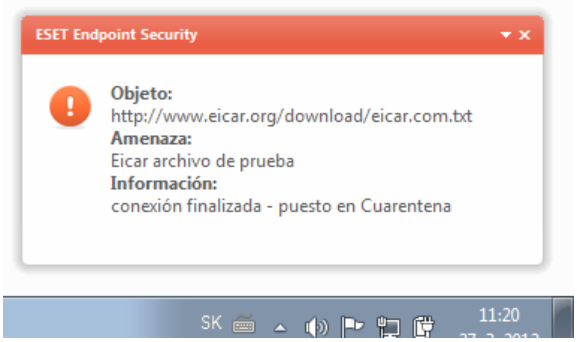
Las amenazas pueden acceder al sistema desde varios puntos de entrada, como páginas web, carpetas compartidas, correo electrónico o dispositivos extraíbles (USB, discos externos, CD, DVD, disquetes, etc.).

Comportamiento estándar

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

- Protección del sistema de archivos en tiempo real
- Protección del tráfico de Internet,
- Protección del cliente de correo electrónico
- Análisis del ordenador a petición

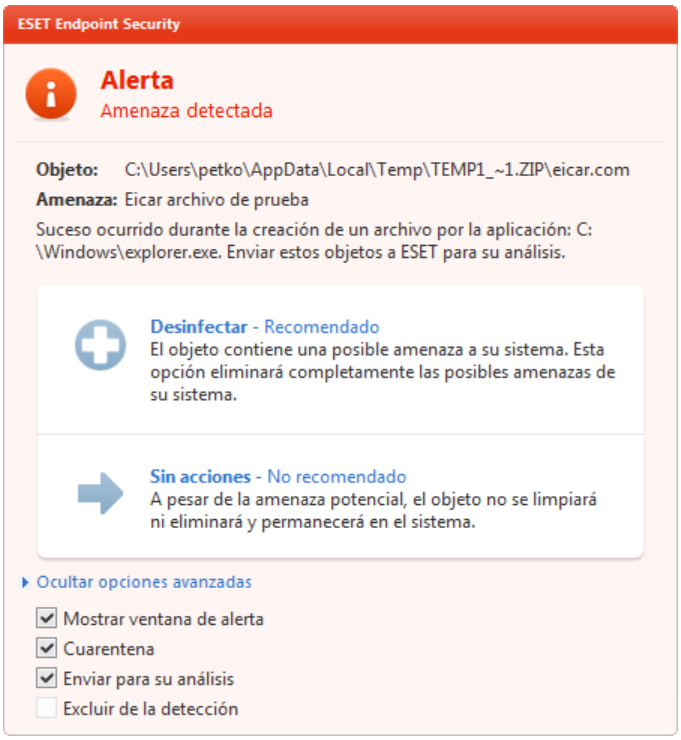
Cada uno de estos componentes utiliza el nivel de desinfección estándar e intentará desinfectar el archivo y moverlo a Cuarentena o finalizar la conexión. Una ventana de notificación se muestra en el área de notificación, situada en la esquina inferior derecha de la pantalla. Para obtener más información 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 una 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).

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, ya que el archivo 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 Security y haga clic en Análisis del ordenador.
- Haga clic en **Análisis estándar** (para obtener más información, consulte Análisis estándar).
- 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.

4.1.2 Unidades extraíbles

ESET Endpoint Security 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 para realizar después de conectar dispositivos externos : seleccione la acción predeterminada que se realizará cuando se inserte un medio extraíble en el ordenador (CD, DVD o USB). Si selecciona la opción **Mostrar opciones de análisis**, se mostrará una ventana en la que puede seleccionar la acción deseada:

- **Analizar ahora**: se realizará un análisis del ordenador a petición en el medio extraíble.
- **Analizar más adelante**: no se realizará ninguna acción y se cerrará la ventana **Nuevo dispositivo detectado**.
- **Configuración**: abre la sección de configuración de medios extraíbles.

Además, ESET Endpoint Security presenta funciones de control de dispositivos, que ofrecen la posibilidad de definir reglas para el uso de dispositivos externos en un ordenador dado. Puede ver más detalles sobre el control de dispositivos, consulte la sección Control de dispositivos.

4.1.3 Control de dispositivos

ESET Endpoint Security permite controlar los dispositivos automáticamente (CD, DVD, USB, etc.). Este módulo le permite analizar, bloquear o ajustar los filtros y permisos ampliados, así como seleccionar el modo de acceso y trabajo de un usuario en un dispositivo dado. Esto puede ser útil cuando el administrador del ordenador quiere impedir que los usuarios inserten dispositivos con contenido no solicitado.

Dispositivos externos admitidos

- CD, DVD y Blu-ray
- Almacenamiento USB
- Dispositivo de FireWire
- Dispositivo de imagen
- Impresora USB
- Bluetooth
- Lector de tarjetas
- Módem
- Puerto LPT/COM

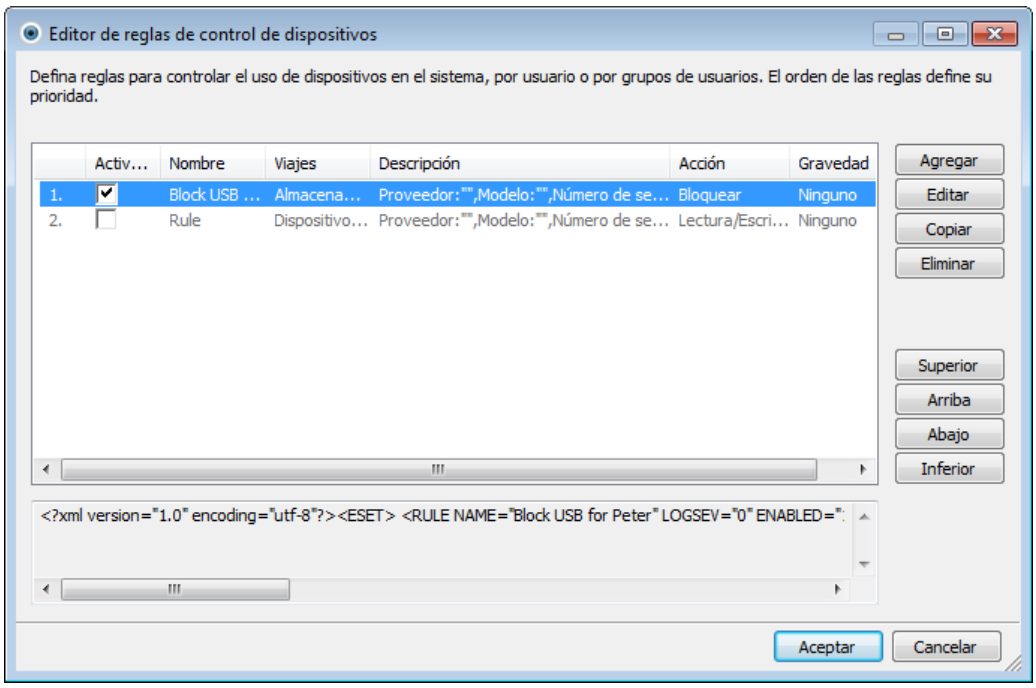
Las opciones de configuración del control de dispositivos se pueden modificar en **Configuración avanzada** (F5) > **Control de dispositivos**.

Al seleccionar la casilla de verificación situada junto a **Integrar en el sistema**, se activa la característica de Control de dispositivos en ESET Endpoint Security; deberá reiniciar el ordenador para que este cambio surta efecto. Una vez activado el Control de dispositivos, se activará **Configurar reglas...**, lo que le permitirá abrir la ventana Editor de reglas de control de dispositivos.

Si el dispositivo externo aplica una regla existente que realiza la acción **Bloquear**, aparecerá una ventana de notificación en la esquina inferior derecha y no se permitirá el acceso al dispositivo.

4.1.3.1 Reglas de control de dispositivos

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

Haga clic en **Agregar** o en **Modificar** para administrar una regla. Haga clic en **Copiar** para crear una nueva regla con opciones predefinidas utilizadas para otra regla seleccionada. Las cadenas XML que se muestran al hacer clic en una regla se pueden copiar en el portapapeles o pueden ayudar a administradores de sistemas a exportar o importar datos

y utilizarlos; por ejemplo en ESET Remote Administrator.

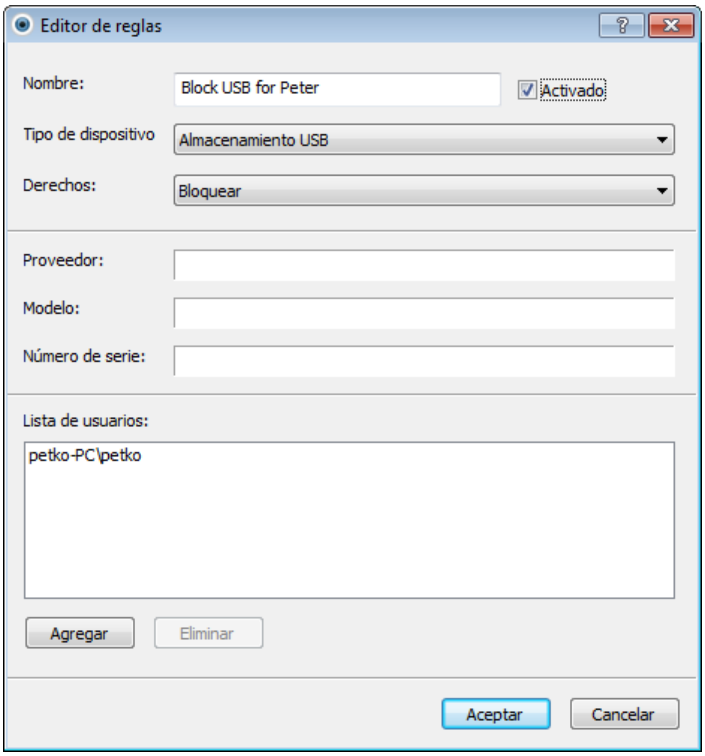
Al mantener pulsado CTRL y hacer clic, puede seleccionar varias reglas y aplicar acciones, como eliminarlas o moverlas hacia arriba o hacia abajo en la lista, a todas las reglas seleccionadas. La casilla de verificación **Activado** desactiva o activa una regla; puede ser útil si no desea eliminar una regla de forma permanente, por si decide utilizarla en el futuro.

El control se efectúa mediante reglas que se clasifican en el orden que determina su prioridad, situándose al principio las reglas con la prioridad más alta.

Puede hacer clic con el botón derecho en una regla para mostrar el menú contextual. Aquí puede definir la severidad de las entradas de registro, si se aplica una regla. Las entradas de registro se pueden ver desde la ventana principal de ESET Endpoint Security en **Herramientas** > **Archivos de registro**.

4.1.3.2 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. Al seleccionar la casilla de verificación situada junto a **Activado**, se desactiva o se activa esta regla. Esto puede resultar útil si no desea eliminar la regla de forma permanente.

Tipo de dispositivo

Elija el tipo de dispositivo externo en el menú desplegable (USB/Bluetooth/FireWire/...). Los tipos de dispositivos se heredan del sistema operativo y se pueden ver en el administrador de dispositivos del sistema cada vez que se conecta un dispositivo al ordenador. El tipo de dispositivo **Almacenamiento óptico** el tipo de dispositivo del menú desplegable se refiere al almacenamiento de los datos en un medio de lectura óptica (p. ej., CD, DVD). Los dispositivos de almacenamiento abarcan discos externos o lectores de tarjetas de memoria convencionales conectados mediante USB o FireWire. Ejemplos de dispositivos de imagen son escáneres o cámaras. Los lectores de tarjetas inteligentes abarcan aquellos con un circuito integrado incrustado, como tarjetas SIM o tarjetas de autenticación.

Derechos

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 uno de los siguientes derechos:

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

Tenga en cuenta que no todos los derechos (acciones) están disponibles para todos los tipos de dispositivos. Si un dispositivo dispone de espacio de almacenamiento, las tres acciones se vuelven disponibles. Para los dispositivos que

no son de almacenamiento, solo hay dos acciones que no están disponibles para Bluetooth (por ejemplo, la acción **Solo lectura**, lo que significa que el dispositivo solo se puede permitir o bloquear).

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

- **Fabricante**: filtrado por nombre o Id. del fabricante.
- **Modelo**: el nombre del dispositivo.
- **Número de serie**: normalmente, los dispositivos 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 las tres descripciones mencionadas quedan vacías, la regla ignorará estos campos al realizar la coincidencia.

Sugerencia: para averiguar los parámetros de un dispositivo, cree una regla de permiso para los tipos de dispositivos adecuados, conecte el dispositivo a su ordenador y, a continuación, compruebe los detalles del dispositivo en el registro de control de dispositivos.

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

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

4.1.4 Sistema de prevención de intrusiones del host (HIPS)

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.

El sistema HIPS se puede encontrar en la sección **Configuración avanzada** (F5) al hacer clic en **Ordenador** > **HIPS**. El estado de HIPS (activado/desactivado) se muestra en la ventana principal de ESET Endpoint Security, en el panel **Configuración** disponible a la derecha de la sección **Ordenador**.

La configuración de HIPS se encuentra en **Configuración avanzada** (F5). Para tener acceso a HIPS en el árbol de configuración avanzada, haga clic en **Ordenador** > **HIPS**. El estado de HIPS (activado/desactivado) se muestra en la ventana principal de ESET Endpoint Security, en el panel **Configuración** disponible a la derecha de la sección Ordenador.

Alerta: solo debe modificar la configuración de HIPS si es un usuario experimentado.

ESET Endpoint Security tiene una tecnología de Autodefensa integrada que impide que el software malicioso dañe o desactive la protección antivirus y antispyware, de modo que el sistema está protegido en todo momento. Los cambios realizados en la configuración de **Activar HIPS** y **Activar la Autodefensa** se aplican después de reiniciar el sistema operativo Windows. También es necesario reiniciar el ordenador para desactivar todo el sistema **HIPS**.

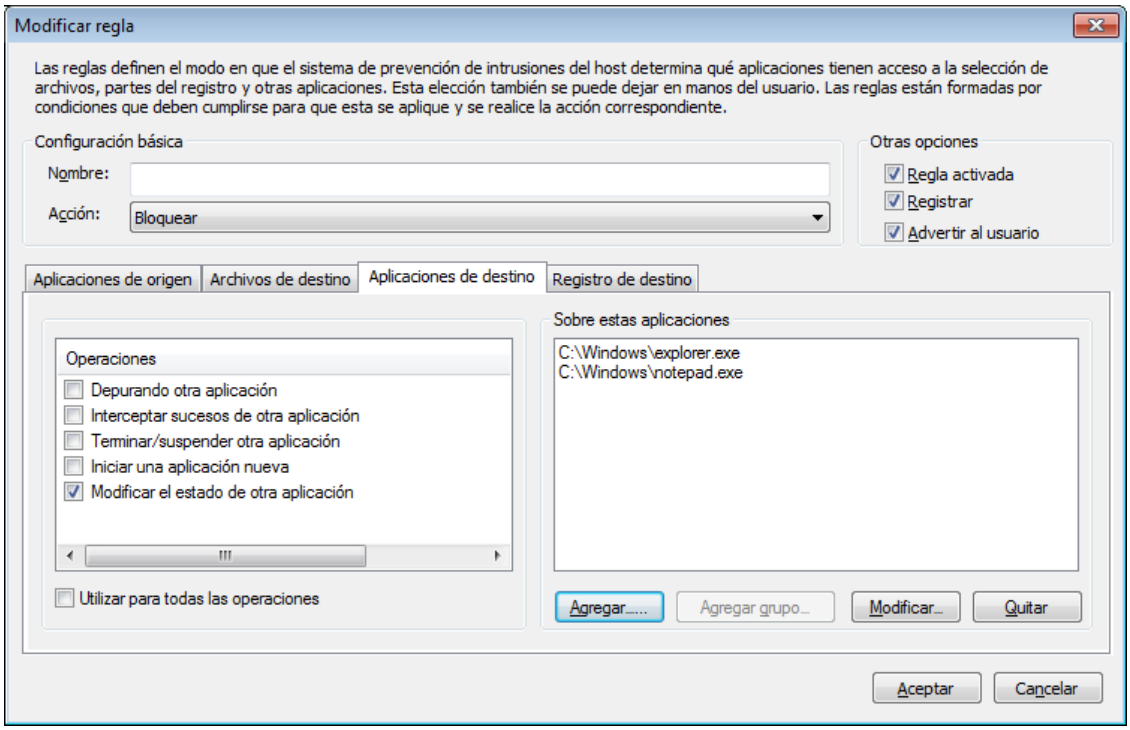
El filtrado se puede realizar en cualquiera de los cuatro modos:

- **Modo automático con reglas**: las operaciones están activadas, salvo las reglas predefinidas que protegen el sistema.
- **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. Al seleccionar **Modo de aprendizaje**, la opción **Notificar sobre el vencimiento del modo de aprendizaje en X días** pasa a estar activa. Una vez que ha transcurrido este período de tiempo, el modo de aprendizaje se desactiva otra vez. El período de tiempo máximo es de 14 días. Cuando ha transcurrido este tiempo, se abre una ventana emergente en la que puede modificar las reglas y seleccionar un modo de filtrado diferente.

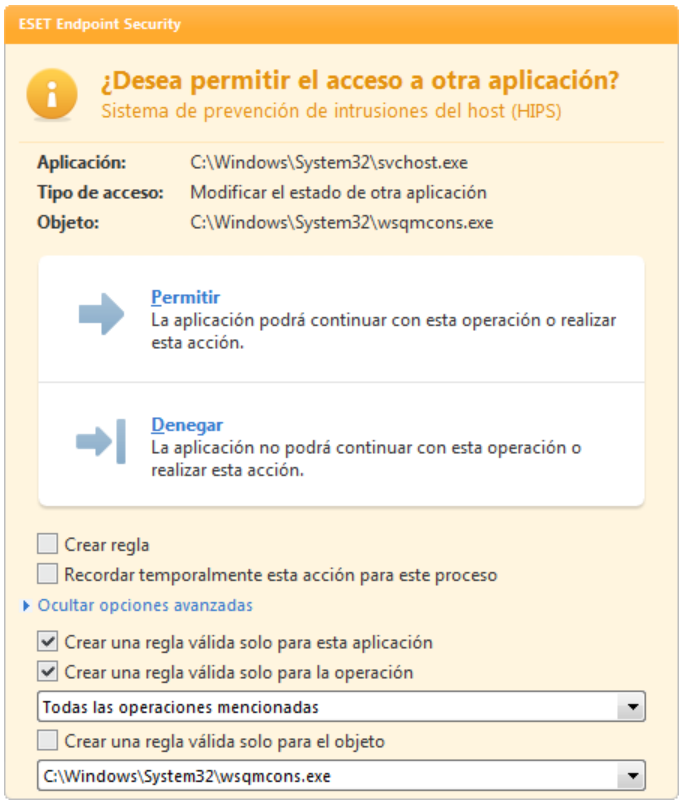
El sistema HIPS supervisa los sucesos del sistema operativo y reacciona de acuerdo con las reglas parecidas a las utilizadas por el cortafuegos personal. Haga clic en **Configurar reglas** para abrir la ventana de gestión de la regla de HIPS. Aquí puede seleccionar, crear, modificar o eliminar reglas.

En el ejemplo siguiente, veremos cómo restringir el comportamiento no deseado de las aplicaciones:

1. Asigne un nombre a la regla y seleccione **Bloquear** en el menú desplegable **Acción**.
2. Abra la ficha **Aplicaciones de destino**. Deje en blanco la ficha **Aplicaciones de origen** para aplicar su nueva regla a todas las aplicaciones que intenten realizar cualquiera de las aplicaciones marcadas en la lista **Operaciones** en las aplicaciones de la lista **Sobre estas aplicaciones**.
3. Seleccione **Modificar el estado de otra aplicación** (todas las operaciones se describen en la ayuda del producto, pulse la tecla F1 en la ventana que sea idéntica a la que aparece a continuación).
4. Agregue las aplicaciones que desee proteger.
5. Active la opción **Advertir al usuario** para mostrar una notificación al usuario cada vez que se aplique la regla.
6. Haga clic en **Aceptar** para guardar la nueva regla.



Si la acción predeterminada es **Avisar**, se mostrará un cuadro de diálogo cada vez que se vaya a realizar una operación. En este cuadro, el usuario puede **Bloquear** o **Permitir** la operación. Si el usuario 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

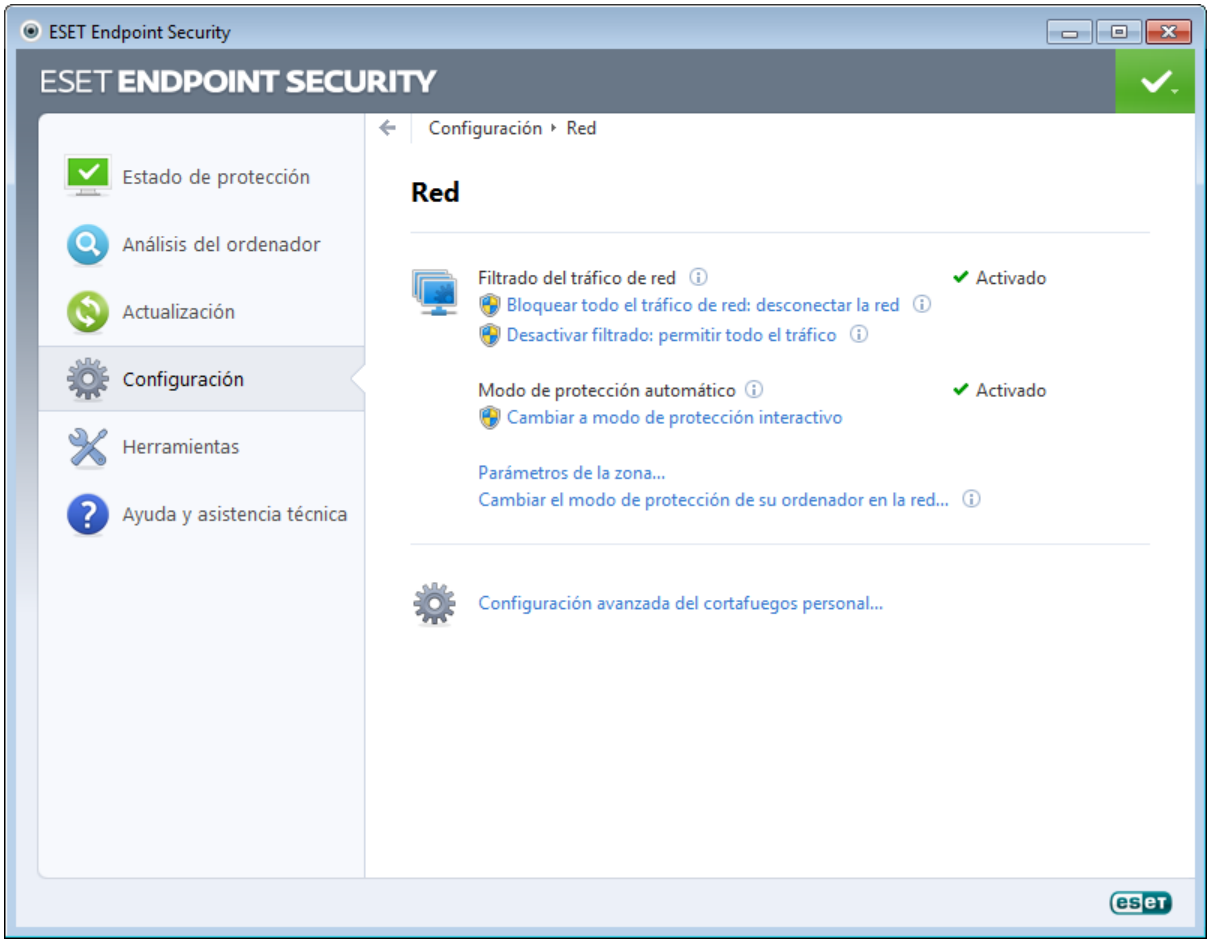
condiciones en las que se permite o se rechaza dicha acción. Los parámetros exactos se pueden consultar haciendo clic en **Mostrar opciones**. Las reglas creadas con este método se tratan igual que las creadas manualmente, por lo que una regla creada desde un cuadro de diálogo puede ser menos específica 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.

La opción **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.

4.2 Red

El cortafuegos personal se encarga de controlar todo el tráfico de red entrante y saliente del sistema. Esta tarea se lleva a cabo permitiendo o denegando conexiones de red individuales en función de las reglas de filtrado especificadas. Proporciona protección frente a ataques procedentes de ordenadores remotos y activa el bloqueo de determinados dispositivos. También ofrece protección antivirus para los protocolos HTTP, POP3 e IMAP. Esta funcionalidad representa un elemento muy importante para la seguridad del ordenador.

Puede consultar la configuración del cortafuegos personal en el panel **Configuración** haciendo clic en el título **Red**. Aquí puede ajustar el modo de filtrado, las reglas y la configuración detallada; También puede acceder a configuraciones más detalladas del programa.



La única forma de bloquear todo el tráfico de red por completo es la opción **Bloquear todo el tráfico de red: desconectar la red**. El cortafuegos personal bloqueará todas las conexiones entrantes y salientes. Utilice esta opción únicamente si considera que existen riesgos de seguridad que requieran la desconexión del sistema de la red.

La opción **Desactivar filtrado: permitir todo el tráfico** realiza la acción contraria al bloqueo de todo el tráfico de red. Si se selecciona, todas las opciones de filtrado del cortafuegos personal se desactivan y se permiten todas las conexiones entrantes y salientes. El resultado es el mismo que cuando el cortafuegos no está disponible. Cuando el filtrado del tráfico de red se encuentra en el estado **Bloqueado**, la opción **Cambiar a modo de filtrado** activa el cortafuegos.

Las opciones siguientes están disponibles cuando se activa el modo de protección automático:

- **Modo de protección automático**: para cambiar el modo de protección, haga clic en la opción **Cambiar al modo de protección interactivo**.
- **Parámetros de la zona**: muestra las opciones de configuración de la zona de confianza.

Las opciones siguientes están disponibles cuando se activa el modo de protección interactivo:

- **Modo de protección interactivo**: para cambiar el modo de protección, haga clic en **Cambiar a modo de filtrado automático** o **Cambiar a modo de filtrado automático con excepciones** en función del modo de filtrado que esté activado en ese momento.
- **Configurar reglas y zonas**: esta opción abre la ventana **Configuración de reglas y zonas**, donde se puede definir el modo de gestión de la comunicación de red por parte del cortafuegos.

Cambiar el modo de protección de su ordenador en la red: esta opción le permite elegir un modo de protección restrictiva o normal.

Configuración avanzada del cortafuegos personal: le permite acceder a las opciones de configuración avanzadas del cortafuego.

4.2.1 Modos de filtrado

Están disponibles cinco modos de filtrado para el cortafuegos personal de ESET Endpoint Security. Los modos de filtrado se pueden encontrar en la sección **Configuración avanzada** al hacer clic en **Red** > **Cortafuegos personal**. El comportamiento del cortafuegos cambia en función del modo seleccionado. Los modos de filtrado influyen igualmente en el nivel de interacción del usuario.

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

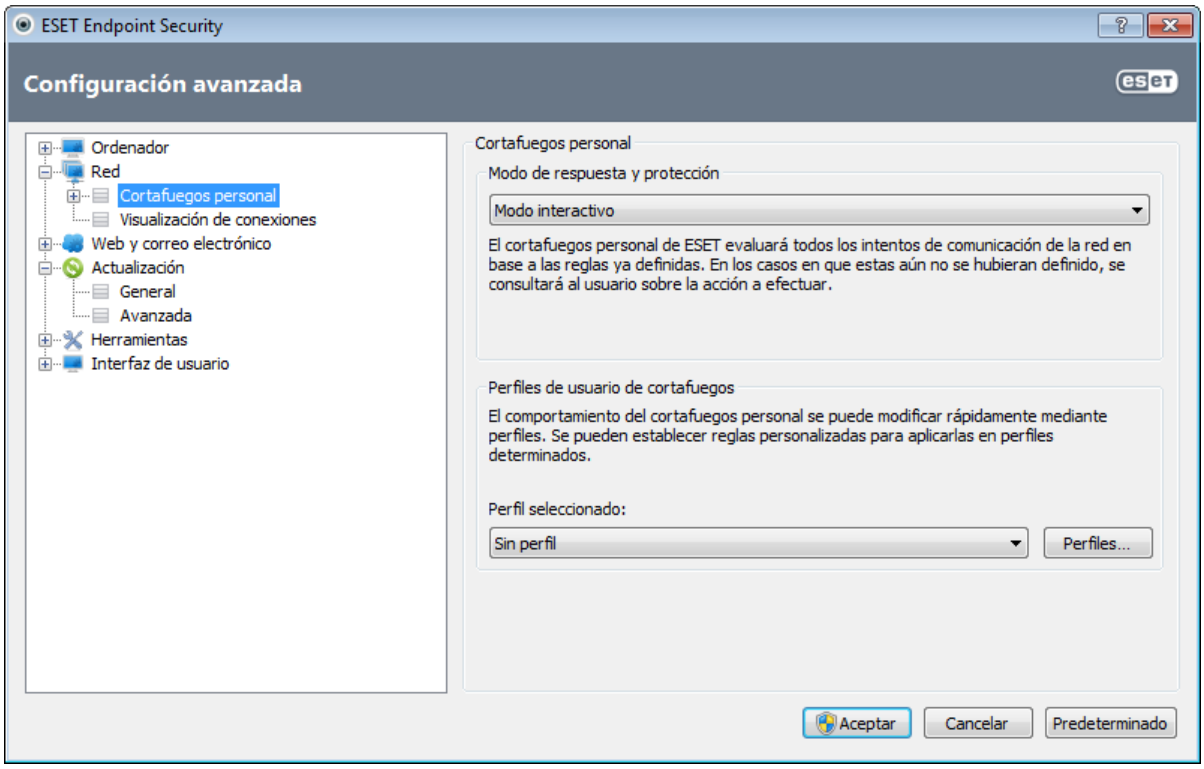
Modo automático: este es el modo predeterminado; es aconsejable para usuarios que optan por un uso sencillo y cómodo del cortafuegos sin necesidad de definir reglas. Este modo permite todo el tráfico saliente para el sistema en cuestión y bloquea todas las conexiones nuevas iniciadas desde la ubicación remota.

Modo automático con excepciones (reglas definidas por el usuario): a las características del modo automático, suma la posibilidad de agregar reglas personalizadas definidas por el usuario.

Modo interactivo: le permite crear una configuración personalizada para el cortafuegos personal. Cuando se detecta una comunicación para la que no existen reglas, aparece un cuadro de diálogo que notifica la existencia de una conexión desconocida. El cuadro de diálogo ofrece la opción de permitir o denegar la comunicación; la decisión de permitirla o denegarla se puede recordar como una regla nueva para el cortafuegos personal. Si el usuario opta por crear una nueva regla en este momento, todas las conexiones futuras de este tipo se permitirán o bloquearán de acuerdo con dicha regla.

Modo basado en reglas: bloquea todas las conexiones que no se hayan definido en una regla específica que las permita. Este modo permite a los usuarios avanzados definir reglas que autoricen únicamente las conexiones especificadas y seguras. El cortafuegos personal bloqueará todas las demás conexiones no especificadas.

Modo de aprendizaje: crea y guarda reglas automáticamente; es adecuado para la configuración inicial del cortafuegos personal. No es necesaria la intervención del usuario, pues ESET Endpoint Security guarda las reglas según los parámetros predefinidos. El modo de aprendizaje no es seguro y solo debe utilizarse hasta que se hayan creado todas las reglas para las comunicaciones necesarias.

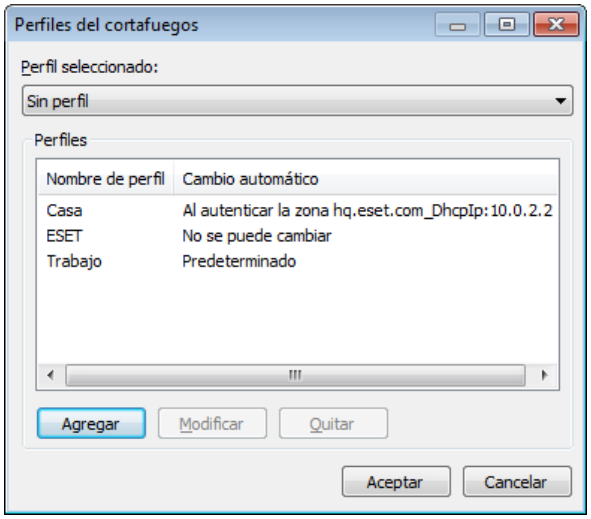


Los perfiles son una herramienta que sirve para controlar el comportamiento del cortafuegos personal de ESET Endpoint Security.

4.2.2 Perfiles del cortafuegos

Los perfiles se pueden utilizar para controlar el comportamiento del cortafuegos personal de ESET Endpoint Security. Cuando cree o edite una regla para el cortafuegos personal, puede asignarla a un perfil específico o a todos los perfiles. Al seleccionar un perfil, solo se aplican las reglas globales (que no tienen un perfil especificado) y las reglas que se han asignado a dicho perfil. Es posible crear varios perfiles con diferentes reglas asignadas, para así poder modificar fácilmente el comportamiento del cortafuegos personal.

Haga clic en el botón **Perfiles** (vea la figura de la sección Modos de filtrado) para abrir la ventana **Perfiles del cortafuegos**, donde están disponibles las opciones **Agregar**, **Modificar** y **Quitar** para perfiles. Tenga en cuenta que para **modificar** o **quitar** un perfil, este no debe estar seleccionado en el menú desplegable **Perfil seleccionado**. Cuando agregue o modifique un perfil, también puede definir condiciones que lo activen.

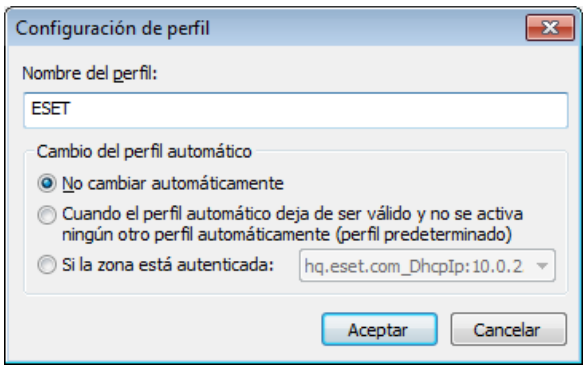


Cuando cree un perfil, puede seleccionar sucesos que lo activen. Están disponibles las opciones siguientes:

- **No cambiar automáticamente**: la activación automática está desactivada (el perfil debe activarse manualmente).
- **Cuando el perfil automático deja de ser válido y no se activa ningún otro perfil automáticamente (perfil predeterminado)**: cuando el perfil automático deja de ser válido (el ordenador se conecta a una red que no es de confianza; consulte la sección Autenticación de red) y no se activa ningún otro perfil en su lugar (el ordenador no se conecta a otra red de confianza), el cortafuegos personal pasará a utilizar este perfil. Esta activación solo puede

utilizarla un perfil.

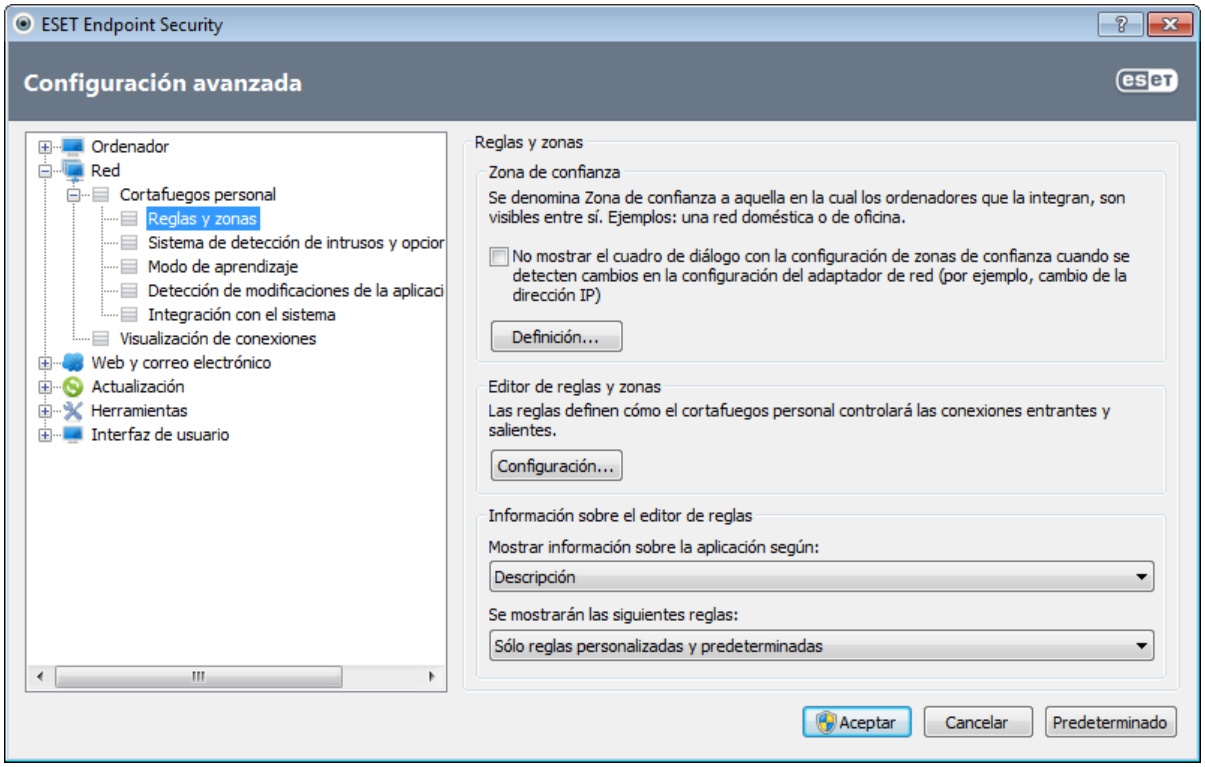
- **Si la zona está autenticada**: este perfil se activará cuando se autentique una zona específica (consulte la sección Autenticación de red).



Cuando el cortafuegos personal cambia de perfil, se muestra una notificación en la esquina inferior derecha, cerca del reloj del sistema.

4.2.3 Configuración y uso de reglas

Las reglas representan un conjunto de condiciones que se utilizan para probar de manera significativa todas las conexiones de red y acciones asignadas a estas condiciones. En el cortafuegos personal, puede definir la acción que desee siempre que se haya establecido una conexión definida por una regla. Para acceder a la configuración del filtro de reglas, vaya a **Configuración avanzada** (F5) > **Red** > **Cortafuegos personal** > **Reglas y zonas**.



Haga clic en el botón **Configuración...** de la sección **Zona de confianza** para ver el cuadro de diálogo Configuración de la zona de confianza. La opción **No mostrar el cuadro de diálogo con parámetros de la zona de confianza...** permite al usuario desactivar la ventana Configuración de la zona de confianza cada vez que se detecta la presencia de una subred nueva. Se utiliza automáticamente la configuración de la zona especificada actualmente.

