ESET NOD32 ANTIVIRUS 8

Guía del usuario

(desarrollada para las versiones 8.0 y posteriores del producto)

Microsoft® Windows® 8.1 / 8 / 7 / Vista / XP / Home Server 2003 / Home Server 2011

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

ESET NOD32 ANTIVIRUS

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

REV. 9/30/2014

Contenido

1. ESET NOD32 Antivirus

ESET NOD32 Antivirus representa un nuevo enfoque de la seguridad informática realmente integrada. La versión más reciente del motor de análisis ThreatSense® garantiza la protección del ordenador gracias a su velocidad y precisión. Estas características lo convierten en un sistema inteligente que está constantemente en alerta frente a ataques y software malintencionado que podrían poner en peligro su ordenador.

ESET NOD32 Antivirus es una solución de seguridad completa que combina la protección máxima con un impacto mínimo en el sistema. Nuestras tecnologías avanzadas utilizan la inteligencia artificial para evitar la infiltración de virus, spyware, troyanos, gusanos, adware, rootkits y otros ataques sin dificultar el rendimiento del sistema ni interrumpir la actividad del ordenador.

Características y ventajas

Antivirus y antiespía	Detecta y desinfecta de forma proactiva más virus, gusanos, troyanos y rootkits, conocidos o no. La tecnología de **Heurística avanzada** detecta incluso el código malicioso nunca visto hasta el momento, protegiéndole de amenazas desconocidas y neutralizándolas antes de que causen daños. **La protección del tráfico de Internet** y el **Anti-Phishing** funcionan supervisando la comunicación entre navegadores web y servidores remotos (incluido SSL). **La protección del cliente de correo electrónico** proporciona control de las comunicaciones por correo electrónico recibidas a través de los protocolos POP3(S) e IMAP(S).
Actualizaciones periódicas	La mejor manera de disfrutar del máximo nivel de seguridad en el ordenador es actualizar la base de firmas de virus y los módulos del programa de forma periódica.
ESET Live Grid (Reputación basada en la nube)	Puede comprobar la reputación de los procesos en ejecución y los archivos directamente desde ESET NOD32 Antivirus.
Control de dispositivos	Analiza automáticamente todas las unidades flash USB, tarjetas de memoria y CD/DVD. Bloquea los medios extraíbles en función del tipo de medio, el fabricante, el tamaño y otros atributos.
Funcionalidad HIPS	Puede personalizar el comportamiento del sistema de forma mucho más precisa, especificar reglas para el registro del sistema, activar procesos y programas y ajustar su configuración de seguridad.
Modo jugador	Pospone todas las ventanas emergentes, las actualizaciones y otras actividades que utilizan gran cantidad de recursos para reservarlos para los juegos u otras actividades de pantalla completa.

Para que las características de ESET NOD32 Antivirus funcionen debe haber una licencia activa. Se recomienda que renueve la licencia de ESET NOD32 Antivirus unas semanas antes de que expire.

1.1 Novedades de la versión 8

La versión 8 de ESET NOD32 Antivirus presenta numerosas pequeñas mejoras:

- **Un modo inteligente nuevo para HIPS**: se encuentra entre el modo automático y el modo interactivo. Es capaz de identificar actividades sospechosas y procesos maliciosos en el sistema.
- **Bloqueador de exploits mejorado**: se ha diseñado para fortificar aquellas aplicaciones que sufren más ataques, como los navegadores de Internet, los lectores de archivos PDF, los clientes de correo electrónico y los componentes de MS Office. Ahora el Bloqueador de exploits es compatible con Java y contribuye a una detección y protección mejores frente a este tipo de vulnerabilidades.
- **Control de dispositivos**: sustitución del control de medios extraíbles utilizado en las versiones 5 y 6. Este módulo le permite analizar, bloquear o ajustar los filtros y permisos ampliados, así como definir los permisos de un usuario para acceder a un dispositivo dado y trabajar en él.

- **Análisis de memoria avanzado**: trabaja conjuntamente con el Bloqueao de exploits para aumentar la protección contra código malicioso que utiliza los métodos de ofuscación y cifrado para evitar su detección por productos de protección antivirus.
- **Mejoras de Anti-phishing**: ahora ESET NOD32 Antivirus bloquea los sitios de fraudes y de phishing. Función de envío de sitios sospechosos y sitios de falso positivo mejorada.
- **Limpiador especializado**: herramienta de desinfección para las 3-5 amenazas más frecuentes.
- **Instalación más fiable y rápida**: incluye un análisis inicial a los 20 minutos de la instalación o el reinicio.
- **Compatibilidad con complemento de correo**: nuestro complemento ahora está integrado en Office 2013 y Windows Live Mail.
- **Compatibilidad mejorada en Windows 8/8.1**: ESET SysRescue ahora es plenamente funcional en Windows 8. Las notificaciones del sistema ahora se muestran en el entorno de Windows 8 para notificarle detecciones de HIPS o de archivos que requieren la interacción del usuario o descargas de aplicaciones potencialmente indeseables.

1.2 Requisitos del sistema

Para un funcionamiento óptimo de ESET NOD32 Antivirus, el sistema debería cumplir los siguientes requisitos de hardware y software:

Procesadores compatibles: Intel® o AMD x86/x64
Sistemas operativos: Microsoft® Windows® 8.1/8/7/Vista/XP SP3 o superior de 32 bits y XP SP2 o superior de 64 bits/ Home Server 2003 SP2 de 32 bits/Home Server 2011 de 64 bits

1.3 Prevención

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

Actualización regular

De acuerdo con las estadísticas de ESET 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 estas amenazas diariamente y preparan y publican actualizaciones para mejorar continuamente el nivel de protección para los usuarios. Para garantizar la máxima eficacia de estas actualizaciones es importante que estén bien configuradas en el sistema. Para obtener más información sobre cómo configurar las actualizaciones, consulte el capítulo Configuración de actualizaciones.

Descarga de parches de seguridad

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

Copia de seguridad de los datos importantes

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

Análisis regular del ordenador en busca de virus

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

Seguimiento de las reglas de seguridad básicas

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

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

2. Instalación

Hay varios métodos para instalar ESET NOD32 Antivirus en su ordenador. Los métodos de instalación pueden variar en función del país y del medio de distribución:

- El Live installer se puede descargar del sitio web de ESET. Este paquete de instalación es universal para todos los idiomas (elija el idioma que desee). Live installer es un pequeño archivo, los archivos adicionales que necesite para instalar ESET NOD32 Antivirus se descargarán automáticamente.

- Instalación sin conexión: este tipo de instalación se utiliza cuando se instala el producto desde un CD o DVD. Utiliza un archivo *.msi* de mayor tamaño que Live installer y que no necesita una conexión a Internet ni archivos adicionales para completar la instalación.

Importante: asegúrese de que no tenga instalados otros programas antivirus en el ordenador antes de instalar ESET NOD32 Antivirus. 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).

2.1 Live installer

Cuando haya descargado el paquete de instalación de *Live installer*, haga doble clic en el archivo de instalación y siga las instrucciones paso a paso de la ventana del instalador.

Importante: para este tipo de instalación debe estar conectado a Internet.

Seleccione el idioma que desee en el menú desplegable **Seleccionar el idioma del producto** y haga clic en **Instalar**. Los archivos de instalación tardarán unos momentos en descargarse.

Cuando haya aceptado el **Acuerdo de licencia para el usuario final**, se le pedirá que configure **ESET Live Grid**. ESET Live Grid ayuda a garantizar que se informe a ESET de forma continua e inmediata sobre las nuevas amenazas a 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 **Sí, deseo participar** está seleccionada de forma predeterminada para activar esta característica.

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.

Haga clic en **Siguiente** para iniciar el proceso de instalación.

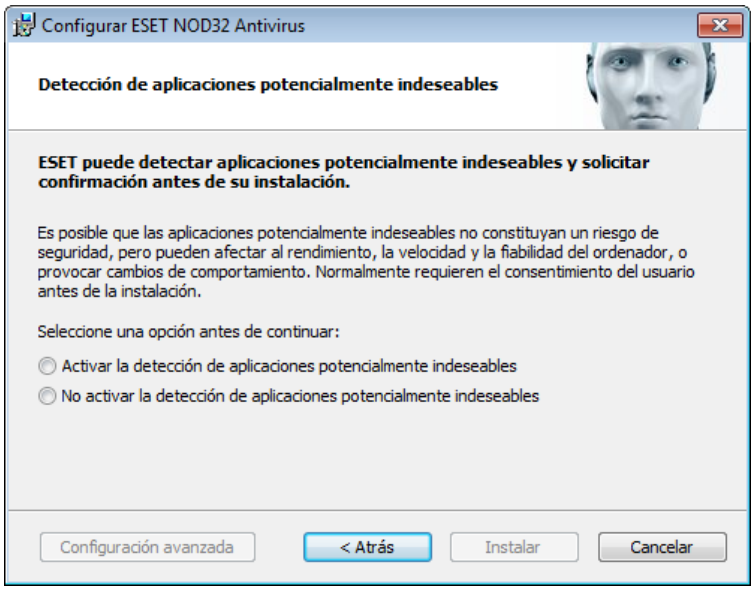
2.2 Instalación sin conexión

Una vez iniciado el paquete de instalación sin conexión (.msi), el asistente de instalación le proporcionará instrucciones para realizar la configuración.

Primero, el programa comprueba si hay una versión más reciente de ESET NOD32 Antivirus y, si se encuentra una versión más reciente, se le notificará en el primer paso del proceso de instalación. Si selecciona la opción **Descargar e instalar la nueva versión**, se descargará la nueva versión y el proceso de instalación continuará. Esta casilla de verificación solo está visible cuando hay disponible una versión más reciente que la versión que está instalando.

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. Después de aceptar, la instalación continuará.

Si desea más instrucciones para completar los siguientes pasos de la instalación, **ESET Live Grid** y **Detección de aplicaciones potencialmente indeseables**, siga las instrucciones de la sección mencionada (consulte "Live installer").



El modo de instalación incluye opciones de configuración adecuadas para la mayoría de los usuarios. Esta configuración proporciona un nivel de seguridad excelente, es fácil de configurar y permite un elevado rendimiento del sistema. La opción **Configuración avanzada** está diseñada para usuarios que tienen experiencia en el ajuste de programas y que desean modificar opciones avanzadas durante la instalación. Haga clic en **Instalar** para iniciar el proceso de instalación y omitir la configuración avanzada.

2.2.1 Configuración avanzada

Después de seleccionar **Configuración avanzada**, se le pedirá que seleccione una ubicación para la instalación. De forma predeterminada, el programa se instala en el siguiente directorio:

C:\Archivos de programa\ESET\ESET NOD32 Antivirus

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

Haga clic en **Siguiente** para configurar 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 **Usar las mismas características establecidas para Internet Explorer (recomendado)** y haga clic en **Siguiente**. Si no utiliza un servidor Proxy, seleccione **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.

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

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

NOTA: normalmente, después de actualizar componentes del programa, es necesario reiniciar el ordenador. Le recomendamos que seleccione **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 **Proteger la configuración con contraseña** e introduzca la contraseña en los campos **Contraseña nueva** y **Confirmar contraseña**. Necesitará esta contraseña para acceder a la configuración de ESET NOD32 Antivirus o cambiarla. Si ambos campos coinciden, haga clic en **Siguiente** para continuar.

Para completar los siguientes pasos de la instalación, **ESET Live Grid** y **Detección de aplicaciones potencialmente indeseables**, siga las instrucciones de la sección del instalador en directo (consulte "Live installer").

Para desactivar la operación de Primer análisis tras la instalación que se suele realizar cuando la instalación finaliza para comprobar si existe código malicioso, anule la selección de la casilla de verificación situada junto a **Activar análisis tras la instalación**. Haga clic en **Instalar**, en la ventana **Preparado para instalar**, para completar la instalación.

2.3 Activación del producto

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

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

Si ha adquirido una versión en caja física del producto, seleccione la opción **Activar mediante una clave de activación**. Normalmente, la clave de activación se encuentra en el interior o en la parte posterior del paquete del producto. Para una correcta activación, la clave de activación se debe introducir tal como se proporciona.

Si ha recibido un nombre de usuario y una contraseña, seleccione **Activar mediante nombre de usuario y contraseña** e introduzca sus credenciales en los campos correspondientes.

Si desea evaluar ESET NOD32 Antivirus antes de adquirir el producto, seleccione la opción **Activar licencia de prueba**. Escriba su dirección de correo electrónico y el país para activar ESET NOD32 Antivirus durante un período de tiempo

limitado. Recibirá la licencia de prueba por correo electrónico. Las licencias de prueba solo se pueden activar una vez por cliente.

Si no tiene una licencia y quiere adquirir una, haga clic en **Comprar licencia**. Será redirigido al sitio web del distribuidor local de ESET.

Seleccione **Activar más tarde** si desea evaluar rápidamente el producto y no quiere activarlo inmediatamente, o si prefiere activar el producto más adelante.

La copia de ESET NOD32 Antivirus también se puede activar directamente desde el programa. Haga clic en el icono Menú del programa situado en la esquina superior derecha o haga clic con el botón derecho en el icono ESET NOD32 Antivirus de la bandeja del sistema y seleccione **Activar el producto...** en el menú.

2.4 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. En la ventana principal del programa, haga clic en **Ayuda y asistencia técnica** y en **Activar licencia**; a continuación, introduzca los datos de licencia que se le proporcionaron con el producto de seguridad de ESET en la ventana Activación del producto.

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, todos en minúsculas.
- No utilizamos la letra L en las contraseñas (se utiliza el número uno (1) en su lugar).
- Un carácter '0' 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.

2.5 Actualización a una versión más reciente

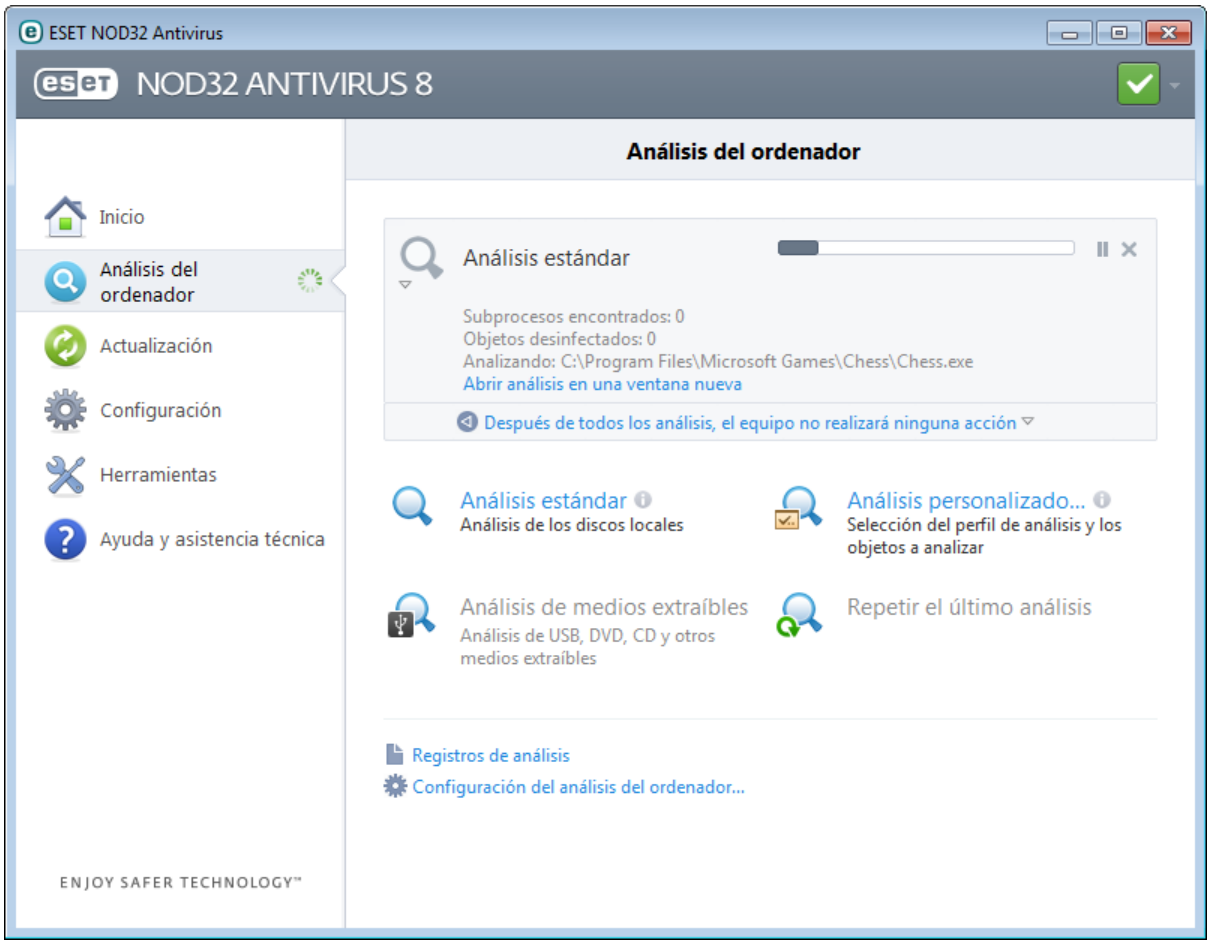
Las versiones nuevas de ESET NOD32 Antivirus implementan mejoras o solucionan problemas que no se pueden arreglar con las actualizaciones automáticas de los módulos de programa. La actualización a una versión más reciente se puede realizar de varias maneras:

1. Actualización automática mediante una actualización del programa.
   Las actualizaciones del programa se distribuyen a todos los usuarios y pueden afectar a determinadas configuraciones del sistema, de modo que se envían tras un largo periodo de pruebas que garantizan su funcionalidad 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 ventana principal del programa haciendo clic en **Instalar/buscar actualizaciones** en la sección **Actualización**.
3. Actualización manual mediante la descarga e instalación de una versión más reciente sobre la instalación existente.

2.6 Primer análisis tras la instalación

Después de instalar ESET NOD32 Antivirus, un análisis del ordenador comenzará 20 minutos después de la instalación o del reinicio del ordenador para comprobar si existe código malicioso.

También puede iniciar un análisis del ordenador manualmente desde la ventana principal del programa haciendo clic en **Análisis del ordenador** > **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 NOD32 Antivirus y su configuración básica.

3.1 Ventana principal del programa

La ventana principal del programa ESET NOD32 Antivirus se divide en dos secciones principales. En la ventana principal, situada a la derecha, se muestra información relativa a la opción seleccionada en el menú principal de la izquierda.

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

Inicio: proporciona información sobre el estado de protección de ESET NOD32 Antivirus.

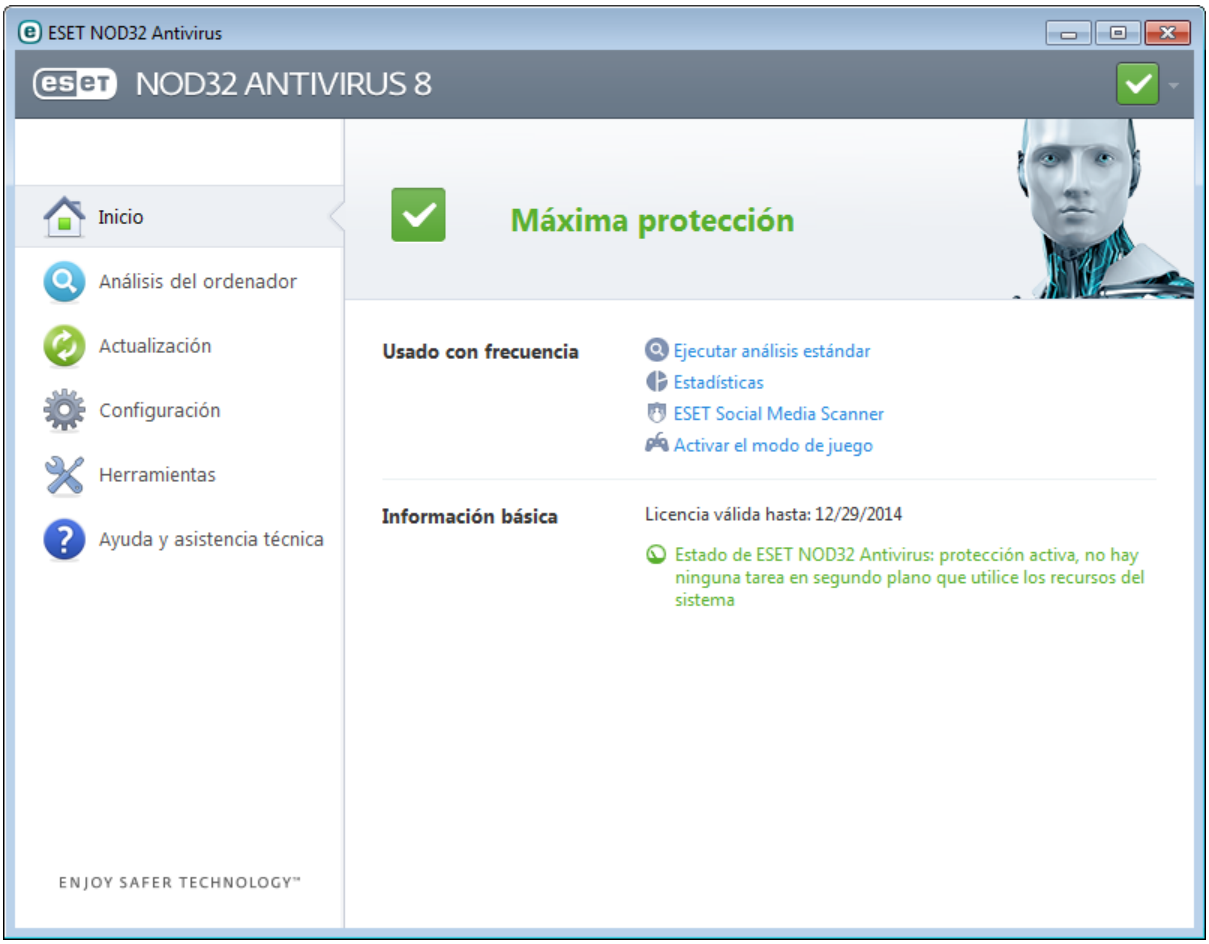
Análisis del ordenador: esta opción le permite configurar e iniciar el análisis estándar o el análisis personalizado.

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

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

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

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

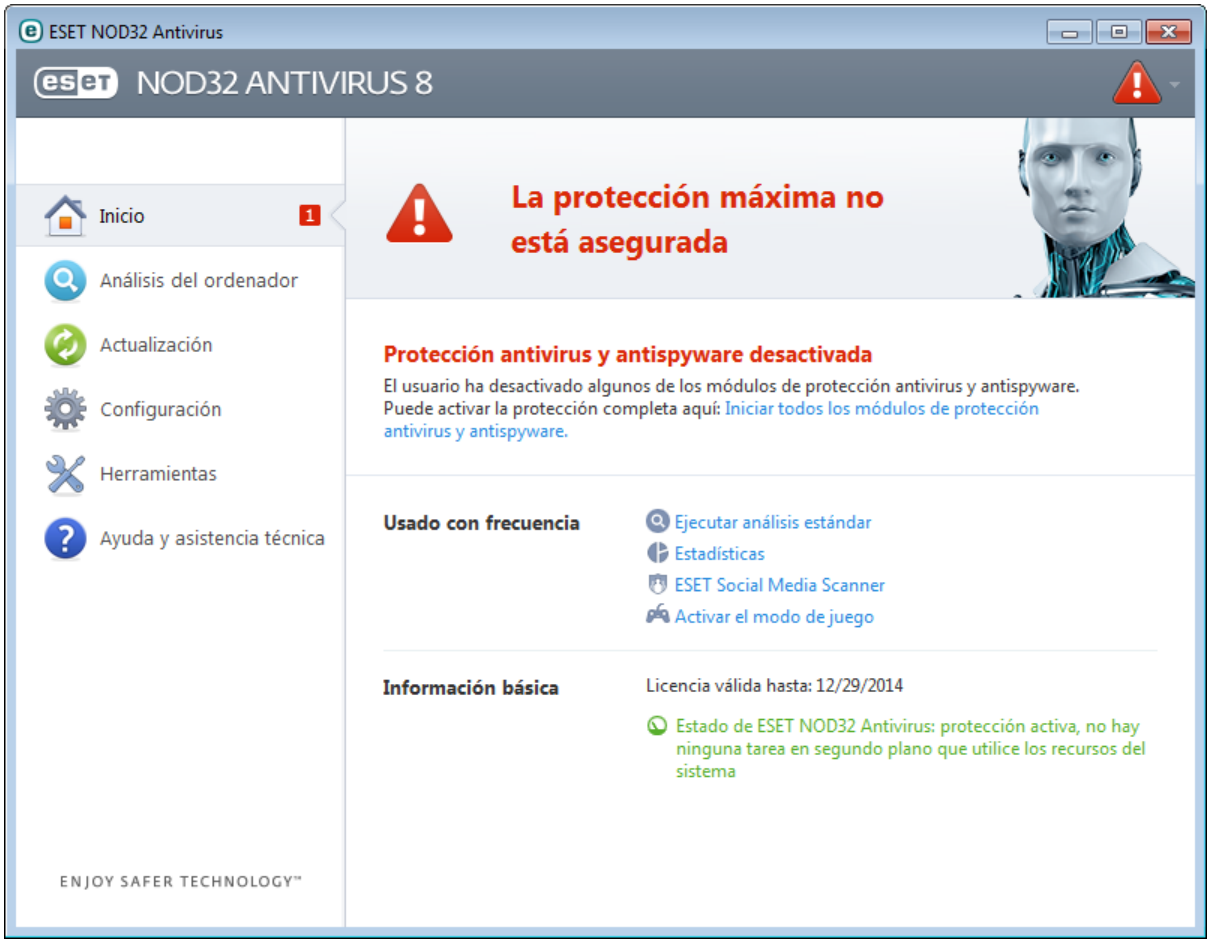


En la pantalla **Inicio** se proporciona información sobre el nivel de seguridad y de protección actual del ordenador. En la ventana de estado también se muestran las características más habituales de ESET NOD32 Antivirus. Aquí también se indica la fecha de expiración del programa, en **Información básica**.

El icono verde y el estado **Máxima protección** verde indican que se garantiza la máxima protección.

¿Qué hacer si el programa no funciona correctamente?

Si los módulos activados están funcionando correctamente, el icono de estado de la protección será verde. Un signo de exclamación rojo o un icono de notificación naranja indican que no se garantiza el nivel de protección máximo. En **Inicio** se mostrará información adicional acerca del estado de protección de cada módulo, así como soluciones sugeridas para restaurar la protección completa. Para cambiar el estado de módulos individuales, haga clic en **Configuración** y seleccione el módulo que desee.



El icono rojo y el estado La protección máxima no está asegurada indican problemas críticos. Existen varios motivos para que se muestre este estado, por ejemplo:

- **Producto no activado**: puede activar ESET NOD32 Antivirus desde **Inicio** haciendo clic en **Activar producto** o en **Comprar ahora**, debajo del estado de la protección.
- **La base de firmas de virus está desactualizada**: este error aparecerá 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 protección antivirus y antiespía está desactivada**: puede volver a activar la protección antivirus y antiespía haciendo clic en **Iniciar todos los módulos de protección antivirus y antiespía**.
- **La licencia ha expirado**: esto se indica mediante el icono de estado de la protección, que se vuelve rojo. Una vez que expire la licencia, el programa no se puede actualizar. Le recomendamos que siga las instrucciones de la ventana de alerta para renovar la licencia.