NOTA: si el cortafuegos personal se establece en el **Modo automático**, algunos ajustes no estarán disponibles.

Haga clic en el botón Configuración... de la sección **Editor de reglas y zonas** para ver la ventana **Configuración de reglas y zonas**, donde se muestra una descripción general de las reglas o zonas (en función de la ficha seleccionada en ese momento). La ventana se divide en dos secciones: En la sección superior se enumeran todas las reglas en una vista abreviada y en la sección inferior se muestra información detallada acerca de la regla seleccionada actualmente en la sección superior. En la parte inferior de la ventana, se encuentran los botones **Nuevo**, **Modificar** y **Eliminar (Supr)**, que le permiten configurar las reglas.

Las conexiones se pueden dividir en entrantes y salientes. Las conexiones entrantes se inician en ordenadores remotos que intenten establecer una conexión con el sistema local y las conexiones salientes funcionan de la forma opuesta, es decir, el sistema local se comunica con el ordenador remoto.

Si se detecta una comunicación desconocida, debe considerar detenidamente el hecho de permitirla o denegarla. Las conexiones no solicitadas, no seguras o desconocidas suponen un riesgo de seguridad para el sistema. Si se establece una conexión de este tipo, debe prestar especial atención al ordenador remoto y a la aplicación que intente conectarse a su ordenador. Muchas amenazas intentan obtener y enviar datos privados, o descargar otras aplicaciones maliciosas en las estaciones de trabajo host. El cortafuegos personal le permite detectar e interrumpir estas conexiones.

Mostrar información sobre la aplicación según: le permite definir la visualización de las aplicaciones en la lista de reglas. Están disponibles las opciones siguientes:

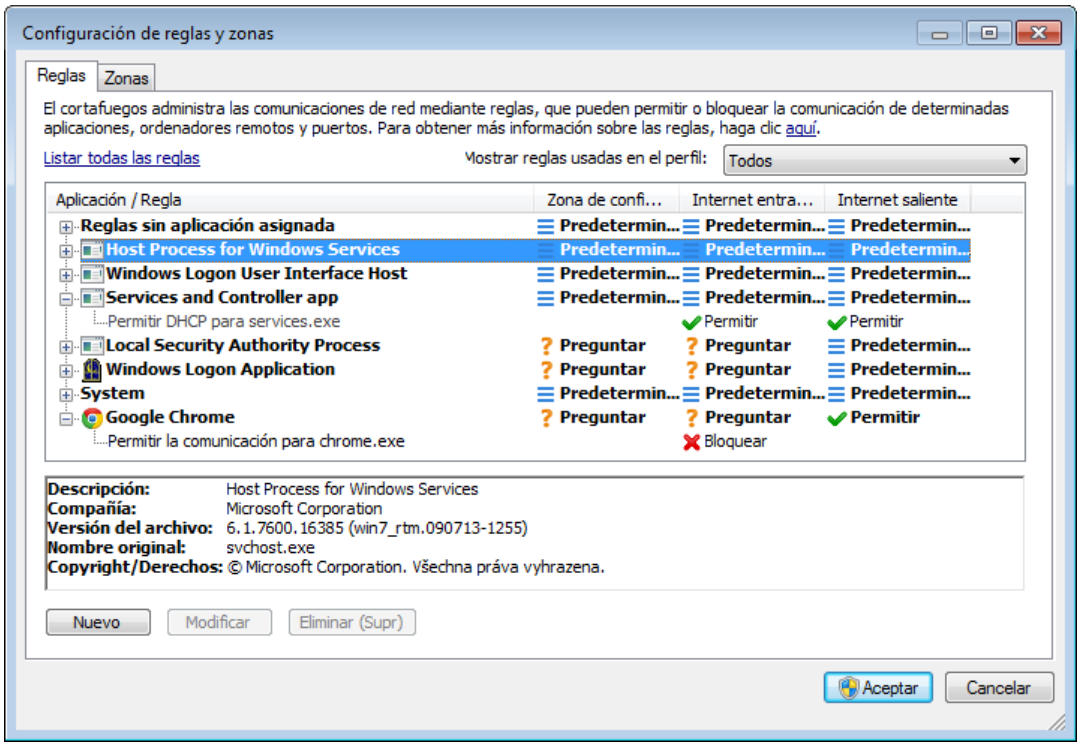
- **Ruta completa**: ruta completa al ejecutable de la aplicación.
- **Descripción**: descripción de la aplicación.
- **Nombre**: nombre del archivo ejecutable de la aplicación

Seleccione el tipo de reglas que se mostrarán en la lista **Se mostrarán las siguientes reglas**:

- **Solo reglas definidas por el usuario**: muestra solo las reglas creadas por el usuario.
- **Solo reglas personalizadas y predeterminadas**: muestra todas las reglas predefinidas predeterminadas y definidas por el usuario.
- **Todas las reglas (incluidas las del sistema)**: se muestran todas las reglas.

4.2.3.1 Configuración de reglas

La configuración de reglas le permite ver todas las reglas aplicadas al tráfico generado por aplicaciones individuales dentro de zonas de confianza e Internet. Las reglas se agregan automáticamente de forma predeterminada, de acuerdo con las reacciones de los usuarios ante una comunicación nueva. Si hace clic en el nombre de la aplicación, podrá ver más información acerca de ella en la parte inferior de esta ventana.



Al comienzo de cada línea correspondiente a una regla aparece un botón que le permite expandir o contraer (+/-) la información. Haga clic en el nombre de la aplicación en la columna **Aplicación/Regla** para que se muestre información acerca de la regla en la parte inferior de esta ventana. Puede utilizar el menú contextual para cambiar el modo de visualización. El menú contextual también se puede utilizar para añadir, editar y eliminar reglas.

Zona de confianza entrante/saliente: acciones relacionadas con la comunicación entrante o saliente dentro de la zona de confianza.

Internet entrante/saliente: acciones relacionadas con la conexión a Internet en la comunicación entrante o saliente.

Para cada tipo (dirección) de comunicación, puede seleccionar estas acciones:

- **Permitir**: para permitir la comunicación.
- **Preguntar**: se le solicitará que elija entre permitir o denegar cada vez que se establece la comunicación.
- **Denegar**: para denegar la comunicación.
- **Específico**: no se puede clasificar con respecto a las demás acciones. Por ejemplo, si el cortafuegos personal autoriza una dirección IP o puerto, no se puede determinar con seguridad si se permiten las comunicaciones entrantes o salientes de una aplicación relacionada.

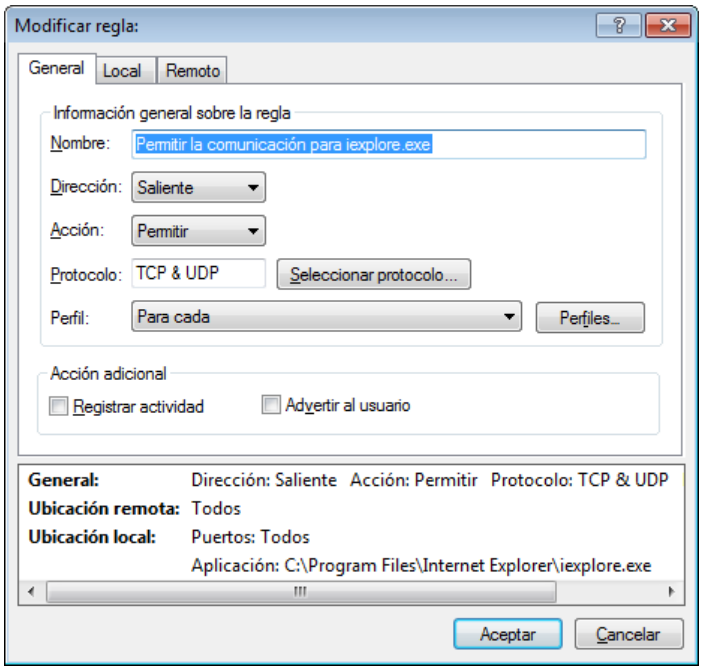
Cuando se instala una nueva aplicación que puede acceder a la red o se lleva a cabo una modificación en una conexión existente (ubicación remota, número de puerto, etc.), es necesario crear una regla nueva. Para modificar una regla existente, compruebe que la ficha **Reglas** esté seleccionada y haga clic en el botón **Modificar**.

4.2.3.2 Modificación de reglas

Esta modificación es necesaria cada vez que se cambia alguno de los parámetros controlados. En este caso, la regla no puede cumplir las condiciones y no es posible aplicar la acción especificada. Si los parámetros han cambiado, es probable que se rechace la conexión en cuestión, lo que puede conllevar problemas relacionados con el funcionamiento de la aplicación correspondiente. Un ejemplo de este caso sería la modificación de la dirección de red o del número de puerto de la ubicación remota.

En la parte superior de la ventana están disponibles las tres fichas siguientes:

- **General**: especifica un nombre de regla, la dirección de la conexión, la acción, el protocolo y el perfil al que se aplicará la regla.
- **Local**: muestra información sobre el punto local de la conexión, incluido el número del puerto local, o el intervalo de puertos, y el nombre de la aplicación que intenta establecer la comunicación.
- **Remoto**: esta ficha contiene información acerca del puerto remoto (o intervalo de puertos). También le permite definir una lista de zonas o direcciones IP remotas para una regla determinada.



Protocolo representa el protocolo de transferencia utilizado para la regla. Haga clic en **Seleccionar protocolo** para abrir la ventana Selección de protocolo.

Todas las reglas están activadas **Para cada** perfil de forma predeterminada. También puede seleccionar un perfil de cortafuegos personalizado con el botón **Perfiles...**.

Si hace clic en **Registro**, la actividad relacionada con la regla se anotará en un registro. La opción **Advertir al usuario** muestra una notificación cuando se aplica la regla.

En el cuadro de diálogo de información se proporciona un resumen de la regla, en la parte inferior de las tres pestañas. Verá la misma información si hace clic en la regla en la ventana principal (**Herramientas** > **Conexiones de red**; haga clic con el botón derecho del ratón en la regla y active la opción **Mostrar detalles** [consulte el capítulo Conexiones de red]).

Cuando cree una regla nueva, debe introducir un nombre para la regla en el campo **Nombre**. Seleccione la dirección a la que se aplicará la regla en el menú desplegable **Dirección**. Defina la acción que se ejecutará cuando una comunicación

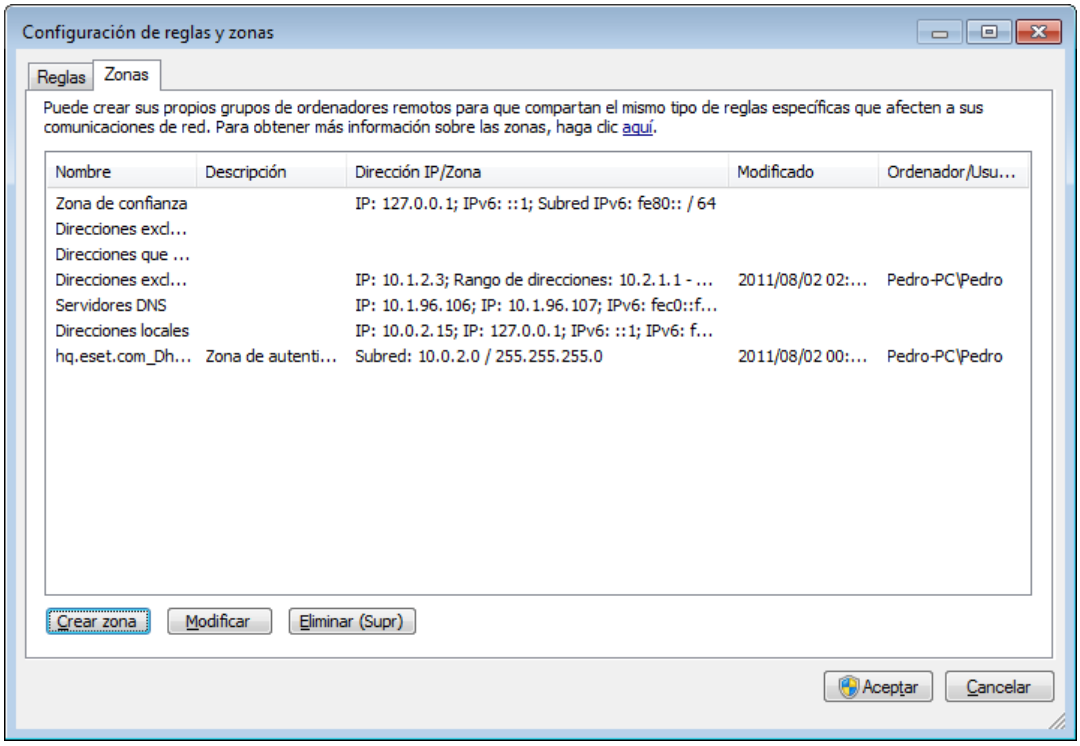
cumpla la regla en el menú desplegable **Acción**.

Un buen ejemplo de la adición de una nueva regla es el de permitir a su navegador de Internet acceder a la red. En este caso, es necesario realizar la siguiente configuración:

- En la pestaña **General** active la comunicación saliente a través de los protocolos TCP y UDP.
- Agregue el proceso que represente la aplicación de su navegador (para Internet Explorer es iexplore.exe) en la pestaña **Local**.
- En la ficha **Remoto**, active el número de puerto 80 únicamente si desea permitir las actividades de búsqueda estándar en Internet.

4.2.4 Configuración de zonas

En la ventana **Parámetros de la zona** se puede especificar el nombre, la descripción, la lista de direcciones de red y la autenticación de la zona (consulte Autenticación de zona: configuración de cliente.



Una zona es una recopilación de direcciones de red que conforman un grupo lógico. A cada dirección del grupo concreto se le asignan reglas similares definidas de manera centralizada para todo el grupo. Un ejemplo de dicho grupo es la **Zona de confianza**. La Zona de confianza representa un grupo de direcciones de red en las que el usuario puede confiar completamente y que no están bloqueadas de forma alguna por el cortafuegos personal.

Para configurar estas zonas, haga clic en el botón **Modificar** de la ficha **Zonas** disponible en la ventana **Configuración de reglas y zonas**. Escriba un **Nombre** y una **Descripción** para la zona y haga clic en el botón **Agregar dirección IPv4/IPv6** para agregar una dirección IP remota.

4.2.4.1 Autenticación de red

En los ordenadores portátiles, se recomienda comprobar la credibilidad de la red con la que se va a establecer la conexión. La zona de confianza se identifica mediante la dirección IP local del adaptador de red. Es frecuente que los ordenadores portátiles accedan a redes con direcciones IP similares a la red de confianza. Si no cambia la configuración de la zona de confianza manualmente a **Protección restrictiva**, el cortafuegos personal seguirá utilizando el modo **Protección con uso compartido**.

Se recomienda utilizar la autenticación de zona para evitar este tipo de situaciones.

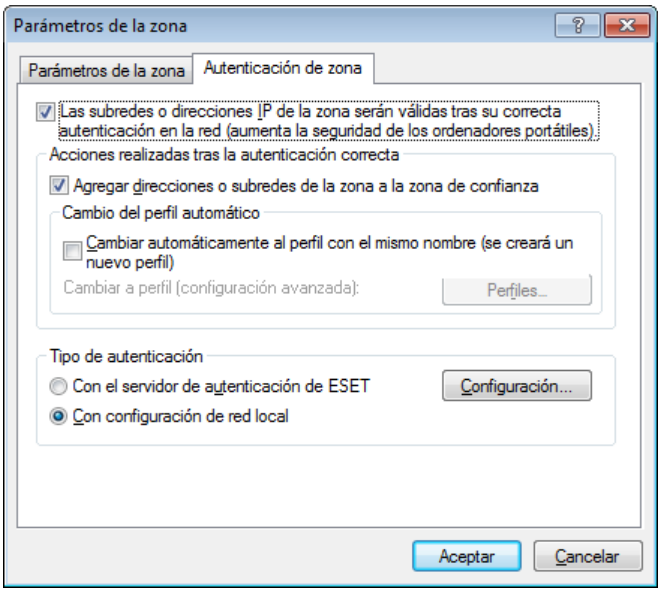
4.2.4.1.1 Autenticación de zona: configuración de cliente

En la ventana **Configuración de reglas y zonas**, haga clic en la ficha **Zonas** y cree una zona nueva con el nombre de la zona autenticada por el servidor. A continuación, haga clic en **Agregar dirección IPv4** y seleccione la opción **Subred** para agregar una máscara de subred que contenga el servidor de autenticación.

Haga clic en la ficha **Autenticación de zona**. Todas las zonas se pueden definir para su autenticación en el servidor. La zona (su dirección IP y subred) será válida cuando se haya autenticado correctamente; esto quiere decir que las acciones como cambiar a un perfil de cortafuegos y agregar una dirección o subred de la zona a la zona de confianza no se realizarán hasta que el usuario se haya autenticado.

Seleccione la opción **Las direcciones IP o subredes de la zona serán válidas...** para crear una zona que no sea válida si la autenticación no se realiza correctamente. Para seleccionar un perfil de cortafuegos personal que se active tras una autenticación de zona correcta, haga clic en el botón **Perfiles**.

Si selecciona la opción **Agregar direcciones o subredes de la zona a la zona de confianza** (recomendado), tras una autenticación correcta se agregarán a la zona de confianza todas las direcciones o subredes de la zona. Si la autenticación falla, las direcciones no se agregarán a la zona de confianza. Si la opción **Cambiar automáticamente al perfil con el mismo nombre (se creará un nuevo perfil)** está activa, se creará un perfil nuevo tras una autenticación correcta. Haga clic en el botón **Perfiles** para abrir la ventana Perfiles del cortafuegos.



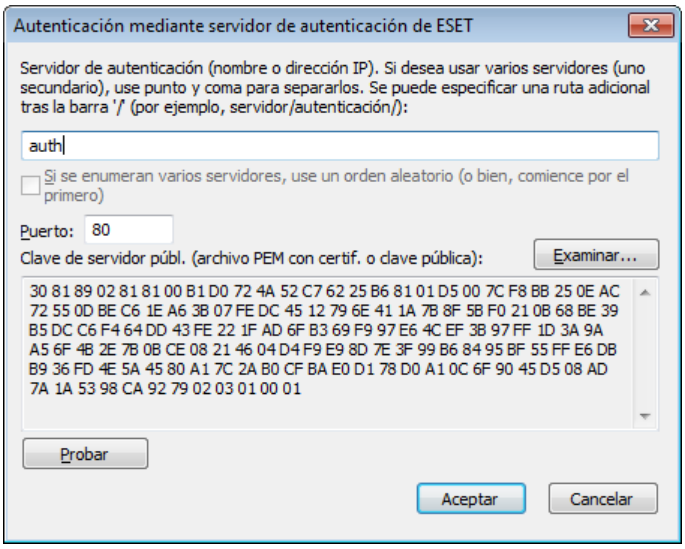
Son posibles dos tipos de autenticación:

1) Con el servidor de autenticación de ESET

La autenticación de zona busca un servidor específico de la red y utiliza el cifrado asimétrico (RSA) para autenticar al servidor. El proceso de autenticación se repite para todas las redes a las que se conecta el ordenador. Haga clic en **Configuración** y especifique un nombre de usuario, un puerto de escucha del servidor y una clave pública correspondiente a la clave de servidor privado (consulte la sección Autenticación de zona: Configuración de servidor). El nombre de servidor se puede especificar en formato de dirección IP, DNS o nombre de NetBios. El nombre de servidor puede ir seguido de la ruta correspondiente a la ubicación de la clave en el servidor (por ejemplo, nombre_servidor_/directorio1/directorio2/autenticación). Especifique varios servidores, separados por punto y coma, para que actúen como servidores alternativos cuando el primero no esté disponible.

La clave pública puede ser un archivo de los tipos siguientes:

- Clave pública cifrada PEM (.pem)
  Esta clave se puede generar con ESET Authentication Server (consulte la sección Autenticación de zona: configuración de servidor).
- Clave pública cifrada
- Certificado de clave pública (.crt)



Haga clic en el botón **Probar** para comprobar la configuración. Si la autenticación es correcta, aparecerá un mensaje Autenticación del servidor correcta. Si la autenticación no está configurada correctamente, aparecerá uno de los mensajes de error siguientes:

Error en la autenticación del servidor. Se ha alcanzado el tiempo máximo para la autenticación.
No se puede acceder al servidor de autenticación. Compruebe el nombre de servidor o la dirección IP, y verifique la configuración del cortafuegos personal del cliente y la sección del servidor.

Error al comunicarse con el servidor.
El servidor de autenticación no está en ejecución. Inicie el servicio del servidor de autenticación (consulte la sección Autenticación de zona: Configuración de servidor).

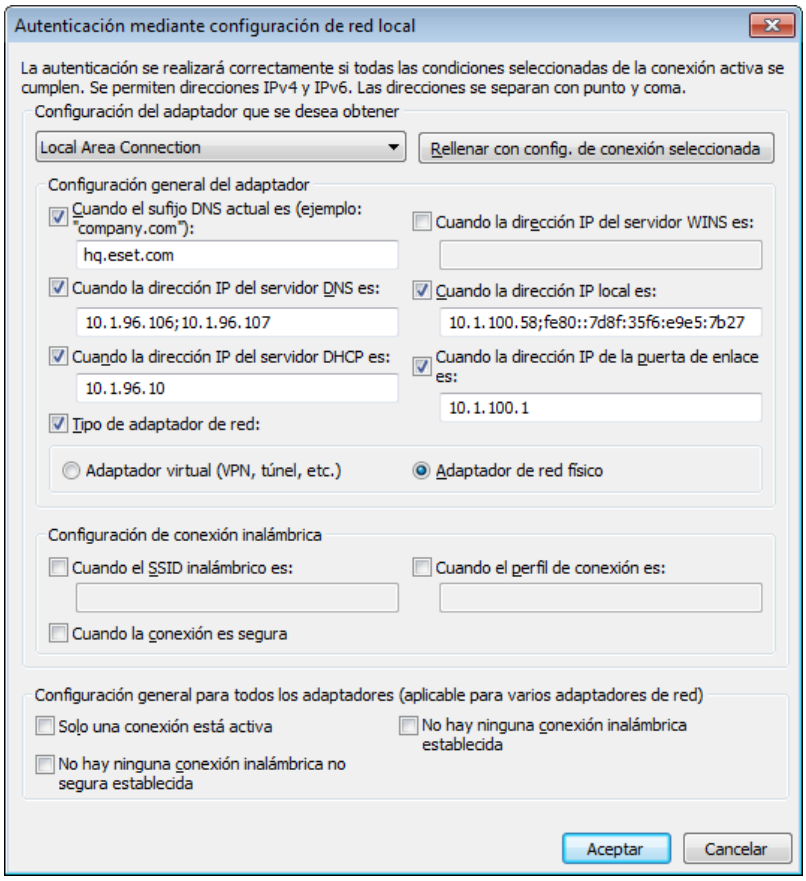
El nombre de la zona de autenticación no coincide con la zona del servidor.
El nombre de la zona configurada no se corresponde con la zona del servidor de autenticación. Compruebe que los nombres de ambas zonas son idénticos.

Error en la autenticación del servidor. No se encontró la dirección del servidor en la lista de direcciones para la zona determinada.
La dirección IP del ordenador que ejecuta el servidor de autenticación no se encuentra en el rango de direcciones IP definido en la configuración de zona actual.

Error en la autenticación del servidor. Probablemente se ha introducido una clave pública no válida.
Compruebe que la clave pública especificada se corresponde con la clave de servidor privado. Asegúrese también de que el archivo de clave pública no está dañado.

2) Con configuración de red local

La autenticación se realiza de acuerdo con los parámetros de un adaptador de red local y es correcta si todos los parámetros seleccionados para la conexión activa son válidos.



4.2.4.1.2 Autenticación de zona: configuración de servidor

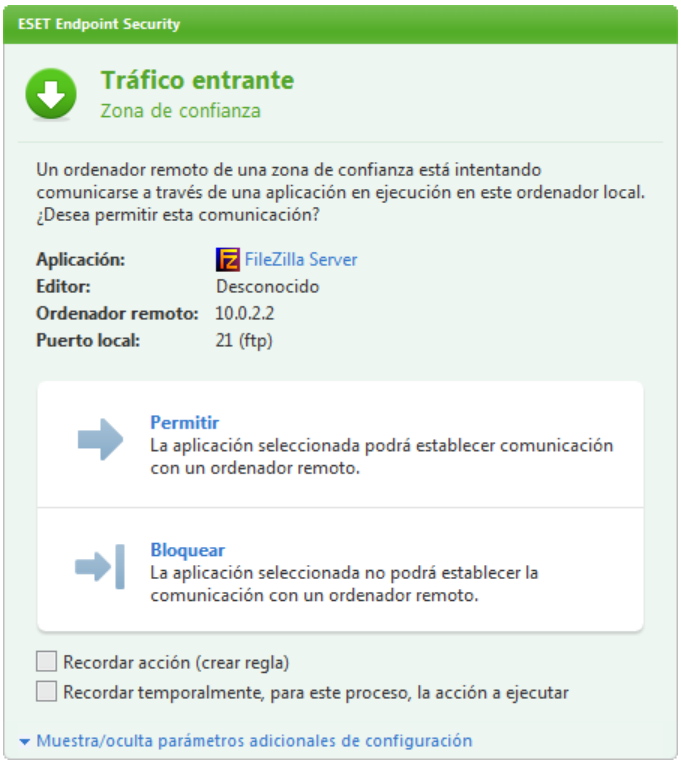
Cualquier ordenador/servidor que esté conectado a la red en cuestión puede iniciar el proceso de autenticación. La aplicación ESET Authentication Server se debe instalar en un ordenador/servidor que siempre esté disponible para la autenticación cuando un cliente intente conectarse a la red. El archivo de instalación de la aplicación ESET Authentication Server se puede descargar del sitio web de ESET.

Una vez que haya instalado la aplicación ESET Authentication Server, aparecerá un cuadro de diálogo (puede acceder a la aplicación haciendo clic en **Inicio** > **Programas** > **ESET** > **ESET Authentication Server**).

Para configurar el servidor de autenticación, introduzca el nombre de la zona de autenticación, el puerto de escucha del servidor (el puerto predeterminado es 80) y la ubicación donde se almacena el par de claves pública y privada. A continuación, genere las claves pública y privada que se utilizarán en el proceso de autenticación. La clave privada permanecerá en el servidor y la clave pública hay que importarla en el cliente, en la sección Autenticación de zona, para configurar una zona en la configuración del cortafuegos.

4.2.5 Establecimiento de una conexión: detección

El cortafuegos personal detecta cualquier conexión de red nueva. El modo del cortafuegos activo determina las acciones que se deben realizar para la nueva regla. Si el **Modo automático** o el **Modo basado en reglas** están activados, el cortafuegos personal realizará las acciones predefinidas sin la interacción del usuario. El modo interactivo muestra una ventana informativa que notifica la detección de una nueva conexión de red, con información adicional acerca de dicha conexión. Tiene la opción de permitir la conexión o de rechazarla (bloquearla). Si permite la misma conexión en el cuadro de diálogo en repetidas ocasiones, es aconsejable que cree una regla nueva para la conexión. Para realizar esta tarea, seleccione la opción **Recordar acción (crear regla)** y guarde la acción como una regla nueva para el cortafuegos personal. Si el cortafuegos reconoce la misma conexión en el futuro, aplicará la regla existente sin necesidad de que intervenga el usuario.



Cuando cree reglas nuevas tenga cuidado de aceptar únicamente conexiones seguras. Si permite todas las conexiones, el cortafuegos personal no podrá cumplir su finalidad. A continuación, se indican una serie de parámetros importantes para las conexiones:

- **Ubicación remota**: permitir únicamente conexiones a direcciones conocidas y de confianza.
- **Aplicación local**: no se aconseja permitir conexiones de aplicaciones y procesos desconocidos.
- **Número de puerto**: en circunstancias normales, se debe permitir la comunicación en puertos comunes (el número de puerto 80 para el tráfico de Internet, por ejemplo).

Con el fin de proliferar, las amenazas informáticas suelen utilizar Internet y conexiones ocultas que les ayudan a infectar sistemas remotos. Si las reglas se configuran correctamente, un cortafuegos personal puede convertirse en una herramienta muy útil para la protección frente a distintos ataques de código malicioso.

4.2.6 Registro

El cortafuegos personal de ESET Endpoint Security guarda todos los sucesos importantes en un archivo de registro que se puede ver directamente en el menú principal. Haga clic en **Herramientas** > **Archivos de registro** y, a continuación, seleccione **Registros del cortafuegos personal de ESET** en el menú desplegable **Registro**.

Los archivos de registro son una valiosa herramienta para la detección de errores e intrusiones en el sistema. Los registros del cortafuegos personal de ESET contienen los siguientes datos:

- Fecha y hora del suceso
- Nombre del suceso
- Origen
- Dirección de la red de destino
- Protocolo de comunicación de red
- Regla aplicada o nombre del gusano (si se identifica)
- Aplicación implicada
- Usuario

Un análisis exhaustivo de estos datos puede ayudarle a detectar posibles intentos de poner en peligro la seguridad del sistema. Existen otros muchos factores que indican posibles riesgos de seguridad y le permiten minimizar el impacto: conexiones demasiado frecuentes desde ubicaciones desconocidas, intentos repetidos de establecer conexiones, comunicación de aplicaciones desconocidas o utilización de números de puertos poco comunes.

4.2.7 Integración con el sistema

El cortafuegos personal ESET Endpoint Security puede trabajar a varios niveles:

- **Todas las funciones están activadas**: el cortafuegos personal está totalmente integrado y sus componentes están activos (opción predeterminada). Si el ordenador está conectado a una red grande o a Internet, se recomienda dejar esta opción activada. Esta es la opción más segura y protege el sistema por completo.
- **El cortafuegos personal está inactivo**: el cortafuegos personal está integrado en el sistema y media en la comunicación de red, pero no comprueba la presencia de amenazas.
- **Analizar solo protocolos de aplicaciones**: solo están activos los componentes del cortafuegos personal que proporcionan análisis de protocolos de aplicaciones (HTTP, POP3, IMAP y sus versiones protegidas). Si no se analizan los protocolos de aplicaciones, se aplican la protección del sistema de archivos en tiempo real y el análisis del ordenador a petición.
- **El cortafuegos personal está completamente desactivado**: seleccione esta opción para anular completamente el registro del cortafuegos personal del sistema. No se ejecuta ningún análisis. Puede ser útil durante el análisis: si se bloquea una aplicación, puede comprobar si está bloqueada por el cortafuegos. Esta es la opción menos segura, por lo que le recomendamos que sea precavido cuando desactive el cortafuegos por completo.

Posponer la actualización del módulo Cortafuegos personal hasta que se reinicie el ordenador: la actualización solo se descargará, y se instalará cuando el ordenador se reinicie.

4.3 Web y correo electrónico

Puede consultar la configuración de la Web y el correo electrónico en el panel **Configuración** haciendo clic en el título **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 característica **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 Security ofrece control de todas las comunicaciones realizadas desde el cliente de correo electrónico (POP3, MAPI, IMAP, HTTP).

La **Protección Antispam** filtra los mensajes de correo electrónico no solicitados.

Desactivar: desactiva la protección de la Web, del correo electrónicoy antispam en los clientes de correo electrónico.

Configurar: abre la configuración avanzada de la protecciónde la Web, el correo electrónico y antispam.

Lista blanca del usuario: abre un cuadro de diálogo en el que puede agregar, modificar o eliminar direcciones de correo electrónico que se consideran seguras. Los mensajes de correo electrónico cuyo remitente se encuentre en la lista blanca no se analizarán en buscan de correo no deseado.

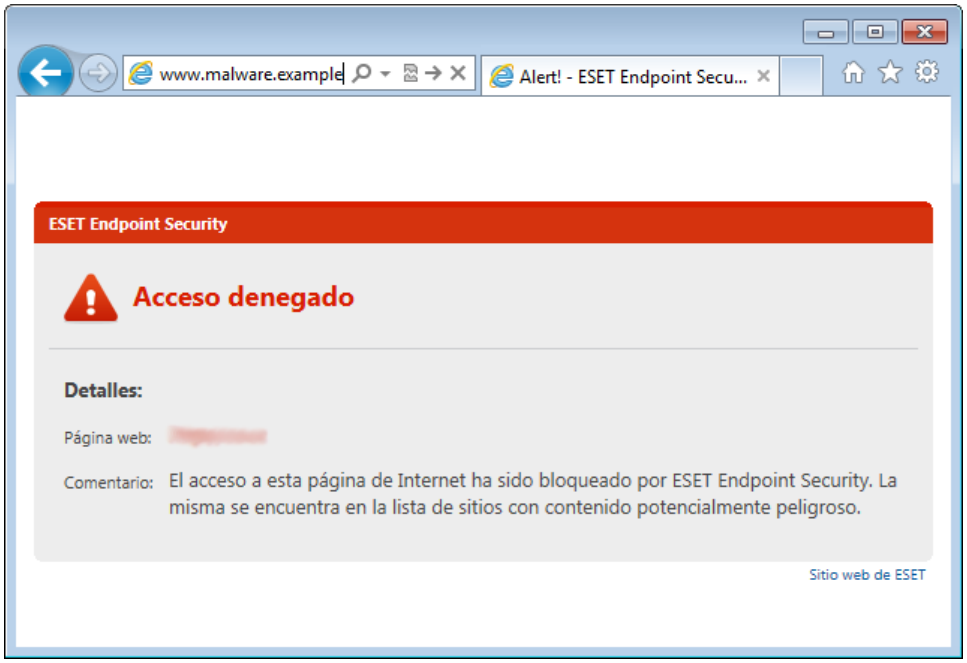
Lista negra del usuario: abre un cuadro de diálogo en el que puede agregar, modificar o eliminar direcciones de correo electrónico que se consideran seguras. Los mensajes de correo electrónico cuyo remitente se encuentre en la lista negra se clasificarán como correo no deseado.

Lista de excepciones del usuario: abre un cuadro de diálogo en el que puede agregar, modificar o eliminar direcciones de correo electrónico que se puedan falsificar y utilizar para el envío de correo no deseado. Los mensajes de correo electrónico cuyo remitente se encuentre en la lista de excepciones se analizarán siempre en buscan de correo no deseado. De forma predeterminada, la lista de excepciones contiene las direcciones de correo electrónico de las cuentas existentes del cliente de correo electrónico.

4.3.1 Protección del tráfico de Internet

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; 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 término phishing define una actividad delictiva que usa técnicas de ingeniería social (manipulación de los usuarios para obtener información confidencial). Puede obtener más información sobre esta actividad en el glosario. ESET Endpoint Security admite protección frente a la suplantación de identidad: se bloquean siempre las páginas web con dicho contenido.



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

4.3.1.1 HTTP, HTTPs

ESET Endpoint Security está configurado de forma predeterminada para utilizar los estándares de la mayoría de los navegadores de Internet. No obstante, las opciones de configuración del análisis HTTP se pueden modificar en **Configuración avanzada** (F5) > **Web y correo electrónico** > **Protección del tráfico de Internet** > **HTTP, HTTPS**. En la ventana principal de **análisis HTTP/HTTPS**, puede seleccionar o anular la selección de la opción **Activar la comprobación del protocolo HTTP**. También puede definir los números de puerto utilizados para la comunicación HTTP. De forma predeterminada, los números de puerto 80,(HTTP), 8080 y 3128 (para servidor Proxy) ya están definidos.

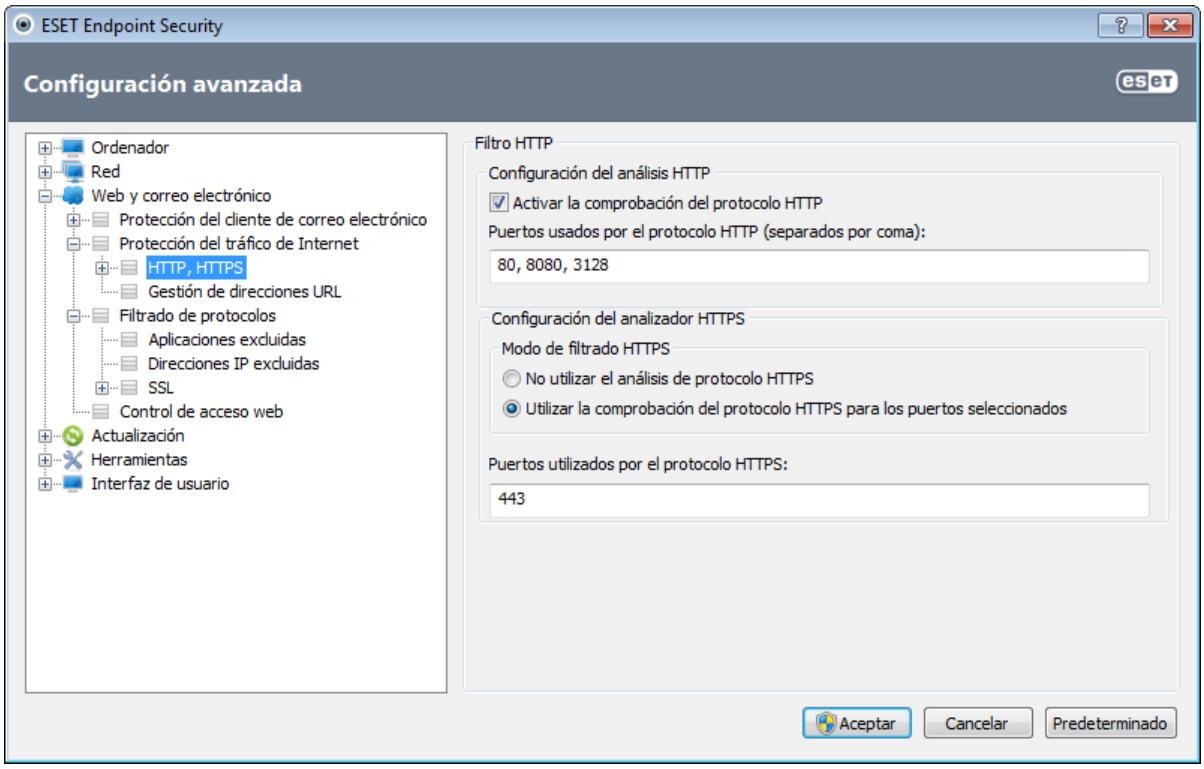
ESET Endpoint Security admite la comprobación del protocolo HTTPS. La comunicación HTTPS utiliza un canal cifrado para transferir información entre el servidor y el cliente. ESET Endpoint Security comprueba la comunicación mediante los métodos de cifrado SSL (capa de sockets seguros) y TLS (seguridad de la capa de transporte). El análisis HTTPS se puede realizar en los siguientes modos:

No utilizar la comprobación del protocolo HTTPS: no se analizará la comunicación cifrada.