El icono naranja indica que la protección de su ordenador es limitada. Por ejemplo, existe un problema al actualizar el programa o la licencia se acerca a la fecha de expiración.
Existen varios posibles motivos para que se muestre este estado, por ejemplo:

- **Alerta de optimización Anti-Theft**: este dispositivo no está optimizado para ESET Anti-Theft. Por ejemplo, una cuenta fantasma no existe inicialmente, sino que se trata de una característica de seguridad que se activa automáticamente cuando se marca un dispositivo como perdido. Puede que necesite crear una

cuenta fantasma utilizando la característica Optimización en la interfaz web de ESET Anti-Theft.

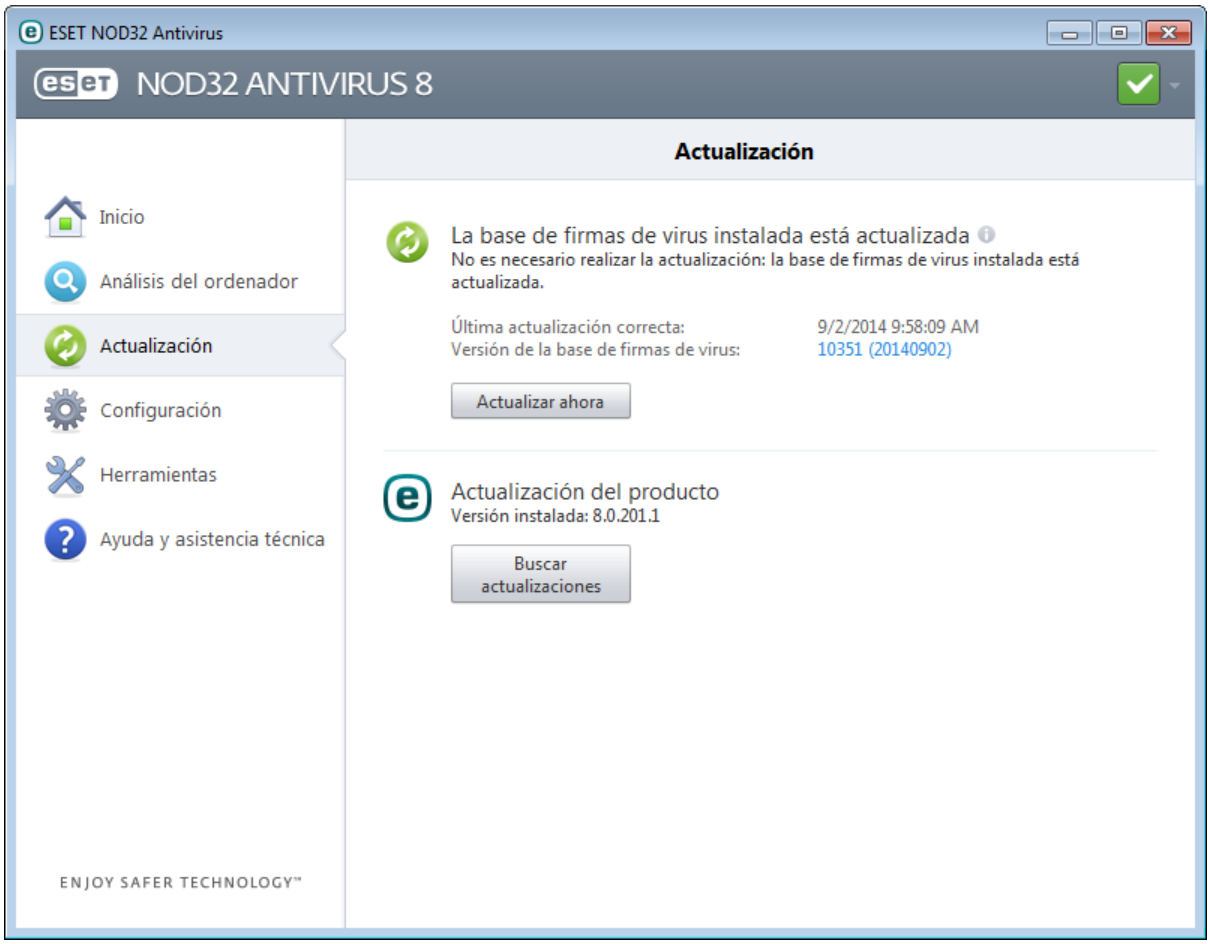
- **El modo jugador está activado**: la activación del modo jugador es un posible riesgo de seguridad. Al activar esta característica, se desactivan todas las ventanas emergentes y la actividad del planificador de tareas se detiene por completo.
- **Su licencia expirará en breve:** esto se indica mediante el icono de estado de la protección, que muestra un signo de exclamación junto al reloj del sistema. Cuando expire la licencia, el programa no se podrá actualizar y el icono del estado de la protección se volverá rojo.

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 todavía necesita ayuda, puede enviar una solicitud de soporte. El servicio de atención al cliente de ESET responderá a sus preguntas y le ayudará a encontrar una solución rápidamente.

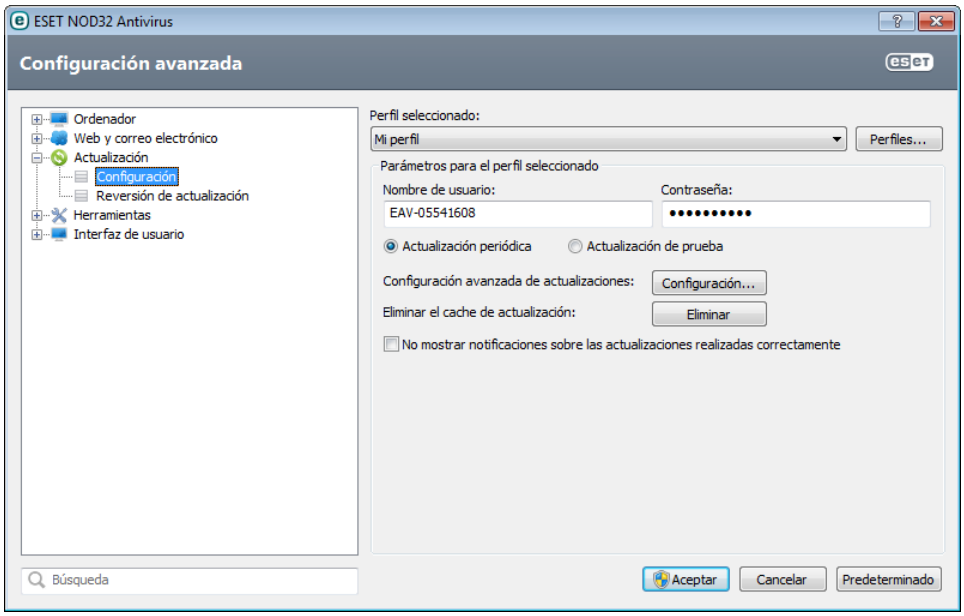
3.2 Actualizaciones

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

Si no ha introducido el nombre de usuario y la contraseña durante la activación de ESET NOD32 Antivirus, se le pedirá que lo haga ahora.

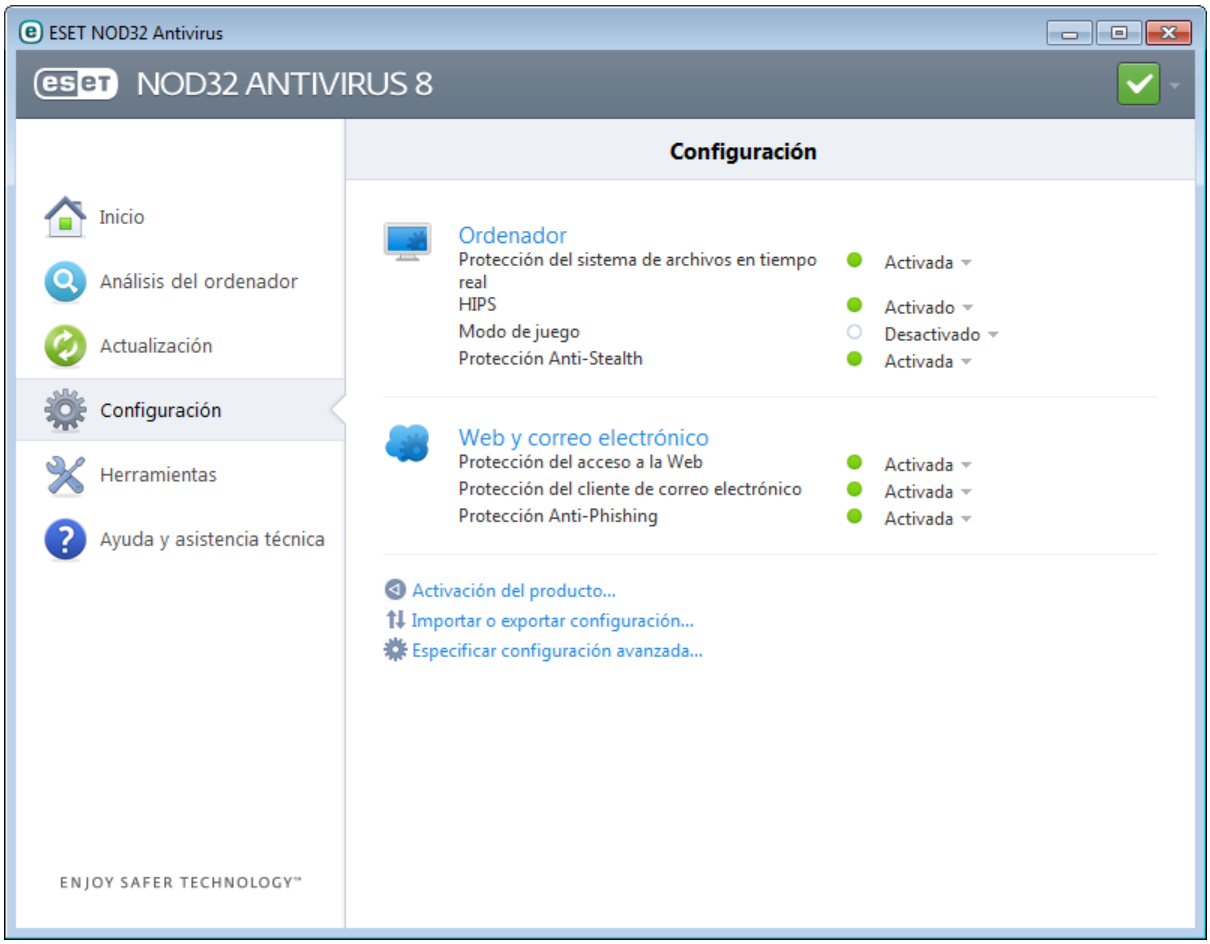


La ventana Configuración avanzada (haga clic en **Configuración** en el menú principal y, a continuación, en **Entrar a la configuración avanzada...**, o bien pulse **F5** en el teclado) ofrece opciones de actualización adicionales. Haga clic en **Actualizar** > **Configuración** en el árbol de configuración avanzada disponible a la izquierda. Para configurar las opciones avanzadas de actualización, como el modo de actualización, el acceso al servidor Proxy y las conexiones de red local, haga clic en el botón **Configuración...** en la ventana **Actualizar**.



4. Uso de ESET NOD32 Antivirus

Las opciones de configuración de ESET NOD32 Antivirus le permiten ajustar los niveles de protección del ordenador.



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

- **Ordenador**
- **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.
- **HIPS**: el sistema HIPS controla los sucesos del sistema operativo y reacciona según un conjunto de reglas personalizado.
- **Modo jugador**: activa o desactiva el modo jugador. Cuando se active el modo de juego, recibirá un mensaje de alerta (posible riesgo de seguridad) y la ventana principal se volverá naranja.
- **Protección Anti-Stealth**: detecta programas peligrosos, como rootkits, que se ocultan del sistema operativo y las técnicas de análisis ordinarias.

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

- **Protección del tráfico de Internet**: si esta opción está activada, se analiza todo el tráfico a través de HTTP o HTTPS para detectar la presencia de software malicioso.
- **La protección del cliente de correo electrónico**: supervisa comunicaciones recibidas a través de los protocolos POP3 e IMAP.
- **Protección Anti-Phishing**: filtra los sitios web sospechosos de distribuir contenido destinado a manipular a los usuarios para que envíen información confidencial.

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

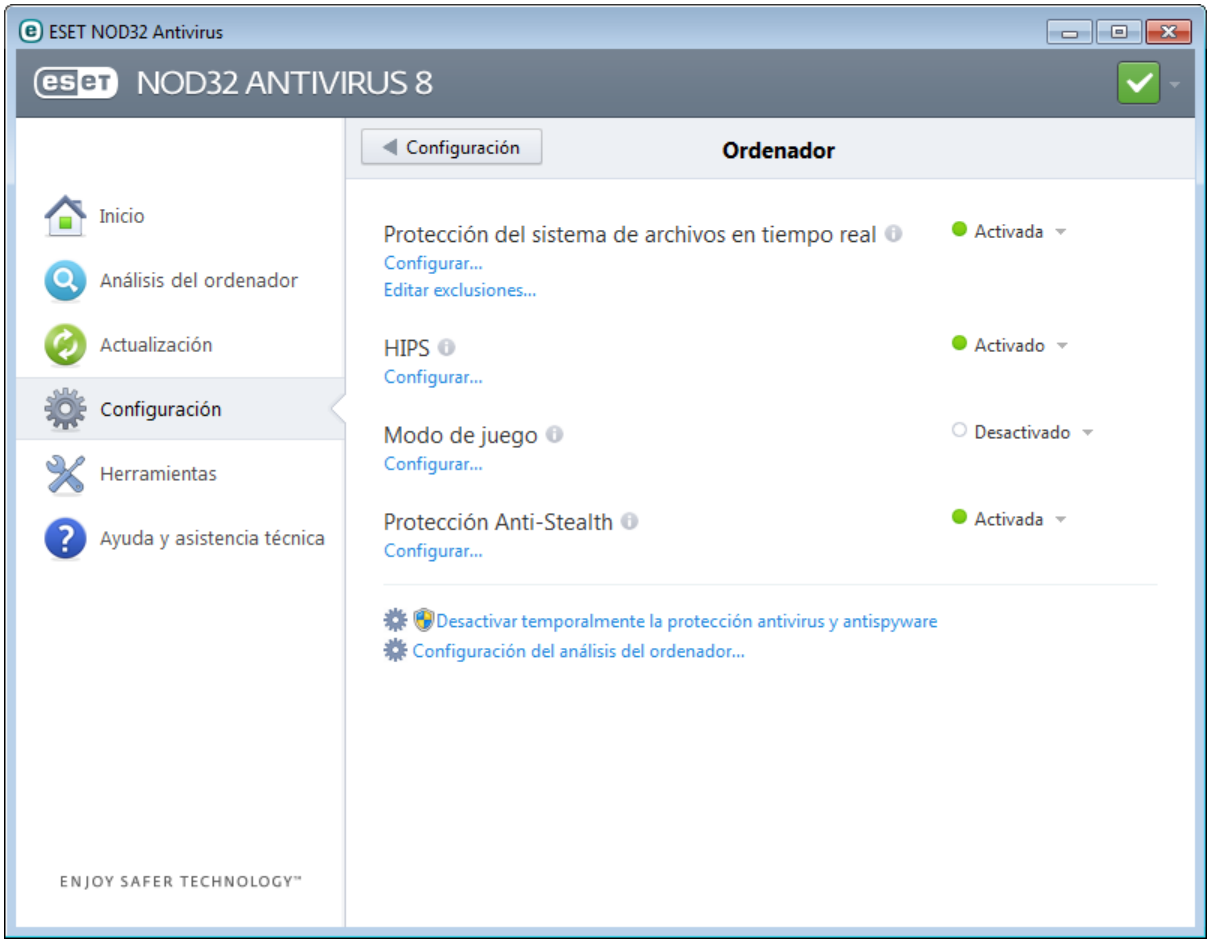
NOTA: si desactiva la protección con este método, todas las partes desactivadas de la protección se activarán al reiniciar el ordenador.

En la parte inferior de la ventana de configuración encontrará opciones adicionales. Utilice el enlace **Activación del producto** para abrir un formulario de registro que active el producto de seguridad de ESET; entonces, recibirá un mensaje de correo electrónico con los datos de autenticación (nombre de usuario y contraseña). 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 **Activado** > **Desactivar durante...** junto al módulo que desee. Tenga en cuenta que esto puede disminuir el nivel de 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. Cuando desactiva la protección, se abre la ventana **Desactivar la protección temporalmente** que le permite determinar durante cuánto tiempo estará desactivada seleccionando un valor en el menú desplegable **Intervalo de tiempo**. 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 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.

Las opciones de análisis para todos los módulos de protección (p. ej. protección del sistema de archivos en tiempo real, protección del tráfico de Internet, etc.) le permiten activar o desactivar la detección de lo siguiente:

- Las **aplicaciones potencialmente indeseables** (PUA) no tienen por qué ser maliciosas, pero pueden afectar al rendimiento del ordenador de forma negativa.
  Puede obtener más información sobre estos tipos de aplicaciones en el glosario.

- Por **aplicaciones potencialmente peligrosas** se entienden programas de software comercial legítimo que tienen el potencial de usarse con fines maliciosos. Entre los ejemplos de este tipo de programas encontramos herramientas de acceso remoto, aplicaciones para detectar contraseñas y registradores de pulsaciones (programas que registran cada tecla pulsada por un usuario). Esta opción está desactivada de manera predeterminada.
  Puede obtener más información sobre estos tipos de aplicaciones en el glosario.
- Entre las **aplicaciones potencialmente peligrosas** se incluyen programas comprimidos con empaquetadores o protectores. Los autores de código malicioso con frecuencia explotan estos tipos de protectores para evitar ser detectados.

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

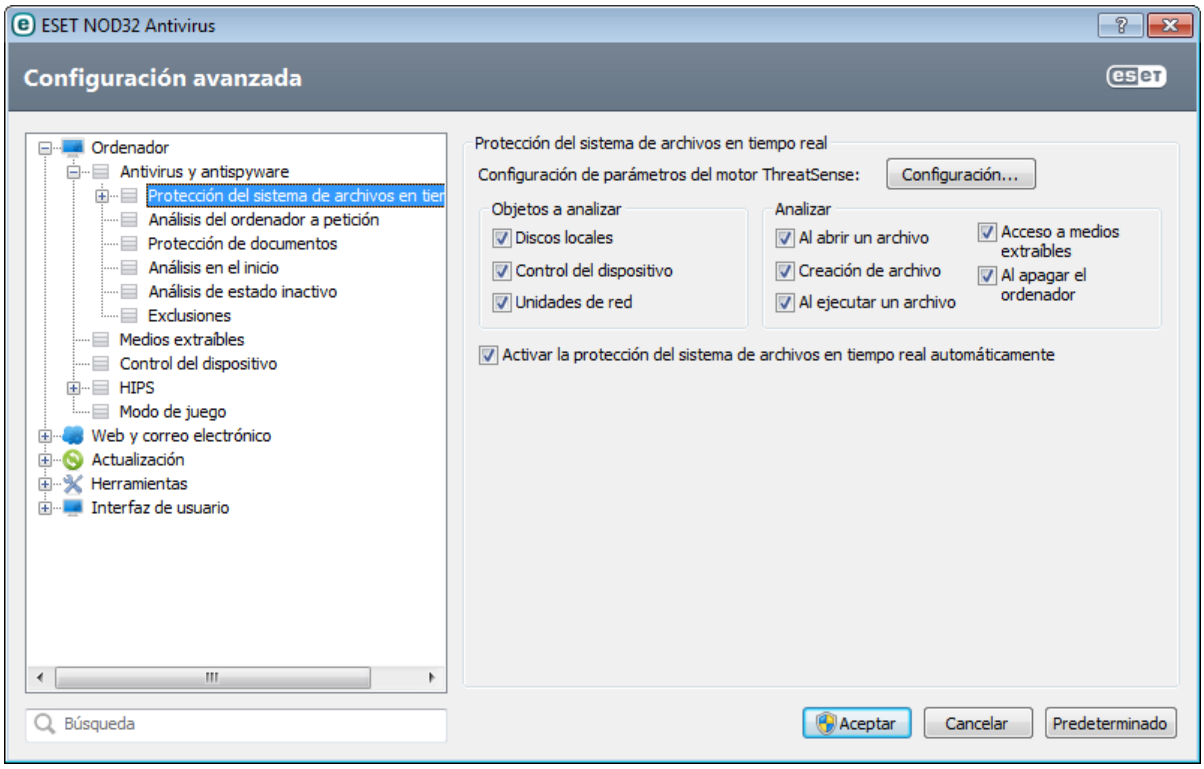
4.1.1.1 Protección del sistema de archivos en tiempo real

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 se puede configurar para que trate de forma diferente a los archivos recién creados y a los archivos existentes. Por ejemplo, puede configurar la protección del sistema de archivos en tiempo real para que supervise más detenidamente los archivos recién creados.

Con el fin de que el impacto en el sistema sea mínimo cuando se utiliza la protección en tiempo real, los archivos que ya se analizaron no se vuelven a analizar (a no ser que se hayan modificado). Los archivos se 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 esta característica 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 expanda **Ordenador** > **Antivirus y antiespía** > **Protección del sistema de archivos en tiempo real**. Haga clic en **Configuración...** junto a **Configuración de parámetros del motor ThreatSense** > **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 desactivar la protección en tiempo real anulando la selección de **Activar la protección del sistema de archivos en tiempo real automáticamente** en la sección **Protección del sistema de archivos en tiempo real** de Configuración avanzada.



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.
Control de dispositivos: discos CD y DVD, almacenamiento USB, dispositivos Bluetooth, etc.
Unidades de red: analiza todas las unidades asignadas.

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

Analizar (análisis cuando se cumpla la condición)

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

- **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.
- **Apagar el ordenador**: activa o desactiva el análisis activado por el apagado del ordenador.

4.1.1.1.1 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 y modificados

La probabilidad de infección en archivos modificados o recién creados es superior que en los archivos existentes. Por eso el programa comprueba estos archivos con parámetros de análisis adicionales. Además de los métodos de análisis basados en firmas habituales, se utiliza la heurística avanzada, que detecta amenazas nuevas antes de que se publique la actualización 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 los archivos ejecutados

- **Heurística avanzada al ejecutar un archivo**: de forma predeterminada, la Heurística avanzada se utiliza al ejecutar archivos. Si esta opción está activada, se recomienda encarecidamente dejar activadas las opciones Optimización inteligente y ESET Live Grid con el fin de mitigar su repercusión en el rendimiento del sistema.
- **Heurística avanzada al ejecutar archivos de medios extraíbles**: 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. En esta ventana, puede personalizar los ajustes mediante las casillas de verificación correspondientes a los diferentes puertos.

4.1.1.1.2 Niveles de desinfección

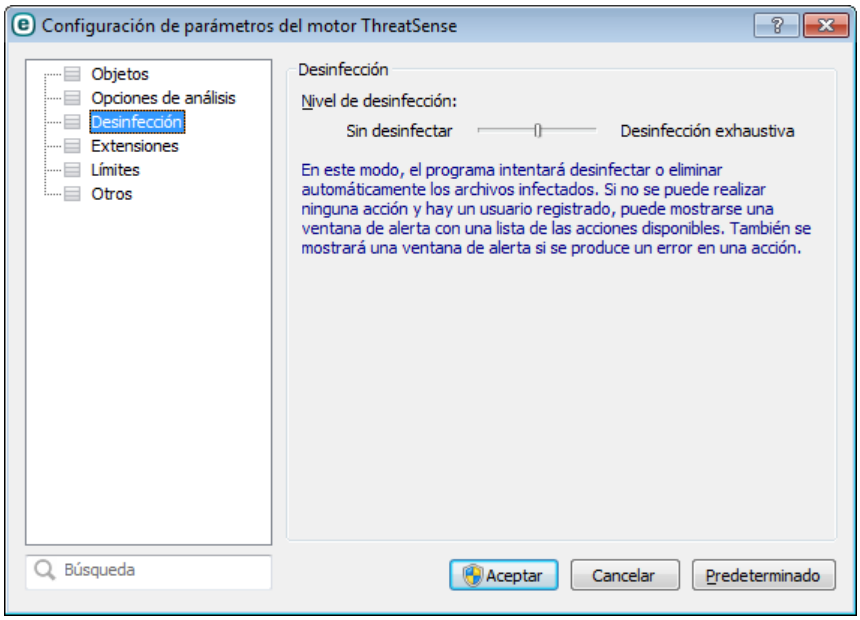
La protección en tiempo real tiene tres niveles de desinfección (para acceder, haga clic en **Configuración...** en la sección **Protección del sistema de archivos en tiempo real** y, a continuación, en **Desinfección**).

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 una notificación en la esquina inferior derecha de la pantalla. Si no es posible seleccionar la acción correcta de manera automática, el programa ofrece otras acciones que seguir. Lo mismo ocurre cuando no se puede completar una acción predefinida.

Desinfección 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.



4.1.1.1.3 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.

Una vez que se ha instalado ESET NOD32 Antivirus, se optimiza toda la configuración para proporcionar a los usuarios el máximo nivel de seguridad del sistema. Para restaurar la configuración predeterminada, haga clic en **Predeterminado** en la parte 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**).

4.1.1.1.4 Análisis de protección en tiempo real

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

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

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

Protección en tiempo real desactivada

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

Si no se activa al iniciar el sistema, probablemente se deba a que la opción **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 cualquier otro programa antivirus que haya en el sistema antes de instalar ESET.

La protección en tiempo real no se inicia

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

4.1.1.2 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 posibles virus que la Protección del sistema de archivos en tiempo real no haya encontrado cuando se registraron en el disco. Este fallo puede deberse a que la protección del sistema de archivos en tiempo real no estaba activada en ese momento, a que la base de firmas de virus está obsoleta o a que el archivo no se detectó como un virus cuando se guardó en el disco.

Están disponibles dos tipos de **Análisis del ordenador**. El **análisis estándar** analiza el sistema rápidamente, sin

necesidad de realizar una configuración adicional de los parámetros de análisis. El **Análisis personalizado** le permite seleccionar perfiles de análisis predefinidos para ubicaciones específicas, así como elegir objetos de análisis específicos.

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 automáticamente en el valor predeterminado. Para obtener más información detallada sobre los tipos de desinfección, consulte Desinfección.

Análisis personalizado

El análisis personalizado le permite 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.

Análisis de medios extraíbles

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

Este tipo de análisis también se puede iniciar haciendo clic en **Análisis personalizado** y después seleccionando **Medios extraíbles** en el menú desplegable **Objetos de análisis** y haciendo clic en **Analizar**.

Consulte 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**. Cómo programar un análisis del ordenador semanal.