Utilizar la comprobación del protocolo HTTPS para los puertos seleccionados Análisis HTTPS solo para puertos definidos en **Puertos utilizados por el protocolo HTTPS**.

Utilizar la comprobación del protocolo HTTPS para los puertos seleccionados: el programa solo analizará aquellas aplicaciones que estén especificadas en la sección navegadores y que utilicen los puertos definidos en **Puertos utilizados por el protocolo HTTPS**. El puerto 443 está configurado de forma predeterminada.

La comunicación cifrada no se analiza. Para activar el análisis de la comunicación cifrada y ver la configuración del análisis, vaya a Comprobación del protocolo SSL en la sección Configuración avanzada (**Web y correo electrónico** > **Filtrado de protocolos** > **SSL**) y active la opción **Analizar siempre el protocolo SSL**.



4.3.1.1.1 Modo activo para navegadores de Internet

ESET Endpoint Security también incluye el submenú **Modo activo**, que define el modo de análisis de los navegadores de Internet.

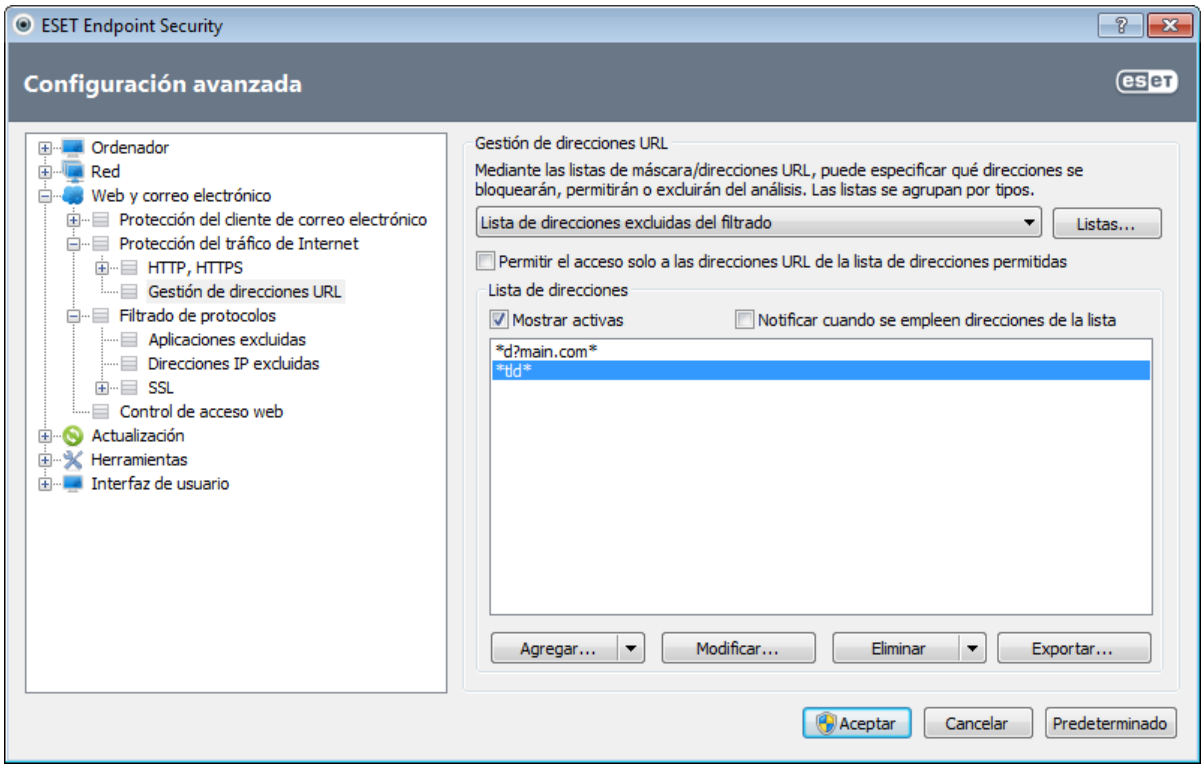
El **modo activo** es útil, ya que analiza los datos transferidos desde aplicaciones que acceden a Internet como un conjunto, independientemente de si están marcadas como navegadores de Internet o no (para obtener más información, consulte Clientes de correo electrónico y web). Si está desactivado el modo activo, la comunicación de las aplicaciones se supervisa gradualmente en lotes. Esto reduce la eficacia del proceso de verificación de datos, pero también ofrece mayor compatibilidad para las aplicaciones incluidas en la lista. Si no se produce ningún problema durante su uso, es recomendable activar el modo de análisis activo mediante la casilla de verificación situada junto a la aplicación deseada. El modo activo funciona de la siguiente manera: cuando una aplicación controlada descarga datos, primero se guardan en un archivo temporal creado por ESET Endpoint Security. Los datos no están disponibles para la aplicación en ese momento. Cuando finaliza la descarga, los datos se analizan para comprobar si hay código malicioso. Si no se detecta ninguna amenaza, los datos se envían a la aplicación original. Este proceso permite un control absoluto de las comunicaciones mediante una aplicación controlada. Si se activa el modo pasivo, los datos se envían paulatinamente a la aplicación original para evitar tiempos de espera.

4.3.1.2 Gestión de direcciones URL

En esta sección puede especificar las direcciones HTTP que desea bloquear, permitir o excluir del análisis. Los botones **Agregar**, **Modificar**, **Quitar** y **Exportar** se utilizan para gestionar las listas de direcciones. No se podrá acceder a los sitios web de la lista de direcciones bloqueadas. Se puede acceder a los sitios web de la lista de direcciones excluidas sin analizarlos en busca de código malicioso. Si selecciona la opción **Permitir el acceso solo a las direcciones URL de la lista de direcciones permitidas**, solo se podrá acceder a las direcciones presentes en la lista de direcciones permitidas; todas las demás direcciones HTTP se bloquearán.

Si añade una dirección URL a la **Lista de direcciones excluidas del filtrado**, esta dirección se excluirá del análisis. También puede permitir o bloquear determinadas direcciones añadiéndolas a la **Lista de direcciones permitidas** o **Lista de direcciones bloqueadas**. Al hacer clic en el botón **Listas...**, se abrirá la ventana **Listas de máscaras/direcciones HTTP** en la que puede **agregar** o **quitar** listas de direcciones. Para poder agregar direcciones URL HTTPS a la lista, la opción **Analizar siempre el protocolo SSL** debe estar activa.

En todas las listas, pueden utilizarse los símbolos especiales * (asterisco) y ? (signo de interrogación). El asterisco sustituye a cualquier cadena de caracteres y el signo de interrogación, a cualquier símbolo. 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. Para activar una lista, seleccione la opción **Lista activa**. Si desea que le notifiquen cuando se introduzca una dirección de la lista actual, seleccione la opción **Notificar cuando se empleen direcciones de la lista**.



Agregar/Desde archivo: Le permite agregar una dirección a la lista, bien manualmente (**Agregar**) o bien desde un archivo de texto sencillo (**Desde archivo**). La opción **Desde archivo** le permite agregar varias máscaras/direcciones URL, que se guardan en un archivo de texto.

Modificar: le permite modificar manualmente direcciones; por ejemplo agregando una máscara ("*" y "?").

Quitar/Quitar todo: haga clic en **Quitar** para quitar la dirección seleccionada de la lista. Para eliminar todas las direcciones, seleccione **Quitar todo**.

Exportar: le permite guardar direcciones de la lista actual en un archivo de texto sencillo.

4.3.2 Protección del cliente de correo electrónico

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 Security 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 que proporciona el motor de análisis ThreatSense. Esto significa que la detección de programas maliciosos tiene lugar incluso antes de que se compare con la base de firmas de virus. 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** > **Web y correo electrónico** > **Protección del cliente de correo electrónico**.

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 en **Configuración** 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 seleccionar las opciones **Notificar en los mensajes recibidos y leídos** y **Notificar en los mensajes enviados**. No es conveniente fiarse de los mensajes con etiquetas sin dudar, ya que pueden omitirse en mensajes HTML problemáticos o pueden ser falsificados por algunos virus. Los mensajes con etiqueta se pueden agregar a los mensajes recibidos y leídos o 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 advertencia en el asunto de los mensajes infectados recibidos y leídos/enviados: active esta casilla de verificación si 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.

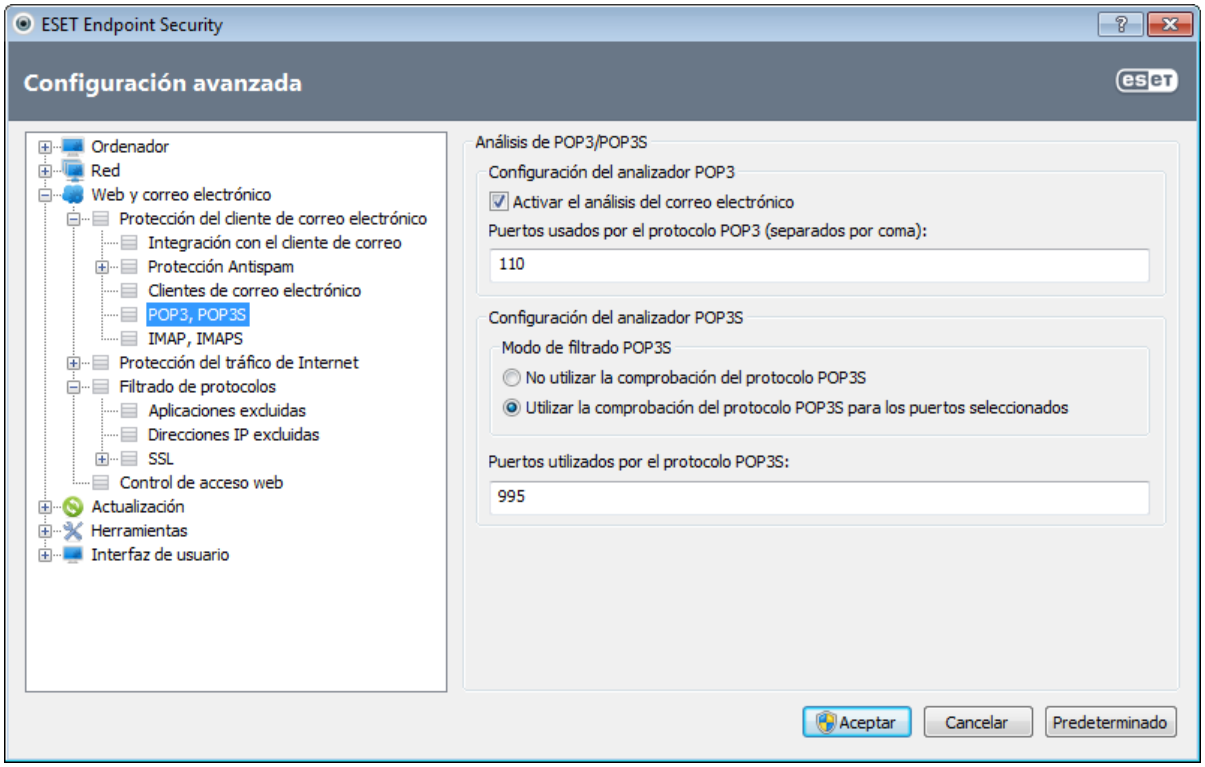
En mensajes infectados, agregar en el Asunto la siguiente etiqueta: modifique esta plantilla si desea modificar el formato de prefijo del asunto de un mensaje infectado. Esta función sustituye el asunto del mensaje "Hello" con un valor de prefijo especificado "[virus]" por el formato siguiente: "[virus]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

4.3.2.1 Filtro POP3, POP3S

El protocolo POP3 es el más utilizado para recibir comunicaciones por correo electrónico en una aplicación de cliente de correo. ESET Endpoint Security proporciona protección para este protocolo, independientemente del cliente de correo electrónico que se utilice.

El módulo de protección que proporciona este control se inicia automáticamente al arrancar el sistema y, después, está activo en la memoria. Para que el módulo funcione correctamente, asegúrese de que está activado. La comprobación del protocolo POP3 se realiza automáticamente sin necesidad de reconfigurar el cliente de correo electrónico. De forma predeterminada, se analizan todas las comunicaciones en el puerto 110, pero se pueden agregar otros puertos de comunicación si es necesario. Cuando haya varios números de puerto, deben delimitarse con una coma.

La comunicación cifrada no se analiza. Para activar el análisis de la comunicación cifrada y ver la configuración del análisis, vaya a Comprobación del protocolo SSL en la sección Configuración avanzada (**Web y correo electrónico** > **Filtrado de protocolos** > **SSL**) y active la opción **Analizar siempre el protocolo SSL**.



En esta sección, puede configurar la comprobación de los protocolos POP3 y POP3S.

Activar la comprobación del protocolo POP3: si esta opción está activada, se comprueba la presencia de software malicioso en todo el tráfico que pasa por POP3.

Puertos usados por el protocolo POP3: se trata de una lista de los puertos que utiliza el protocolo POP3 (de forma predeterminada, 110).

ESET Endpoint Security también admite la comprobación del protocolo POP3S. Este tipo de comunicación utiliza un canal cifrado para transferir información entre el servidor y el cliente. ESET Endpoint Security comprueba la comunicación mediante los métodos de cifrado SSL (capa de sockets seguros) y TLS (seguridad de la capa de transporte).

No utilizar la comprobación de POP3S: no se analizará la comunicación cifrada.

Utilizar la comprobación del protocolo POP3S para los puertos seleccionados: marque esta opción para activar el análisis POP3S solo de los puertos definidos en **Puertos utilizados por el protocolo POP3S**.

Puertos utilizados por el protocolo POP3S: consiste en una lista de puertos POP3S sujetos a análisis (de forma

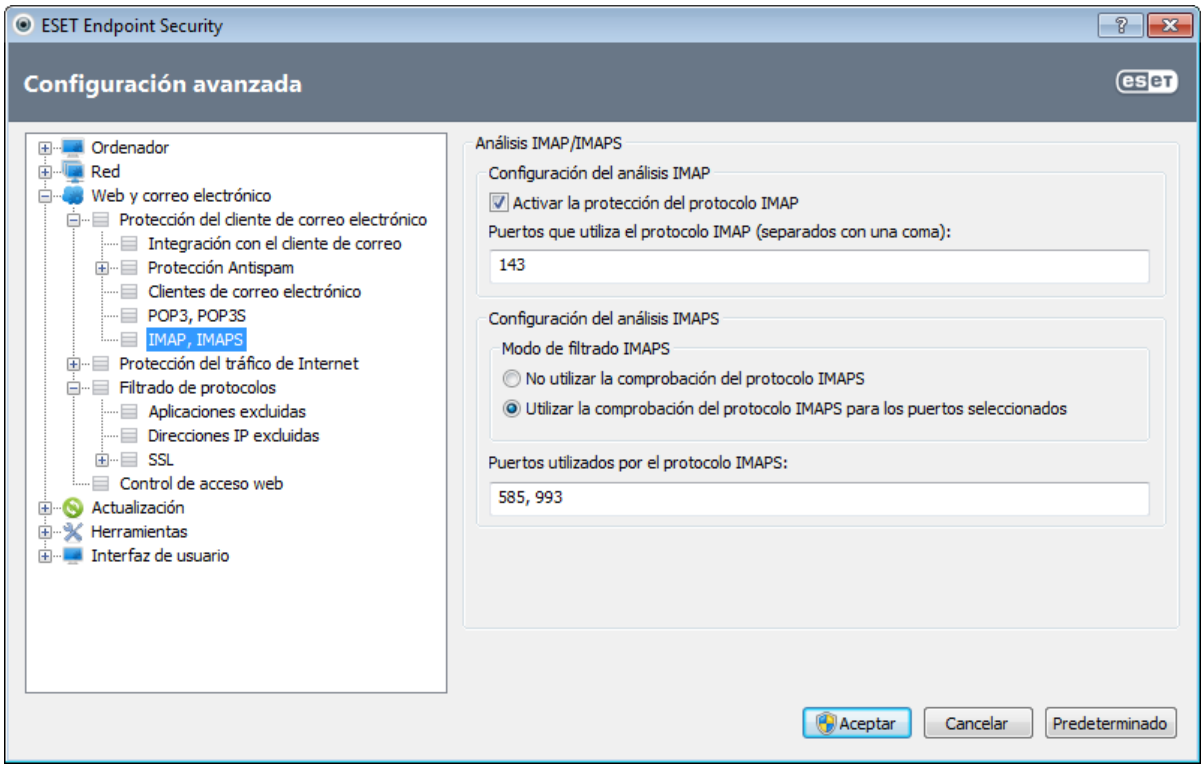
predeterminada, 995).

4.3.2.2 Control del protocolo IMAP o IMAPS

El Protocolo de acceso a mensajes de Internet (IMAP) es otro protocolo de Internet para la recuperación de mensajes de correo electrónico. IMAP presenta algunas ventajas sobre POP3; por ejemplo, permite la conexión simultánea de varios clientes al mismo buzón de correo y mantiene la información de estado (si el mensaje se ha leído, contestado o eliminado). ESET Endpoint Security ofrece protección para este protocolo independientemente del cliente de correo electrónico que se utilice.

El módulo de protección que proporciona este control se inicia automáticamente al arrancar el sistema y, después, está activo en la memoria. Para que el módulo funcione correctamente, asegúrese de que está activado; el control del protocolo IMAP se realiza automáticamente sin necesidad de reconfigurar el cliente de correo electrónico. De forma predeterminada, se analizan todas las comunicaciones en el puerto 143, pero se pueden agregar otros puertos de comunicación si es necesario. Cuando haya varios números de puerto, deben delimitarse con una coma.

La comunicación cifrada no se analiza. Para activar el análisis de la comunicación cifrada y ver la configuración del análisis, vaya a Comprobación del protocolo SSL en la sección Configuración avanzada (**Web y correo electrónico** > **Filtrado de protocolos** > **SSL**) y active la opción **Analizar siempre el protocolo SSL**.

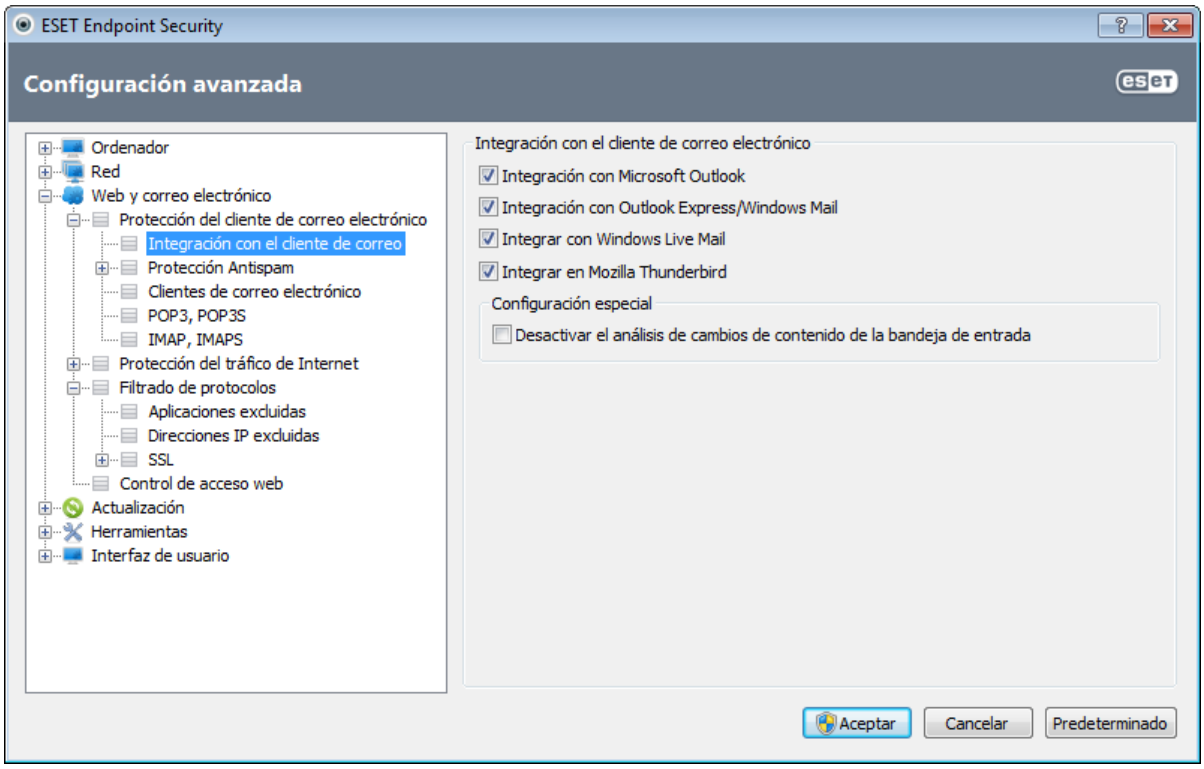


4.3.2.3 Integración con clientes de correo electrónico

La integración de ESET Endpoint Security 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, esta integración se puede activar en ESET Endpoint Security. Al activar la integración, la barra de herramientas de ESET Endpoint Security se inserta directamente en el cliente de correo electrónico, aumentando así la eficacia de la protección de correo electrónico. Las opciones de integración están disponibles en **Configuración** > **Especificar configuración avanzada** > **Web y correo electrónico** > **Protección del cliente 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, Windows Live Mail y Mozilla Thunderbird. Para ver una lista de clientes de correo electrónico compatibles y sus versiones, consulte el siguiente artículo de la base de conocimientos de ESET.

Seleccione la casilla de verificación situada junto a **Desactivar el análisis de cambios de contenido de la bandeja de entrada** si experimenta una ralentización del sistema cuando trabaja con su cliente de correo electrónico. Esta situación puede darse cuando descarga correo electrónico de Kerio Outlook Connector Store.



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).

4.3.2.3.1 Configuración de la protección del cliente de correo electrónico

El módulo de protección cliente de correo electrónico admite los siguientes clientes de correo electrónico: Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail y Mozilla Thunderbird. La protección de correo electrónico funciona como un complemento para estos programas. La principal ventaja del control 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.

Análisis de mensajes

Correo recibido: activa el análisis de los mensajes recibidos.
Analizar correo saliente: activa el análisis de los mensajes enviados.
Correo leído: activa el análisis de los mensajes leídos.

Acción a ejecutar en correos 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 mensajes a la carpeta Elementos eliminados: los mensajes infectados se moverán automáticamente a la carpeta **Elementos eliminados**.
Mover mensajes a la carpeta: especifique la carpeta personalizada a la que desea mover el correo infectado que se detecte.

Otros

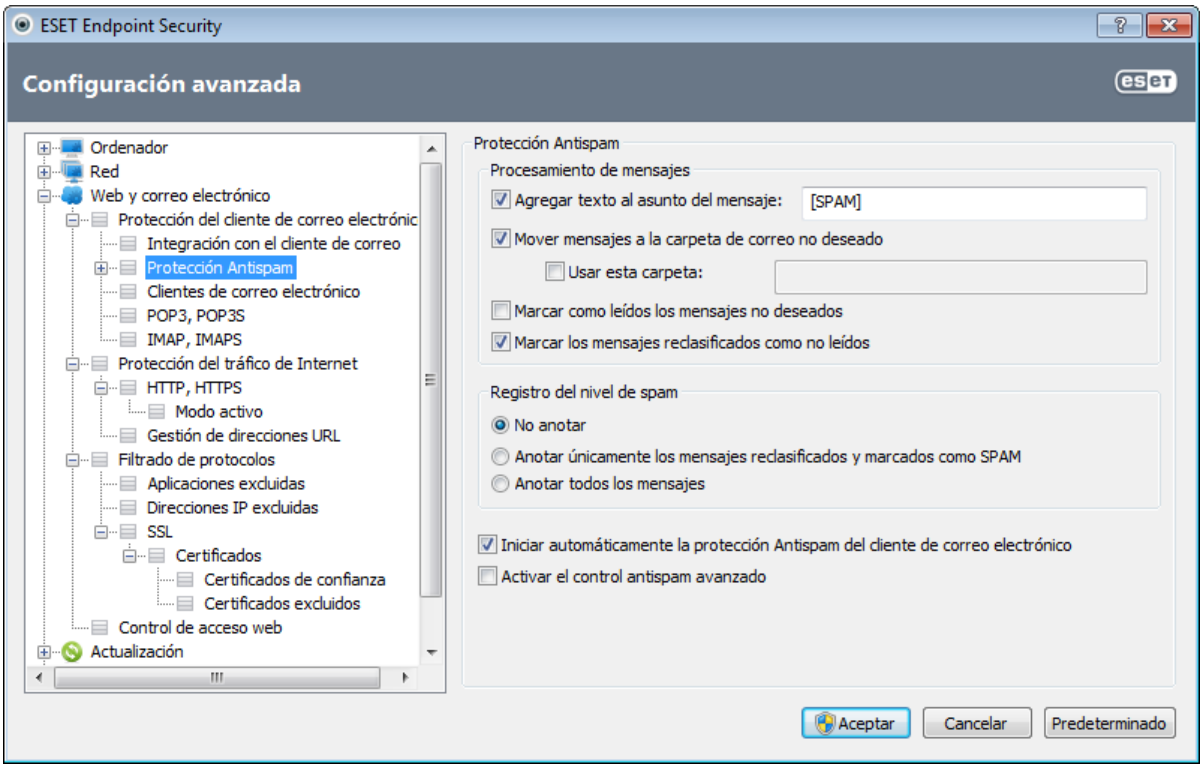
Repetir análisis después de actualizar: activa el nuevo análisis tras una actualización de la base de firmas de virus.
Incluir los análisis de otros módulos: al seleccionar esta opción, el módulo de protección de correo electrónico acepta los resultados del análisis de otros módulos de protección.

4.3.2.4 Eliminar amenazas

Si se recibe un mensaje de correo electrónico infectado, aparecerá una ventana de alerta, donde se muestra el nombre del remitente, el correo electrónico y el nombre de la amenaza. En la parte inferior de la ventana, las opciones **Desinfectar**, **Eliminar** o **Sin acciones (informar)** están disponibles para el objeto detectado. En casi todos los casos, recomendamos la selección de **Desinfectar** o **Eliminar**. En situaciones especiales, cuando desee recibir el archivo infectado, seleccione **Sin acciones (informar)**. Si la opción **Desinfección exhaustiva** está activada, aparecerá una ventana de información sin opciones disponibles para objetos infectados.

4.3.3 Protección Antispam

El correo electrónico no deseado (spam) es uno de los problemas más graves de la comunicación electrónica; representa hasta el 80 % de todas las comunicaciones por correo electrónico. La protección antispam sirve para protegerse frente a este problema. El módulo Antispam combina varios principios muy eficaces para ofrecer un filtrado superior para su bandeja de entrada esté siempre desinfectada.



Un principio importante en la detección del correo no deseado es la capacidad de reconocer correo electrónico no solicitado a partir de listas de direcciones de confianza predefinidas (lista blanca) y de direcciones de correo no deseado (lista negra). Todas las direcciones de su lista de contactos se agregan automáticamente a la lista blanca, así como todas las demás direcciones que marque como seguras.

El principal método utilizado para detectar correo no deseado es el análisis de las propiedades de los mensajes de correo electrónico. Los mensajes recibidos se analizan con criterios básicos contra correo no deseado (definiciones de mensajes, heurística estadística, algoritmos reconocidos y otros métodos únicos) y el valor del índice resultante determina si un mensaje es deseado o no deseado.

La protección antispam de ESET Endpoint Security le permite definir varios parámetros para las listas de correo. Están disponibles las siguientes opciones:

Iniciar automáticamente la protección Antispam del cliente de correo electrónico: activa y desactiva la protección antispam del cliente de correo electrónico.

Procesamiento de mensajes

Agregar texto al asunto del mensaje: le permite agregar un prefijo personalizado a la línea de asunto de los mensajes que se han clasificado como correo electrónico no deseado. La expresión predeterminada es "[SPAM]".

Mover mensajes a la carpeta de correo no deseado: si está activada, los mensajes no deseados se moverán a la carpeta predeterminada de correo basura.

Usar esta carpeta: esta opción mueve el correo no deseado a una carpeta definida por el usuario.

Marcar como leídos los mensajes no deseados: seleccione esta opción para marcar el correo no deseado como leído de forma automática. Esto le ayudará a centrar su atención en los mensajes "desinfectados".

Marcar los mensajes reclasificados como no leídos: se mostrarán como no leídos los mensajes que originalmente se clasificaron como correo no deseado, pero que después se marcaron como "desinfectados".

Registro del nivel de spam

El motor antispam de ESET Endpoint Security asigna un nivel de spam a cada uno de los mensajes analizados. El mensaje se anotará en el registro de antispam (**ESET Endpoint Security** > **Herramientas** > **Archivos de registro** > **Protección Antispam**).

- **No anotar**: la celda **Nivel** del registro de protección antispam estará vacía.
- **Anotar únicamente los mensajes reclasificados y marcados como SPAM**: utilice esta opción si desea registrar un nivel de spam para los mensajes marcados como correo no deseado.
- **Anotar todos los mensajes**: todos los mensajes se anotarán en el registro con un nivel de spam.

Iniciar automáticamente la protección Antispam del cliente de correo electrónico: si activa esta opción, la protección antispam se activará automáticamente al iniciar el sistema.

Activar el control antispam avanzado: se descargarán bases de datos frente al correo no deseado, lo que aumentará las capacidades antispam y producirá mejores resultados.

ESET Endpoint Security admite la protección antispam para Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail y Mozilla Thunderbird.

4.3.3.1 Agregar direcciones a las listas blanca y negra

Puede añadir a la lista blanca las direcciones de correo electrónico de las personas con las que se comunica a menudo para garantizar que los mensajes enviados desde estas direcciones no se clasifican como correo no deseado. Las direcciones de correo no deseado conocidas se pueden añadir a la lista negra, de modo que siempre se clasifiquen como correo no deseado. Para añadir una dirección nueva a la lista blanca o la lista negra, haga clic con el botón derecho del ratón en la dirección de correo y seleccione **ESET Endpoint Security** > **Agregar a la lista blanca** o **Agregar a la lista negra**; también puede hacer clic en el botón **Direcciones de confianza** o **Direcciones de correo no deseado** de la barra de herramientas contra correo no deseado de ESET Endpoint Security en el cliente de correo electrónico.

Este proceso también se aplica a direcciones de correo no deseado. Si una dirección de correo electrónico aparece en la lista negra, todos los mensajes de correo electrónico enviados desde esa dirección se clasifican como no deseados.

4.3.3.2 Marcar mensajes como correo no deseado

Cualquier mensaje visualizado en su cliente de correo electrónico se puede marcar como correo no deseado. Para hacerlo, haga clic con el botón derecho del ratón sobre el mensaje y haga clic en **ESET Endpoint Security** > **Reclasificar como correo no deseado** o en **Direcciones de correo no deseado** en la barra de herramientas contra correo no deseado de ESET Endpoint Security, disponible en la sección superior del cliente de correo electrónico.

Los mensajes reclasificados se mueven automáticamente a la carpeta SPAM, pero la dirección de correo electrónico del remitente no se agrega a la lista negra. Del mismo modo, los mensajes se pueden clasificar como "deseados". Si los mensajes de la carpeta **Correo basura** se clasifican como deseados, se moverán a la carpeta original. Cuando se marca un mensaje como deseado, la dirección del remitente no se agrega automáticamente a la lista blanca.

4.3.4 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 control funciona de manera automática, independientemente del navegador de Internet o el cliente de correo electrónico utilizado. Vaya a **Filtrado de protocolos** > **SSL** para obtener información sobre la comunicación cifrada SSL.

Activar el control sobre el contenido del protocolo de la aplicación: si esta opción está activada, el análisis antivirus comprobará todo el tráfico HTTP(S), POP3(S) e IMAP(S).

NOTA: la arquitectura Plataforma de filtrado de Windows (WFP) se empezó a aplicar en Windows Vista Service Pack 1 y Windows 7, y se utiliza para comprobar la comunicación de red. Las opciones siguientes no se encuentran disponibles porque la tecnología WFP utiliza técnicas de supervisión especiales:

- **Puertos HTTP y POP3**: limita el redireccionamiento del tráfico al servidor Proxy interno únicamente para puertos HTTP y POP3.
- **Aplicaciones marcadas como navegadores de Internet y clientes de correo electrónico**: limita el redireccionamiento del servidor Proxy interno solo para las aplicaciones marcadas como navegadores y clientes de correo electrónico (**Web y correo electrónico** > **Filtrado de protocolos** > **Clientes de correo electrónico y web**).
- **Puertos y aplicaciones marcados como navegadores de Internet o clientes de correo electrónico**: permite el redireccionamiento de todo el tráfico de los puertos HTTP y POP3, así como de toda la comunicación de las aplicaciones marcadas como navegadores y clientes de correo electrónico en el servidor Proxy interno.

4.3.4.1 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 7, 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.

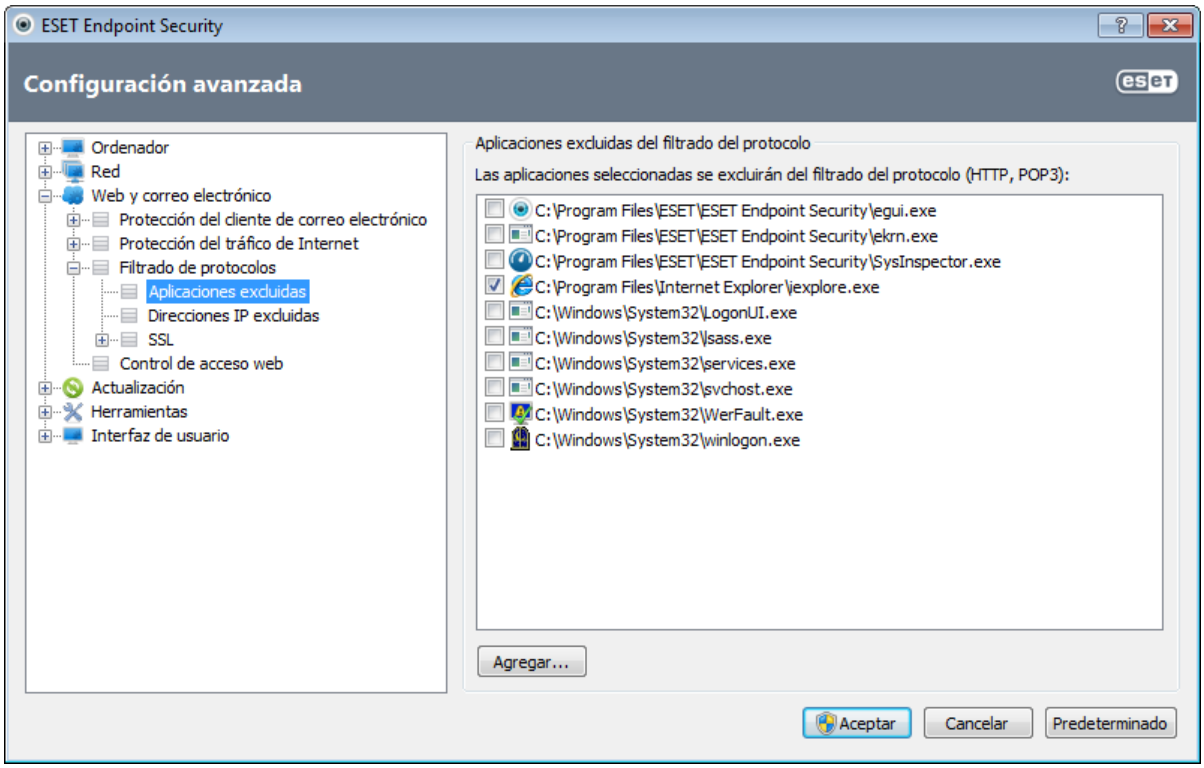
Dada la ingente cantidad de código malicioso que circula en Internet, la navegación segura es un aspecto crucial para la protección de los ordenadores. Las vulnerabilidades de los navegadores web y los vínculos fraudulentos sirven de ayuda a este tipo de código para introducirse en el sistema de incógnito; por este motivo, ESET Endpoint Security se centra en la seguridad de los navegadores web. Cada aplicación que acceda a la red se puede marcar como un navegador de Internet. La casilla de verificación tiene dos estados:

- **Sin marcar**: la comunicación de las aplicaciones se filtra solamente para los puertos especificados.
- **Marcada**: la comunicación se filtra siempre (aunque se configure un puerto diferente).

4.3.4.2 Aplicaciones excluidas

Para excluir del filtrado de contenido la comunicación de aplicaciones de red específicas, selecciónelas en la lista. No se comprobará la presencia de amenazas en la comunicación HTTP/POP3/IMAP de las aplicaciones seleccionadas. Se recomienda utilizar esta opción únicamente en aplicaciones que no funcionen correctamente cuando se comprueba su comunicación.

Las aplicaciones y los servicios en ejecución estarán disponibles aquí de forma automática. Haga clic en el botón **Agregar** para seleccionar manualmente una aplicación que no se muestre en la lista del filtrado de protocolos.

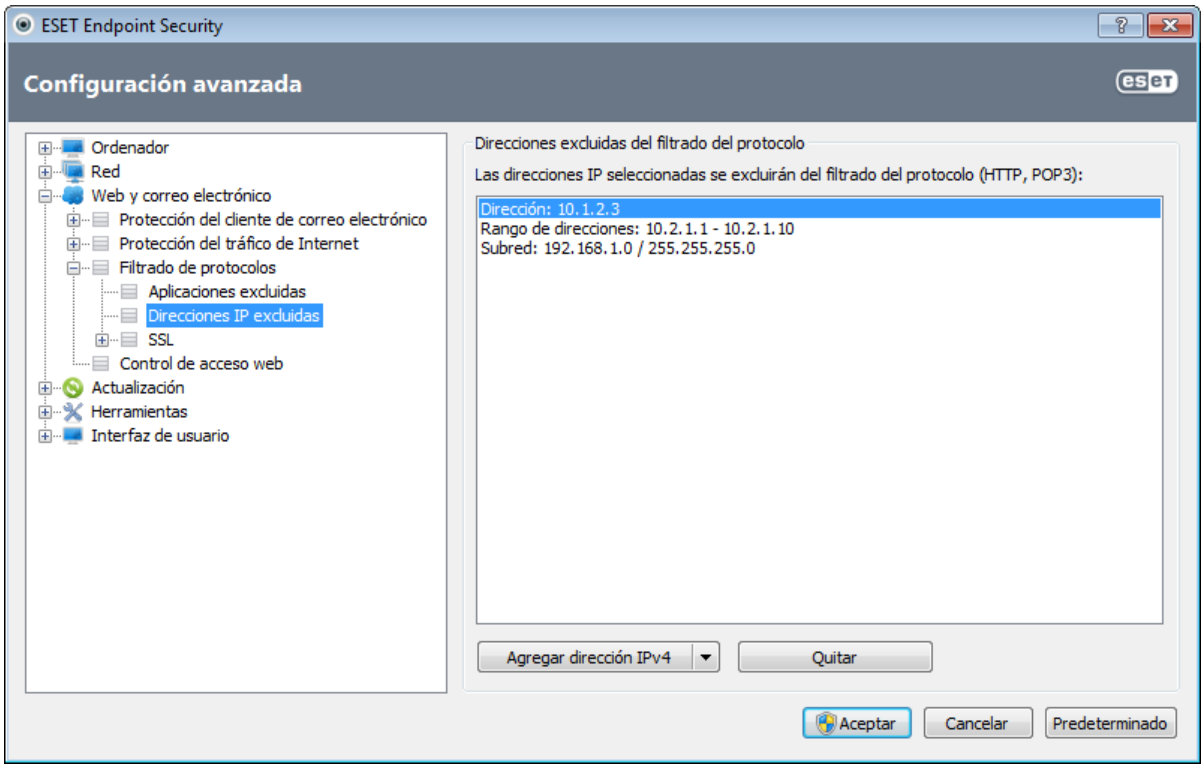


4.3.4.3 Direcciones IP excluidas

Las entradas de la lista de direcciones se excluyen del 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 de confianza.

Agregar dirección IPv4/IPv6: esta opción le permite agregar una dirección IP, un intervalo de direcciones o una subred de un punto remoto al que aplicar la regla.

Quitar: elimina las entradas seleccionadas de la lista.



4.3.4.3.1 Agregar dirección IPv4

Esta opción le permite agregar una dirección IP, un rango de direcciones o una subred de un punto remoto a la que se debe aplicar la regla. El protocolo de Internet versión 4 es la versión más antigua, pero sigue siendo la más utilizada.

Dirección única: agrega la dirección IP de un ordenador individual al que debe aplicarse la regla (por ejemplo, 192.168.0.10).

Rango de direcciones: especifique las direcciones IP inicial y final para delimitar el intervalo de direcciones (de varios ordenadores) al que se aplicará la regla (por ejemplo, de 192.168.0.1 a 192.168.0.99).

Subred: grupo de ordenadores definido por una dirección IP y una máscara.

Por ejemplo, 255.255.255.0 es la máscara de red del prefijo 192.168.1.0/24 (es decir, el intervalo de direcciones de 192.168.1.1 a 192.168.1.254).

4.3.4.3.2 Agregar dirección IPv6

Esta opción le permite agregar una dirección IPv6 o una subred de un punto remoto al que se aplica la regla. Esta es la versión más reciente del protocolo de Internet, que sustituirá a la versión 4 anterior.

Dirección única: agrega la dirección IP de un ordenador individual al que debe aplicarse la regla, (por ejemplo, 2001:718:1c01:16:214:22ff:fec9:ca5).

Subred: grupo de ordenadores definido por una dirección IP y una máscara (por ejemplo: 2002:c0a8:6301:1::1/64).

4.3.4.4 Comprobación del protocolo SSL

ESET Endpoint Security le permite comprobar los protocolos encapsulados en el protocolo SSL. Puede utilizar varios modos de análisis para las comunicaciones protegidas mediante el protocolo SSL: certificados de confianza, certificados desconocidos o certificados excluidos del análisis de comunicaciones protegidas mediante el protocolo SSL.

Analizar siempre el protocolo SSL: 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 ha agregado a la lista de certificados de confianza), se permite la comunicación con el servidor y se filtra el contenido del canal de comunicación.

Preguntar sobre sitios no visitados (se pueden hacer exclusiones): 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.

No analizar el protocolo SSL: si se selecciona esta opción, el programa no analizará las comunicaciones a través de SSL.

Aplicar las excepciones creadas basadas en los certificados: activa el uso de las exclusiones especificadas en los certificados excluidos y de confianza para analizar la comunicación mediante SSL. Para que esta opción se encuentre disponible, debe seleccionar **Analizar siempre el protocolo SSL**.

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

4.3.4.4.1 Certificados

Para que la comunicación SSL funcione correctamente en los navegadores y clientes de correo electrónico, es fundamental que el certificado raíz de ESET (spol s r. o.) se agregue a la lista de certificados raíz conocidos (editores). Por lo tanto, la opción **Añadir 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 o 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.

En algunos casos, el certificado no se puede comprobar mediante el archivo de autoridades certificadoras de confianza (por ejemplo, VeriSign). Esto significa que el certificado ha sido autofirmado 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 empresas grandes (como los bancos) utilizan certificados firmados por TRCA. Si está seleccionada la opción **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. Se mostrará un cuadro de diálogo de selección que le permite marcar el certificado como de confianza o excluirlo. Si el certificado no se encuentra en la lista de TRCA, la ventana se mostrará en rojo, y si está en dicha la vista, la ventana se mostrará en verde.

La opción **Bloquear las comunicaciones que utilicen el certificado** se puede seleccionar para que se terminen todas las conexiones cifradas con el sitio que utilicen un certificado sin verificar.

Si el certificado no es válido o está dañado, significa que ha expirado o que la autofirma no es correcta. En este caso, se recomienda bloquear las comunicaciones que utilicen dicho certificado.

4.3.4.4.1.1 Certificados de confianza

Además del archivo de autoridades certificadoras de confianza integrado, donde ESET Endpoint Security almacena los certificados de confianza, puede crear una lista personalizada de certificados de confianza. Esta lista se puede ver en **Configuración avanzada** (F5) > **Web y correo electrónico** > **Filtrado de protocolos** > **SSL** > **Certificados** > **Certificados de confianza**. ESET Endpoint Security utilizará los certificados de esta lista para comprobar el contenido de las comunicaciones cifradas.

Para eliminar los elementos seleccionados de la lista, haga clic en el botón **Quitar**. Haga clic en la opción **Mostrar** (o haga doble clic en el certificado) para ver información sobre el certificado seleccionado.

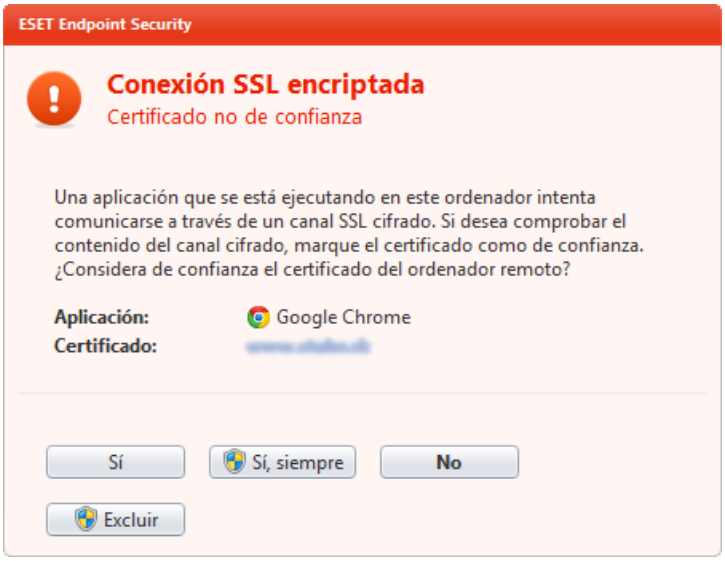
4.3.4.4.1.2 Certificados excluidos

La sección Certificados excluidos contiene certificados que se consideran seguros. No se buscarán amenazas en el contenido de las comunicaciones cifradas que utilicen los certificados de la lista. Se recomienda excluir únicamente los certificados web que tengan una garantía de seguridad y cuya comunicación no sea necesario comprobar. Para eliminar los elementos seleccionados de la lista, haga clic en el botón **Quitar**. Haga clic en la opción **Mostrar** (o haga doble clic en el certificado) para ver información sobre el certificado seleccionado.

4.3.4.4.1.3 Conexión SSL cifrada

Si el ordenador está configurado para análisis del protocolo SSL, es posible que se abra un cuadro de diálogo solicitándole que seleccione una acción cuando hay un intento de establecer una comunicación cifrada (utilizando un certificado desconocido). El cuadro de diálogo contiene la siguiente información: nombre de la aplicación que inició la comunicación y nombre del certificado utilizado.

Si no se encuentra el certificado en el archivo de autoridades certificadoras de confianza, se considerará que no es de confianza.



Están disponibles las siguientes acciones para certificados:

Sí: el certificado se marca temporalmente como de confianza para la sesión actual. No se mostrará la ventana de alerta en el siguiente intento de utilizar el certificado.

Sí, siempre: marca el certificado como de confianza y lo agrega a la lista de certificados de confianza. No se muestra ninguna ventana de alerta para los certificados de confianza.

No: marca el certificado como de no confianza para la sesión actual. La ventana de alerta se mostrará en el siguiente intento de utilizar el certificado.

Excluir: agrega el certificado a la lista de certificados excluidos y los datos transferidos a través del canal cifrado no se analizan.

4.4 Control de acceso web

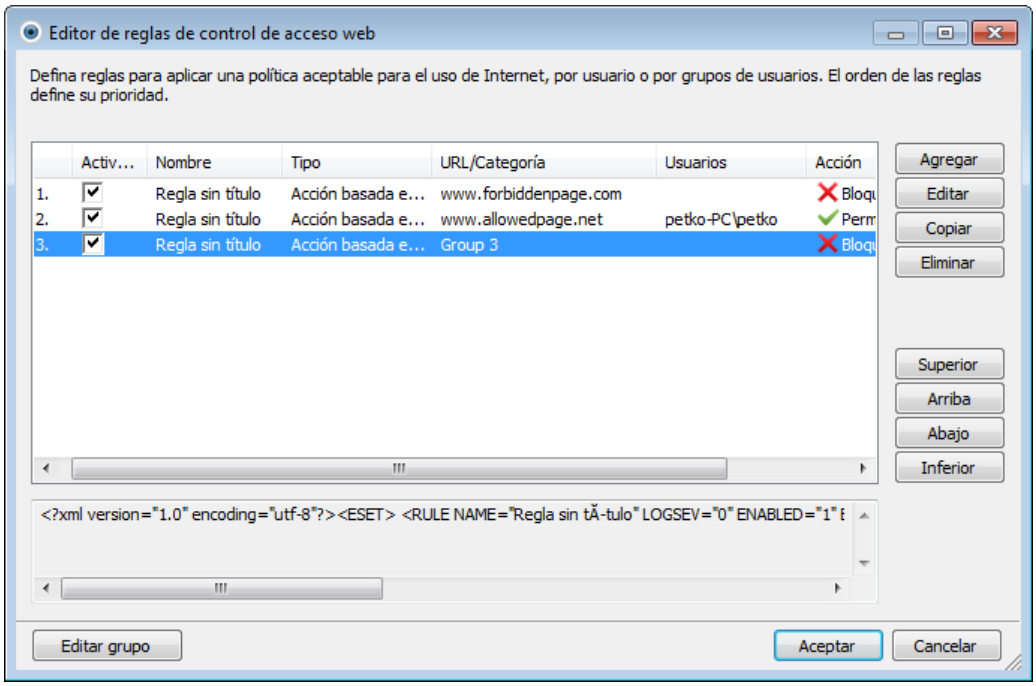
La sección Control de acceso web le permite configurar las opciones que impiden que su empresa corra el riesgo de responsabilidad jurídica, como puede ser el caso de sitios web que infringen los derechos de propiedad intelectual. El objetivo es impedir que los empleados accedan a páginas con contenido inapropiado o perjudicial o páginas que puedan afectar negativamente a la productividad en el trabajo.

Control de acceso web le permite bloquear las páginas web que puedan contener material que podría resultar ofensivo. Además, los los jefes o los administradores de sistemas pueden prohibir el acceso a más de 27 categorías predefinidas y más de 140 subcategorías de sitios web.

Las opciones de configuración del control de acceso web se pueden modificar en **Configuración avanzada** (F5) > **Control de acceso web**. La casilla de verificación junto a **Integrar en el sistema** integra el control de acceso web en ESET Endpoint Security y activa **Configurar reglas...** para acceder a la ventana Editor de reglas de control de acceso web.

4.4.1 Reglas de control de acceso web

La ventana **Editor de reglas de control de dispositivos** muestra las reglas existentes para direcciones URL y categorías de páginas web.



La lista de reglas contiene varias descripciones de una regla, como nombre, tipo de bloqueo, acción que debe realizarse tras coincidir una regla de control de acceso web y la gravedad de registro.

Haga clic en **Agregar** o en **Modificar** para administrar una regla. Haga clic en **Copiar** para crear una nueva regla con opciones predefinidas utilizadas para otra regla seleccionada. Las cadenas XML que se muestran al hacer clic en una regla se pueden copiar en el portapapeles o pueden ayudar a administradores de sistemas a exportar o importar datos y utilizarlos; por ejemplo en ESET Remote Administrator.

Al mantener pulsado CTRL y hacer clic, puede seleccionar varias reglas y aplicar acciones, como eliminarlas o moverlas hacia arriba o hacia abajo en la lista, a todas las reglas seleccionadas. La casilla de verificación **Activado** desactiva o activa una regla; puede ser útil si no desea eliminar una regla de forma permanente, por si decide utilizarla en el futuro.

El control se efectúa mediante reglas que se clasifican en el orden que determina su prioridad, situándose al principio las reglas con la prioridad más alta.

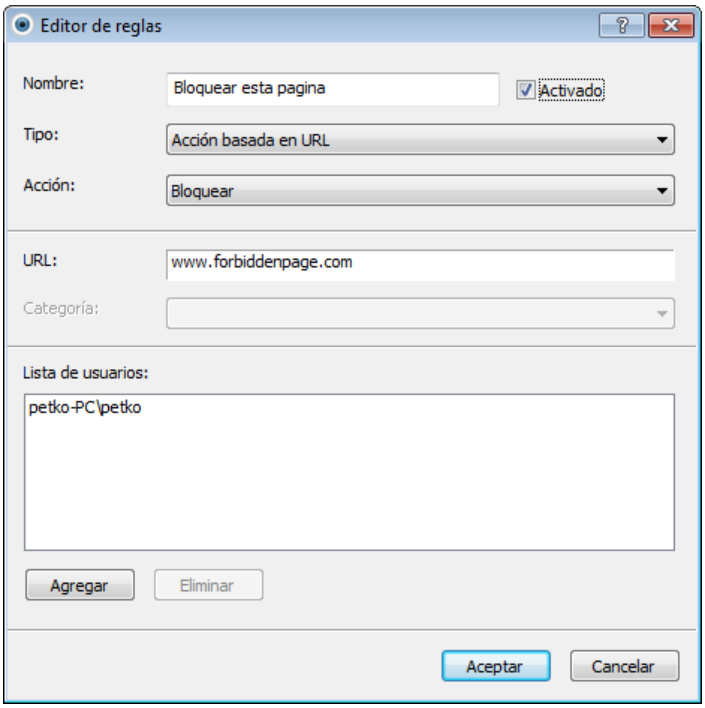
Puede hacer clic con el botón derecho en una regla para mostrar el menú contextual. Aquí puede definir la severidad de las entradas de registro, si se aplica una regla. Las entradas de registro se pueden ver desde la ventana principal de ESET Endpoint Security en **Herramientas** > **Archivos de registro**.

Haga clic en **Modificar grupo** para abrir la ventana de editor de grupos, en la que puede agregar o eliminar categorías y

subcategorías predefinidas que pertenezcan a un grupo correspondiente.

4.4.2 Adición de reglas de control de acceso web

La ventana Reglas de control de acceso web le permite crear o modificar la regla de filtrado de control de acceso web.



Introduzca una descripción de la regla en el campo **Nombre** para mejorar la identificación. Al seleccionar la casilla de verificación situada junto a **Activado**, se desactiva o se activa esta regla. Esto puede resultar útil si no desea eliminar la regla de forma permanente.

Tipo de acción

- **Acción basada en URL**: acceso al sitio web en cuestión. Introduzca la dirección URL adecuada en el campo **URL**.
- **Acción basada en categoría**: tras seleccionar esta opción, se debe seleccionar una categoría en el menú desplegable **Categoría**.

En las listas de direcciones URL, no pueden utilizarse los símbolos especiales * (asterisco) y ? (signo de interrogación). Por ejemplo, las direcciones de páginas web con varios TLD se deben escribir manualmente (ejemplopágina.com, ejemplopágina.sk, etc.). Cuando introduce un dominio en la lista, todo el contenido ubicado en este dominio y todos los subdominios (por ejemplo, sub.ejemplopágina.com) se bloqueará o permitirá en función de la acción basada en URL elegida.

Acción

- **Permitir**: se permitirá el acceso a la dirección URL o a la categoría.
- **Bloquear**: bloquea la dirección URL o la categoría.

Lista de usuarios

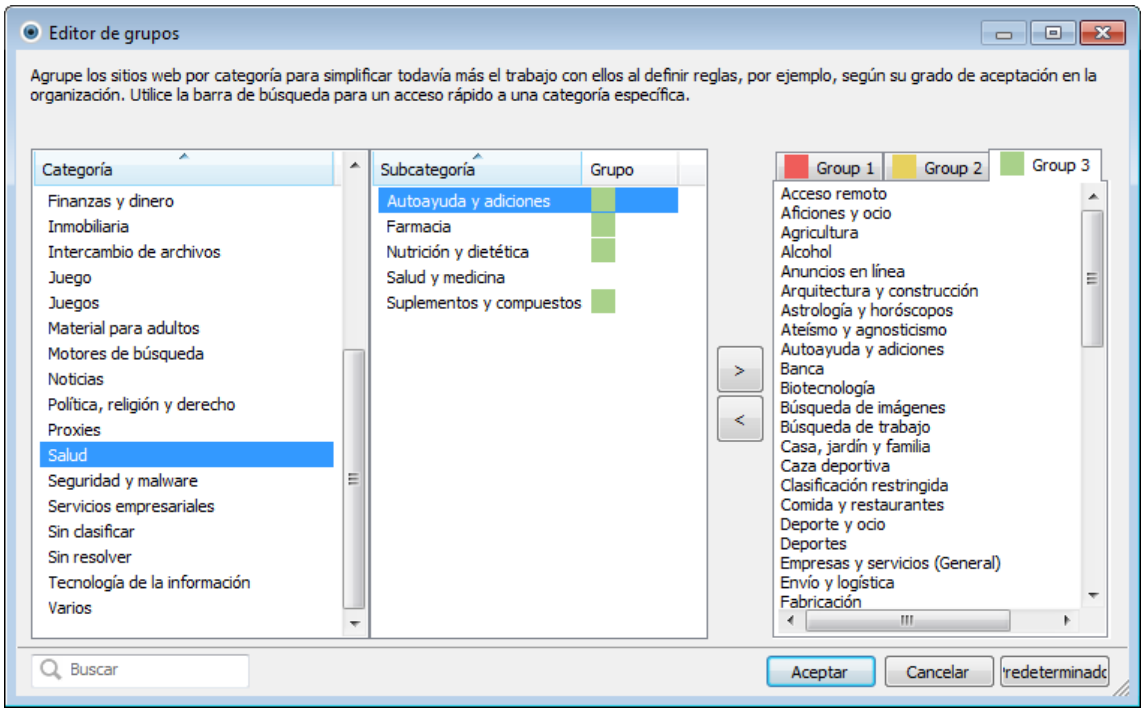
- **Agregar**: abre el cuadro de diálogo **Tipo de objeto: Usuarios o grupos**, que le permite seleccionar los usuarios que desee.
- **Eliminar**: elimina del filtro al usuario seleccionado.

4.4.3 Editor de grupos

La ventana Editor de grupos se divide en dos partes. La parte derecha de la ventana contiene una lista de categorías y subcategorías. Seleccione una categoría en la lista de **categorías** para mostrar sus subcategorías. La mayoría de las subcategorías pertenecen a un grupo marcado con un color.

Un grupo de color rojo contiene subcategorías para adultos y/o inadecuadas en general. Por otro lado, un grupo verde incluye categorías de páginas web que se pueden considerar aceptables.

Use las flechas para agregar una subcategoría seleccionada a un grupo seleccionado o eliminarla de dicho grupo.



Nota: una subcategoría puede pertenecer a un solo grupo. Existen subcategorías que no están incluidas en los grupos predefinidos (por ejemplo, Juegos). Para hacer coincidir una subcategoría deseada mediante un filtro de control de acceso web, agréguela a un grupo deseado. Si la subcategoría que se está agregando ya está incluida en otro grupo, se eliminará de este otro grupo y se agregarla al grupo seleccionado.

Busque un grupo introduciendo términos de búsqueda en el campo **Buscar** que se encuentra en la esquina inferior izquierda de la ventana.

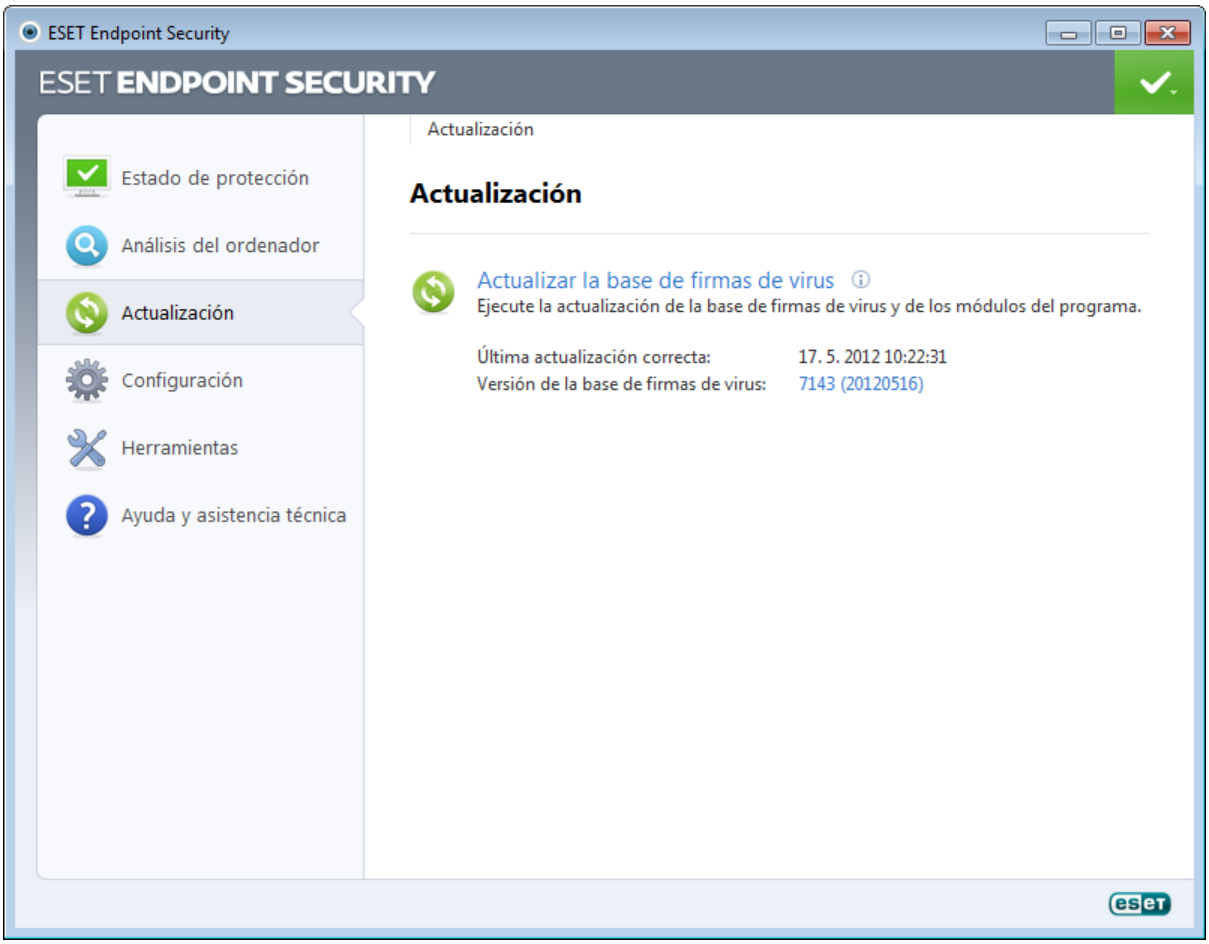
4.5 Actualización del programa

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

Haga clic en **Actualizar** en la ventana principal del programa para comprobar el estado de la actualización, así como la fecha y la hora de la última actualización y si es necesario actualizar el programa. La ventana principal también indica la versión de la base de firmas de virus. Esta indicación numérica es un enlace activo al sitio web de ESET, donde se muestran todas las firmas agregadas en la actualización correspondiente.

También tiene a su disposición la opción de iniciar el proceso de actualización de forma manual, con la opción **Actualizar la base de firmas de virus ahora**. La actualización de la base de firmas de virus y la actualización de 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 (nombre de usuario y la contraseña) durante la instalación, puede introducir el nombre de usuario y la contraseña cuando realice la actualización para acceder a los servidores de actualización de ESET.

NOTA: ESET le proporcionará el nombre de usuario y la contraseña una vez que haya adquirido ESET Endpoint Security.

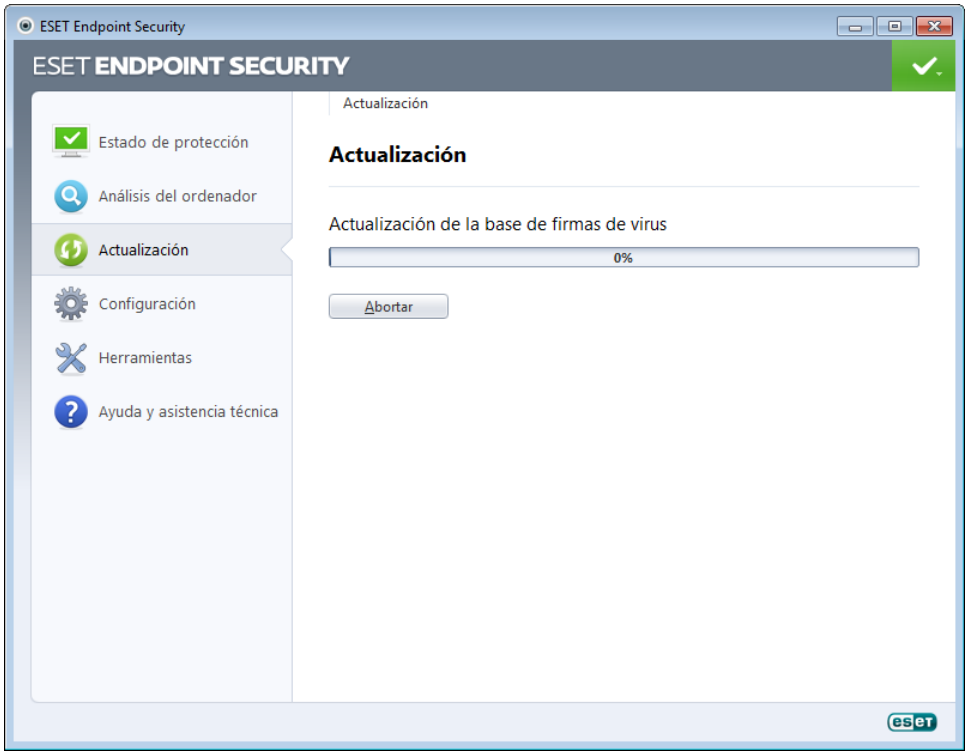


Última actualización correcta: fecha de la última actualización. Asegúrese de que hace referencia a una fecha reciente, lo que significa que la base de firmas de virus es actual.

Base de firmas de virus: el número de la base de firmas de virus, que también es un enlace activo al sitio web de ESET. Haga clic en esta opción para ver una lista de todas las firmas agregadas con la actualización.

Proceso de actualización

El proceso de descarga se inicia al hacer clic en **Actualizar la base de firmas de virus ahora**. 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 **Anular**.

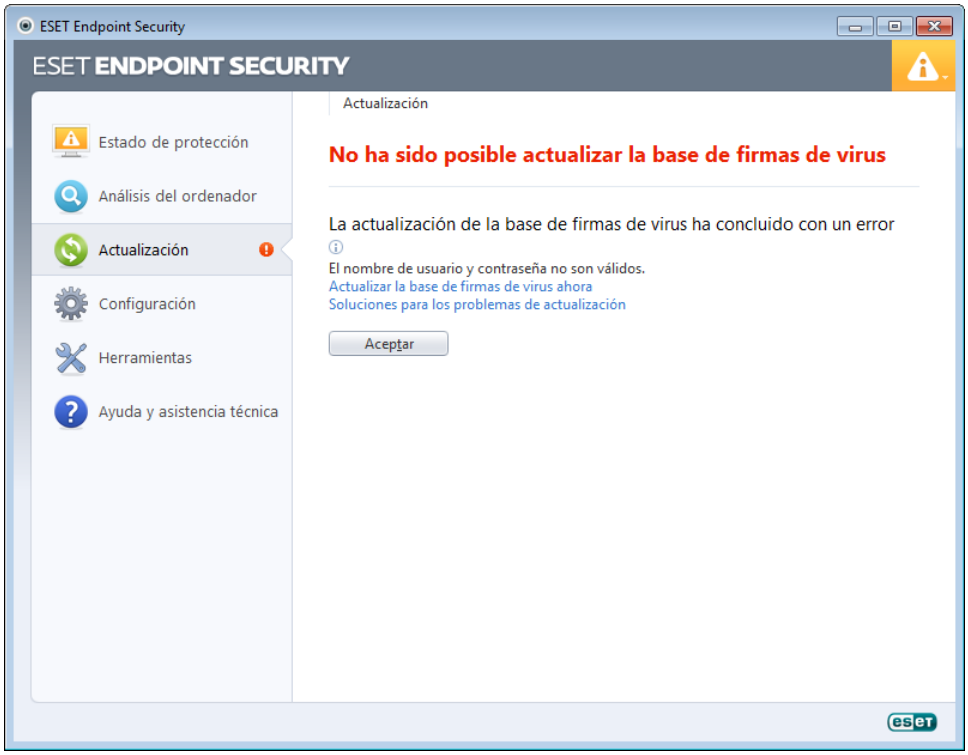


Importante: en circunstancias normales, si las actualizaciones se descargan adecuadamente, se mostrará el mensaje **No es necesario realizar la actualización: la base de firmas de virus instalada está actualizada** en la ventana **Actualización**. En caso contrario, el programa no estará actualizado y es más vulnerable a la infección. Actualice la base de firmas de virus tan pronto como sea posible. De lo contrario, se mostrará uno de los mensajes siguientes:

La base de firmas de virus se encuentra desactualizada: este error aparece tras varios intentos sin éxito de actualizar la base de firmas de virus. 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 siguientes **No ha sido posible actualizar la base de firmas de virus** sobre actualizaciones incorrectas:

1. **El nombre de usuario y contraseña no son válidos**: el nombre de usuario y la contraseña se han escrito incorrectamente en la configuración de actualización. Recomendamos que compruebe sus datos de autenticación. La ventana Configuración avanzada (haga clic en **Configuración** en el menú principal y, a continuación, en **Especificar configuración avanzada**, o pulse F5 en el teclado) ofrece opciones de actualización adicionales. Haga clic en **Actualizar** > **General** en el árbol de configuración avanzada para escribir un nombre de usuario y una contraseña nuevos.

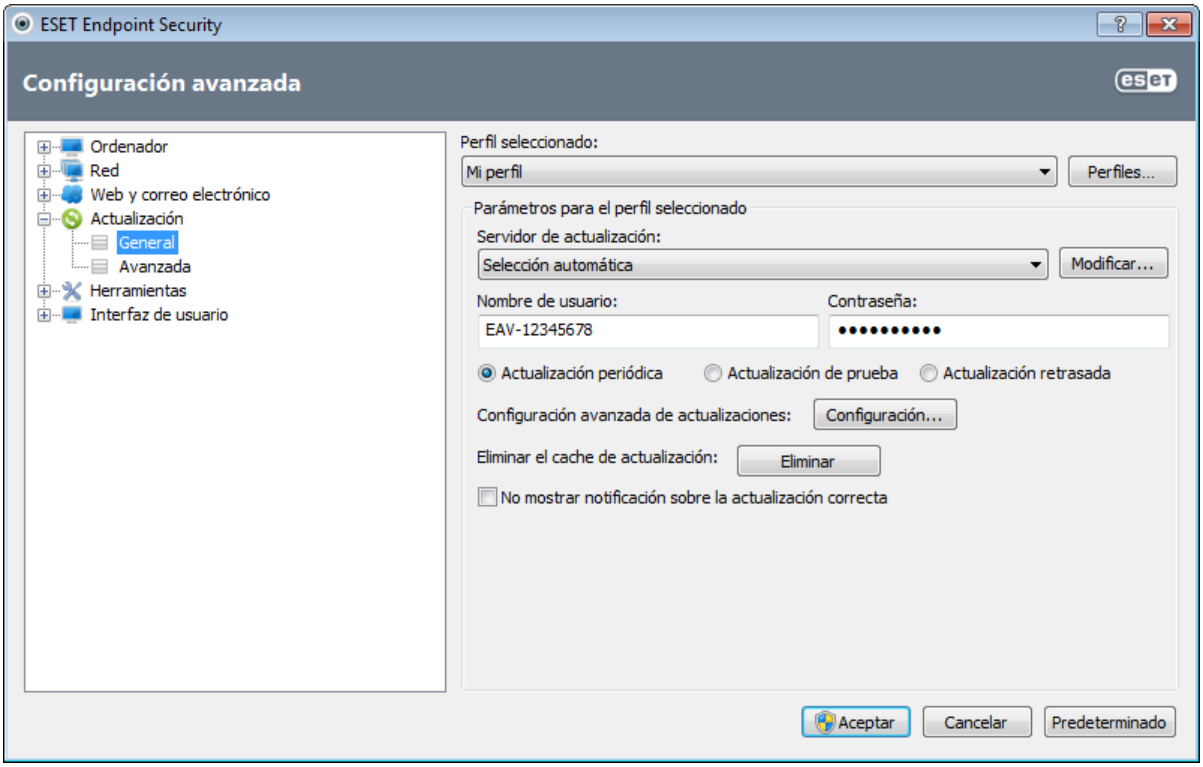


2. **Ha ocurrido un error mientras se descargaban los archivos de actualización**: el error puede deberse a una configuración de la conexión a Internet. Es recomendable que compruebe la conectividad a Internet (por ejemplo, abriendo un sitio web en el navegador web). Si el sitio web no se abre, es probable 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.

4.5.1 Configuración de actualizaciones

Las opciones de configuración de actualización están disponibles en el árbol de **Configuración avanzada** (tecla F5) haciendo clic en **Actualizar** > **General**. En esta sección se especifica la información del origen de la actualización, como los servidores de actualización y sus datos de autenticación. De forma predeterminada, el menú desplegable **Servidor de actualización** está configurado en **Selección automática** para garantizar que los archivos de actualización se descargarán del servidor ESET cuando la carga de la red sea menor.

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



El perfil de actualización que se utiliza actualmente se muestra en el menú desplegable **Perfil seleccionado**. Haga clic en **Perfiles** para crear un perfil nuevo.

Puede acceder a la lista de servidores de actualización disponibles desde el menú desplegable **Servidor de actualización**. El servidor de actualización es la ubicación donde se almacenan las actualizaciones. Si utiliza un servidor ESET, deje seleccionada la opción predeterminada **Selección automática**. Para agregar un nuevo servidor, haga clic en **Modificar** en la sección **Parámetros para el perfil seleccionado** y, a continuación, haga clic en el botón **Agregar**.

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 mediante SSL, el servidor de actualización debe configurarse de la forma siguiente:
https://nombre_del_ordenador_o_su_dirección_IP:2221

La autenticación de los servidores de actualización se basa en el **nombre de usuario** y la **contraseña** generados y enviados tras la compra. Al utilizar un servidor Mirror local, la verificación dependerá de su configuración. De manera predeterminada, no se requiere ningún tipo de verificación, es decir, los campos **Nombre de usuario** y **Contraseña** se dejan en blanco.

Las actualizaciones de prueba (la opción **Actualización de prueba**) son actualizaciones que han superado rigurosas pruebas internas y, por lo general, 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, el modo 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. La lista de módulos actuales está disponible en **Ayuda y asistencia técnica** > **Acerca de ESET Endpoint Security**. Se recomienda que los usuarios básicos dejen la opción **Actualización periódica** seleccionada de forma predeterminada. Los usuarios empresariales pueden seleccionar la opción **Actualización retrasada** para actualizar desde servidores de actualización especiales que ofrezcan nuevas versiones de

bases de datos de virus con un retraso de al menos x horas, es decir, de bases de datos comprobadas en un entorno real y que , por lo tanto, se consideran estables.

Haga clic en el botón **Configuración** situado junto a **Configuración avanzada de actualizaciones** para mostrar una ventana que contenga opciones avanzadas de actualización.

Si tiene problemas con la actualización, haga clic en el botón **Borrar** para eliminar de la carpeta los archivos de actualización temporales.

No mostrar notificación sobre la 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.

4.5.1.1 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, ya que les permite crear un perfil alternativo para las propiedades de conexión a Internet que cambian periódicamente.

El menú desplegable **Perfil seleccionado** muestra el perfil seleccionado actualmente, definido en **Mi perfil** de forma predeterminada. Para crear un perfil nuevo, haga clic en el botón **Perfiles** y, a continuación, en el botón **Agregar**; después, introduzca su **nombre de perfil**. Cuando cree un perfil nuevo, en el menú desplegable **Copiar parámetros desde el perfil** puede seleccionar un perfil existente para copiar su configuración.

En la ventana Configuración de perfil, puede especificar el servidor de actualización de una lista de servidores disponibles o agregar un servidor nuevo. Puede acceder a la lista de servidores de actualización actuales desde el menú desplegable **Servidor de actualización**. Para agregar un nuevo servidor, haga clic en **Modificar** en la sección **Parámetros para el perfil seleccionado** y, a continuación, haga clic en el botón **Agregar**.

4.5.1.2 Configuración avanzada de actualizaciones

Para ver la configuración avanzada de actualizaciones, haga clic en el botón **Configuración**. Las opciones avanzadas de la configuración de actualizaciones son **Tipo de actualización**, **Servidor Proxy HTTP**, **LAN** y **Mirror**.

4.5.1.2.1 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. Se puede realizar de manera automática, sin la intervención del usuario, o configurar de modo que este reciba una notificación de la actualización. 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:

- **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.
- **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.
- **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.

Tras una actualización de componentes del programa, es posible que deba reiniciar el ordenador para que los módulos dispongan de todas las funciones. La sección **Reiniciar después de actualizar los componentes del programa** le permite seleccionar unas de las opciones siguientes:

- **Nunca reiniciar el ordenador**: nunca se le pedirá que reinicie el sistema, aunque sea necesario. Tenga en cuenta que esta opción no es recomendable, pues es posible que su ordenador no funcione correctamente hasta que lo vuelva a reiniciar.
- **Si es necesario, ofrecer reiniciar el ordenador**: esta es la opción predeterminada. Después de actualizar los componentes del programa, se le pedirá que reinicie el ordenador mediante un cuadro de diálogo.
- **Si es necesario, reiniciar el ordenador sin avisar**: después de actualizar los componentes del programa, el ordenador se reiniciará (si es necesario).

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.

Si está seleccionada 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**, el programa mostrará una notificación.