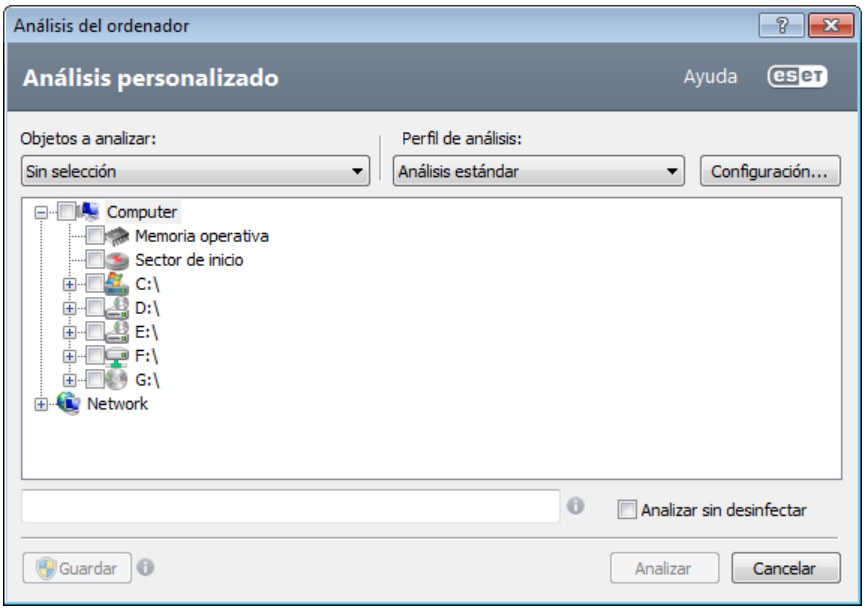
4.1.1.2.1 Iniciar análisis personalizado

Si no desea analizar todo el disco, sino un objeto determinado, puede usar la herramienta de análisis personalizado haciendo clic en **Análisis del ordenador** > **Análisis personalizado** y seleccionando una opción en el menú desplegable **Objetos de análisis** o seleccionando objetos específicos en la estructura de carpetas (árbol).

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

- **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.

Para acceder rápidamente a un objeto de análisis o agregar directamente un objeto deseado (carpeta o archivos), 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.



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

Puede elegir un perfil en el menú desplegable **Perfil de análisis** que se utilizará para analizar los objetos seleccionados. El perfil predeterminado es **Análisis estándar**. Hay otros dos perfiles de análisis predefinidos llamados **Análisis en profundidad** y **Análisis del menú contextual**. Estos perfiles de análisis utilizan distintos parámetros del motor ThreatSense. Haga clic en **Configuración...** para configurar en detalle el perfil de análisis elegido en el menú Perfil de análisis. Las opciones disponibles se describen en Configuración del análisis.

Haga clic en **Guardar** para guardar los cambios realizados en la selección de objetos, incluidas las selecciones realizadas en la estructura de árbol de carpetas.

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

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

4.1.1.2.2 Progreso del análisis

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

NOTA: es normal que algunos archivos, como los archivos protegidos con contraseña o que son utilizados exclusivamente por el sistema (por lo general, archivos *pagefile.sys* y determinados archivos de registro), no se puedan analizar.

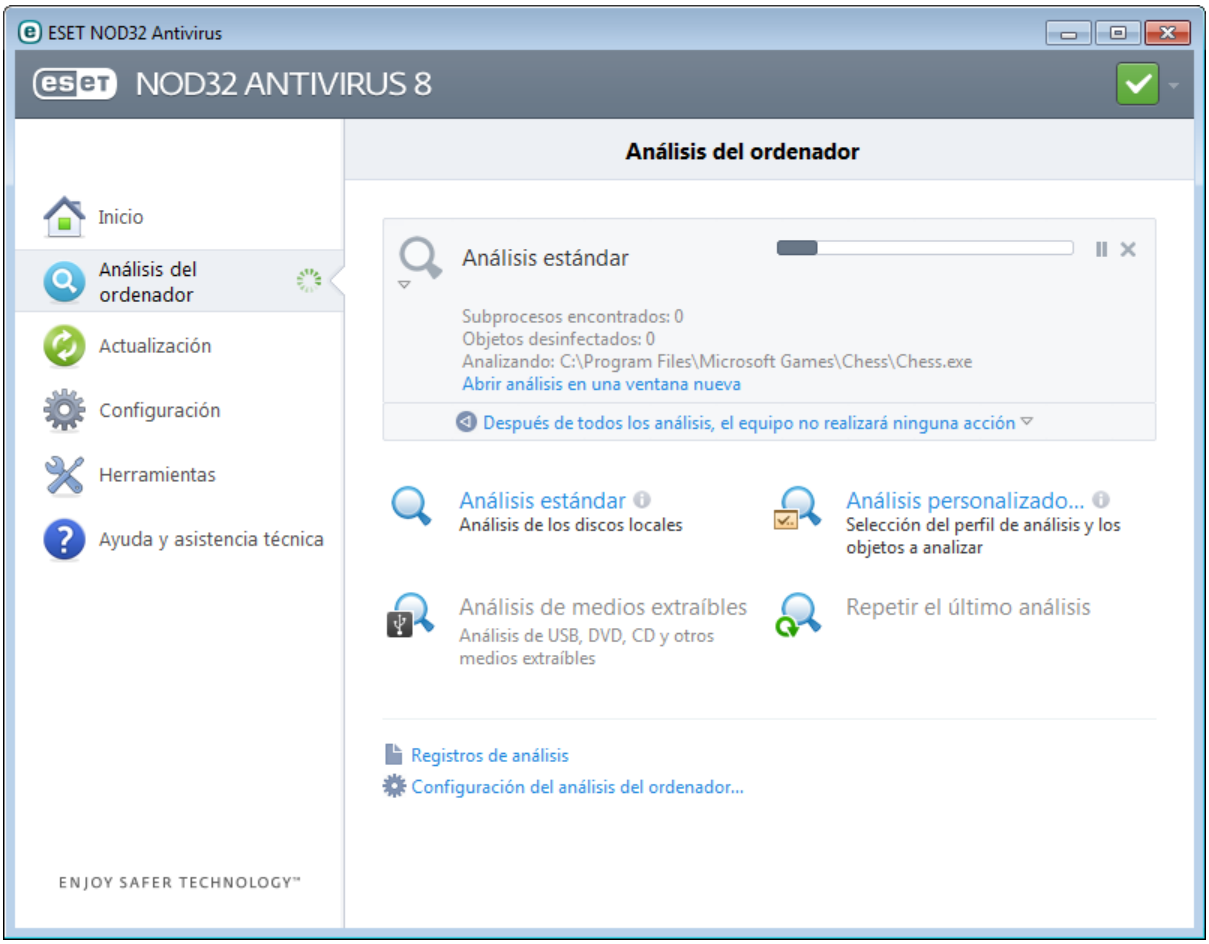
La barra de progreso muestra el porcentaje de objetos ya analizados en comparación con el porcentaje de objetos pendientes. El valor se calcula a partir del número total de objetos incluidos en el análisis.

Sugerencias:

Haga clic en la lupa o en la flecha para ver los detalles acerca del análisis que se está ejecutando en ese momento. Puede ejecutar otro análisis paralelo haciendo clic en **Análisis estándar** o **Análisis personalizado...**

Objetos: muestra el número total de objetos analizados, las amenazas encontradas y las desinfectadas durante un análisis.

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



Después de todos los análisis el ordenador no realiza ninguna acción: activa un apagado o reinicio programado cuando finaliza el análisis del ordenador. Cuando finalice el análisis, se abrirá un cuadro de diálogo de confirmación de apagado con un tiempo de espera de 60 segundos. Vuelva a hacer clic en esta opción para desactivar la acción seleccionada.

4.1.1.2.3 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 de estado inactivo** > **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 **Administración de perfiles**, haga clic en **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**. Ajuste los parámetros restantes a sus requisitos y guarde el nuevo perfil.

4.1.1.3 Análisis en el inicio

De forma predeterminada, la comprobación automática de los archivos en el inicio se realizará al iniciar el sistema o durante actualizaciones de 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 **Comprobación de la ejecución de archivos en el inicio** y en **Modificar...** En el último paso, aparece la ventana Verificación de la ejecución de archivos en el inicio (consulte el siguiente capítulo para obtener más detalles).

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

4.1.1.3.1 Comprobación de la ejecución de archivos en el inicio

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

El menú desplegable **Nivel de análisis** especifica la profundidad del análisis para los archivos que se ejecutan al iniciar el sistema. Los archivos se organizan en orden ascendiente de acuerdo con los siguientes criterios:

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

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

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

- **Normal**: con carga media del sistema.
- **Baja**: con carga baja 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.

4.1.1.4 Análisis de estado inactivo

Se puede configurar y activar el análisis de estado inactivo en **Configuración avanzada** en **Ordenador** > **Antivirus y antiespía** > **Análisis de estado inactivo**. Cuando el ordenador se encuentra en estado inactivo, se lleva a cabo un análisis silencioso de todos los discos locales del ordenador. Consulte Activadores de la detección del estado inactivo para ver una lista completa de condiciones que se deben cumplir para activar el análisis de estado inactivo.

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

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

La última opción disponible aquí es Configuración de parámetros del motor ThreatSense. Haga clic en **Configuración...** si desea modificar varios parámetros de análisis (por ejemplo, métodos de detección).

4.1.1.5 Exclusiones

Las exclusiones le permiten excluir archivos y carpetas del análisis. Para garantizar que se analizan todos los objetos en busca de amenazas, le recomendamos que solo cree exclusiones cuando sea absolutamente necesario. No obstante, puede que haya situaciones en las que necesite excluir un objeto, como por ejemplo entradas de una base de datos grande que ralenticen el ordenador durante el análisis o software que entre en conflicto con el análisis.

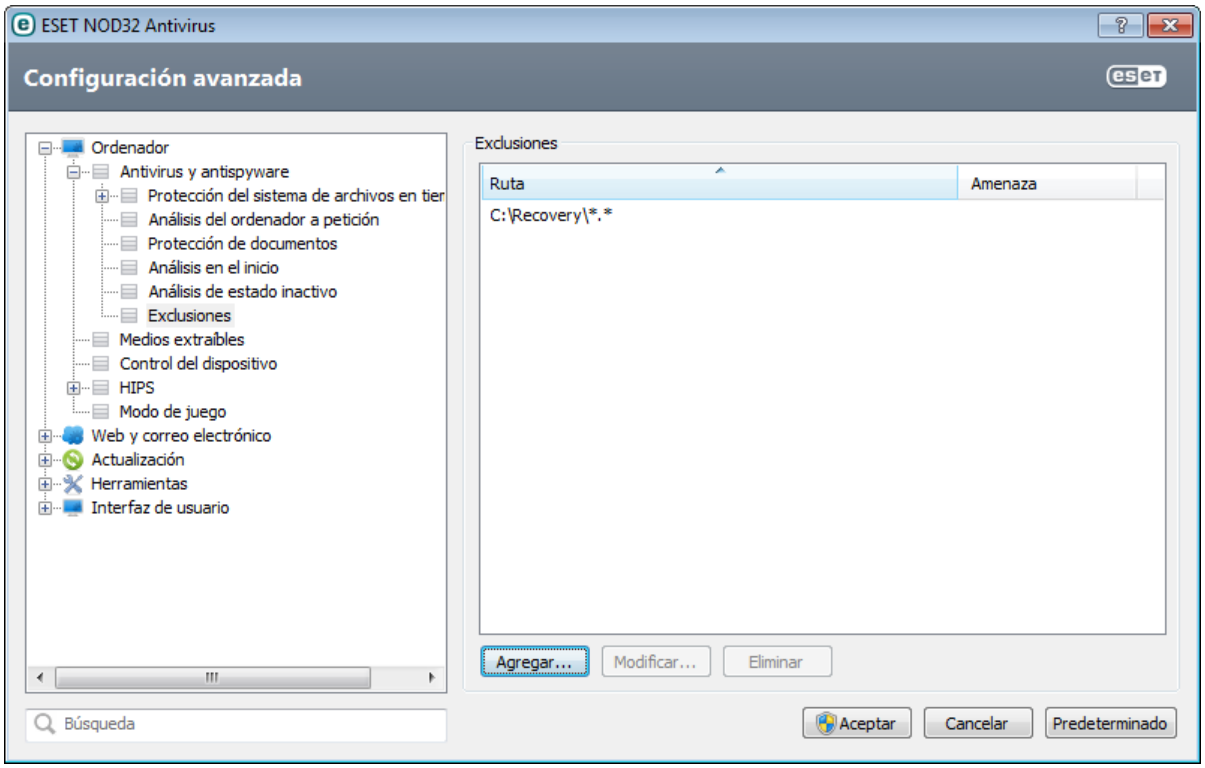
Para excluir un objeto del análisis:

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).



Nota: el módulo de protección del sistema de archivos en tiempo real o de análisis del ordenador no detectará las amenazas que haya contenidas en un archivo si este cumple los criterios de exclusión del 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. 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. Se puede crear en la ventana de alerta de amenaza que informa de la amenaza (haga clic en **Muestra/oculta parámetros adicionales de configuración** y, a continuación, seleccione **Excluir de la detección**) o en **Configuración** >

Cuarentena, haciendo clic con el botón derecho del ratón en el archivo en cuarentena y seleccionando **Restaurar y excluir de la detección** en el menú contextual.

Agregar: excluye los objetos de la detección.

Modificar: le permite modificar las entradas seleccionadas.

Quitar: elimina las entradas seleccionadas.

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. Utiliza una combinación de análisis de código, emulación de código, firmas genéricas y firmas de virus que funcionan de forma conjunta para mejorar en gran medida la seguridad del sistema. El motor de análisis es capaz de controlar varios flujos de datos de forma simultánea, de manera que maximiza la eficacia y la velocidad de detección. Además, la tecnología ThreatSense elimina los rootkits eficazmente.

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

- Los tipos de archivos y extensiones que se deben analizar.
- La combinación de diferentes métodos de detección.
- Los niveles de desinfección, etc.

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

- Protección del sistema de archivos en tiempo real.
- Protección de documentos.
- Protección del cliente de correo electrónico.
- Protección del tráfico de Internet.
- Análisis del ordenador.