4.5.1.2.2 Servidor Proxy

Para acceder a las opciones de configuración del servidor Proxy de un perfil de actualización dado, haga clic en **Actualización** en el árbol de configuración avanzada (F5) y, a continuación, en el botón **Configuración** disponible a la derecha de **Configuración avanzada de actualizaciones**. Haga clic en la ficha **Servidor Proxy HTTP** y seleccione una de estas tres opciones:

- **Utilizar la configuración predeterminada**
- **No usar servidor Proxy**
- **Conexión a través de un servidor Proxy específico**

Si selecciona la opción **Utilizar la configuración predeterminada**, se utilizarán las opciones de configuración del servidor Proxy ya especificadas en la sección **Herramientas** > **Servidor Proxy** del árbol de configuración avanzada.

Seleccione la opción **No usar servidor Proxy** para especificar que no se utilice ningún servidor Proxy para actualizar ESET Endpoint Security.

La opción **Conexión a través de un servidor Proxy específico** debe seleccionarse si:

- Para actualizar ESET Endpoint Security, es necesario utilizar un servidor Proxy diferente al especificado en la configuración global (**Herramientas** > **Servidor Proxy**). En este caso, será necesario especificar la configuración aquí: **Dirección del servidor Proxy**, **Puerto** de comunicación, **Nombre de usuario** y **Contraseña** del servidor Proxy, si es necesario.
- La configuración del servidor Proxy no se ha definido globalmente, pero ESET Endpoint Security se conecta a un servidor Proxy para las actualizaciones.
- El ordenador se conecta a Internet mediante un servidor Proxy. La configuración se toma de Internet Explorer durante la instalación del programa; no obstante, si esta cambia (por ejemplo, al cambiar de proveedor de Internet), compruebe que la configuración del servidor Proxy HTTP es correcta en esta ventana. De lo contrario, el programa no se podrá conectar a los servidores de actualización.

La configuración predeterminada del servidor Proxy es **Utilizar la configuración predeterminada**.

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 Security, que únicamente debe proporcionar si sabe que es necesaria una contraseña para acceder a Internet a través de un servidor Proxy.

4.5.1.2.3 Conexión a la red local

Para realizar una actualización desde un servidor local en el que se ejecute un sistema operativo basado en NT, es necesario autenticar todas las conexiones de red de forma predeterminada. En la mayoría de los casos, las cuentas de sistema local no disponen de los derechos suficientes para la carpeta Mirror (que contiene copias de archivos de actualización). En este caso, escriba su nombre de usuario y contraseña en la sección de configuración de actualizaciones o especifique una cuenta con la que el programa pueda acceder al servidor de actualización (Mirror).

Para configurar este tipo de cuenta, haga clic en la ficha **Red local**. La sección **Conectarse a la red local como** incluye las opciones **Cuenta de sistema (predeterminada)**, **Usuario actual** y **Especificar usuario**.

Seleccione la opción **Cuenta de sistema (predeterminada)** para utilizar la cuenta de 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.

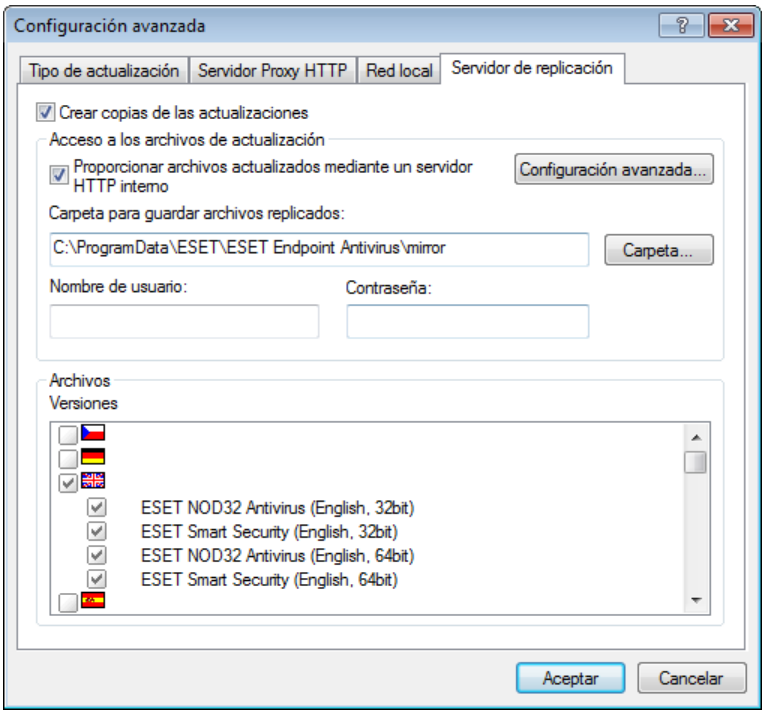
Alerta: Cuando se selecciona **Usuario actual** o **Especificar usuario**, puede producirse un error al cambiar la identidad del programa para el usuario deseado. Por este motivo, se recomienda que introduzca los datos de autenticación de la red local en la sección principal de configuración de actualizaciones, 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 la opción **Desconectar del servidor después de actualizar** si la conexión al servidor permanece activa incluso después de haber descargado las actualizaciones.

4.5.1.2.4 Creación de copias de actualización: Mirror

ESET Endpoint Security le permite crear copias de los archivos de actualización, que puede utilizar para actualizar otras estaciones de trabajo disponibles en la red. Creación de la "imagen": 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. Se descargan de manera centralizada al servidor mirror local y, después, se distribuyen a todas las estaciones de trabajo, por lo que se evita 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 mirror local están disponibles (después de agregar una clave de licencia válida en el administrador de licencias, que se encuentra en la sección Configuración avanzada de actualizaciones de ESET Endpoint Security) en la sección de configuración avanzada de actualizaciones. Para acceder a esta sección, pulse F5 y haga clic en **Actualizar** en el árbol de configuración avanzada; a continuación, haga clic en el botón **Configuración...** situado junto a **Configuración avanzada de actualizaciones** y seleccione la ficha **Mirror**.



El primer paso para configurar el Mirror es seleccionar la opción **Crear copias de las actualizaciones**. 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.

Proporcionar archivos actualizados mediante el servidor HTTP interno: si se activa esta opción, se puede acceder a los archivos actualizados a través de HTTP sin necesidad de introducir el nombre de usuario ni la contraseña. Haga clic en Configuración avanzada para configurar las opciones ampliadas del servidor Mirror.

Nota: el servidor de HTTP necesita SP2 y versiones posteriores en Windows XP.

Los métodos de activación del Mirror se describen detalladamente en la sección Actualización desde el servidor Mirror. Recuerde que existen dos métodos básicos para configurar el servidor mirror: la carpeta que contiene los archivos de actualización se puede presentar como una carpeta de red compartida o como 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. Haga clic en **Carpeta** 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 introducir 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/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.

Cuando configure el Mirror, el usuario también puede establecer las versiones de idioma en las que desea descargar las copias de actualización; estas deben ser compatibles con el servidor Mirror configurado por el usuario. La configuración de la versión de idioma se encuentra en la lista **Versiones disponibles**.

4.5.1.2.4.1 Actualización desde el servidor Mirror

Existen dos métodos básicos para configurar el servidor Mirror: la carpeta que contiene los archivos de actualización se puede presentar como una carpeta de red compartida o como un servidor HTTP.

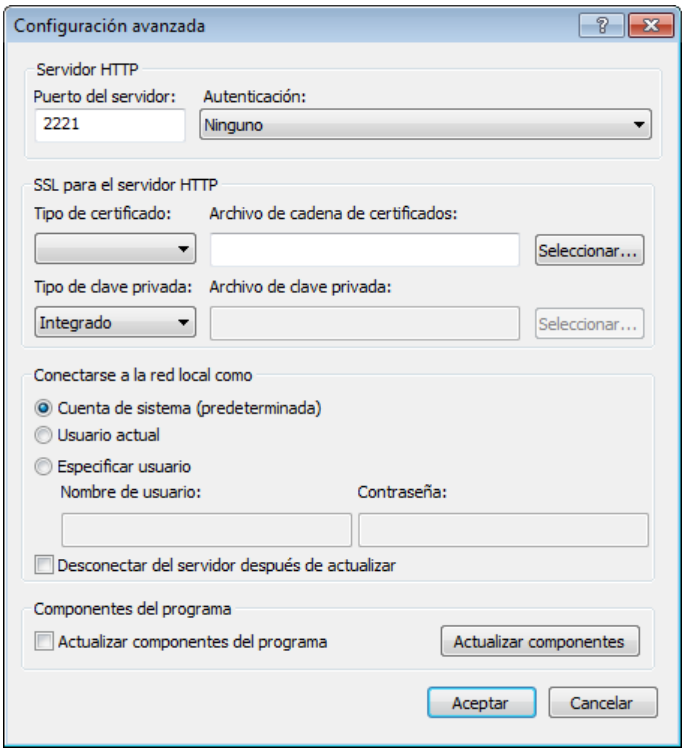
Acceso al servidor Mirror mediante un servidor HTTP interno

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 de actualizaciones** (ficha **Mirror**) y seleccione la opción **Crear mirror de las actualizaciones**.

En la sección **Configuración avanzada** 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 debe utilizar dicho servidor. 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 estas opciones: **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.

Alerta: 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 Security que vaya a crearla.

Agregue el **archivo de cadena de certificados** (o genere un certificado autorizado) si desea ejecutar el servidor HTTP con compatibilidad HTTPS (SSL). Están disponibles los siguientes tipos: **ASN**, **PEM** y **PFX**. Se pueden descargar archivos de actualización mediante el protocolo HTTPS, que ofrece más seguridad. 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 definida como **Integrada** de forma predeterminada (y por tanto, la opción **Archivo de clave privada** está desactivada de forma predeterminada), lo que significa que la clave privada forma parte del archivo de cadena de certificados seleccionado.



Una vez completada la configuración del mirror, vaya a las estaciones de trabajo y agregue un nuevo servidor de actualizaciones. Para hacerlo, siga estos pasos:

- Abra **ESET Endpoint SecurityConfiguración avanzada** y haga clic en **Actualizar** > **General**.
- Haga clic en **Modificar...** a la derecha del menú desplegable **Servidor de actualización** y agregue un nuevo servidor utilizando uno de los formatos siguientes:
  http://dirección_IP_de_su_servidor:2221
  https://dirección_IP_de_su_servidor:2221 (si se utiliza SSL)
- Seleccione el servidor que acaba de agregar en la lista de servidores de actualización.

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 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 Security desde la carpeta Mirror.

A continuación, configure el acceso al servidor Mirror en la sección **Configuración avanzada de actualizaciones** de la ficha **Mirror** mediante la desactivación de la opción **Proporcionar archivos actualizados mediante un 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 **Configuración avanzada** (F5) de ESET Endpoint Security y haga clic en **Actualizar** > **General**. Haga clic en el botón **Configuración** y, a continuación, en la ficha **LAN**. Esta configuración es la misma que se aplica a las actualizaciones, tal como se describe en la sección Conexión a la red local.

Cuando haya terminado de configurar el servidor Mirror, continúe con las estaciones de trabajo y establezca \\UNC\RUTA como servidor de actualización. Esta operación se puede completar con los pasos siguientes:

- Abra la Configuración avanzada de ESET Endpoint Security y haga clic en **Actualizar** > **General**.
- Haga clic en **Modificar...** junto al servidor de actualización y agregue un nuevo servidor con el formato \\UNC\RUTA.
- Seleccione el servidor que acaba de agregar en la lista de servidores de actualización.

NOTA: para un correcto funcionamiento, 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 Mirror local. Si la casilla de verificación junto a **Actualizar los componentes del programa** está seleccionada, no es necesario hacer clic en **Actualizar componentes** porque los archivos se copian en el Mirror local automáticamente cuando se encuentran disponibles. Consulte Tipo de actualización para obtener más información acerca de las actualizaciones de los componentes del programa.

4.5.1.2.4.2 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 casos anteriores. A continuación, se ofrece información general acerca de los problemas más frecuentes durante la actualización desde el Mirror:

ESET Endpoint Security 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 Security 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. Como resultado, 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.

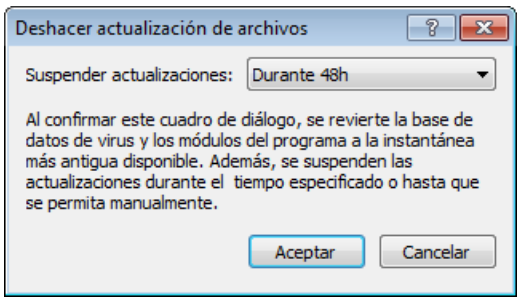
ESET Endpoint Security notifica un error al conectarse al servidor de imagen: la comunicación del puerto definida para acceder a la versión HTTP del Mirror está bloqueada.

4.5.1.3 Deshacer actualización

Si sospecha que una nueva actualización de la base de datos de virus puede ser inestable o estar dañada, puede revertir a la versión anterior y desactivar cualquier actualización durante un período de tiempo seleccionado. También puede activar actualizaciones desactivadas con anterioridad.

ESET Endpoint Security ofrece funcionalidad de copia de seguridad y restauración (lo que también se conoce como reversión) de módulos de la base de datos de virus. Para crear instantáneas de bases de datos de virus, deje seleccionada la casilla de verificación **Crear instantáneas de archivos actualizados**. El campo **Número de instantáneas almacenadas localmente** define el número de instantáneas de bases de datos de virus anteriores almacenadas en el sistema de archivos del ordenador local.

Si hace clic en **Revertir** (**Configuración avanzada** (F5) > **Actualizar** > **Avanzado**), deberá seleccionar un intervalo de tiempo en el menú desplegable **Suspender actualizaciones** que representa el período de tiempo en el que estarán interrumpidas las actualizaciones de la base de firmas de virus y del módulo del programa.

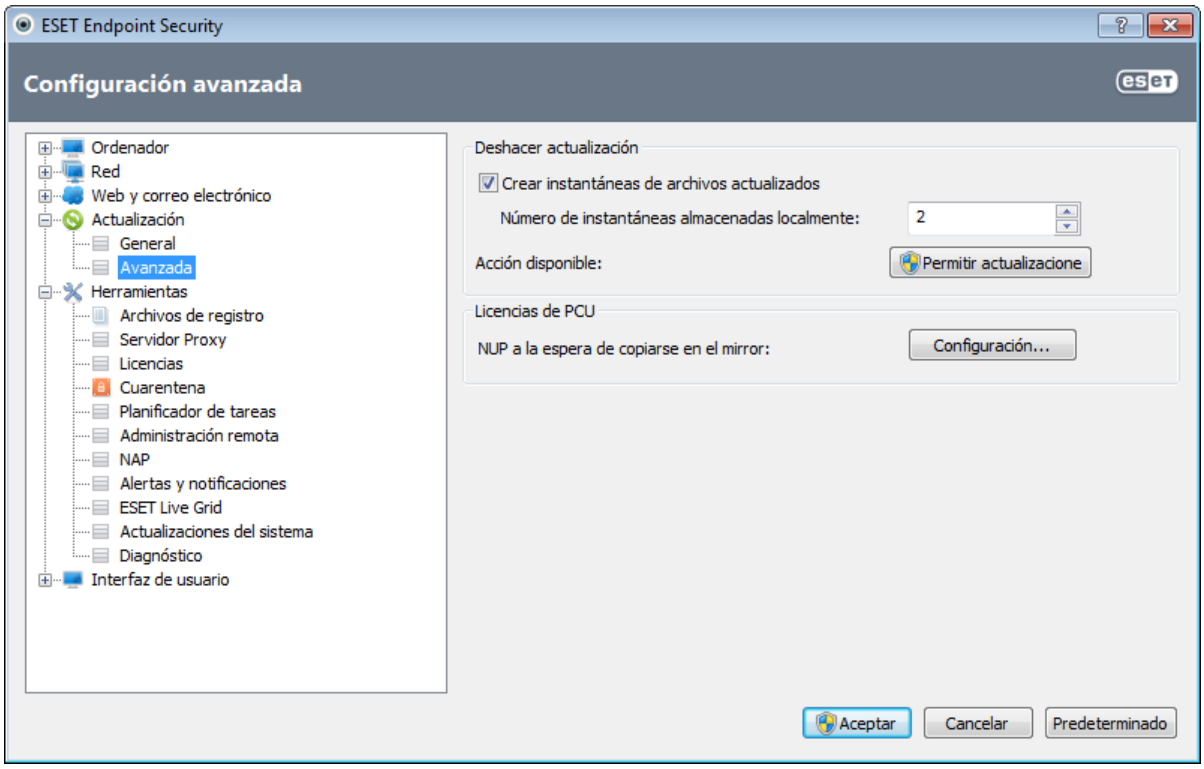


Seleccione **Hasta que se revoque** si desea permitir manualmente actualizaciones periódicas. Como esto representa un riesgo de seguridad potencial, no recomendamos que se seleccione esta opción.

Si está activada una reversión, el botón **Revertir** se convierte en **Permitir actualizaciones**. No se permitirán actualizaciones para el intervalo de tiempo seleccionado en el menú desplegable Intervalo de tiempo. La versión de base de datos de firmas de virus se degrada a la más antigua disponible y se almacena como instantánea en el sistema de archivos del ordenador local.

Ejemplo: supongamos que el número 6871 es la versión más reciente de la base de datos de firmas de virus. 6870 y 6868 se almacenan como instantáneas de base de datos de firmas de virus. Observe que 6869 no está disponible porque, por ejemplo, el ordenador estuvo apagado durante un largo período de tiempo. Si ha introducido 2 (dos) en el campo **Número de instantáneas almacenadas localmente** y hace clic en **Revertir**, la base de firmas de virus se restaurará a la versión número 6868. Este proceso puede tardar bastante. Compruebe si la versión de base de datos de firmas de virus se ha degradado en la ventana principal del programa de ESET Endpoint Security en la sección Actualizar.

Las opciones de configuración del servidor mirror local están disponibles (después de agregar una clave de licencia válida en el administrador de licencias, que se encuentra en la sección Configuración avanzada de ESET Endpoint Security). Si utiliza la estación de trabajo como mirror, las copias de las actualizaciones deben haber aceptado el acuerdo de licencia de usuario final (EULA) más reciente antes de crearse como archivos de actualización de copias para actualizar otras estaciones de trabajo ubicadas en la red. Si hay disponible una versión más reciente del EULA durante la actualización, aparecerá un cuadro de diálogo con 60 segundos de tiempo de espera para confirmarlo. Para hacerlo manualmente, haga clic en **Configuración...** en la sección **Licencias PCU** de esta ventana.



4.5.2 Cómo crear tareas de actualización

Las actualizaciones se pueden activar manualmente al hacer clic en **Actualizar la base de firmas de virus ahora** 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** > **Planificador de tareas**. Las siguientes tareas están activadas de forma predeterminada en ESET Endpoint Security:

- **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 la sección Planificador de tareas.

4.6 Herramientas

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

Este menú incluye las herramientas siguientes:

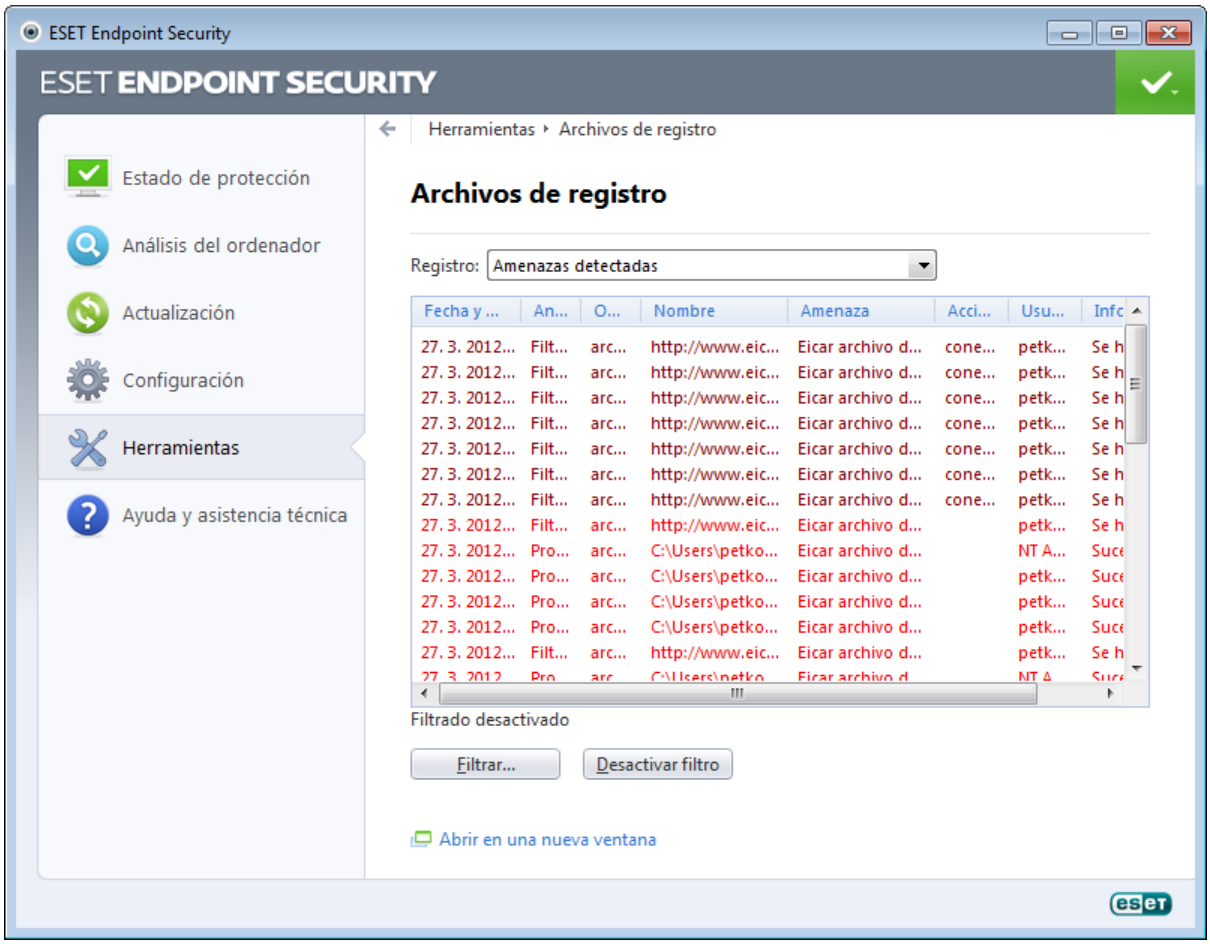
- Archivos de registro
- Estadísticas de protección
- Observar actividad
- Procesos en ejecución
- Planificador de tareas
- Cuarentena
- Conexiones de red
- ESET SysInspector

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

ESET SysRescue: abre el asistente de creación de ESET SysRescue.

4.6.1 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. El registro constituye 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 Security, donde también se pueden archivar registros.



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 ofrece información detallada acerca de las amenazas detectadas por los módulos de ESET Endpoint Security. 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 Security se registran en los registros de sucesos. El registro de sucesos contiene información sobre sucesos y errores que se produjeron en el programa. Esta opción se ha diseñado para que los administradores del sistema y los usuarios puedan solucionar 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 los resultados de todos los análisis manuales o programados completados. Cada línea se corresponde con un control informático individual. Haga doble clic en cualquier entrada para ver los detalles del análisis correspondiente.
- **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.
- **Cortafuegos personal**: el registro del cortafuegos muestra todos los ataques remotos detectados por el cortafuegos personal. Aquí encontrará información sobre todos los ataques a su ordenador. En la columna Suceso se incluyen los ataques detectados. En la columna Origen se proporciona más información sobre el atacante. En la columna Protocolo se indica el protocolo de comunicación que se utilizó para el ataque. El análisis del registro del cortafuegos puede ayudarle a detectar a tiempo amenazas del sistema, para así poder evitar el acceso no autorizado al sistema.

- **Protección Antispam**: contiene los registros relacionados con los mensajes de correo electrónico que se marcaron como correo no deseado.
- **Control de acceso web**: muestra las direcciones URL bloqueadas o permitidas y sus categorías. Las columnas Acción realizada informan de cómo se aplicaron las reglas de filtrado.
- **Control de dispositivos**: contiene registros de los dispositivos o medios extraíbles conectados al ordenador. Solo los dispositivos con su regla de control de dispositivos respectiva 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 directamente en el portapapeles seleccionando la entrada y haciendo clic en **Copiar** (o con el acceso directo Ctrl + C). Utilice las teclas CTRL y SHIFT para seleccionar varias entradas.

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

- **Filtrar registros del mismo tipo**: tras activar este filtro, solo verá registros del mismo tipo (diagnósticos, advertencias, ...).
- **Filtrar/Buscar**:al hacer clic en esta opción, se abre la ventana **Filtrado de registros**, donde puede definir los criterios de filtrado.
- **Desactivar filtro**: borra todos los ajustes del filtro (tal como se describe arriba).
- **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.
- **Desplazar registro**: deje esta opción activada para desplazarse automáticamente por los registros antiguos y ver los registros activos en la ventana **Archivos de registro**.

4.6.1.1 Mantenimiento de registros

La configuración de archivos de registro de ESET Endpoint Security está disponible en la ventana principal del programa. Haga clic en **Configuración** > **Especificar configuración avanzada** > **Herramientas** > **Archivos de registro** . La sección de archivos de registros se utiliza para definir cómo se gestionarán los registros. El programa elimina automáticamente los registros antiguos para ahorrar espacio en el disco duro. Puede especificar las siguientes opciones para los archivos de registro:

Eliminar automáticamente los registros con una antigüedad de más de (días): las entradas de registro anteriores al número de días especificado se eliminarán de manera automática.

Optimizar los archivos de registro automáticamente: si se marca esta opción, los archivos de registro se desfragmentarán automáticamente si el porcentaje es superior al valor especificado en **Si la cantidad de registros eliminados supera el (%)**.

Haga clic en **Optimizar ahora** para iniciar la desfragmentación de los archivos de registro. Todas las entradas de registro vacías se eliminan durante este proceso, lo cual aumenta el rendimiento y la velocidad durante el proceso de registro. Esta mejora es especialmente notable cuando los registros contienen muchas entradas.

Nivel mínimo de detalle al registrar: especifica el nivel de contenido mínimo de los sucesos que se van a registrar.

- **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".
- **Grave**: registra únicamente los errores graves (errores al iniciar la protección antivirus, cortafuegos personal, etc.).

Haga clic en **Activar protocolo de texto** para almacenar registros en otro formato de archivo y fuera de los archivos de registro:

- **Tipo**: si elige el formato de archivo **Sin formato**, los registros se almacenarán en un archivo de texto; los datos irán separados por pestañas. Se aplica lo mismo al formato de archivo separado por comas **CSV**. Si elige **Suceso**, los registros se almacenarán en el registro de sucesos de Windows (se puede ver mediante el visor de sucesos del panel de control) en lugar del de archivos.
- **Directorio de destino**: lugar en el que se almacenarán los archivos (aplicable solo con Sin formato/CSV). Cada sección del registro cuenta con su propio archivo con nombre de archivo predefinido (por ejemplo, virlog.txt para la sección

Amenazas detectadas de los archivos de registro si usa el formato de archivo de texto sin formato para almacenar registros).

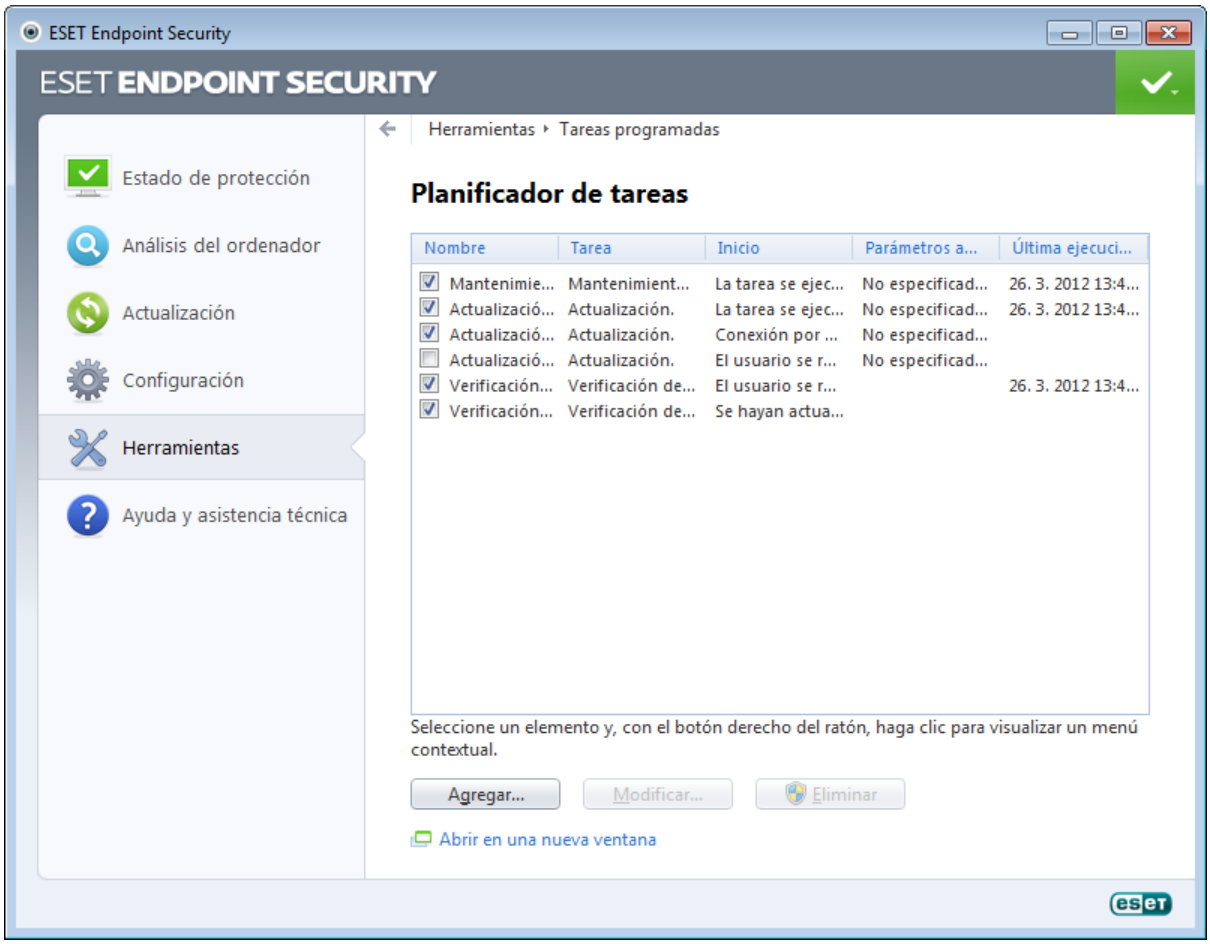
El botón **Eliminar registro** borra todos los registros almacenados seleccionados actualmente en el menú desplegable **Tipo**.

4.6.2 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 Security 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 de base de firmas de virus, análisis de virus, 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** 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.



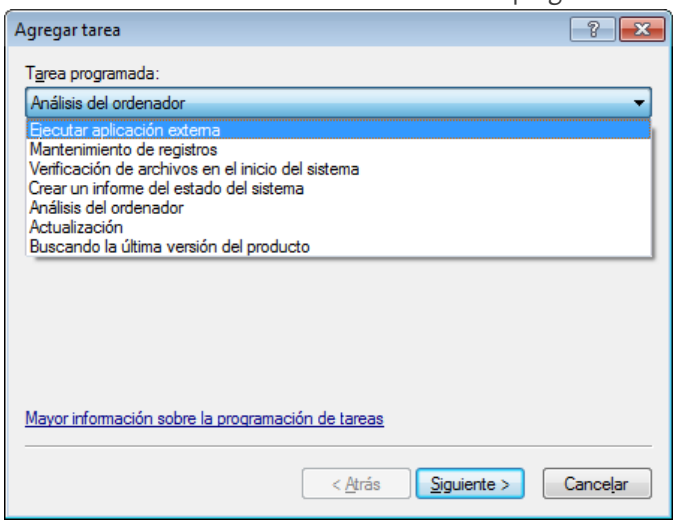
De forma predeterminada, en el **Planificador de tareas** se muestran las siguientes tareas programadas:

- **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)
- **Verificación de la ejecución de archivos en el inicio** (después de actualizar correctamente la base de firmas de virus)

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

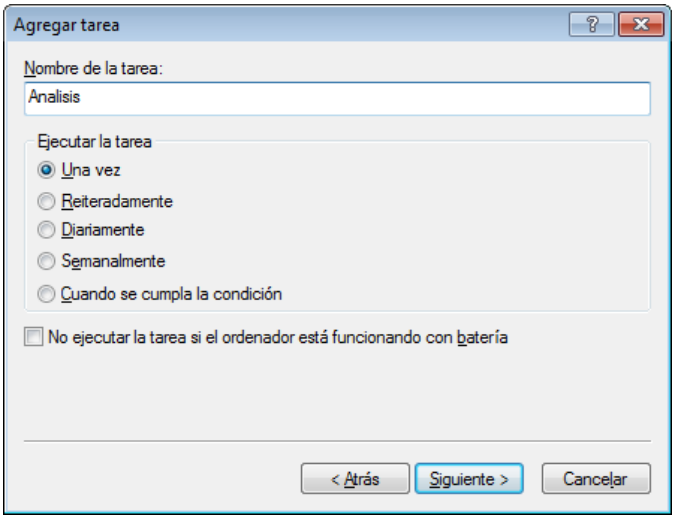
Agregar una nueva tarea

1. Haga clic en **Agregar...**, en la parte inferior de la ventana.
2. Seleccione la tarea deseada en el menú desplegable.



3. Introduzca un nombre de tarea y seleccione una de las opciones de programación:

- **Una vez**: la tarea se ejecutará solo una vez en la fecha y la hora predefinidas.
- **Reiteradamente**: la tarea se ejecutará en el intervalo especificado (en horas).
- **Diariamente**: la tarea se ejecutará cada día a la hora especificada.
- **Semanalmente** : la tarea se ejecutará una o varias veces por semana, el día/días y la hora seleccionados.
- **Cuando se cumpla la condición**: la tarea se ejecutará tras un suceso especificado.



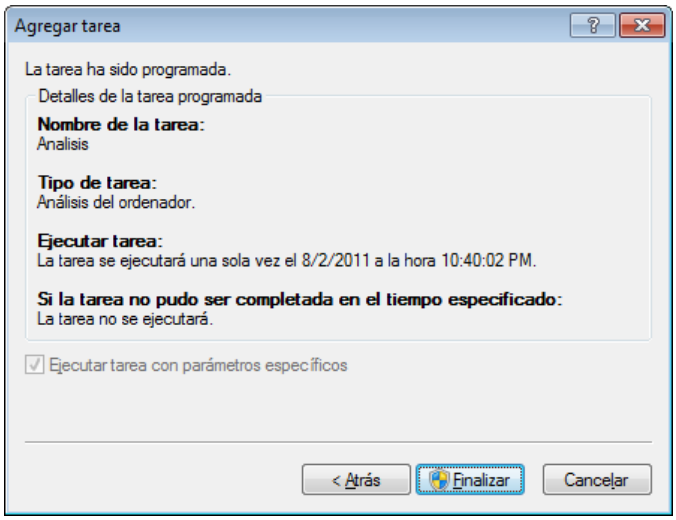
4. Según la opción de programación seleccionada en el paso anterior, se mostrará uno de estos cuadros de diálogo:

- **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.

5. Si la tarea no se pudo ejecutar en el tiempo predefinido, puede especificar cuándo se ejecutará de nuevo:

- Esperar hasta la próxima activación programada
- Ejecutar la tarea tan pronto como sea posible
- Ejecutar la tarea inmediatamente si el tiempo transcurrido desde la última ejecución es superior a -- horas

6. En el último paso, puede revisar la tarea que desea programar. Haga clic en **Finalizar** para aplicar la tarea.



4.6.2.1 Creación de tareas nuevas

Para crear una tarea nueva en el Planificador de tareas, haga clic en el botón **Agregar** 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 (controladores, aplicaciones, etc.) y evalúa el nivel de riesgo de cada componente.
- **Análisis del ordenador**: analiza los archivos y las carpetas del ordenador.
- **Actualizar**: programa una tarea de actualización mediante la actualización de la base de firmas de virus y los módulos del programa.

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**. Haga clic en **Siguiente** para introducir el nombre de la tarea en el campo **Nombre de la tarea**. Seleccione la frecuencia de la tarea. Están disponibles las opciones siguientes: **Una vez**, **Reiteradamente**, **Diariamente**, **Semanalmente** y **Cuando se cumpla la condición**. Utilice la opción **No ejecutar la tarea si el ordenador está funcionando con batería** para minimizar los recursos del sistema cuando un portátil está funcionando con la alimentación de la batería. Según la frecuencia seleccionada, se le solicitarán diferentes parámetros de actualización. 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 tres opciones siguientes:

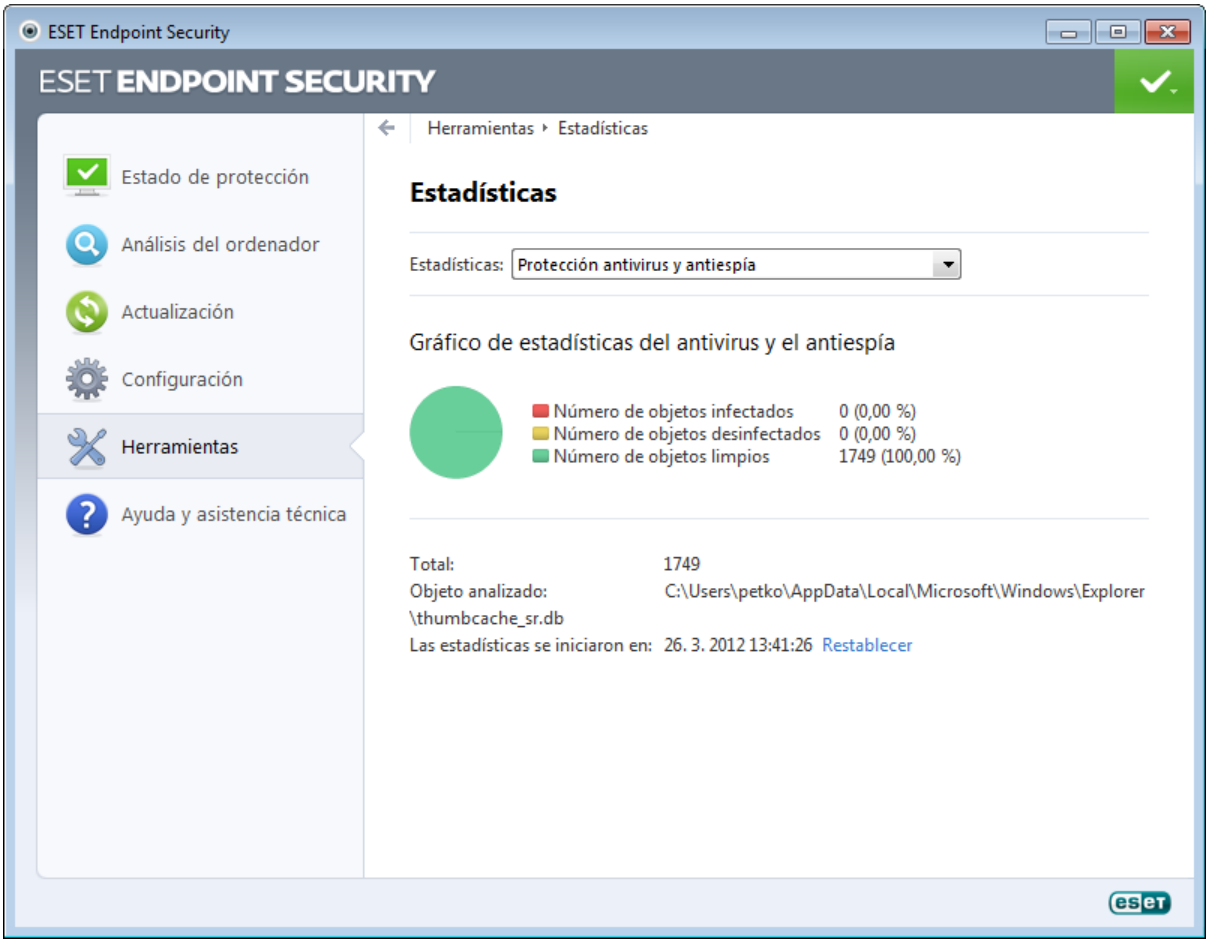
- **Esperar hasta la próxima activación programada**
- **Ejecutar la tarea tan pronto como sea posible**
- **Ejecutar la tarea inmediatamente si el tiempo transcurrido desde la última ejecución supera el intervalo especificado** (el intervalo puede definirse utilizando el cuadro Intervalo de la tarea)

En el paso siguiente, se muestra una ventana de resumen que contiene información acerca de la tarea programada actualmente; la opción **Ejecutar tarea con parámetros específicos** debe activarse automáticamente. Haga clic en el botón **Finalizar**.

Aparecerá un cuadro de diálogo que permite al usuario elegir los perfiles que desea utilizar para la tarea programada. En este paso, el usuario puede especificar un perfil principal y otro alternativo, que se utilizará si la tarea no se puede completar con el perfil principal. Para confirmar, haga clic en **Aceptar** en la ventana de **Perfiles de actualización**. La nueva tarea se agregará a la lista de tareas programadas actualmente.

4.6.3 Estadísticas de protección

Para ver un gráfico de datos estadísticos relacionados con los módulos de protección de ESET Endpoint Security, 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.



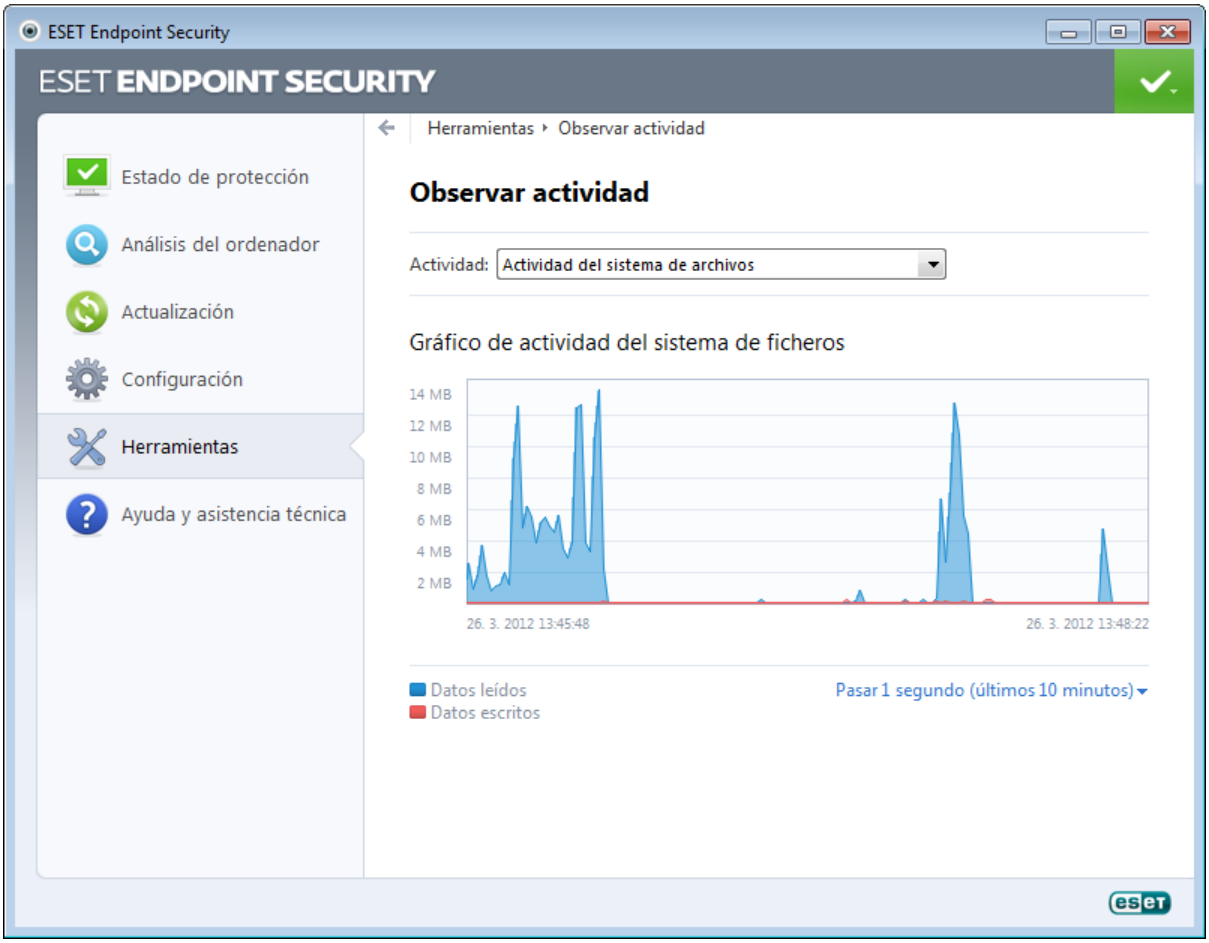
Están disponibles los siguientes gráficos de estadísticas:

- **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**: muestra únicamente los objetos descargados por navegadores web.
- **Protección antispam del cliente de correo electrónico**: muestra el historial de estadísticas de correo no deseado desde el último inicio.

Debajo de los gráficos de estadísticas, se muestra el número total de objetos analizados, el último objeto analizado y la marca de tiempo de los datos estadísticos. Haga clic en **Restablecer** para borrar toda la información estadística.

4.6.4 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. Para cambiar el intervalo de tiempo, haga clic en la opción **Pasar 1...** disponible en la parte inferior derecha de la ventana.



Están disponibles las opciones siguientes:

- **Pasar 1 segundo (últimos 10 minutos)**: 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 los 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.

En el menú desplegable **Actividad** también puede seleccionar la visualización de la **Actividad de red**. La visualización y las opciones del gráfico para la **Actividad del sistema de archivos** y la **Actividad de red** son las mismas, con la única diferencia de que el último muestra datos recibidos (azul) y datos enviados (rojo).

4.6.5 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:

- **Comparar**: compara dos registros existentes.
- **Crear**: crea un registro nuevo. Espere hasta que el registro de ESET SysInspector esté completo (**estado** Creado).
- **Eliminar**: elimina de la lista los registros seleccionados.

Al hacer clic con el botón derecho del ratón en uno o varios de los registros seleccionados, se mostrarán las siguientes opciones del menú contextual:

- **Mostrar**: abre el registro seleccionado en ESET SysInspector (igual que al hacer doble clic en un registro).
- **Eliminar todos**: elimina todos los registros.
- **Exportar**: exporta el registro a un archivo .xml .xml comprimido.

4.6.6 ESET Live Grid

ESET Live Grid (la próxima generación de ESET ThreatSense.Net) es un sistema avanzado de alerta que combate las amenazas emergentes según su reputación. El laboratorio de virus de ESET utiliza la transmisión en tiempo real de información relacionada con las amenazas procedente de la nube para actualizar sus mecanismos de defensa y ofrecer un nivel de protección constante. 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 Live Grid. Existen dos opciones:

1. La activación de ESET Live Grid no es obligatoria. El software no perderá funcionalidad y seguirá recibiendo la mejor protección que ofrecemos.
2. Puede configurar ESET Live Grid para enviar información anónima acerca de nuevas amenazas y sobre la ubicación del nuevo código malicioso. 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 Live Grid 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 Security está configurado para enviar archivos sospechosos para su análisis detallado en los laboratorios 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.

En el menú de configuración de ESET Live Grid se ofrecen varias opciones para activar y desactivar ESET Live Grid, que sirve para enviar archivos sospechosos e información estadística anónima a los laboratorios de ESET. Puede acceder a este menú desde el árbol de configuración avanzada haciendo clic en **Herramientas** > **ESET Live Grid**.

Participar en ESET Live Grid : activa o desactiva ESET Live Grid, que sirve para enviar archivos sospechosos e información estadística anónima a los laboratorios de ESET.

No enviar estadísticas: seleccione esta opción si no desea enviar información anónima acerca de su ordenador desde ESET Live Grid. Esta información está relacionada con las amenazas detectadas recientemente y puede incluir el nombre de la amenaza, la fecha y la hora de detección, la versión de ESET Endpoint Security, la versión del sistema operativo del ordenador y la configuración regional. Normalmente, las estadísticas se envían al servidor de ESET una o dos veces al día.

No enviar archivos: los archivos sospechosos que recuerdan a las amenazas en su contenido o comportamiento no se

envían a ESET para que realice un análisis con la tecnología ESET Live Grid.

Configuración avanzada: abre una ventana con más opciones de configuración de ESET Live Grid.

Si utilizó ESET Live Grid anteriormente pero lo desactivó, es posible que aún haya paquetes de datos pendientes de envío. Incluso después de su desactivación, estos paquetes se enviarán a ESET en la siguiente ocasión. Después, no se crearán más paquetes.

4.6.6.1 Archivos sospechosos

En la ficha **Archivos** de la configuración avanzada de ESET Live Grid puede configurar el modo de envío de amenazas al laboratorio de virus de ESET para su análisis.

Si encuentra un archivo sospechoso, puede enviarlo a nuestros laboratorios para su análisis. Si resulta ser una aplicación maliciosa, su detección se agregará a la siguiente actualización de la base de firmas de virus.

Filtro de exclusión: esta opción le permite excluir del envío determinados archivos o carpetas. Los archivos mostrados en la lista nunca se enviarán al laboratorio de ESET para su análisis, aunque contengan código sospechoso. Esta opción puede ser útil, por ejemplo, para excluir archivos que puedan contener información confidencial, como documentos u hojas de cálculo. 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.

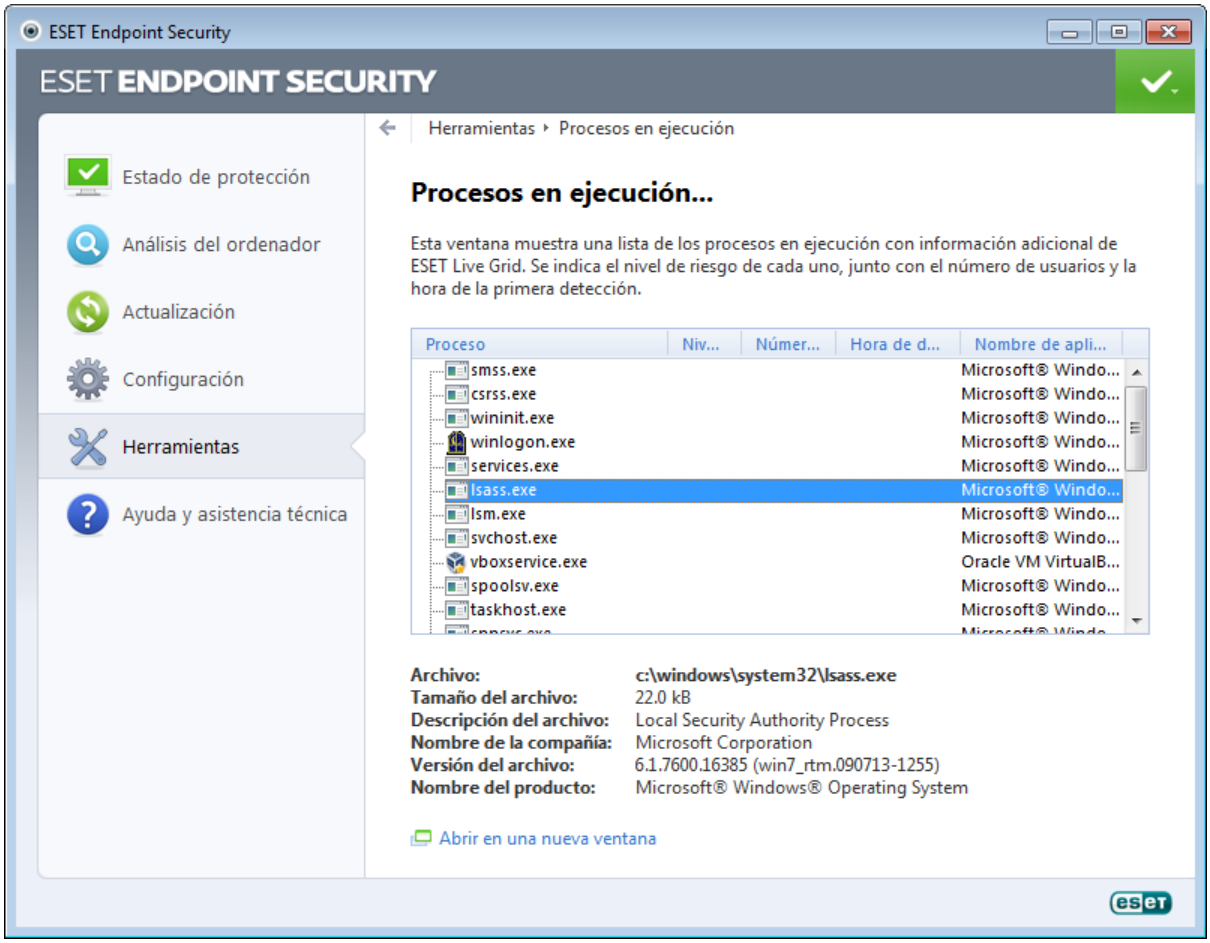
Correo electrónico de contacto (opcional): su correo electrónico de contacto se puede enviar con cualquier archivo sospechoso y puede servir para localizarle si se necesita más información para el análisis. Tenga en cuenta que no recibirá una respuesta de ESET, a no ser que sea necesaria más información.

En esta sección, también puede elegir si los archivos y la información estadística se enviarán mediante ESET Remote Administrator o directamente a ESET. Si quiere asegurarse de que los archivos sospechosos y la información estadística se entregarán a ESET, seleccione la opción **Mediante administración remota o directamente a ESET**. En este caso, los archivos y las estadísticas se envían por todos los medios disponibles. El envío de archivos sospechosos mediante administración remota envía los archivos y las estadísticas al servidor de administración remota, lo que garantizará su envío posterior a los laboratorios de virus de ESET. Si se selecciona la opción **Directamente a ESET**, todos los archivos sospechosos y la información estadística se envían directamente al laboratorio de virus de ESET desde el programa.

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

4.6.7 Procesos en ejecución

Los procesos en ejecución indica los programas o procesos que se están ejecutando en el ordenador e informa a ESET de forma inmediata y continua de las nuevas amenazas. ESET Endpoint Security proporciona información detallada sobre los procesos en ejecución para proteger a los usuarios con la tecnología ESET Live Grid.



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.

Nivel de riesgo: generalmente, la tecnología ESET Endpoint Security y ESET Live Grid 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, pondera el potencial de actividad maliciosa. Según estas heurísticas, a los objetos se les asignará un nivel de riesgo desde el valor "1: correcto" (verde) hasta "9: peligroso" (rojo).

NOTA: las aplicaciones conocidas marcadas con un Correcto (verde) son totalmente seguras (incluidas en lista blanca) y no se analizarán; esto aumentará 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 Live Grid se encarga de recopilar esta información.

Tiempo de detección: tiempo transcurrido desde que la tecnología ESET Live Grid detectó la aplicación.

NOTA: cuando una aplicación está marcada 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, puede enviarlo para su análisis 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.

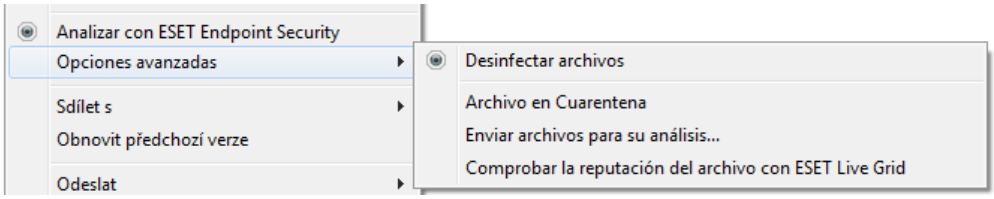
Nombre de aplicación: nombre de un programa o un proceso.

Abrir en una ventana nueva: la información de los procesos en ejecución se abrirá en una ventana nueva.

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

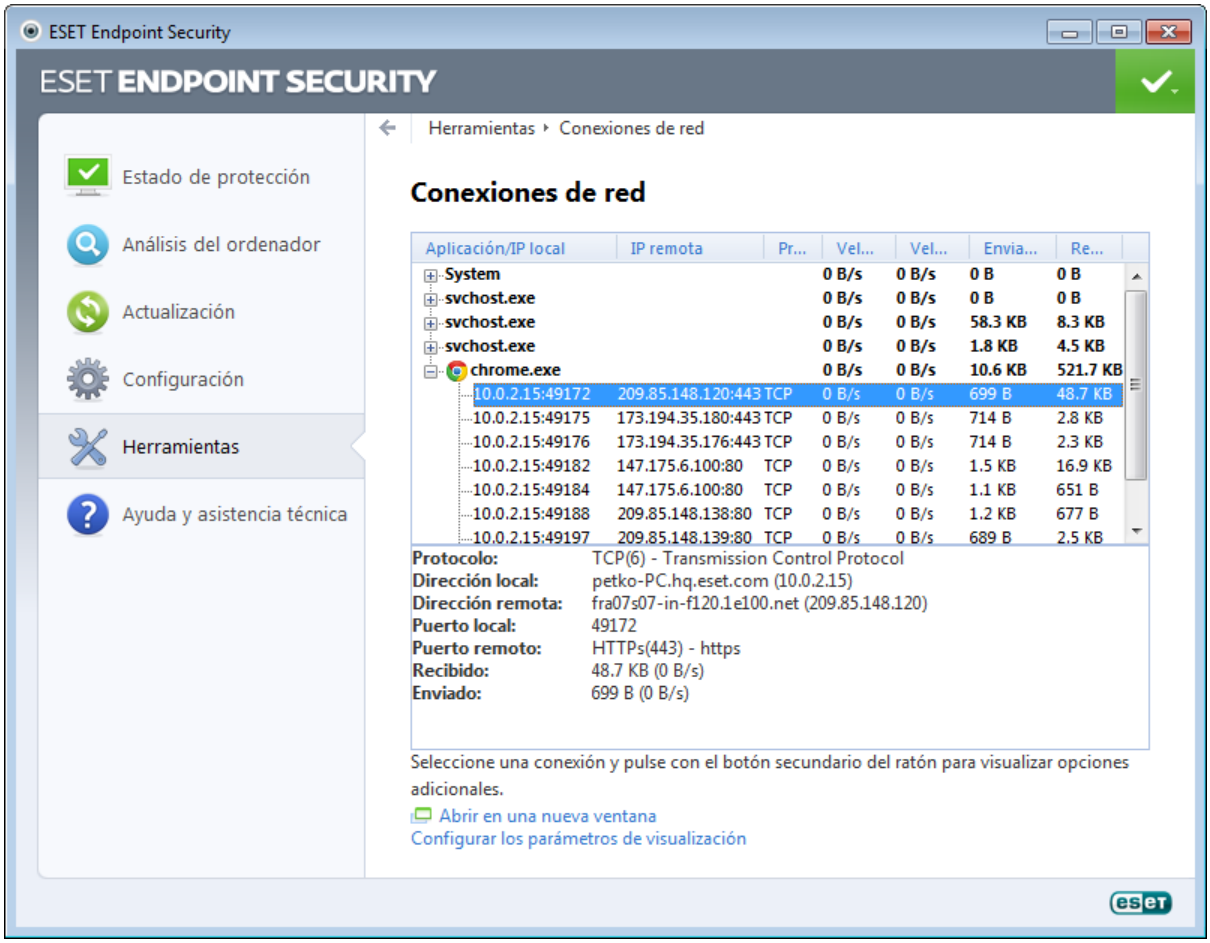
- **Archivo**: ubicación de una aplicación en el ordenador.
- **Tamaño del archivo**: tamaño del archivo en KB (kilobytes) o MB (megabytes).
- **Descripción del archivo**: características del archivo en función de la descripción del sistema operativo.
- **Nombre de la compañía**: nombre del proveedor o el proceso de la aplicación.
- **Versión del archivo**: información sobre el editor de la aplicación.
- **Nombre del producto**: nombre de la aplicación o nombre comercial.

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 Live Grid**.



4.6.8 Conexiones de red

En la sección Conexiones de red, puede ver una lista de las conexiones activas y pendientes. Esto le ayuda a controlar todas las aplicaciones que establecen conexiones salientes.



En la primera línea se muestra el nombre de la aplicación y la velocidad de transferencia de datos. Para ver la lista de conexiones establecidas por la aplicación (e información más detallada), haga clic en **+**.

Aplicación/IP local: nombre de la aplicación, direcciones IP locales y puertos de comunicación.

IP remota: dirección IP y número de puerto de un ordenador remoto determinado.

Protocolo: protocolo de transferencia utilizado.

Velocidad de carga/velocidad de descarga: la velocidad actual de los datos salientes y entrantes.

Enviados/recibidos: cantidad de datos intercambiados dentro de la conexión.

Abrir en una nueva ventana: muestra información en una ventana separada.

La opción **Configurar los parámetros de visualización...** de la pantalla de conexiones de red introduce la estructura de configuración avanzada en la sección, permitiéndole modificar las opciones de visualización de conexiones:

Resolver nombres: si es posible, todas las direcciones de red se mostrarán en formato DNS y no lo harán en el formato numérico de dirección IP.

Solo mostrar las conexiones bajo el protocolo TCP: la lista muestra únicamente las conexiones que pertenecen al protocolo TCP.

Mostrar conexiones con puertos abiertos en los cuales el ordenador esté en escucha: seleccione esta opción para mostrar únicamente conexiones en las que no haya ninguna comunicación establecida actualmente, pero en las que el sistema haya abierto un puerto y esté esperando una conexión.

Mostrar también conexiones internas locales: seleccione esta opción únicamente para mostrar conexiones en las que la ubicación remota sea un sistema local, lo que se denominan conexiones localhost.

Haga clic con el botón derecho del ratón en una conexión para ver más opciones, como:

Denegar la comunicación para la conexión: finaliza la comunicación establecida. Esta opción solo está disponible al hacer clic en una conexión activa.

Mostrar detalles: seleccione esta opción para mostrar información detallada sobre la conexión seleccionada.

Velocidad de actualización: selecciona la frecuencia de actualización de las conexiones activas.

Actualizar ahora: vuelve a cargar la ventana Conexiones de red.

Las opciones siguientes están disponibles al hacer clic en una aplicación o proceso, no en una conexión activa:

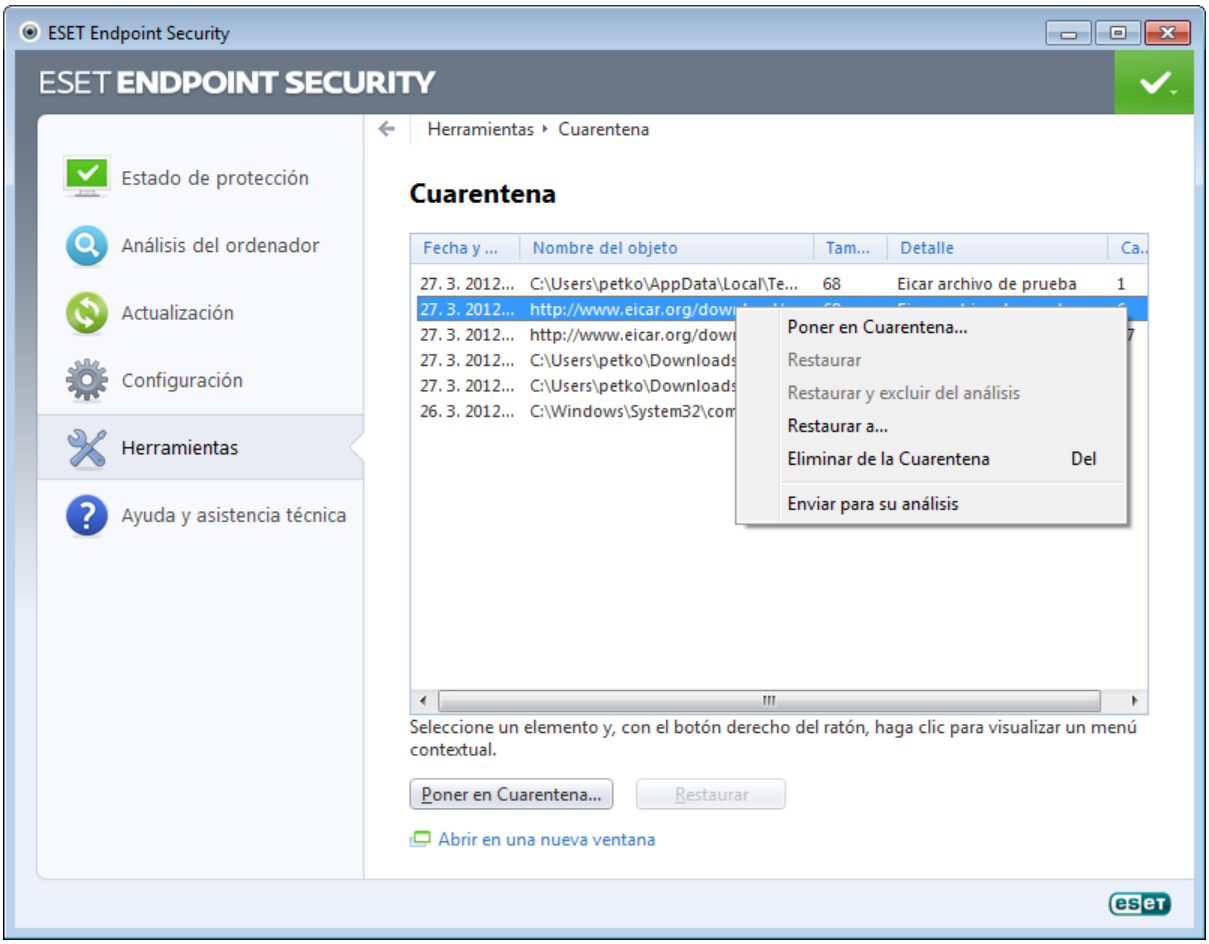
Bloquear temporalmente la conexión: rechaza las conexiones actuales de una aplicación determinada. Si se establece una nueva conexión, el cortafuegos utiliza una regla predefinida. La descripción de la configuración puede encontrarse en la sección Reglas y zonas.

Permitir temporalmente la conexión: permite las conexiones actuales de una aplicación determinada. Si se establece una nueva conexión, el cortafuegos utiliza una regla predefinida. La descripción de la configuración puede encontrarse en la sección Reglas y zonas.

4.6.9 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 Security 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 a los laboratorios 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 que contiene varias amenazas).

Puesta de archivos en cuarentena

ESET Endpoint Security copia en cuarentena automáticamente los archivos eliminados (si no ha cancelado esta opción en la ventana de alerta). Si lo desea, puede copiar en cuarentena cualquier archivo sospechoso de forma manual, haciendo clic en el botón **Cuarentena...**. En este caso, el archivo original no 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. Utilice la opción **Restaurar**, disponible en el menú contextual que se abre al hacer clic con el botón derecho del ratón en el archivo en la ventana de cuarentena, para realizar esta tarea. i un archivo está marcado como Aplicación potencialmente indeseable, se activa la opción **Restaurar y excluir del análisis**. Puede obtener más información sobre este tipo de aplicación en el glosario El menú contextual también ofrece la opción **Restaurar a...**, que le permite restaurar archivos en una ubicación distinta a la original de la cual se eliminaron.

NOTA: si el programa ha puesto en cuarentena un archivo no dañino por error, excluyalo 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 determinado incorrectamente que un archivo está infectado (por ejemplo, por el análisis heurístico del código) 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.

4.6.10 Envío de archivos para el análisis

El cuadro de diálogo de envío de archivos le permite enviar un archivo a ESET para que lo analice; esta opción está disponible en **Herramientas** > **Enviar archivo para su análisis**. Si encuentra un archivo en su ordenador que se comporta de manera sospechosa, puede enviarlo al laboratorio de virus de ESET para su análisis. Si resulta que el archivo es una aplicación maliciosa, su detección se agregará a una de las siguientes actualizaciones.

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 un archivo a ESET, asegúrese de que cumple uno o más de los siguientes criterios:
- El archivo no se detecta en absoluto.
- El archivo 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.

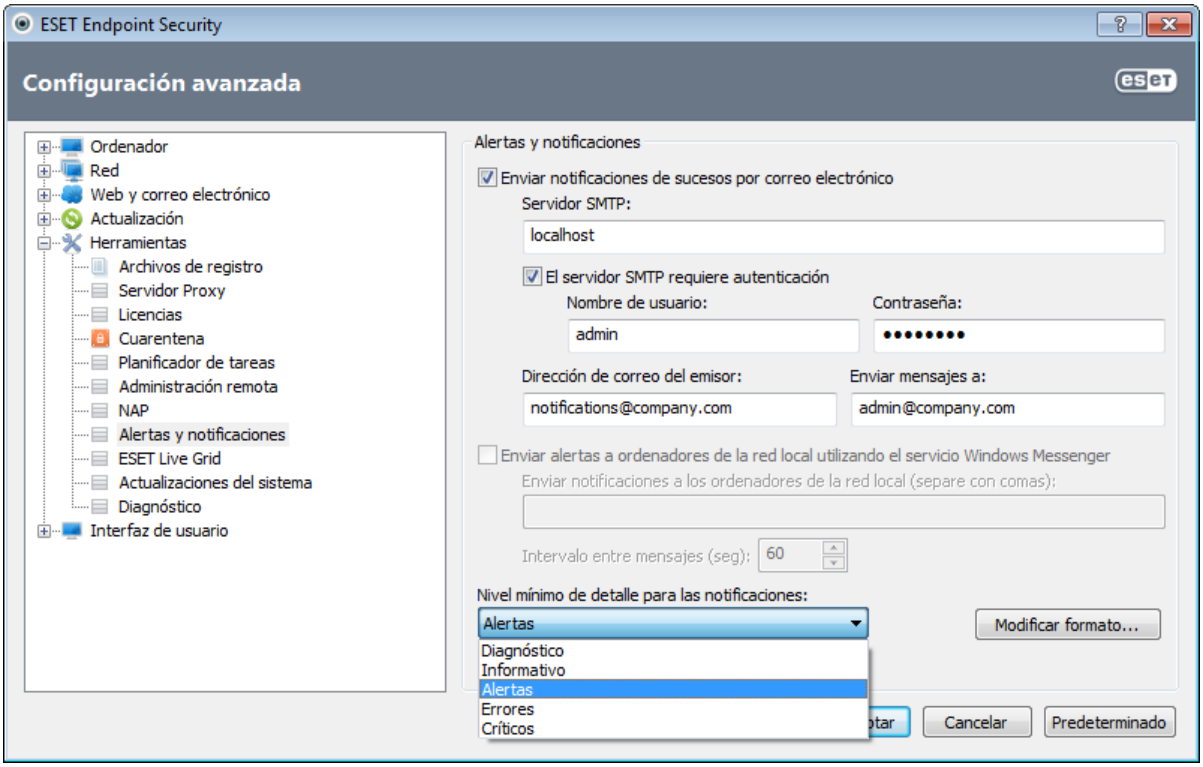
Seleccione la descripción en el menú desplegable **Motivo de envío del archivo** que mejor se ajuste a su mensaje:
- **Archivo sospechoso**,
- **Falso positivo** (archivos que se detectan como amenazas pero no están infectados)
- y **Otros**.

Archivo: la ruta del archivo 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.

4.6.11 Alertas y notificaciones

ESET Endpoint Security es compatible con el envío de correos electrónicos si se produce un evento con el nivel de detalle seleccionado Haga clic en la casilla de verificación **Enviar notificaciones de sucesos por correo electrónico** para activar esta característica y activar las notificaciones por correo electrónico.



Servidor SMTP: el servidor SMTP utilizado para enviar notificaciones.

Nota: los servidores SMTP con cifrado SSL/TLS no son compatibles con ESET Endpoint Security.

El servidor SMTP requiere autenticación: si el servidor SMTP requiere autenticación, estos campos deberían cumplimentarse con un nombre de usuario y contraseña 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.

Enviar mensajes a: este campo especifica la dirección de correo del receptor, que se mostrará en el encabezado de los mensajes de notificación.

Enviar alertas a ordenadores de la red local utilizando el servicio Windows: seleccione esta casilla de verificación para enviar mensajes a ordenadores de la red local a través del servicio de mensajería de Windows®.

Enviar notificaciones a los ordenadores de la red local (separe con comas): escriba los nombres de los ordenadores que recibirán notificaciones a través del servicio de mensajería de Windows®.

Intervalo entre mensajes (seg): para cambiar la longitud del intervalo entre notificaciones enviadas a través de la red local, escriba el intervalo de tiempo deseado en segundos.

Nivel mínimo de detalle para las notificaciones: especifica el nivel mínimo de detalle de las notificaciones que se van a enviar.

Modificar formato: las comunicaciones entre el programa y un usuario o administrador de sistema 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 es el óptimo en la mayoría de los casos. En algunas circunstancias, tendrá que cambiar el formato del mensaje. Para ello, haga clic en Modificar formato....

4.6.11.1 Formato de mensajes

Aquí puede configurar el formato de los mensajes de sucesos que aparece en los ordenadores remotos.

Los mensajes de alerta de amenaza y de notificación 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.

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

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

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

Usar caracteres del alfabeto local: convierte un mensaje de correo electrónico a la codificación de caracteres ANSI basándose en la configuración regional de Windows (p. ej., windows-1250). Si deja esta opción sin marcar, se convertirá y codificará un mensaje en ACSII de 7 bits (p. ej., "á" se cambiará a "a" y un símbolo desconocido, a "?").

Usar codificación de caracteres locales: 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 (ááíóú).

4.6.12 Actualizaciones del sistema

La característica Windows Update es un componente importante de protección de los usuarios de software malicioso, por eso es fundamental instalar las actualizaciones de Microsoft Windows en cuanto se publiquen. ESET Endpoint Security 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.

4.6.13 Diagnóstico

El diagnóstico proporciona volcados de memoria de los procesos de ESET (p. ej., 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 Security. Están disponibles dos tipos de volcados:

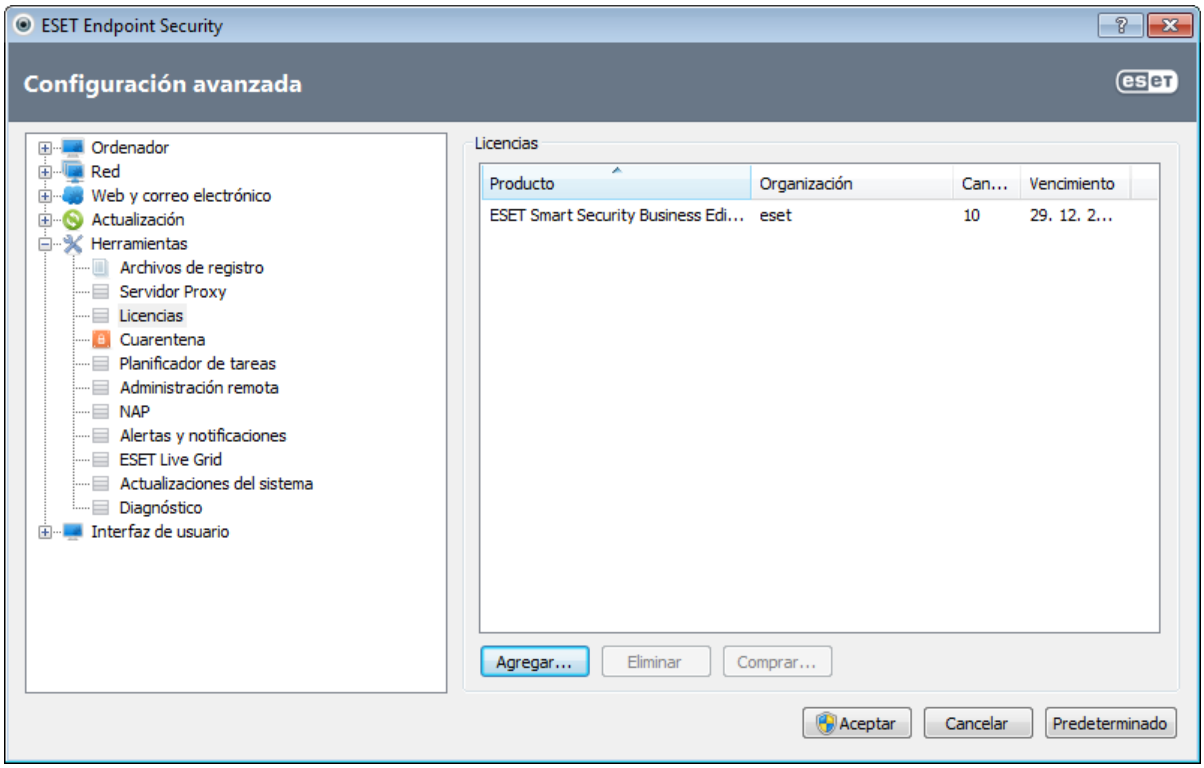
- **Volcado de memoria completo**: registra todo el contenido de la memoria del sistema cuando una aplicación se detiene de forma inesperada. Los volcados de memoria completos pueden contener datos de procesos que se estaban ejecutando cuando se generó el volcado.
- **Minivolcado**: registra la información mínima necesaria para identificar el motivo del bloqueo inesperado de la aplicación. Este tipo de volcado puede resultar útil cuando el espacio es limitado. Sin embargo, dada la poca información que proporciona, 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.
- Seleccione **No generar volcado de memoria** (opción predeterminada) para desactivar esta característica.

Directorio de destino: directorio en el que se genera el volcado durante el bloqueo. Haga clic en **Abrir carpeta** para

abrir este directorio en una ventana nueva del Explorador de Windows.