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

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 las bases de firmas de virus anterior no conocían. La desventaja es que existe una probabilidad muy pequeña de falsas alarmas.

Heurística avanzada/DNA/Firmas inteligentes: la heurística avanzada es una de las tecnologías que utiliza ESET NOD32 Antivirus para la detección proactiva de amenazas. Permite detectar código malicioso desconocido a partir de su funcionalidad mediante el método de emulación. Este nuevo traductor de binarios le ayuda a burlar los trucos para evitar la emulación que utilizan los escritores de código malicioso. La última versión presenta una forma de emulación de código totalmente nueva que se basa en la traducción de binarios. Este nuevo traductor de binarios le ayuda a burlar los trucos para evitar la emulación que utilizan los escritores de código malicioso. Además de estas mejoras, el análisis basado en DNA se ha actualizado con el fin de mejorar la detección genérica y el tratamiento del código malicioso actual con mayor precisión.

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.

4.1.1.6.4 Extensiones

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 se ha seleccionado **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 **Analizar archivos sin extensión**. **No analizar archivos sin extensión** está disponible cuando se activa **Analizar todos los archivos**.

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

Con los botones **Agregar** y **Quitar**, puede activar o prohibir el análisis de extensiones de archivo específicas. 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, haga clic en **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 **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 realiza 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 el sellado de tiempo 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

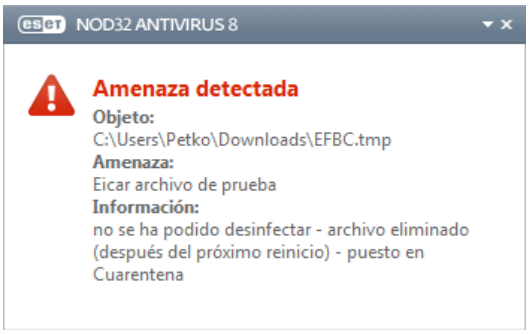
Las amenazas pueden acceder al sistema desde varios puntos de entrada, como páginas web, carpetas compartidas, correo electrónico o dispositivos extraíbles (USB, discos externos, CD, DVD, disquetes, etc.).

Comportamiento estándar

Como ejemplo general de cómo ESET NOD32 Antivirus gestiona las amenazas, estas se pueden detectar mediante:

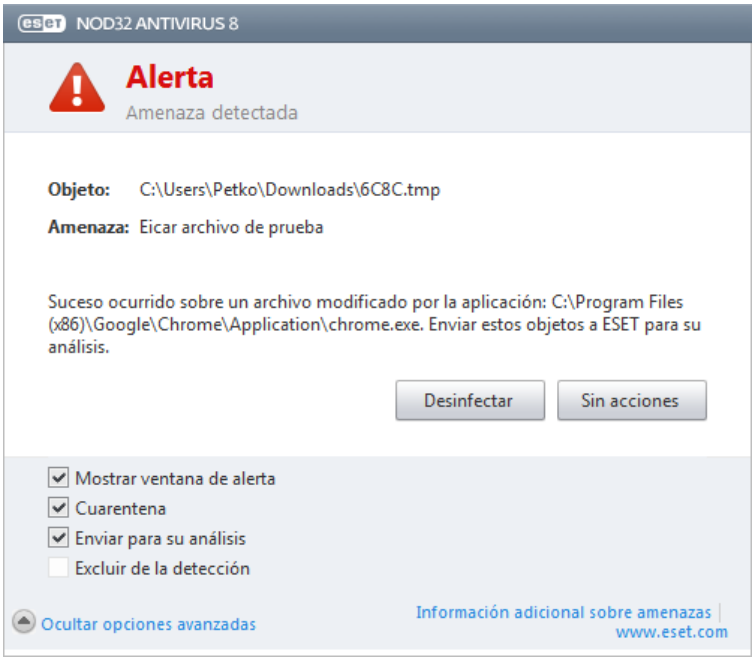
- Protección del sistema de archivos en tiempo real
- Protección del acceso a la Web
- Protección de clientes de correo electrónico
- Análisis de estado inactivo

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



Desinfección y eliminación

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



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

Si un proceso del sistema "bloquea" o está utilizando un archivo infectado, por lo general solo se eliminará cuando

se haya publicado (normalmente, tras reiniciar el sistema).

Múltiples amenazas

Si durante un análisis del ordenador no se desinfectaron algunos archivos infectados (o el Nivel de desinfección se estableció en **Sin desinfectar**), aparecerá una ventana de alerta solicitándole que seleccione las acciones que llevar a cabo en esos archivos. Seleccione las acciones para los archivos (las acciones se establecen individualmente para cada archivo de la lista) y, a continuación, haga clic en **Finalizar**.

Eliminar amenazas en archivos comprimidos

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

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

- Abra ESET NOD32 Antivirus y haga clic en Análisis del ordenador.
- Haga clic en **Análisis estándar** (para obtener más información, consulte Análisis del ordenador).
- Una vez que haya finalizado el análisis, revise el registro para consultar el número de archivos analizados, infectados y desinfectados.

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

4.1.1.8 Protección de documentos

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

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

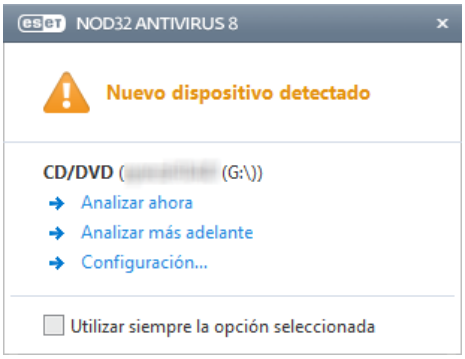
Esta característica se activa mediante aplicaciones que utilizan la Antivirus API de Microsoft (por ejemplo, Microsoft Office 2000 y superior, o Microsoft Internet Explorer 5.0 y superior).

4.1.2 Medios extraíbles

ESET NOD32 Antivirus permite analizar los medios extraíbles (CD, DVD, USB, etc.) de forma automática. Este módulo le permite analizar un medio insertado. Esto puede ser útil cuando el administrador del ordenador quiere impedir que los usuarios utilicen medios extraíbles con contenido no solicitado.

Para modificar la acción que se realizará cuando se introduce un medio extraíble (CD, DVD, USB, etc.) en el ordenador, pulse **F5** para abrir la ventana Configuración avanzada y expanda **Ordenador** > **Antivirus y antiespía** > **Medio extraíble** y seleccione la acción predeterminada en el menú desplegable **Acción que debe efectuarse cuando se insertan medios extraíbles**. 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 de estado inactivo 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.



4.1.3 Control de dispositivos

ESET NOD32 Antivirus permite controlar los dispositivos automáticamente (CD, DVD, USB, etc.). Este módulo le permite analizar, bloquear o ajustar los filtros y permisos ampliados, así como establecer los permisos de un usuario para acceder a un dispositivo dado y trabajar en él. Esto puede ser útil cuando el administrador del ordenador quiere impedir que los usuarios inserten dispositivos con contenido no solicitado.

Dispositivos externos admitidos

- CD/DVD
- Almacenamiento en disco
- Almacenamiento en FireWire

Nota: el control de dispositivos en ESET Endpoint Security o ESET Endpoint Antivirus que se utiliza en entornos empresariales admite más tipos de dispositivos externos.

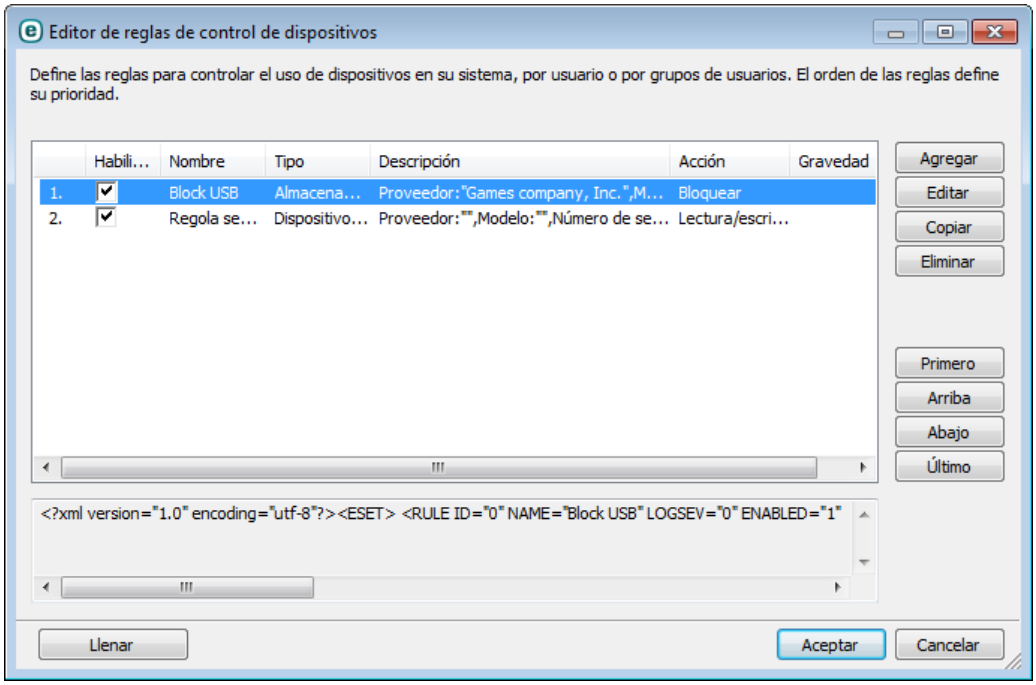
Las opciones de configuración del control de dispositivos se pueden modificar en **Configuración avanzada** (F5) > **Ordenador** > **Control de dispositivos**.

Al seleccionar la casilla de verificación situada junto a **Integrar en el sistema** se activa la característica de control de dispositivos en ESET NOD32 Antivirus; deberá reiniciar el ordenador para que se aplique este cambio. Una vez que el control de dispositivos esté activado, se activará **Configurar reglas...**, lo que le permitirá abrir la ventana Editor de reglas de control de dispositivos.

Si el dispositivo externo insertado 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 el nombre, el tipo de dispositivo externo, la acción que debe realizarse tras conectar un dispositivo externo al ordenador y la gravedad del registro.

Haga clic en **Agregar** o en **Modificar** para administrar una regla. 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 para 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.

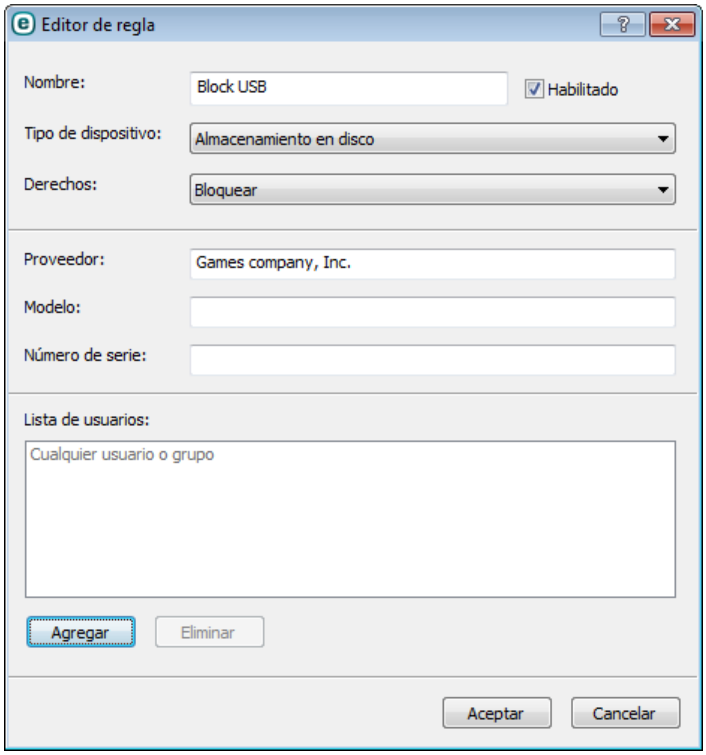
El control se efectúa mediante reglas que se clasifican en el orden que determina su prioridad, situándose al principio las reglas con la prioridad más alta.

Puede hacer clic con el botón derecho en una regla para mostrar el menú contextual. Aquí puede definir el nivel de detalle (gravedad) de las entradas de registro de una regla. Las entradas de registro se pueden ver desde la ventana principal de ESET NOD32 Antivirus en **Herramientas** > **Archivos de registro**.

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

4.1.3.2 Añadir reglas al 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** 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. Los lectores de tarjetas inteligentes abarcan aquellos con un circuito integrado incrustado, como tarjetas SIM o tarjetas de autenticación. Ejemplos de dispositivos de imagen son escáneres o cámaras; estos dispositivos no proporcionan información sobre los usuarios, sino únicamente sobre sus acciones. Esto significa que los dispositivos de imagen solo se pueden bloquear globalmente.

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 permitirá el acceso de lectura al dispositivo.
- **Lectura/Escritura**: se permitirá 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, **Solo lectura**, lo que significa que los dispositivos Bluetooth solo se pueden permitir o bloquear).

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

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

Nota: si las tres descripciones mencionadas quedan vacías, la regla ignorará estos campos al realizar la coincidencia. Los parámetros de filtrado de todos los campos de texto distinguen entre mayúsculas y minúsculas y no se aceptan los caracteres comodín (*, ?). Se deben escribir exactamente igual que el fabricante.

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.

Tenga en cuenta que no todos los dispositivos se pueden limitar mediante reglas de usuario (por ejemplo, los dispositivos de imagen no proporcionan información sobre los usuarios, sino únicamente sobre las acciones realizadas).

4.1.4 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.

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 NOD32 Antivirus, 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 NOD32 Antivirus tiene una tecnología de *Autodefensa* integrada que impide que el software malicioso dañe o desactive la protección antivirus y antispyware. *Autodefensa* protege los archivos y las claves del registro considerados cruciales para el funcionamiento de ESET NOD32 Antivirus y garantiza que el software potencialmente malicioso no tenga privilegios para realizar modificaciones en estas ubicaciones.

Los cambios realizados en la configuración de **Activar HIPS** y **Activar la Autodefensa** se aplicarán después de reiniciar Windows. También es necesario reiniciar el ordenador para desactivar el sistema **HIPS**.

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

Análisis de memoria avanzado: trabaja conjuntamente con el Bloqueao de exploits para aumentar la protección contra código malicioso que utiliza los métodos de ofuscación y cifrado para evitar su detección por productos de protección antivirus. Puede obtener más información sobre este tipo de protección en el glosario.

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

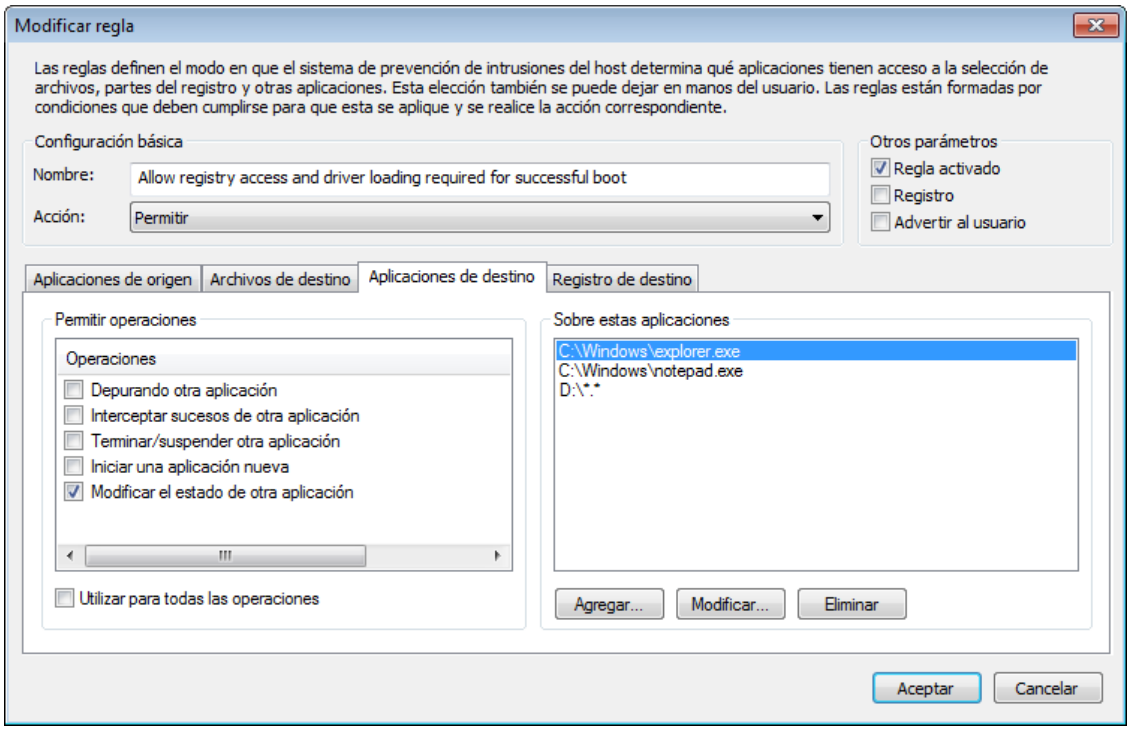
- **Modo automático con reglas**: las operaciones están activadas y se utiliza un conjunto de reglas predefinidas para proteger el sistema.
- **Modo inteligente**: solo se informará al usuarios de los sucesos muy sospechosos.
- **Modo interactivo**: el usuario debe confirmar las operaciones.
- **Modo basado en reglas**: las operaciones no definidas por una regla se pueden bloquear.
- **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 transcurrido el periodo de tiempo definido en **Notificar sobre el vencimiento del modo de aprendizaje en X días**, el modo de aprendizaje se vuelve a desactivar. 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.

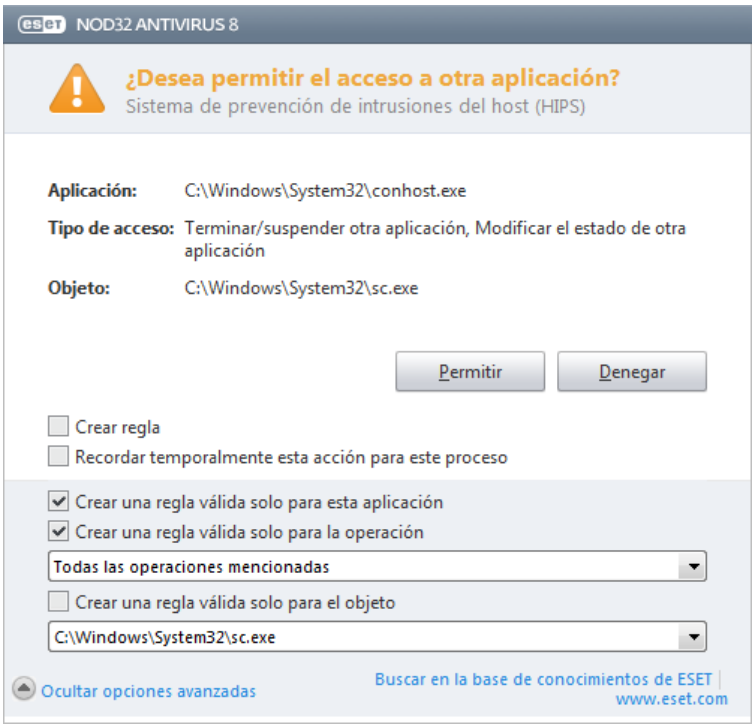
El sistema HIPS supervisa los sucesos del sistema operativo y reacciona de acuerdo con las reglas parecidas a las utilizadas por el cortafuegos personal en ESET Smart Security. Haga clic en **Configurar reglas...** para abrir la ventana de gestión de la regla de HIPS. Aquí puede seleccionar, crear, modificar 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 operaciones seleccionadas 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, a la que puede acceder pulsando la tecla F1).
4. **Agregue** una o varias aplicaciones que desee proteger.
5. Seleccione la casilla de verificación **Advertir al usuario** para mostrar una notificación siempre que se aplique una regla.
6. Haga clic en **Aceptar** para guardar la nueva regla.



Si selecciona **Preguntar** como la acción predeterminada, ESET NOD32 Antivirus mostrará un cuadro de diálogo cada vez que se ejecute una operación. Puede seleccionar entre **rechazar** y **permitir** la operación. Si no elige una acción, esta se seleccionará en función de las reglas predefinidas.



El cuadro de diálogo **¿Desea permitir el acceso a otra aplicación?** 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. Haga clic en **Mostrar opciones avanzadas** para definir los parámetros exactos de la nueva regla. Las reglas creadas de esta forma 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 otro cuadro de diálogo si los parámetros de su conjunto de reglas anterior no se aplican a la situación.

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

4.1.5 Modo de juego

El modo de juego 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. 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.

Si desea activar o desactivar el modo jugador, lo puede hacer en la ventana principal del programa al hacer clic en **Configuración** > **Ordenador** > **Activar** en **Modo jugador**; asimismo puede activarlo en el árbol de configuración avanzada (F5) al expandir **Ordenador**, hacer clic en **Modo jugador** y seleccionar la casilla de verificación junto a **Activar el modo jugador**. Activar el modo de juego constituye un riesgo de seguridad potencial, por lo que el icono de estado de la protección disponible en la barra de tareas se volverá naranja y mostrará un signo de alerta. Esta alerta también se puede ver en la ventana principal del programa donde verá el mensaje **El modo jugador está activado** en naranja.

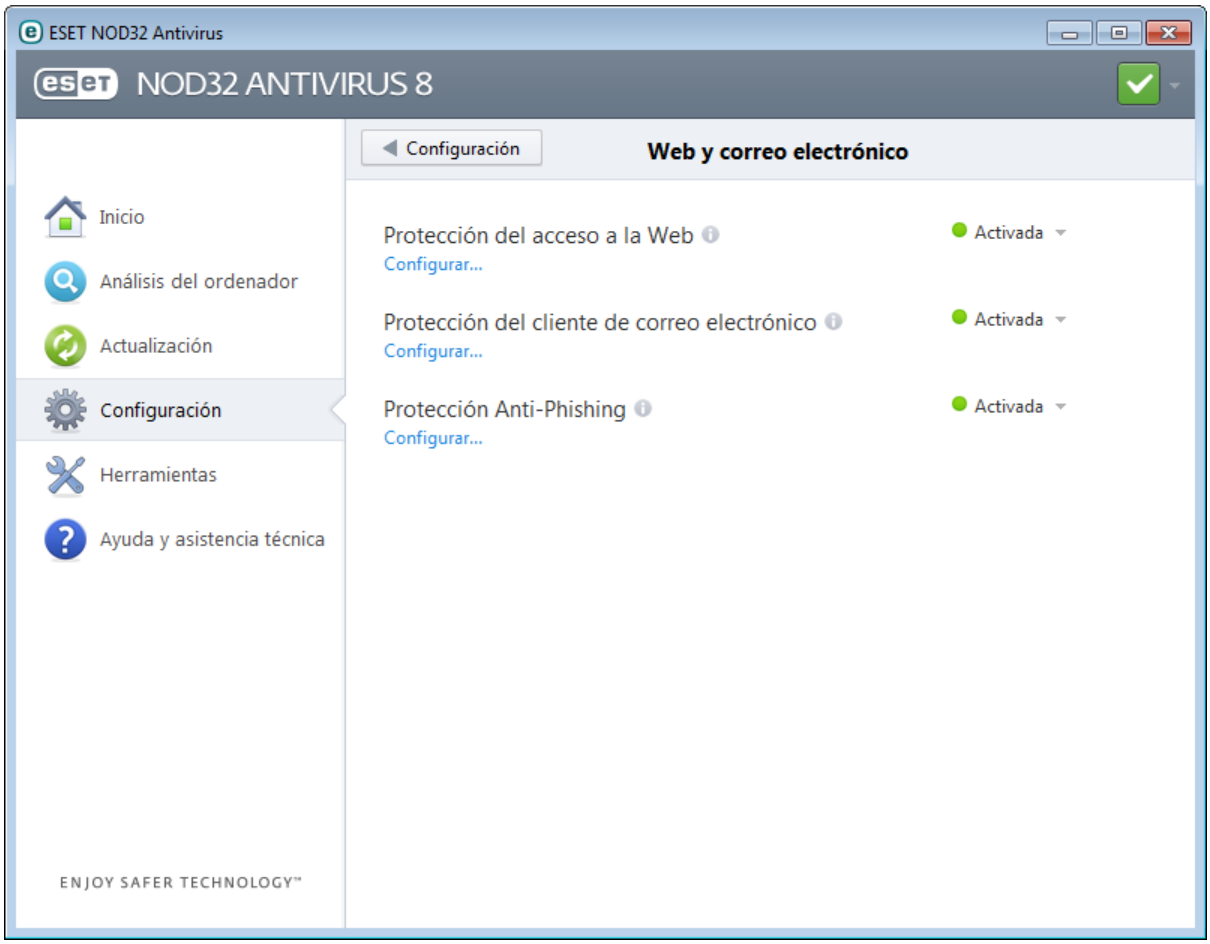
Si selecciona **Activar el modo jugador automáticamente cuando se ejecuten aplicaciones a pantalla completa**, el modo jugador se activará cuando inicie una aplicación a pantalla completa y se detendrá automáticamente cuando cierre dicha aplicación. Esta función es muy útil para que el modo jugador se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

También puede seleccionar **Desactivar el modo jugador automáticamente después de X minutos** y definir la

cantidad de tiempo (el valor predeterminado es 1 minuto) tras el cual el modo jugador se desactivará automáticamente.

4.2 Web y correo electrónico

Puede consultar la configuración web y del correo electrónico en el panel **Configuración** haciendo clic en **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**.

Haga clic en **Configurar** para abrir opciones de protección de web/correo electrónico/anti-phishing en la configuración avanzada.

La 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 NOD32 Antivirus ofrece control de todas las comunicaciones realizadas a y desde el cliente de correo electrónico (POP3, MAPI, IMAP, HTTP).

Protección Anti-Phishing le permite bloquear páginas web conocidas por distribuir contenido de phishing. Le recomendamos encarecidamente que deje Anti-Phishing activado.

Puede desactivar temporalmente el módulo de protección de web/correo electrónico/anti-phishing haciendo clic en **Activado**.

4.2.1 La 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 NOD32 Antivirus ofrece control de todas las comunicaciones desde el cliente de correo electrónico (POP3, MAPI, IMAP, HTTP). Al examinar los mensajes entrantes, el programa utiliza todos los métodos de análisis avanzados incluidos en el motor de análisis ThreatSense. Esto significa que la detección de programas maliciosos tiene lugar incluso antes de que se compare con 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** > **La 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 **Notificar en los mensajes recibidos y leídos** o **Notificar en los mensajes enviados**. Tenga en cuenta que en ocasiones puntuales es posible que los mensajes con etiqueta se omitan en mensajes HTML problemáticos o sean falsificados por algunos virus. Los mensajes con etiqueta se pueden agregar a los mensajes recibidos y leídos, a los mensajes enviados o a ambos. Las opciones disponibles son:

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

Agregar una advertencia en el asunto de los mensajes infectados recibidos y leídos/enviados: seleccione 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.

4.2.1.1 Integración con clientes de correo electrónico

La integración de ESET NOD32 Antivirus con clientes de correo electrónico aumenta el nivel de protección activa frente a código malicioso en los mensajes de correo electrónico. Si su cliente de correo electrónico es compatible, la integración se puede activar en ESET NOD32 Antivirus. Al activar la integración, la barra de herramientas de ESET NOD32 Antivirus 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** > **Entrar a la configuración avanzada...** > **Web y correo electrónico** > **La 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 y Windows Live Mail. 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. Esto puede suceder cuando recupera 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).