4.6.14 Licencias

En la sección **Licencias**, puede administrar las claves de licencia de ESET Endpoint Security y otros productos de ESET, como ESET Remote Administrator. Las claves de licencia se proporcionan después de la compra, junto con el nombre de usuario y la contraseña. Para **agregar/quitar** una clave de licencia, haga clic en el botón correspondiente de la ventana del administrador de licencias (**Licencias**). Puede acceder al administrador de licencias desde el árbol de configuración avanzada haciendo clic en **Herramientas** > **Licencias**.



La clave de licencia es un archivo de texto que contiene información acerca del producto adquirido: su propietario, número de licencias y fecha de expiración.

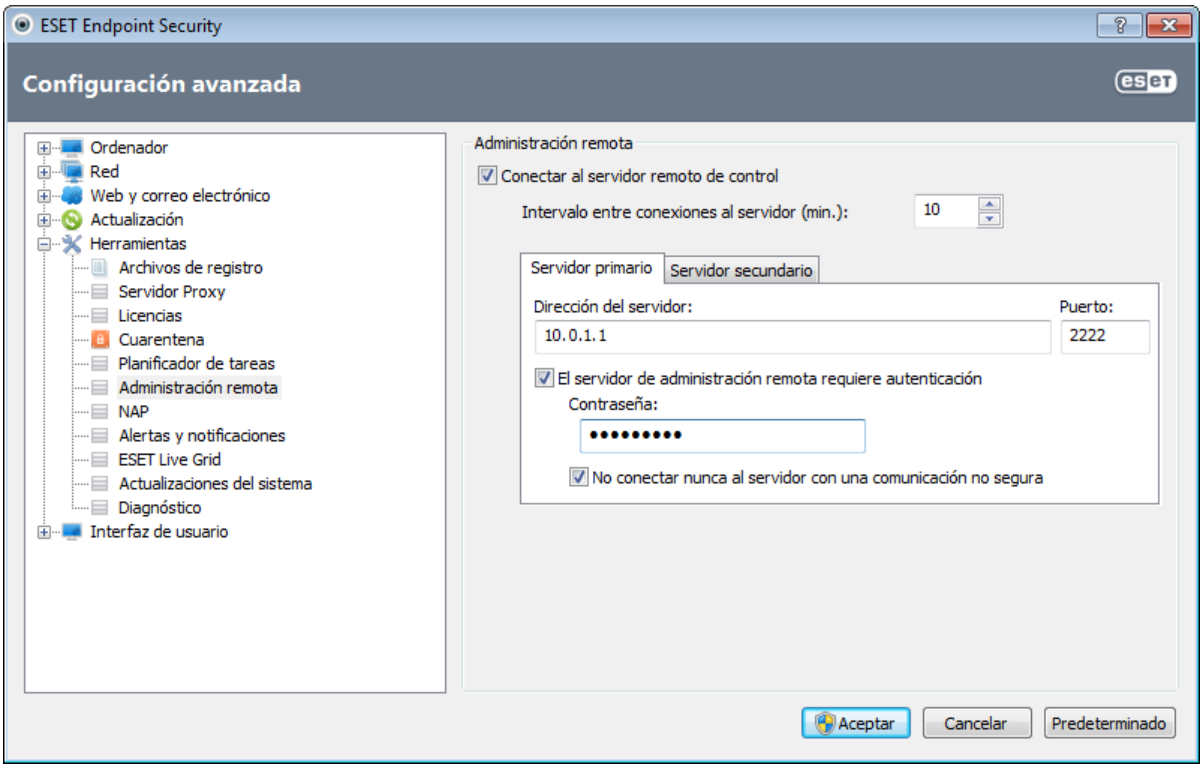
La ventana del administrador de licencias le permite cargar y ver el contenido de una clave de licencia mediante el botón **Agregar**, de modo que puede ver su información en el administrador. Para eliminar un archivo de licencia de la lista, selecciónelo y haga clic en **Eliminar**.

Si una clave de licencia ha expirado y desea renovarla, haga clic en el botón **Comprar** para acceder a la tienda en línea.

4.6.15 Administración remota

ESET Remote Administrator (ERA) es una potente herramienta que sirve para gestionar las directivas de seguridad y obtener información general sobre la seguridad global en una red. Es especialmente útil cuando se aplica a redes de gran tamaño. ERA no se limita a aumentar la seguridad, sino que también facilita la administración de ESET Endpoint Security en estaciones de trabajo cliente. Puede instalar, configurar, ver registros, programar actualizaciones de tareas, analizar tareas, etc. La comunicación entre los productos de seguridad de ESET y ESET Remote Administrator (ERAS) requiere una correcta configuración en ambos extremos.

Las opciones de configuración de la administración remota están disponibles en la ventana principal del programa ESET Endpoint Security. Haga clic en **Configuración** > **Especificar configuración avanzada** > **Herramientas** > **Administración remota**.



Para activar la administración remota, seleccione la opción **Conectar al servidor de administración remota**. Así, podrá acceder a las opciones que se describen a continuación:

Intervalo entre conexiones al servidor (min.):: esta opción le indica con qué frecuencia se conectará el producto de seguridad de ESET a ERAS para enviar los datos.

Servidor primario, servidor secundario: normalmente, basta con configurar el servidor primario. Si ejecuta varios servidores ERA en la red, tiene la opción de añadir otra conexión del servidor ERA secundario. Esta conexión le servirá como solución de restauración. De este modo, si el servidor primario deja de estar accesible, la solución de seguridad de ESET se pondrá en contacto automáticamente con el servidor ERA secundario y, simultáneamente, intentará restablecer la conexión con el servidor primario. Cuando esta conexión vuelva a estar activa, la solución de seguridad de ESET utilizará de nuevo el servidor primario. La configuración de dos perfiles del servidor de administración remota es ideal para clientes móviles con clientes que se conecten tanto desde la red local como desde fuera de la red.

Dirección del servidor: especifique el nombre del servidor DNS o la dirección IP del servidor que ejecuta ERAS.

Puerto: este campo contiene un puerto del servidor predefinido utilizado para la conexión. Se recomienda dejar la configuración predeterminada del puerto en 2222.

Intervalo entre conexiones al servidor (min.): esta opción determina la frecuencia con que ESET Endpoint Security se conectará al ERA Server. Si se establece en 0, la información se enviará cada 5 segundos.

El servidor de administración remota requiere autenticación: le permite introducir una contraseña para conectarse a ERA Server, si es necesario.

No conectar nunca al servidor con una comunicación no segura: seleccione esta opción para desactivar la conexión de servidores ERA cuando se permita el acceso no autenticado (consulte **ERA Console** > **Opciones del servidor** > **Seguridad** > **Activar acceso no autenticado para clientes**).

Haga clic en **Aceptar** para confirmar los cambios y aplicar la configuración. ESET Endpoint Security utilizará esta configuración para conectarse a ERA Server.

4.7 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 Gráficos le permite ajustar el aspecto visual del programa y los efectos utilizados.

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 Ocultar ventanas de notificación. Aquí puede comprobar su estado, ver más información o eliminarlas de esta ventana.

Si desea disponer del máximo nivel de seguridad del software de seguridad, proteja la configuración mediante una contraseña para impedir los cambios no autorizados con la herramienta Configuración de acceso.

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 Security en el menú contextual.

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.

4.7.1 Gráficos

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

En la sección **Elementos de la interfaz de usuario**, la opción **Interfaz gráfica de usuario** debería desactivarse si los elementos gráficos ralentizan el ordenador o provocan otros problemas. Asimismo, es posible desactivar la interfaz gráfica para usuarios con discapacidades visuales, ya que podría entrar en conflicto con aplicaciones especiales que se utilizan para leer el texto que aparece en pantalla.

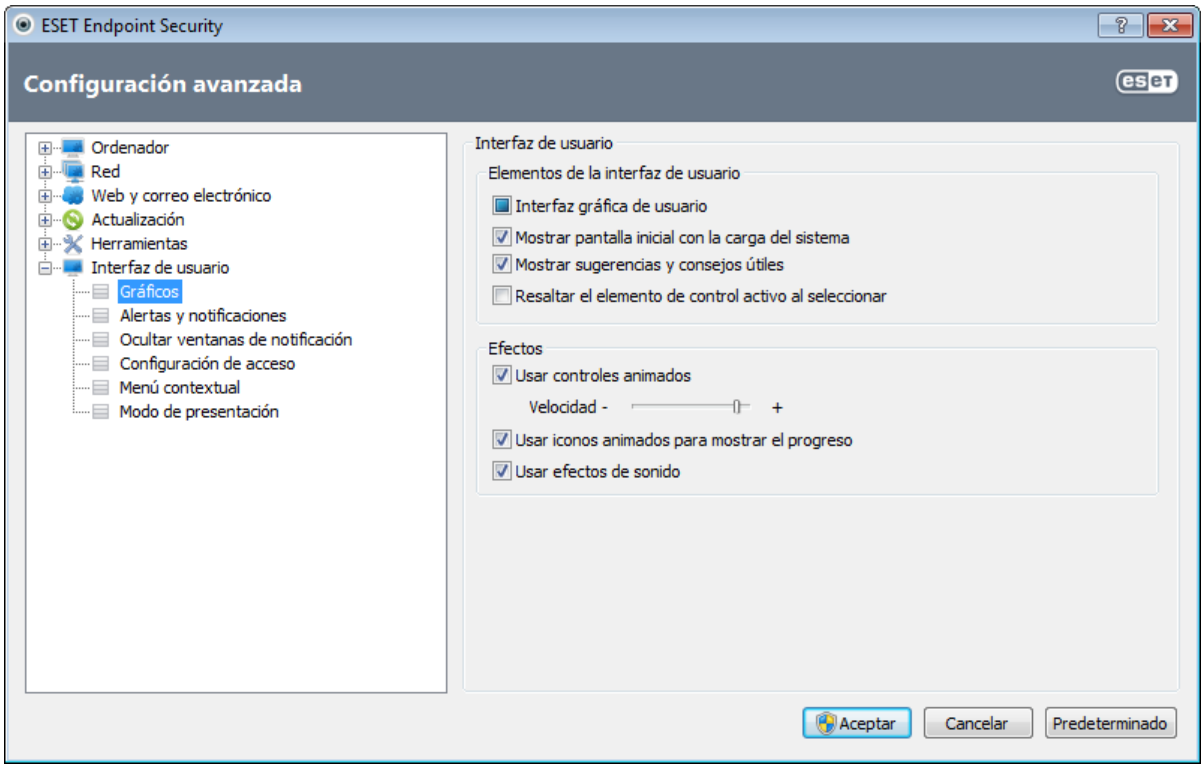
Si desea desactivar la pantalla inicial de ESET Endpoint Security, anule la selección de la opción **Mostrar pantalla inicial con la carga del sistema**.

Si se activa la opción **Mostrar sugerencias y consejos útiles**, se mostrará una breve descripción de cualquier opción cuando se coloque el cursor sobre ella. Si se activa la opción **Resaltar el elemento de control activo al seleccionar**, el sistema resaltará cualquier elemento que se encuentre en el área activa del cursor del ratón. El elemento resaltado se activará al hacer clic con el ratón.

Para aumentar o disminuir la velocidad de los efectos animados, seleccione la opción **Usar controles animados** y mueva la barra deslizante **Velocidad** a la izquierda o la derecha.

Para activar el uso de iconos animados para mostrar el progreso de varias operaciones, seleccione la opción **Usar iconos animados para mostrar el progreso**.

Si desea que el programa reproduzca un sonido cuando se produzca un suceso importante, seleccione **Usar efectos de sonido**. Tenga en cuenta que el sonido solo se reproducirá durante la ejecución de un análisis del ordenador o cuando haya finalizado.



4.7.2 Alertas y notificaciones

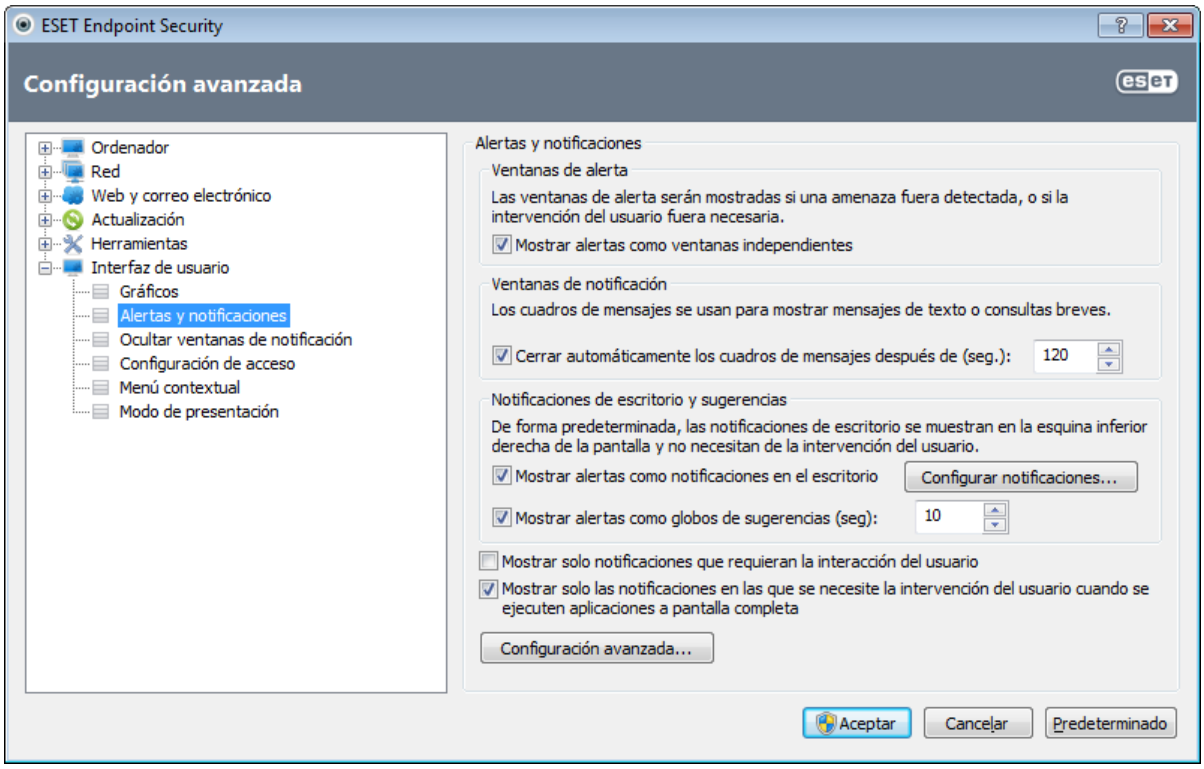
La sección de **Alertas y notificaciones** de **Interfaz de usuario** le permite configurar cómo gestiona ESET Endpoint Security las notificaciones del sistema (por ejemplo, mensajes de actualización correcta) y las alertas de amenaza. También puede definir si se muestra la hora y el nivel de transparencia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

El primer elemento es **Mostrar alertas**. Si desactiva esta opción, 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).

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

Las notificaciones del escritorio y los globos de sugerencias son medios de información que no requieren ni ofrecen 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 la opción **Mostrar alertas como notificaciones en el escritorio**. Haga clic en el botón **Configurar notificaciones** para acceder a opciones avanzadas como, por ejemplo, la modificación del tiempo de visualización de las notificaciones y la transparencia. Para obtener una vista previa del comportamiento de las notificaciones, haga clic en el botón **Vista previa**.

Para configurar la duración del tiempo de visualización de los globos de sugerencias, consulte la opción **Mostrar alertas como globos de sugerencias (seg.)** e introduzca el intervalo deseado en el campo adyacente.



La opción **Mostrar solo notificaciones que requieran la interacción del usuario** le permite cambiar las alertas y notificaciones que no requieren la intervención del usuario. Seleccione **Mostrar solo las notificaciones en las que se necesite la intervención del usuario cuando se ejecuten aplicaciones a pantalla completa** para eliminar todas las notificaciones que no sean interactivas.

Haga clic en **Configuración avanzada** para especificar más opciones de configuración de **Alertas y notificaciones**.

4.7.2.1 Configuración avanzada

En el menú desplegable **Nivel mínimo de detalle de los eventos a mostrar**, puede seleccionar el nivel de gravedad inicial de las alertas y notificaciones que se mostrarán.

- **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".
- **Grave**: registra únicamente los errores graves (errores al iniciar la protección antivirus, cortafuegos personal, 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.

4.7.3 Ocultar ventanas de notificación

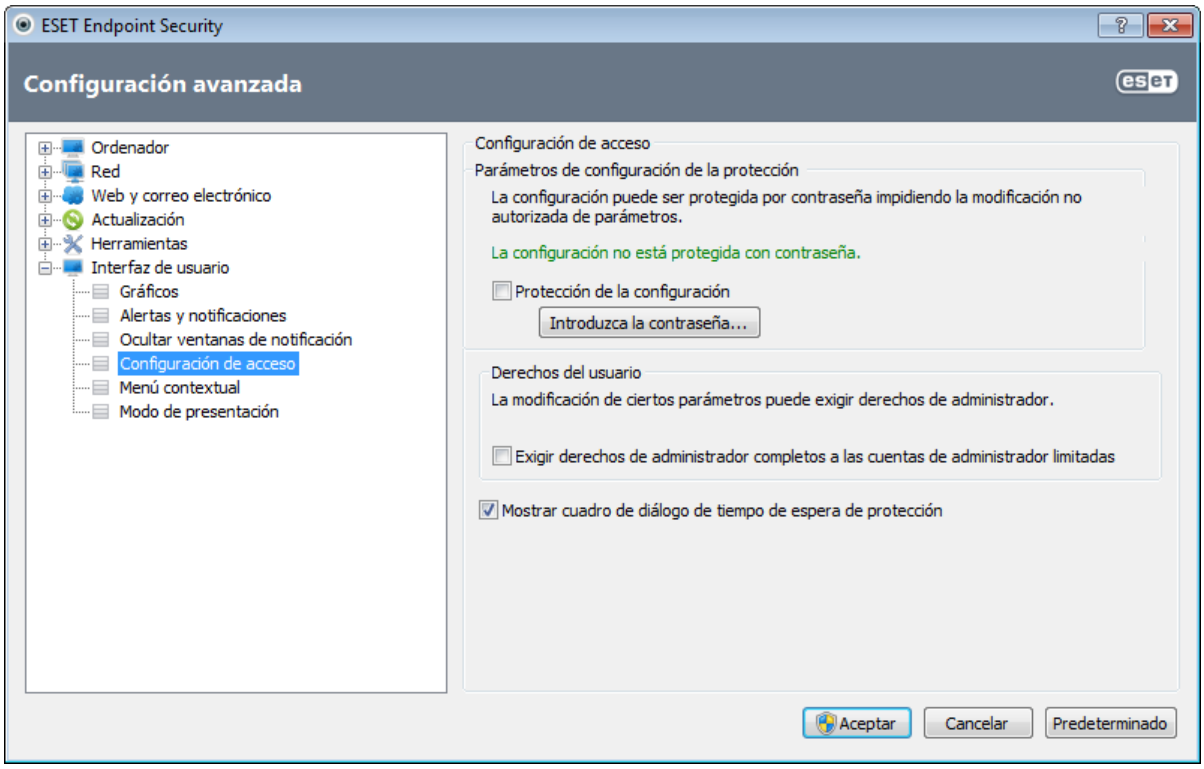
Si se seleccionó la opción **No mostrar este mensaje de nuevo** para cualquier ventana de notificación (alerta) que se haya mostrado anteriormente, esta aparecerá en la lista de ventanas de notificación ocultas. Las acciones que ahora se ejecutan automáticamente aparecen en la columna con el título **Confirmar**.

Mostrar: muestra una vista previa de las ventanas de notificación que no se muestran actualmente y para las que se ha configurado una acción automática.

Quitar: quita los elementos de la lista **Cuadros de mensajes ocultos**. Todas las ventanas de notificación eliminadas de la lista aparecerán de nuevo.

4.7.4 Configuración de acceso

Para ofrecer un nivel de seguridad máxima para su sistema, es esencial que ESET Endpoint Security se haya configurado correctamente. Una configuración incorrecta puede provocar la pérdida de datos importantes. Esta opción se encuentra en el submenú **Configuración de acceso** de la **Interfaz de usuario** en el árbol de configuración avanzada. Para evitar modificaciones no autorizadas, los parámetros de configuración de ESET Endpoint Security se pueden proteger mediante contraseña.



Protección de la configuración: bloquea o desbloquea los parámetros de configuración del programa. Seleccione o deseleccione la casilla de verificación para abrir la ventana Configuración de la contraseña.

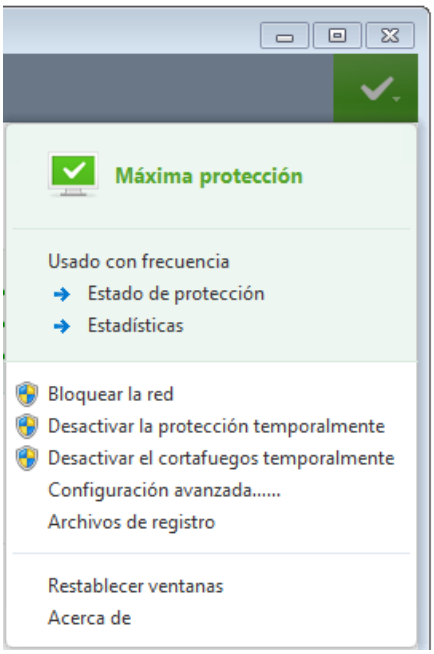
Para configurar o cambiar una contraseña para proteger los parámetros de configuración, haga clic en **Introduzca la contraseña...**.

Exigir derechos de administrador completos a las cuentas de administrador limitadas: seleccione esta opción 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). Entre estas modificaciones se incluye la desactivación de los módulos de protección y del cortafuegos.

Mostrar cuadro de diálogo de tiempo de espera de protección: este diálogo se muestra si la opción está seleccionada al desactivar la protección de forma temporal desde el menú del programa o la sección **ESET Endpoint Security** > **Configuración**. Un menú desplegable **Intervalo de tiempo** en la ventana **Desactivar la protección temporalmente** indica el período de tiempo durante el que estarán desactivadas todas las partes seleccionadas de la protección.

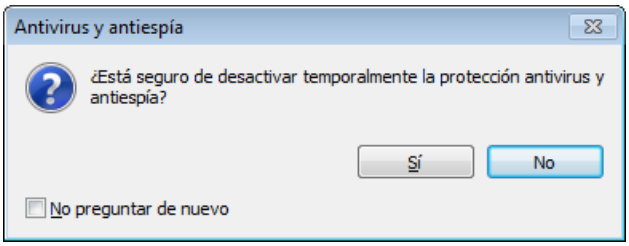
4.7.5 Menú del programa

En el menú del programa principal están disponibles algunas de las opciones de configuración y características más importantes.

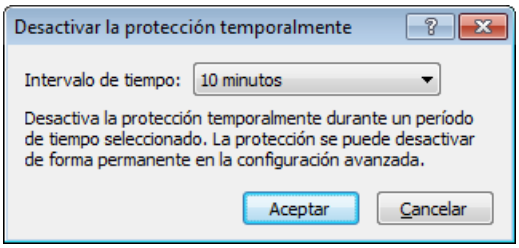


Usado con frecuencia: muestra las partes de ESET Endpoint Security que se utilizan con mayor frecuencia. Puede acceder a estar secciones rápidamente desde el menú del programa.

Desactivar la protección temporalmente: muestra el cuadro de diálogo de confirmación que desactiva la Protección antivirus y antiespía, que protege el sistema de los ataques maliciosos mediante el control de archivos, Internet y la comunicación por correo electrónico. Seleccione la casilla de verificación **No preguntar de nuevo** para evitar este tipo de mensajes en el futuro.



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



Bloquear la red: el cortafuegos personal bloqueará todo el tráfico de Internet y de la red, tanto el entrante como el saliente.

Desactivar el cortafuegos temporalmente: desactiva el cortafuegos. Consulte el capítulo Integración con el sistema del cortafuegos personal para obtener más información.

Configuración avanzada: seleccione esta opción para ver el árbol de **Configuración avanzada**. Esta ventana también se puede abrir pulsando la tecla F5 o desde **Configuración** > **Especificar 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.

Restablecer ventanas: esta opción restablece el tamaño y la posición predeterminados de la ventana de ESET

Endpoint Security.

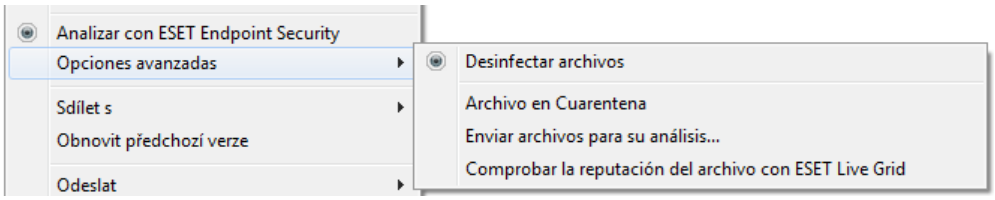
Acerca de: proporciona información del sistema y detalles acerca de la versión instalada de ESET Endpoint Security, así como de los módulos del programa instalados. Aquí también puede encontrar la fecha de expiración de la licencia. En la parte inferior, puede encontrar información sobre el sistema operativo y los recursos del sistema.

4.7.6 Menú contextual

El menú contextual aparecerá tras hacer clic con el botón derecho en el objeto seleccionado. El menú enumera todas las opciones que se pueden realizar en el objeto.

Es posible integrar elementos de control de ESET Endpoint Security en el menú contextual. En el árbol de configuración avanzada tiene a su disposición más opciones de configuración para esta funcionalidad, en **Interfaz de usuario** > **Menú contextual**.

Integrar el programa dentro del menú contextual: integre los elementos de control de ESET Endpoint Security en el menú contextual.



En el menú desplegable **Tipo de menú**, están disponibles las opciones siguientes:

- **Completo (analizar primero)**: activa todas las opciones del menú contextual; el menú principal mostrará la opción **Analizar con ESET Endpoint Security**.
- **Completo (desinfectar primero)**: activa todas las opciones del menú contextual; el menú principal mostrará la opción **Desinfectar con ESET Endpoint Security**.
- **Solo analizar** Solo aparecerá la opción **Analizar con ESET Endpoint Security** en el menú contextual.
- **Solo desinfectar**: solo aparecerá la opción **Desinfectar con ESET Endpoint Security** en el menú contextual.

4.7.7 Modo de presentación

Modo de presentación es una característica para usuarios que exigen un uso del software sin interrupciones y sin ventanas emergentes, así como una menor carga de la CPU. Modo de presentación también se puede utilizar para que las presentaciones no se vean interrumpidas por la actividad del módulo antivirus. Al activar esta característica, se desactivan todas las ventanas emergentes y la actividad del planificador de tareas se detiene por completo. La protección del sistema sigue ejecutándose en segundo plano, pero no requiere la intervención del usuario.

Puede activar o desactivar el Modo de presentación en la ventana principal del programa haciendo clic en **Configuración** > **Ordenador** y en **Activar** en **Modo de presentación**; en el árbol de configuración avanzada (F5) expandiendo **Interfaz de usuario**, haciendo clic en **Modo de presentación** y seleccionando la casilla de verificación situada junto a **Activar el Modo de presentación**. 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. También verá esta alerta en la ventana del programa principal, donde verá El modo de presentación está activado en naranja.

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

También puede seleccionar la opción **Desactivar el Modo de presentación automáticamente después de X minutos** y definir la cantidad de tiempo (el valor predeterminado es 1 minuto). Esta opción se utiliza únicamente cuando el modo de presentación se necesita durante un período de tiempo específico, y después se desea desactivarlo.

NOTA: si el cortafuegos personal está en modo interactivo y el modo de presentación está activado, podría tener problemas para conectarse a Internet. Esto puede ser un problema si el juego necesita conexión a Internet. Por lo general, se le solicita que confirme dicha acción (si se ha definido ninguna regla o excepción de comunicación), pero la intervención del usuario está desactivada en el modo de presentación. La solución pasa por definir una regla de comunicación para cada una de las aplicaciones que pueda entrar en conflicto con este comportamiento, o utilizar un modo de filtrado diferente en el cortafuegos personal. Recuerde también que si el modo de presentación está activado y accede a una página web o aplicación que presente un riesgo de seguridad potencial, esta podría bloquearse sin que se muestre ninguna explicación o alerta, ya que la intervención del usuario está desactivada.

5. Usuario avanzado

5.1 Servidor Proxy

En las redes LAN de gran tamaño, un servidor Proxy puede mediar en la conexión del ordenador a Internet. Si este es el caso, es necesario definir los siguientes ajustes. De lo contrario, el programa no se podrá actualizar de manera automática. En ESET Endpoint Security, 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 Security. Todos los módulos que requieran conexión a Internet utilizarán estos parámetros.

Para especificar la configuración del servidor Proxy en este nivel, seleccione la casilla de verificación **Conexión mediante servidor Proxy** y, a continuación, 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 la casilla de verificación **El servidor Proxy requiere autenticación** e introduzca un **nombre de usuario** y una **contraseña** válidos en los campos correspondientes. Haga clic en el botón **Detectar servidor Proxy** para detectar y rellenar la configuración del servidor Proxy de forma automática. Se copiarán los parámetros especificados en Internet Explorer.

NOTA: esta característica no recupera los datos de autenticación (nombre de usuario y contraseña), de modo que el usuario debe proporcionarlos.

En segundo lugar, la configuración del servidor Proxy se puede establecer en la Configuración avanzada de actualizaciones (sección **Actualización** del árbol de **configuración avanzada**). Esta configuración se aplica al perfil de actualización dado y se recomienda para ordenadores portátiles que suelen recibir actualizaciones de firmas de virus de diferentes ubicaciones. Para obtener más información sobre esta configuración, consulte la sección Configuración avanzada de actualizaciones.

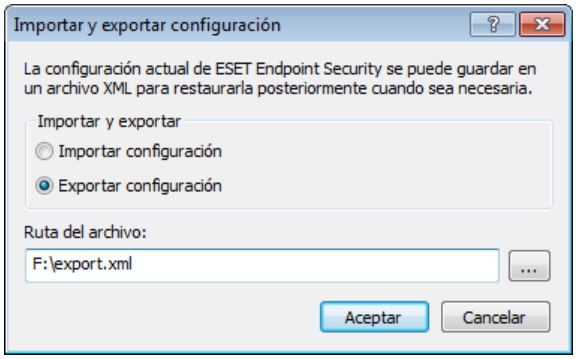
5.2 Importar y exportar configuración

La opción de importar y exportar configuraciones de ESET Endpoint Security está disponible en **Configuración**.

Tanto en la importación como en la exportación se utiliza el tipo de archivo .xml. La importación y la exportación son útiles para realizar copias de seguridad de la configuración actual de ESET Endpoint Security y, así, poder utilizarla más adelante. La opción de exportación de configuración también es de utilidad para los usuarios que desean utilizar su configuración preferida de ESET Endpoint Security en varios sistemas, ya que les permite importar fácilmente el archivo .xml para transferir los ajustes deseados.

Importar la configuración es muy fácil. En la ventana principal del programa, haga clic en **Configuración** > **Importar y exportar configuración** y, a continuación, seleccione la opción **Importar configuración**. Introduzca la ruta 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 y exportar configuración...**. Seleccione la opción **Exportar configuración** e introduzca el **Nombre de archivo** del archivo de configuración (por ejemplo, export.xml). Utilice el navegador para seleccionar la ubicación del ordenador donde desee guardar el archivo de configuración.



5.3 Accesos directos del teclado

Los accesos directos que se pueden utilizar en ESET Endpoint Security son:

Ctrl + G	desactiva la GUI del producto
Ctrl + I	abre la página de ESET SysInspector
Ctrl + L	abre la página Archivos de registro
Ctrl + S	abre la página Planificador de tareas
Ctrl + Q	abre la página Cuarentena
Ctrl + U	abre un cuadro de diálogo en el que puede definir el nombre de usuario y la contraseña
Ctrl + R	restablece la ventana al tamaño y la posición predeterminados en la pantalla

Puede utilizar los siguientes accesos directos del teclado para mejorar la navegación en el producto de seguridad de ESET:

F1	abre las páginas de ayuda
F5	abre la configuración avanzada
Flechas arriba/abajo	navegación por los elementos del producto
*	expande el nodo del árbol de configuración avanzada
-	contrae el nodo del árbol de configuración avanzada
TABULADOR	mueve el cursor en una ventana
Esc	cierra el cuadro de diálogo activo

5.4 Línea de comandos

El módulo antivirus de ESET Endpoint Security 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
/adware	analizar en busca de adware/spyware/riskware (predeterminado)
/no-adware	no analizar en busca de adware/spyware/riskware
/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)
/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. Opciones disponibles: none (ninguno), standard (estándar, predeterminado), strict (estricto), rigorous (riguroso), delete (eliminar)
/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.

5.5 ESET SysInspector

5.5.1 Introducción a ESET SysInspector

ESET SysInspector es una aplicación que examina el ordenador a fondo y muestra los datos recopilados de forma exhaustiva. Información como los controladores y aplicaciones instalados, las conexiones de red o entradas de registro importantes pueden ayudarle a investigar el comportamiento sospechoso del sistema debido a la incompatibilidad de software o hardware o a la infección de código malicioso.

Puede acceder a ESET SysInspector de dos formas: desde la versión integrada en las soluciones ESET Security o descargando la versión independiente (SysInspector.exe) del sitio web de ESET de forma gratuita. Las dos versiones tienen una función idéntica y los mismos controles del programa. Solo se diferencian en el modo de gestión de los resultados. Tanto la versión independiente como la versión integrada le permiten exportar instantáneas del sistema en un archivo .xml y guardarlas en el disco. No obstante, la versión integrada también le permite almacenar las instantáneas del sistema directamente en **Herramientas** > **ESET SysInspector** (excepto ESET Remote Administrator).

ESET SysInspector tardará un rato en analizar el ordenador; el tiempo necesario puede variar entre 10 segundos y unos minutos, según la configuración de hardware, el sistema operativo y el número de aplicaciones instaladas en el ordenador.

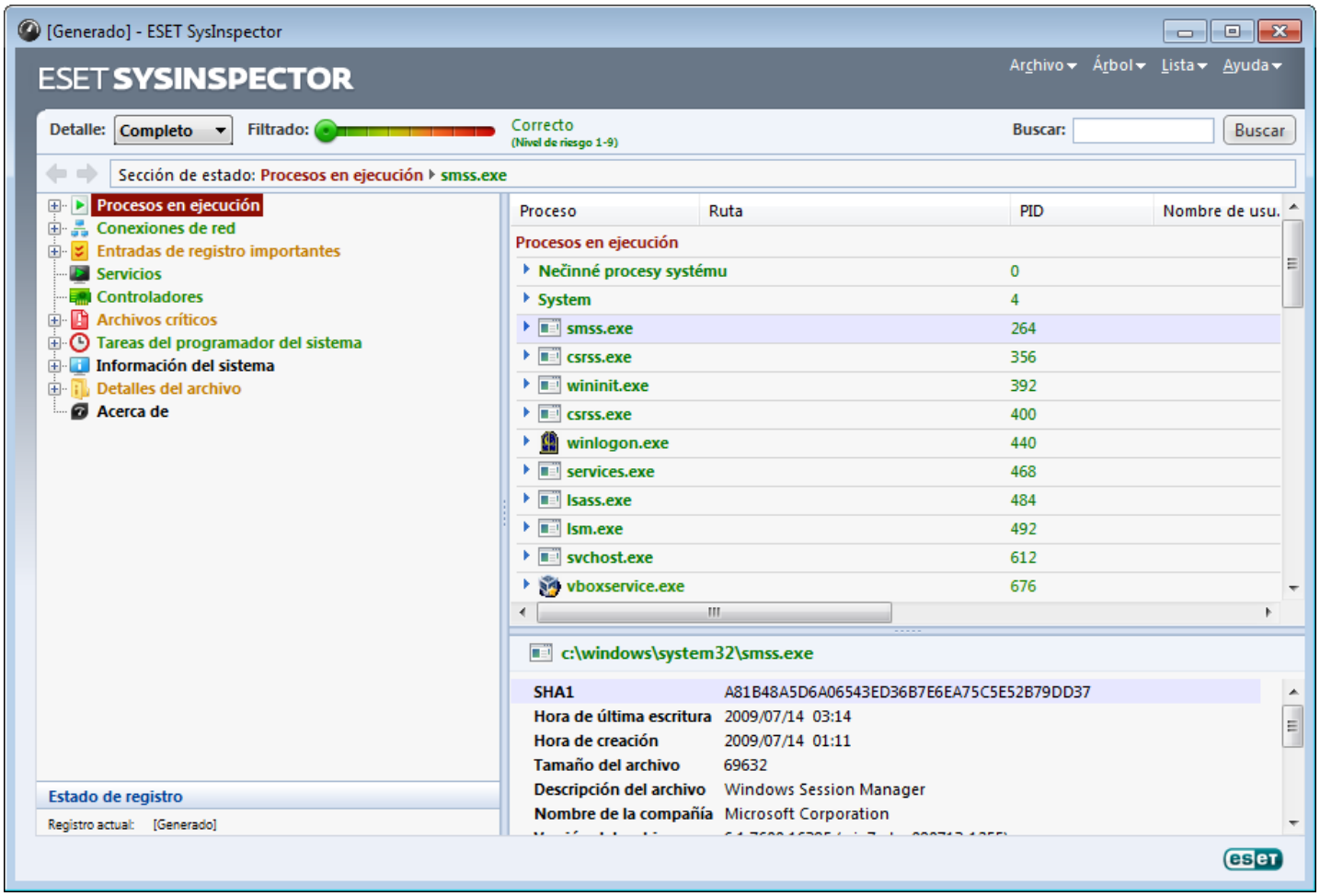
5.5.1.1 Inicio de ESET SysInspector

Para iniciar ESET SysInspector simplemente tiene que ejecutar el archivo SysInspector.exe que descargó del sitio web de ESET.

Espere mientras la aplicación examina el sistema. El proceso de inspección puede tardar varios minutos, en función del hardware de su ordenador y de los datos que se vayan a recopilar.

5.5.2 Interfaz de usuario y uso de la aplicación

Para un uso sencillo, la ventana principal se divide en cuatro secciones: Controles de programa, en la parte superior de la ventana principal; la ventana de navegación, situada a la izquierda; la ventana Descripción, situada a la derecha en el medio; y la ventana Detalles, situada a la derecha, en la parte inferior de la ventana principal. En la sección Estado de registro se enumeran los parámetros básicos de un registro (filtro utilizado, tipo de filtro, si el registro es resultado de una comparación, etc.).



5.5.2.1 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 **Para enviar**. 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 almacenados de ESET SysInspector se pueden abrir previamente arrastrándolos y soltándolos en la ventana principal.

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 para que pueda trabajar con ella más fácilmente. El modo "Básico", le permite acceder a la información utilizada para buscar soluciones a problemas comunes del sistema. En el modo "Medio", el programa muestra menos detalles. En el modo "Completo", ESET SysInspector muestra toda la información necesaria para solucionar problemas muy específicos.

Filtrado de elementos

Es la mejor opción para buscar entradas de registro o archivos sospechosos en el sistema. Ajuste el control deslizante para filtrar los elementos por su nivel de riesgo. Si el control deslizante se coloca lo más a la izquierda posible (nivel de riesgo 1), se mostrarán todos los elementos. Al mover el control deslizante a la derecha, el programa filtra todos los elementos menos los 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 está colocado lo más a la derecha posible, el programa mostrará solo los elementos dañinos conocidos.

Todos los elementos que tengan un nivel de riesgo entre 6 y 9 pueden constituir un riesgo de seguridad. Si utiliza 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 de nivel de riesgo.

Buscar

Esta opción se puede utilizar para buscar rápidamente un elemento específico por su nombre completo o parcial. Los resultados de la solicitud de búsqueda aparecerán en la ventana Descripción.

Retorno

Al hacer clic en la flecha 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, por eso 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.

5.5.2.2 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 cada uno de los nodos en subnodos. Para abrir o contraer un nodo, haga doble clic en el nombre del nodo o haga clic en + o −, junto al nombre del nodo. A medida que explora la estructura de árbol de nodos y subnodos en la ventana de navegación, encontrará información variada de cada nodo en la ventana Descripción. Si examina los elementos en la ventana Descripción, es posible que se muestre información adicional de cada uno de los elementos en la ventana Detalles.

A continuación, se encuentran las descripciones de los nodos principales de la ventana de navegación e información relacionada en las ventanas Descripción y Detalles.

Procesos en ejecución

Este nodo contiene información sobre las aplicaciones y los procesos que se ejecutan al generar el registro. En la ventana 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, el nivel de riesgo del archivo, etc.

La ventana Detalles contiene información adicional de los elementos seleccionados en la ventana Descripción como, por ejemplo, el tamaño del archivo o su hash.

NOTA: un sistema operativo incluye varios componentes kernel importantes que se ejecutan 24 horas al día, 7 días de la semana, y proporcionan funciones básicas y esenciales para otras aplicaciones de usuario. En determinados casos, estos procesos aparecen en la herramienta ESET SysInspector con una ruta de archivo que comienza por \??\. Estos símbolos proporcionan optimización de prelanzamiento de esos procesos; son seguros para el sistema; son seguros para el sistema.

Conexiones de red

La ventana 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 Detalles contiene información adicional de los elementos seleccionados en la ventana 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 Descripción, puede encontrar los archivos que están relacionados con entradas de registro específicas. Puede ver información adicional en la ventana Detalles.

Servicios

La ventana Descripción contiene una lista de archivos registrados como Windows Services (Servicios de Windows). En la ventana Detalles, puede consultar el modo de inicio definido para el servicio e información específica del archivo.

Controladores

Una lista de los controladores instalados en el sistema.

Archivos críticos

En la ventana 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 tareas desencadenadas por el Programador de tareas de Windows a una hora o con un intervalo de tiempo especificados.

Información del sistema

Contiene información detallada sobre el hardware y el software, así como información sobre las variables de entorno, los derechos de usuario establecidos y registros de sucesos del sistema.

Detalles del archivo

Una lista de los archivos del sistema importantes y los archivos de la carpeta Archivos de programa. Encontrará información adicional específica de los archivos en las ventanas Descripción y Detalles.

Acerca de...

Información sobre la versión de ESET SysInspector y la lista de módulos de programa.

5.5.2.2.1 Accesos directos del teclado

Los accesos directos que se pueden utilizar en ESET SysInspector son:

Archivo

Ctrl + O	abre el registro existente
Ctrl + S	guarda los registros creados

Generar

Ctrl + G	genera una instantánea estándar del estado del ordenador
Ctrl + H	genera una instantánea del 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
-	disminuye el nivel de riesgo
+	aumenta el nivel de riesgo
Ctrl + 9	modo de filtrado, nivel igual o mayor
Ctrl + O	modo de filtrado, nivel igual únicamente

Ver

Ctrl + 5	ver por proveedor, todos los proveedores
Ctrl + 6	ver por proveedor, solo Microsoft
Ctrl + 7	ver por proveedor, todos los demás proveedores
Ctrl + 3	muestra todos los detalles
Ctrl + 2	muestra la mitad de los detalles
Ctrl + 1	visualización básica
Retroceso	retrocede un espacio
Espacio	avanza un espacio
Ctrl + W	expande el árbol
Ctrl + Q	contrae el árbol

Otros controles

Ctrl + T	va a la ubicación original del elemento tras seleccionarlo en los resultados de búsqueda
Ctrl + P	muestra información básica sobre un elemento
Ctrl + A	muestra toda la información sobre un elemento
Ctrl + C	copia el árbol del elemento actual
Ctrl + X	copia elementos
Ctrl + B	busca información en Internet acerca de los archivos seleccionados
Ctrl + L	abre la carpeta en la que se encuentra el archivo seleccionado
Ctrl + R	abre la entrada correspondiente en el editor de registros
Ctrl + Z	copia una ruta de acceso a un archivo (si el elemento está asociado a un archivo)
Ctrl + F	activa el campo de búsqueda
Ctrl + D	cierra los resultados de búsqueda
Ctrl + E	ejecuta el script de servicio

Comparación

Ctrl + Alt + O	abre el registro original/comparativo
Ctrl + Alt + R	cancela la comparación
Ctrl + Alt + 1	muestra todos los elementos
Ctrl + Alt + 2	muestra solo los elementos agregados, el registro mostrará los elementos presentes en el registro actual
Ctrl + Alt + 3	muestra solo los elementos eliminados, el registro mostrará los elementos presentes en el registro anterior
Ctrl + Alt + 4	muestra solo los elementos sustituidos (archivos incluidos)
Ctrl + Alt + 5	muestra solo las diferencias entre registros
Ctrl + Alt + C	muestra la comparación
Ctrl + Alt + N	muestra el registro actual
Ctrl + Alt + P	abre el registro anterior

Varios

F1	ver ayuda
Alt + F4	cerrar programa
Alt + Shift + F4	cerrar programa sin preguntar
Ctrl + I	estadísticas de registro

5.5.2.3 Comparar

La característica Comparar permite al usuario comparar dos registros existentes. El resultado de esta característica es un conjunto de elementos no comunes a ambos registros. Esta opción es útil para realizar un seguimiento de los cambios realizados en el sistema; se trata de una herramienta útil para detectar la actividad de código malicioso.

Una vez iniciada, la aplicación crea un registro nuevo, que aparecerá en una ventana nueva. Vaya a **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, utilice el menú **Archivo** > **Abrir registro**. En la ventana principal del programa, ESET SysInspector muestra siempre un registro a la vez.

La comparación de dos registros le permite ver simultáneamente un registro activo y un registro guardado en un archivo. Para comparar registros, utilice la opción **Archivo** -> **Comparar registros** y elija **Seleccionar archivo**. El registro seleccionado se comparará con el registro activo en la ventana principal del programa. El registro comparativo solo muestra las diferencias entre los dos registros.

NOTA: si compara dos archivos de registro, seleccione **Archivo** > **Guardar registro** para guardarlo como archivo ZIP. Se guardarán ambos archivos. Si abre posteriormente dicho archivo, los registros contenidos en el mismo se compararán automáticamente.

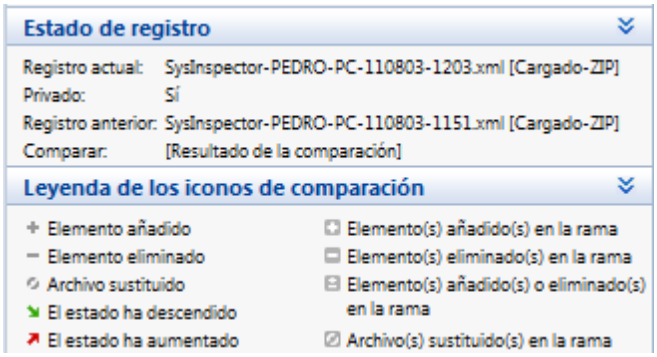
Junto a los elementos mostrados, ESET SysInspector muestra símbolos que identifican las diferencias entre los registros comparados.

Los elementos marcados con un – solo se encuentran en el registro activo y no están presentes en el registro comparativo abierto. Los elementos marcados con un + están presentes solo en el registro abierto, no en el registro activo.

Descripción de todos los símbolos que pueden aparecer junto a los elementos:

- + Nuevo valor que no se encuentra en el registro anterior.
- La sección de estructura de árbol contiene valores nuevos.
- – Valor eliminado que solo se encuentra en el registro anterior.
- La sección de estructura de árbol contiene valores eliminados.
- Se ha cambiado un valor o archivo.
- La sección de estructura de árbol contiene valores o archivos modificados.
- Ha disminuido el nivel de riesgo, o este 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, además de mostrar los nombres de los registros que se están comparando.



Los registros comparativos se pueden guardar en un archivo para consultarlos más adelante.

Ejemplo

Genere y guarde un registro, que incluya información original sobre el sistema, en un archivo con el nombre previo.xml. Tras realizar los cambios en el sistema, abra ESET SysInspector y deje 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, vaya a **Archivo** > **Comparar registros**. El programa creará un registro comparativo con las diferencias entre ambos registros.

Se puede lograr el mismo resultado con la siguiente opción de la línea de comandos:

SysIsnpector.exe actual.xml previo.xml

5.5.3 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 de usuario
/privacy	genera un registro que no incluye la información confidencial
/zip	almacena el registro resultante directamente en el disco, en un archivo comprimido
/silent	oculta la barra de progreso del proceso de generación del registro
/help, /?	muestra información acerca de los parámetros de la línea de comandos

Ejemplos

Para cargar un registro determinado directamente en el navegador, utilice: SysInspector.exe "c:\clientlog.xml"
Para generar un registro en una ubicación actual, utilice: SysInspector.exe /gen
Para generar un registro en una carpeta específica, utilice: SysInspector.exe /gen="c:\folder\"
Para generar un registro en una carpeta o ubicación específica, utilice: SysInspector.exe /gen="c:\folder\mynewlog.xml"
Para generar un registro que no incluya la información confidencial directamente como archivo comprimido, utilice: SysInspector.exe /gen="c:\mynewlog.zip" /privacy /zip
Para comparar dos registros, utilice: SysInspector.exe "current.xml" "original.xml"

NOTA: si el nombre del archivo o la carpeta contiene un espacio, debe escribirse entre comillas.

5.5.4 Script de servicio

El script de servicio es una herramienta que ayuda a los clientes que utilizan ESET SysInspector eliminando fácilmente del sistema los objetos no deseados.

El script de servicio permite al usuario exportar el registro completo de ESET SysInspector o las partes que seleccione. Después de exportarlo, puede marcar los objetos que desea eliminar. A continuación, puede ejecutar el registro modificado para eliminar los objetos marcados.

El script de servicio es ideal para los 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 tiene la sospecha de que el ordenador está infectado por un virus que el antivirus no detecta, siga estas instrucciones:

- Ejecute ESET SysInspector para generar una nueva instantánea del sistema.
- Seleccione el primer y el último elementos de la sección de la izquierda (en la estructura de árbol) mientras mantiene pulsada la tecla Mayús.
- Haga clic con el botón secundario en los objetos seleccionados y elija la opción **Exportar las secciones seleccionadas al script de servicio** en el menú contextual.
- Los objetos seleccionados se exportarán a un nuevo registro.
- 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 que no ha marcado ningún archivo u objeto importante del sistema operativo.
- Abra ESET SysInspector, haga clic en **Archivo** > **Ejecutar script de servicio** e introduzca la ruta del script.
- Haga clic en **Aceptar** para ejecutar el script.

5.5.4.1 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 la opción **Exportar todas las secciones al script de servicio** o la opción **Exportar secciones seleccionadas al script de servicio**.

NOTA: cuando se comparan dos registros, el script de servicio no se puede exportar.

5.5.4.2 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 listan 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.

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, reducirán a valores de 0 bytes o 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 listan 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 listan 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
[...]
```

Al ejecutar el script, las unidades seleccionadas se detendrán. Tenga en cuenta que algunas unidades no se permitirán a sí mismas detenerse.

09) Critical files (Archivos críticos)

En esta sección se proporciona información sobre los archivos 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.

5.5.4.3 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.

Se abrirá un cuadro de diálogo para indicarle que el script se ha ejecutado correctamente.

Si el script no se puede procesar por completo, se mostrará un cuadro 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 un cuadro 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 incoherencias (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.

5.5.5 Preguntas frecuentes

¿Es necesario contar con privilegios de administrador para ejecutar ESET SysInspector?

ESET SysInspector no requiere privilegios de administrador para su ejecución, pero sí es necesario utilizar una cuenta de administrador para acceder a parte de la información que recopila. Si lo ejecuta como usuario estándar o usuario restringido, se recopilará menos información sobre 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, seleccione **Archivo** > **Guardar registro** en el menú principal. Los registros se guardar con formato XML. Por defecto, los archivos se guardan en el directorio %USERPROFILE%\My Documents\, con una convención de nombre de archivo de "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 seleccione **Archivo** > **Abrir registro** en el menú principal. 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 opción de arrastrar y soltar entre ventanas con permisos de seguridad distintos.

¿Hay una especificación disponible para el formato de archivo de registro? ¿Y un kit de desarrollo de software?

Actualmente, no se encuentra disponible ninguna especificación para el formato del archivo de registro, ni un conjunto de herramientas de programación, ya que la aplicación 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 determinado?

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, pondera 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. Con el fin de comprobar la veracidad del certificado, el sistema operativo contacta con una autoridad de certificados para comprobar la identidad del editor del software. Este es el comportamiento normal de todos los programas firmados digitalmente en Microsoft Windows.

¿En qué consiste la tecnología Anti-Stealth?

La tecnología Anti-Stealth proporciona un método efectivo de detección de programas peligrosos (rootkits).

Si el sistema recibe el ataque de código malicioso que se comporta como un rootkit, los datos del usuario podrían dañarse o ser robados. Sin una herramienta especial contra programas peligrosos (rootkit), resulta casi imposible detectar programas peligrosos.

¿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 primero si el archivo contiene una firma digital. Si se encuentra una firma digital, se validará el archivo utilizando esa información. Si no se

encuentra una firma digital, el ESI comenzará a buscar el archivo CAT correspondiente (Security Catalog - %systemroot %\system32\catroot) que contenga información sobre el archivo ejecutable en proceso. Si se encuentra el archivo CAT, la firma digital de dicho archivo se utilizará para el proceso de validación del archivo ejecutable.

Esta es la razón por la que a veces encontramos archivos marcados como "Firmados por MS" pero con un "Nombre de compañía" diferente.

Ejemplo:

Windows 2000 incluye la aplicación HyperTerminal, que se encuentra en C:\Archivos de programa\Windows NT. El archivo ejecutable de la aplicación principal no está firmado digitalmente; sin embargo, ESET SysInspector lo marca como archivo firmado por Microsoft. La razón es la referencia que aparece en C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat que lleva a C:\Archivos de programa\Windows NT\hypertrm.exe (archivo ejecutable principal de la aplicación HyperTerminal), y sp4.cat está digitalmente firmado por Microsoft.

5.5.6 ESET SysInspector como parte de ESET Endpoint Security

Para abrir la sección ESET SysInspector en ESET Endpoint Security, 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 ordenador o las tareas programadas. Se puede acceder a todas las operaciones con instantáneas del sistema (como crear, ver, comparar, eliminar y exportar) simplemente haciendo clic una o dos veces.

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 instantánea 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, utilice la opción del menú contextual **Mostrar**. 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**: crea un registro nuevo. Debe introducir antes un breve comentario acerca del registro. Para ver el progreso de la creación de instantáneas (de la instantánea que se está generando), consulte la columna **Estado**. Todas las instantáneas completadas aparecen marcadas con el estado **Creada**.
- **Eliminar/Eliminar todo**: elimina entradas de la lista.
- **Exportar**: guarda la entrada seleccionada en un archivo XML (y también en una versión comprimida).

5.6 ESET SysRescue

ESET SysRescue es una utilidad que le permite crear un disco de arranque que contenga soluciones ESET Security; puede ser ESET NOD32 Antivirus, ESET Smart Security o incluso de algunos de los productos orientados al servidor. La principal ventaja de ESET SysRescue es que, aun teniendo un acceso directo al disco y a todo el sistema de archivos, la solución ESET Security se puede ejecutar con independencia del sistema operativo host. Gracias a esto, es posible eliminar las amenazas que normalmente no se podrían suprimir como, por ejemplo, cuando el sistema operativo se está ejecutando.

5.6.1 Requisitos mínimos

ESET SysRescue funciona en el entorno de preinstalación de Microsoft Windows (Windows PE) versión 2.x, que se basa en Windows Vista.

Windows PE forma parte del paquete gratuito Kit de instalación automatizada de Windows (Windows AIK), que debe instalarse previamente para poder crear ESET SysRescue (http://go.eset.eu/AIK). Debido a la compatibilidad con la versión de 32 bits de Windows PE, es necesario utilizar un paquete de instalación de ESET Security de 32 bits para la creación de ESET SysRescue en sistemas de 64 bits. ESET SysRescue es compatible con Windows AIK 1.1 y versiones posteriores.

NOTA: como el tamaño de Windows AIK es superior a 1 GB, se requiere una conexión a Internet de alta velocidad para que no haya problemas en la descarga.

ESET SysRescue está disponible en soluciones ESET Security, versión 4.0 y versiones posteriores.

Sistemas operativos compatibles

- Windows 7
- Windows Vista
- Windows Vista Service Pack 1
- Windows Vista Service Pack 2
- Windows Server 2008
- Windows Server 2003 Service Pack 1 con KB926044
- Windows Server 2003 Service Pack 2
- Windows XP Service Pack 2 con KB926044
- Windows XP Service Pack 3

5.6.2 Cómo crear un CD de recuperación

Para iniciar el asistente de ESET SysRescue, haga clic en **Inicio** > **Programas** > **ESET** > **ESET Endpoint Security** > **ESET SysRescue**.

En primer lugar, el asistente comprueba si está instalado Windows AIK y un dispositivo adecuado para la creación de medios de arranque. Si Windows AIK no está instalado en el ordenador (o está dañado o mal instalado), el asistente le ofrecerá la opción de instalarlo o de escribir la ruta de acceso a la carpeta en la que se encuentre (http://go.eset.eu/AIK).

NOTA: como el tamaño de Windows AIK es superior a 1 GB, se requiere una conexión a Internet de alta velocidad para que no haya problemas en la descarga.

En el siguiente paso, seleccione el medio de destino donde se ubicará ESET SysRescue.

5.6.3 Selección de objetivo

Además de en CD, DVD y USB, también puede guardar ESET SysRescue en un archivo ISO. Posteriormente, puede grabar esta imagen ISO en un CD o DVD, o utilizarla de algún otro modo (por ejemplo, en un entorno virtual como VMware o VirtualBox).

Si selecciona USB como medio de destino, es posible que la función de inicio falle en determinados ordenadores. En algunas versiones de la BIOS se pueden producir problemas de comunicación entre la administración de arranque y la BIOS (p. ej., en Windows Vista). El arranque tiene lugar con el siguiente mensaje de error:

```
Archivo: \boot\bcd
estado: 0xc000000e
Información: se ha producido un error al intentar leer los datos de la configuración de arranque.
```

Si le aparece este mensaje, le recomendamos que seleccione como medio un CD en lugar de un dispositivo USB.

5.6.4 Configuración

Antes de empezar a crear ESET SysRescue, el asistente de instalación muestra los parámetros de compilación en el último paso del asistente de ESET SysRescue. Si desea modificar estos parámetros, haga clic en el botón **Cambiar**. Entre las opciones disponibles, se incluyen:

- Carpetas
- ESET Antivirus
- Avanzadas
- Protocolo de Internet
- Dispositivo USB de arranque (cuando se selecciona el dispositivo USB de destino)
- Grabación (cuando está seleccionada la unidad de CD/DVD de destino)

El botón **Crear** no está activo si no se especifica ningún paquete de instalación MSI o si no se instala ninguna solución ESET Security en el ordenador. Para seleccionar un paquete de instalación, haga clic en el botón **Cambiar** y vaya a la ficha **ESET Antivirus**. Además, si no rellena el nombre de usuario y la contraseña (**Cambiar** > **ESET Antivirus**), el botón **Crear** aparecerá atenuado.

5.6.4.1 Carpetas

Carpeta temporal es un directorio de trabajo que contiene los archivos necesarios durante la compilación de ESET SysRescue.

La **carpeta ISO** es donde se guarda el archivo ISO resultante una vez completada la compilación.

La lista de esta ficha muestra todas las unidades de red locales y asignadas, así como el espacio libre disponible. Si alguna de las carpetas se ubica en una unidad con espacio libre insuficiente, le recomendamos que seleccione otra unidad que tenga más espacio libre disponible. De lo contrario, la compilación puede finalizar antes de tiempo por falta de espacio libre en el disco.

Aplicaciones externas: le permite especificar programas adicionales que se ejecutarán o instalarán tras el inicio de un medio de ESET SysRescue.

Incluir aplicaciones externas: le permite agregar programas externos a la compilación de ESET SysRescue.

Carpeta seleccionada: carpeta donde se encuentran los programas que agregarán al disco de ESET SysRescue.

5.6.4.2 ESET Antivirus

Para crear un CD de ESET SysRescue, puede seleccionar dos orígenes de archivos ESET para la compilación.

Carpeta ESS/EAV: archivos que ya se encuentran en la carpeta del ordenador donde se ha instalado la solución ESET Security.

Archivo MSI: se utilizan los archivos que se encuentran en el instalador de MSI.

A continuación, tiene la posibilidad de actualizar la ubicación de los archivos (.nup). Por lo general, se recomienda la opción predeterminada **Carpeta ESS/EAV/Archivo MSI**. En algunos casos, se puede elegir una **Carpeta de actualización** personalizada; por ejemplo, para utilizar una versión anterior o más reciente de la base de firmas de virus.

Puede utilizar una de las fuentes de nombre de usuario y contraseña que aparecen a continuación:

ESS/EAV instalado: el nombre de usuario y la contraseña se copian de la versión instalada actualmente de la solución ESET Security.

Del usuario: se utilizan el nombre de usuario y la contraseña introducidos en los cuadros de texto correspondientes.

NOTA: la solución ESET Security del CD de ESET SysRescue se actualiza a través de Internet o mediante la solución ESET Security instalada en el ordenador donde se ejecuta el CD de ESET SysRescue.

5.6.4.3 Configuración avanzada

En la ficha **Avanzadas**, puede optimizar el CD de ESET SysRescue en función de la cantidad de memoria del ordenador. Seleccione **576 MB o más** para escribir el contenido del CD en la memoria operativa (RAM). Si selecciona **Menos de 576 MB**, se accederá temporalmente al CD de recuperación cuando WinPE se ejecute.

En la sección **Controladores externos** puede insertar controladores para su hardware específico (normalmente, un adaptador de red). WinPE se basa en Windows Vista SP1, que es compatible con un gran abanico de productos de hardware, pero a veces el hardware no se reconoce. Si esto sucede, tendrá que agregar el controlador manualmente. Hay dos maneras de agregar un controlador a la compilación de ESET SysRescue: manualmente (con el botón **Agregar**) y de forma automática (con el botón **Búsq. auto.**). Si lo agrega manualmente, debe seleccionar la ruta de acceso al archivo .inf correspondiente (el archivo *.sys aplicable también debe estar presente en esta carpeta). Si lo agrega automáticamente, el controlador se busca de forma automática en el sistema operativo del ordenador en cuestión. La adición automática se recomienda únicamente cuando ESET SysRescue se utiliza en un ordenador que tiene el mismo adaptador de red que el ordenador con el que se creó el CD de ESET SysRescue. Durante la creación de ESET SysRescue, el controlador se agrega a la compilación para que el usuario no tenga que buscarlo posteriormente.

5.6.4.4 Protocolo de Internet

En esta sección puede configurar la información básica de la red y configurar las conexiones predefinidas después de ESET SysRescue.

Seleccione **Dirección IP privada automática** para obtener la dirección IP automáticamente del servidor DHCP (Protocolo de configuración dinámica de host).

Esta conexión de red también puede utilizar una dirección IP especificada manualmente (también conocida como dirección IP estática). Seleccione **Personalizar** para configurar la IP correctamente. Si selecciona esta opción, debe especificar una **Dirección IP** y, para las conexiones de Internet de alta velocidad y LAN, una **Máscara de subred**. En **Servidor DNS preferido** y **Servidor DNS alternativo**, escriba la dirección de los servidores DNS principal y alternativo.

5.6.4.5 Dispositivo de arranque USB

Si ha seleccionado un dispositivo USB como medio de destino, puede seleccionar uno de los dispositivos USB disponibles en la ficha **Dispositivo de arranque USB** (en caso de que haya más dispositivos USB).

Seleccione el **Dispositivo** de destino adecuado para la instalación de ESET SysRescue.

Alerta: el dispositivo USB seleccionado se formateará durante la creación de ESET SysRescue, y se eliminarán todos los datos que contenga.

Si selecciona la opción **Formato rápido**, se eliminarán todos los archivos de la partición, pero no se comprobará la existencia de sectores erróneos en el disco. Utilice esta opción si el dispositivo USB ya se ha formateado previamente y está seguro de que no está dañado.

5.6.4.6 Grabar

Si ha seleccionado CD/DVD como medio de destino, puede especificar los parámetros de grabación adicionales en la ficha **Grabar**.

Eliminar archivo ISO: marque esta opción para eliminar el archivo ISO de forma temporal una vez que se haya creado el CD de ESET SysRescue.

Eliminación activada: le permite seleccionar un borrado rápido o un borrado completo.

Dispositivo de grabación: seleccione la unidad que se utilizará para grabar.

Alerta: esta es la opción predeterminada. Si se utiliza un CD/DVD regrabable, se borrarán todos los datos contenidos en dicho CD/DVD.

La sección Medio contiene información sobre el medio introducido en el dispositivo de CD/DVD.

Velocidad de grabación: seleccione la velocidad deseada en el menú desplegable. Las capacidades de su dispositivo de grabación y el tipo de CD/DVD utilizado deben tenerse en cuenta a la hora de seleccionar la velocidad de grabación.

5.6.5 Trabajo con ESET SysRescue

Para que el CD, DVD o USB de recuperación funcione eficazmente, debe iniciar el ordenador desde el medio de arranque de ESET SysRescue. La prioridad de arranque se puede modificar en el BIOS. También puede ejecutar el menú de inicio durante el inicio del ordenador. Normalmente, esto se hace con una de las teclas F9-F12, en función de la versión de la placa base/BIOS que utilice.

Después de arrancar desde un medio de arranque, se iniciará la solución ESET Security. Como ESET SysRescue solo se utiliza en situaciones específicas, algunos módulos de protección y características del programa presentes en la versión estándar de la solución ESET Security no son necesarios. La lista se limitará a **Análisis del ordenador**, **Actualizar** y algunas secciones de **Configuración**. La capacidad para actualizar la base de firmas de virus es la característica más importante de ESET SysRescue, por lo que se recomienda actualizar el programa antes de iniciar un análisis del ordenador.

5.6.5.1 Uso de ESET SysRescue

Supongamos que hay ordenadores de la red están infectados por un virus que modifica los archivos ejecutables (.exe). La solución ESET Security puede desinfectar todos los archivos excepto explorer.exe, que no se puede desinfectar ni en el modo seguro. Esto se debe a que explorer.exe, como uno de los procesos esenciales de Windows, se inicia también en modo seguro. La solución ESET Security no podría realizar ninguna acción en al archivo, que seguiría infectado.

En esta situación, podría utilizar ESET SysRescue para solucionar el problema. ESET SysRescue no necesita ningún componente del sistema operativo host y, por lo tanto, puede procesar (desinfectar, eliminar, etc.) cualquier archivo del disco.

6. Glosario

6.1 Tipos de amenazas

Una amenaza es un software malicioso que intenta entrar en el ordenador de un usuario y dañarlo.

6.1.1 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.

6.1.2 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.

6.1.3 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 malintencionados 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.

6.1.4 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 en el proceso normal de análisis. Los usuarios de ESET Endpoint Security tienen la ventaja de la tecnología Anti-Stealth, que también puede detectar y eliminar rootkits activos.

6.1.5 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 navegador. 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.

6.1.6 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.

6.1.7 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 Security 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.

6.1.8 Aplicaciones potencialmente indeseables

Las **aplicaciones potencialmente indeseables** (PUA) no tienen por qué ser maliciosas, pero pueden afectar al rendimiento del ordenador de forma negativa. Dichas aplicaciones suelen necesitar que se consienta su instalación. Si se encuentran en su ordenador, el sistema se comportará de manera diferente (en comparación con el estado en el que se encontraba antes de la instalación). Los cambios más importantes son:

- Se abren ventanas nuevas que no se habían visto anteriormente (ventanas emergentes, anuncios, etc.).
- Activación y ejecución de procesos ocultos.
- Mayor uso de los recursos del sistema.
- Cambios en los resultados de búsqueda.
- La aplicación se comunica con servidores remotos.

6.2 Tipos de ataques remotos

Existen muchas técnicas especiales que permiten a los atacantes poner en peligro a sistemas remotos. Se dividen en varias categorías.

6.2.1 Ataques por denegación de servicio (DoS)

DoS, o denegación de servicio, es un intento de impedir la disponibilidad de un ordenador o una red para sus usuarios. La comunicación entre usuarios afectados se bloquea y no se puede continuar de una manera funcional. Normalmente, los ordenadores expuestos a ataques DoS necesitan reiniciarse para funcionar correctamente.

En la mayoría de casos, los objetivos son servidores web y la intención es que no estén disponibles para los usuarios durante un período de tiempo determinado.

6.2.2 Envenenamiento DNS

Mediante el envenenamiento DNS (servidor de nombres de dominio), los piratas informáticos pueden engañar al servidor DNS de cualquier ordenador para que crea que los datos falsos que le proporcionan son legítimos y auténticos. La información falsa se almacena en caché durante un período de tiempo determinado, de modo que los piratas informáticos pueden volver a escribir las respuestas DNS de direcciones IP. Como resultado, los usuarios que intentan acceder a sitios web en Internet descargarán virus o gusanos en sus ordenadores en lugar de su contenido original.

6.2.3 Ataques de 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. Los gusanos de la red explotan las vulnerabilidades de seguridad de varias aplicaciones. Debido a la disponibilidad de Internet, se pueden extender por todo el mundo en cuestión de horas desde su lanzamiento y, en algunos casos, incluso en cuestión de minutos.

La mayoría de los ataques de gusanos (Sasser, SqlSlammer) se pueden evitar usando la configuración de seguridad predeterminada del cortafuegos o bloqueando los puertos que no están protegidos o no se usan. También es esencial actualizar el sistema operativo con los parches de seguridad más recientes.

6.2.4 Análisis de puertos

El análisis de puertos sirve para determinar los puertos del ordenador que están abiertos en un host de red. El software de análisis de puertos se ha diseñado para encontrar dichos puertos.

Un puerto de ordenador es un punto virtual que administra los datos entrantes y salientes; esto es crucial desde el punto de vista de la seguridad. En una red grande, la información recopilada por el análisis de puertos puede ayudar a identificar vulnerabilidades potenciales. Este uso es legítimo.

Sin embargo, con frecuencia, los delincuentes informáticos usan los análisis de puertos para vulnerar la seguridad. Su primer paso es enviar paquetes a cada puerto. En función del tipo de respuesta, es posible determinar los puertos que están en uso. El análisis en sí no causa daños, pero tenga en cuenta que esta actividad puede revelar vulnerabilidades potenciales y permitir a los atacantes tomar el control de ordenadores remotos.

Se aconseja a los administradores de red que bloqueen todos los puertos no usados y protejan aquellos que están en uso contra el acceso no autorizado.

6.2.5 Desincronización TCP

La desincronización TCP es una técnica que se usa en ataques de secuestro de TCP. Se desencadena mediante un proceso en el que el número secuencial en paquetes entrantes difiere del número secuencial previsto. Se rechazan los paquetes con un número secuencial no previsto (o se guardan en el almacén del búfer, si están presentes en la ventana de comunicación actual).

En caso de desincronización, ambos puntos finales de comunicación rechazan los paquetes recibidos; en este punto, los atacantes remotos pueden infiltrar y proporcionar paquetes con un número secuencial correcto. Los atacantes incluso pueden manipular o modificar la comunicación.

El objetivo de los ataques de secuestro de TCP es interrumpir las comunicaciones servidor-cliente o de igual a igual. Muchos ataques se pueden evitar usando autenticación para cada segmento de TCP. También se aconseja usar las configuraciones recomendadas para sus dispositivos de red.

6.2.6 Transmisión SMB

SMBRelay y SMBRelay2 son programas especiales para llevar a cabo un ataque contra ordenadores remotos. Los programas aprovechan el protocolo para compartir archivos Bloque de mensajes del servidor, que tiene capas en NetBIOS. La mayoría de los usuarios que comparten una carpeta o directorio en la red local utilizan este protocolo de uso compartido de archivos.

Dentro de la comunicación de red local, se intercambian hashes de contraseña.

SMBRelay recibe una conexión en los puertos UDP 139 y 445, transmite los paquetes intercambiados por el cliente y el servidor, y los modifica. Una vez realizada la conexión y la autenticación, el cliente se desconecta. SMBRelay crea una nueva dirección IP virtual. Se puede acceder a la nueva dirección con el comando "use net \\192.168.1.1". Después, cualquiera de las funciones de red de Windows puede usar la dirección. SMBRelay transmite la comunicación del protocolo SMB, excepto la relacionada con la negociación y la autenticación. Los atacantes remotos pueden usar la dirección IP, siempre que el ordenador cliente esté conectado.

SMBRelay2 funciona según el mismo principio que SMBRelay, con la diferencia de que usa nombres de NetBIOS en lugar de direcciones IP. Ambos pueden realizar ataques "hombre en medio". Estos ataques permiten a los atacantes remotos leer, insertar y modificar mensajes intercambiados entre dos puntos finales de comunicación sin ser detectados. Normalmente, los ordenadores expuestos a dichos ataques dejan de responder o se reinician inesperadamente.

Para evitar ataques, es recomendable utilizar contraseñas o claves de autenticación.

6.2.7 Ataques ICMP

El ICMP (Protocolo de mensajes de control de Internet) es un protocolo de Internet muy conocido y utilizado. Se usa fundamentalmente en ordenadores en red para enviar distintos mensajes de error.

Los ataques remotos intentan aprovecharse de los puntos débiles del protocolo ICMP, que está diseñado para la comunicación unidireccional sin autenticación. De esta forma, los ataques remotos pueden activar los denominados ataques DoS (por denegación de servicio) o los ataques que proporcionan a individuos no autorizados acceso a paquetes entrantes y salientes.

Entre los ejemplos más habituales de ataques ICMP se encuentran los ataques "flood" mediante Ping, "flood" de ICMP_ECHO y los ataques Smurf (denegación de servicios). Los ordenadores expuestos al ataque ICMP son significativamente más lentos (afecta a todas las aplicaciones que usen Internet) y tienen problemas para conectarse a Internet.

6.3 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 e información falsa, así como la difusión de software malicioso (malware). 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 bandeja de entrada.
- 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.

6.3.1 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.

6.3.2 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.

6.3.3 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, etc.), 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.

6.3.4 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, etc.), 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.

6.3.4.1 Reglas

En el contexto de las soluciones antispam y los clientes de correo electrónico, las reglas son herramientas para manipular funciones de correo electrónico que constan de dos partes lógicas:

1. Condición (por ejemplo, un mensaje entrante de una dirección concreta).
2. Acción (por ejemplo, la eliminación del mensaje o su transferencia a una carpeta específica).

El número y la combinación de reglas varía en función de la solución antispam. Estas reglas sirven como medidas contra el correo no deseado. Ejemplos típicos:

- 1. Condición: un correo electrónico entrante contiene algunas palabras que suelen aparecer en los mensajes de correo no deseado.
  2. Acción: eliminar el mensaje.

- 1. Condición: un correo electrónico entrante contiene un archivo adjunto con una extensión .exe.
  2. Acción: eliminar el archivo adjunto y enviar el mensaje al buzón de correo.
- 1. Condición: recibe un correo electrónico entrante de su jefe.
  2. Acción: mover el mensaje a la carpeta "Trabajo".

Es recomendable que, en los programas antispam, use una combinación de reglas para facilitar la administración y filtrar el correo no deseado de forma más eficaz.

6.3.4.2 Lista blanca

Por lo general, una lista blanca es una lista de elementos o personas aceptados o a los que se ha concedido permiso. El término "lista blanca de correo electrónico" es una lista de contactos de los que el usuario desea recibir mensajes. Estas listas blancas se basan en palabras clave que se buscan en direcciones de correo electrónico, nombres de dominios o direcciones IP.

Si una lista blanca funciona en "modo de exclusividad", no se recibirán los mensajes procedentes de otras direcciones, dominios o direcciones IP. Si la lista no es exclusiva, estos mensajes no se eliminarán, sino que se filtrarán de alguna otra forma.

Las listas blancas se basan en el principio opuesto al de las listas negras. Las listas blancas son relativamente fáciles de mantener, más que las listas negras. Es recomendable que use tanto una lista blanca como una lista negra para filtrar el correo no deseado de forma más eficaz.

6.3.4.3 Lista negra

Por lo general, una lista negra es una lista de personas o elementos prohibidos o no aceptados. En el mundo virtual, es una técnica que permite aceptar mensajes de todos los usuarios que no se incluyan en dicha lista.

Existen dos tipos de listas negras: las que crean los usuarios con su aplicación antispam y las profesionales, creadas por instituciones especializadas que las actualizan periódicamente y que se pueden encontrar en Internet.

Las listas negras son esenciales para bloquear con éxito el correo no deseado; sin embargo, son difíciles de mantener, ya que todos los días aparecen nuevos elementos que se deben bloquear. Le recomendamos que utilice una lista blanca y una lista negra para filtrar con mayor eficacia el correo no deseado.

6.3.4.4 Control del servidor

El control del servidor es una técnica que sirve para identificar correo electrónico no deseado en masa a partir del número de mensajes recibidos y las reacciones de los usuarios. Cada mensaje deja una "huella" digital única basada en el contenido del mensaje. El número de identificación exclusivo no indica nada sobre el contenido del mensaje de correo electrónico. Dos mensajes idénticos tendrán huellas idénticas, mientras que los mensajes diferentes tendrán huellas diferentes.

Si se marca un mensaje como no deseado, su huella se envía al servidor. Si el servidor recibe más huellas idénticas (correspondientes a un determinado mensaje no deseado), la huella se guarda en la base de datos de huellas de correo no deseado. Al analizar mensajes entrantes, el programa envía las huellas de los mensajes al servidor que, a su vez, devuelve información sobre las huellas correspondientes a los mensajes ya marcados por los usuarios como no deseados.