4.2.1.1.1 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 y Windows Live Mail. La protección de correo electrónico funciona como un complemento para estos programas. La principal ventaja del complemento es el hecho de que es independiente del protocolo utilizado. Cuando el cliente de correo electrónico recibe un mensaje cifrado, este se descifra y se envía para el análisis de virus.

Análisis de mensajes

Correo recibido: activa el análisis de los mensajes recibidos.
Correo enviado: 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

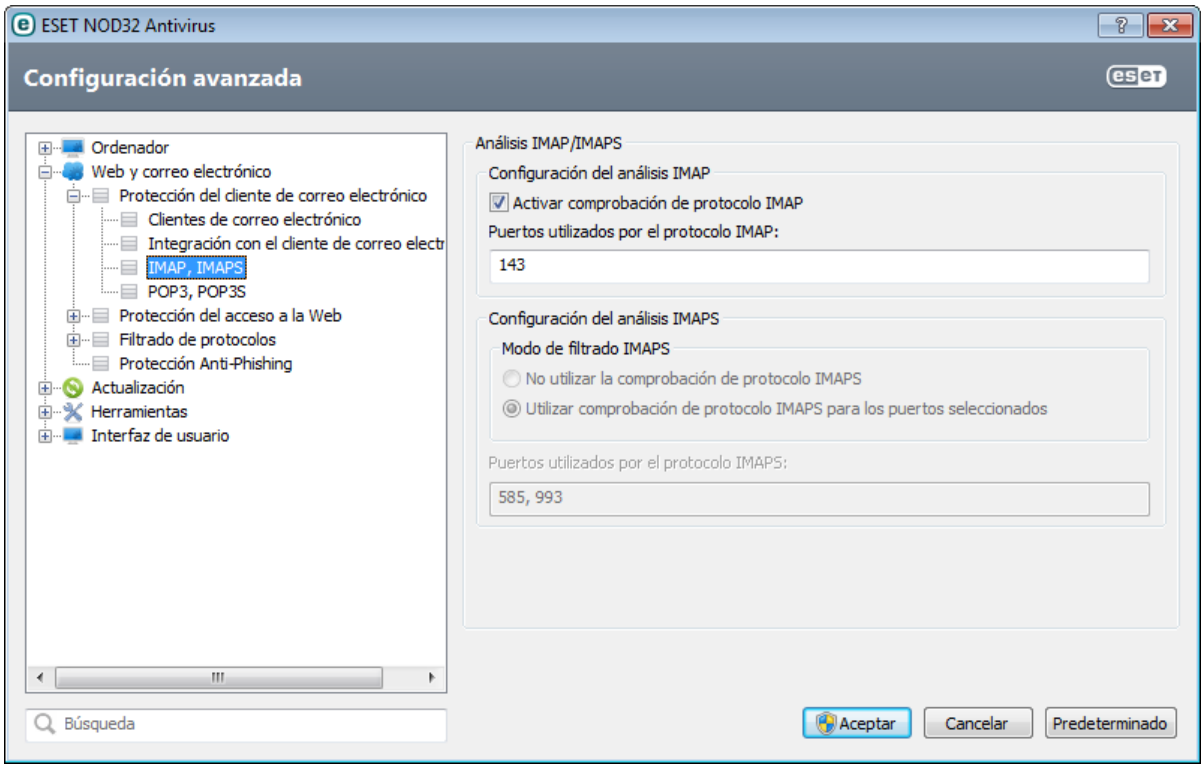
Repetir análisis después de actualizar: activa el nuevo análisis tras una actualización de la base de firmas de virus.
Incluir los análisis de otros módulos: al seleccionar esta opción, el módulo de protección de correo electrónico acepta los resultados del análisis de otros módulos de protección.

4.2.1.2 Análisis IMAP, 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 conserva la información de estado (si el mensaje se ha leído, contestado o eliminado). ESET NOD32 Antivirus 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. 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**.



4.2.1.3 Filtro POP3, POP3S

El protocolo POP3 es el más utilizado para recibir comunicaciones por correo electrónico en una aplicación de cliente de correo. ESET NOD32 Antivirus 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 NOD32 Antivirus 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 NOD32 Antivirus 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.

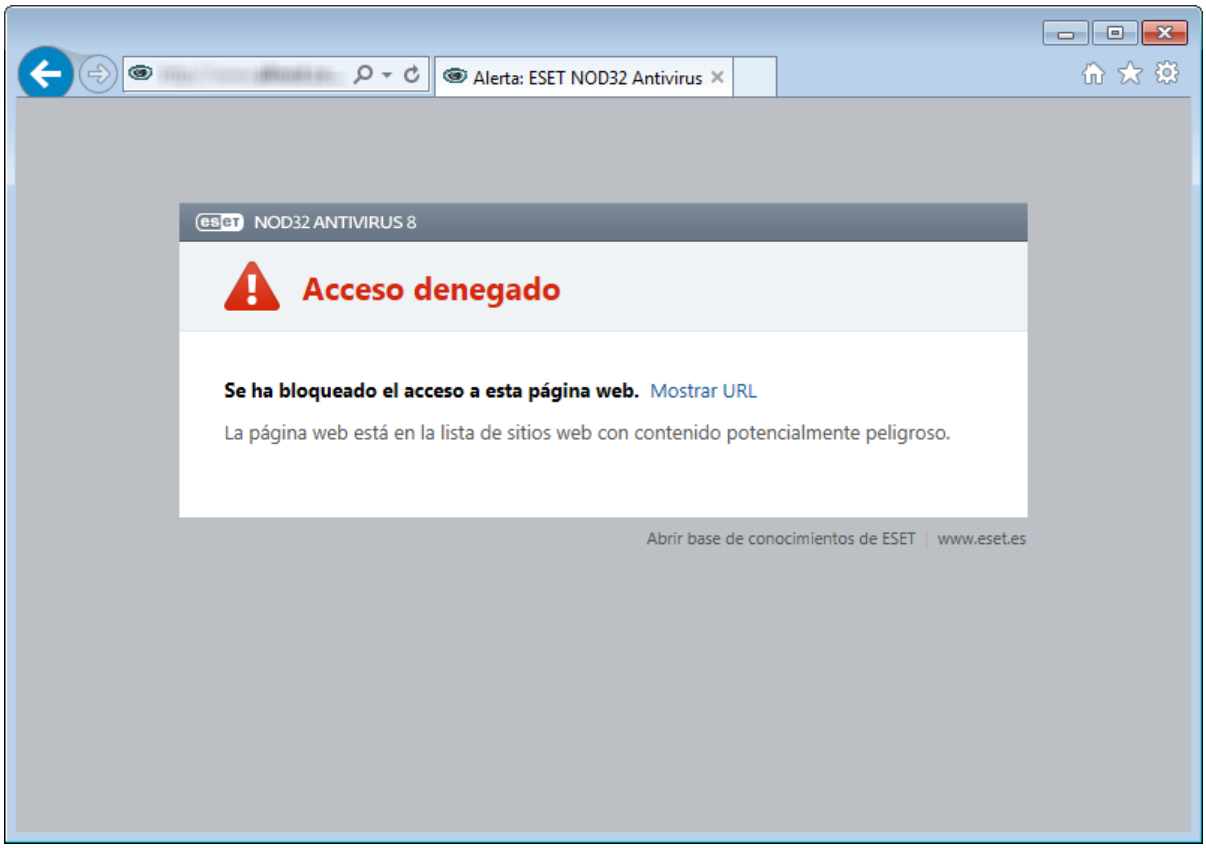
Utilizar la comprobación del protocolo POP3S para los puertos seleccionados: marque esta opción para activar el análisis POP3S solo de los puertos definidos en **Puertos utilizados por el protocolo POP3S**.

Puertos utilizados por el protocolo POP3S: consiste en una lista de puertos POP3S sujetos a análisis (de forma predeterminada, 995).

4.2.2 Protección del acceso a 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. La protección del tráfico de Internet funciona supervisando la comunicación entre navegadores web y servidores remotos, y cumple con las reglas HTTP (Protocolo de transferencia de hipertexto) y HTTPS (comunicación cifrada).

Le recomendamos encarecidamente que active la opción de protección del tráfico de Internet. Se puede acceder a esta opción desde la ventana principal de ESET NOD32 Antivirus accediendo a **Configuración** > **Web y correo electrónico** > **Protección del tráfico de Internet**. Se bloqueará siempre el acceso a las páginas web conocidas por tener contenido malicioso.



4.2.2.1 HTTP, HTTPs

ESET NOD32 Antivirus 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 **Filtro HTTP**, puede seleccionar o anular la selección de **Activar el análisis HTTPS**. 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 NOD32 Antivirus admite la comprobación del protocolo HTTPS. La comunicación HTTPS utiliza un canal cifrado para transferir información entre el servidor y el cliente. ESET NOD32 Antivirus 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: el programa solo analizará aquellas aplicaciones que estén especificadas en la sección Clientes de correo electrónico y web y que utilicen los puertos definidos en **Puertos utilizados por el protocolo HTTPS**. El puerto 443 está configurado de forma predeterminada.

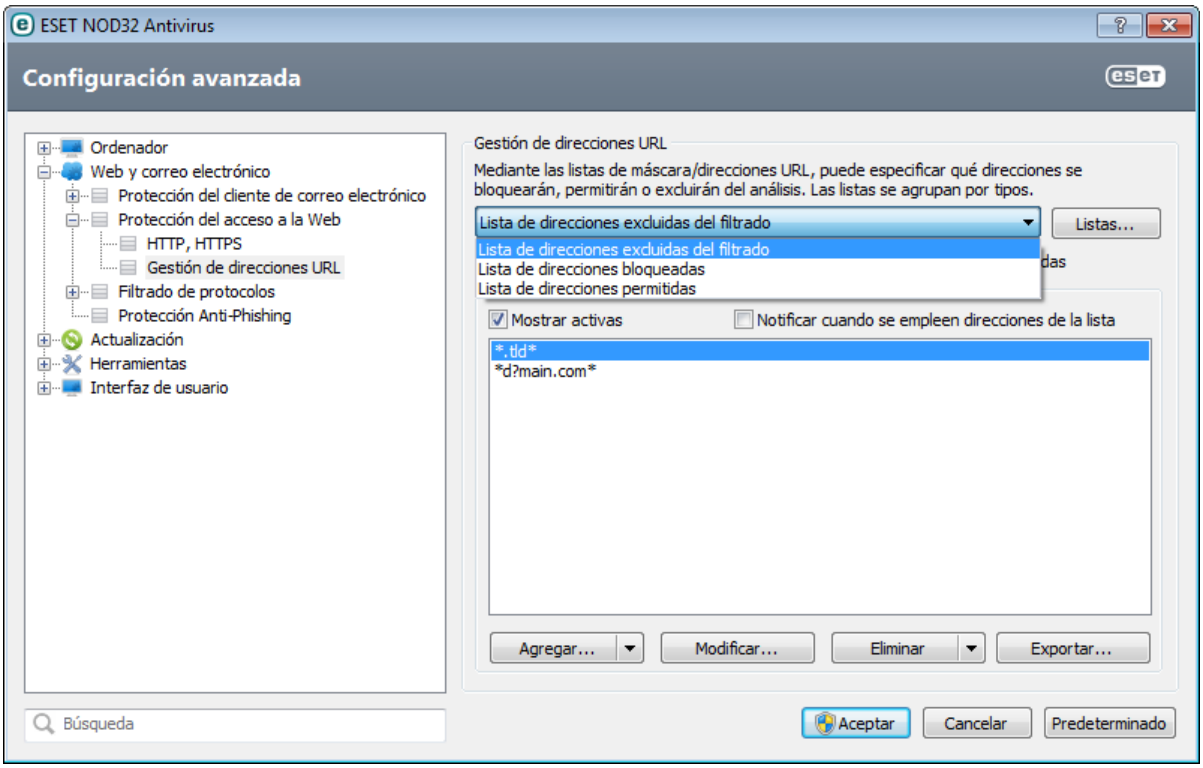
La comunicación cifrada no se analiza. Para activar el análisis de la comunicación cifrada y ver la configuración del análisis, vaya a Comprobación del protocolo SSL en la sección Configuración avanzada (**Web y correo electrónico** > **Filtrado de protocolos** > **SSL**) y active la opción **Analizar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

4.2.2.2 Gestión de direcciones URL

En esta sección puede especificar las direcciones HTTP que desea bloquear, permitir o excluir del análisis. **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 **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**. Haga clic en **Listas...** para abrir 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 seleccionada.

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. Consulte Agregar dirección HTTP/máscara de dominio para obtener información sobre cómo detectar un dominio completo con todos sus subdominios de forma segura. Para activar una lista, seleccione la opción **Lista activa**. Si desea que le notifiquen cuando se introduzca una dirección de la lista actual, seleccione **Notificar cuando se empleen direcciones de la lista**.



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

Modificar: permite modificar direcciones manualmente; 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.

4.2.3 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.

Integrar en el sistema: activa el controlador de la funcionalidad de filtrado de protocolos de ESET NOD32 Antivirus.

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 nueva Plataforma de filtrado de Windows (WFP) se aplica, en primer lugar, a Windows Vista Service Pack 1, Windows 7 y Windows Server 2008, y se trata de una arquitectura que 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, POP3 e IMAP**: limita el redireccionamiento del tráfico al servidor Proxy interno únicamente para los puertos correspondientes.
- **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 correspondientes, así como de toda la comunicación de las aplicaciones marcadas como navegadores y clientes de correo electrónico en el servidor Proxy interno.

4.2.3.1 Clientes de correo electrónico y web

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

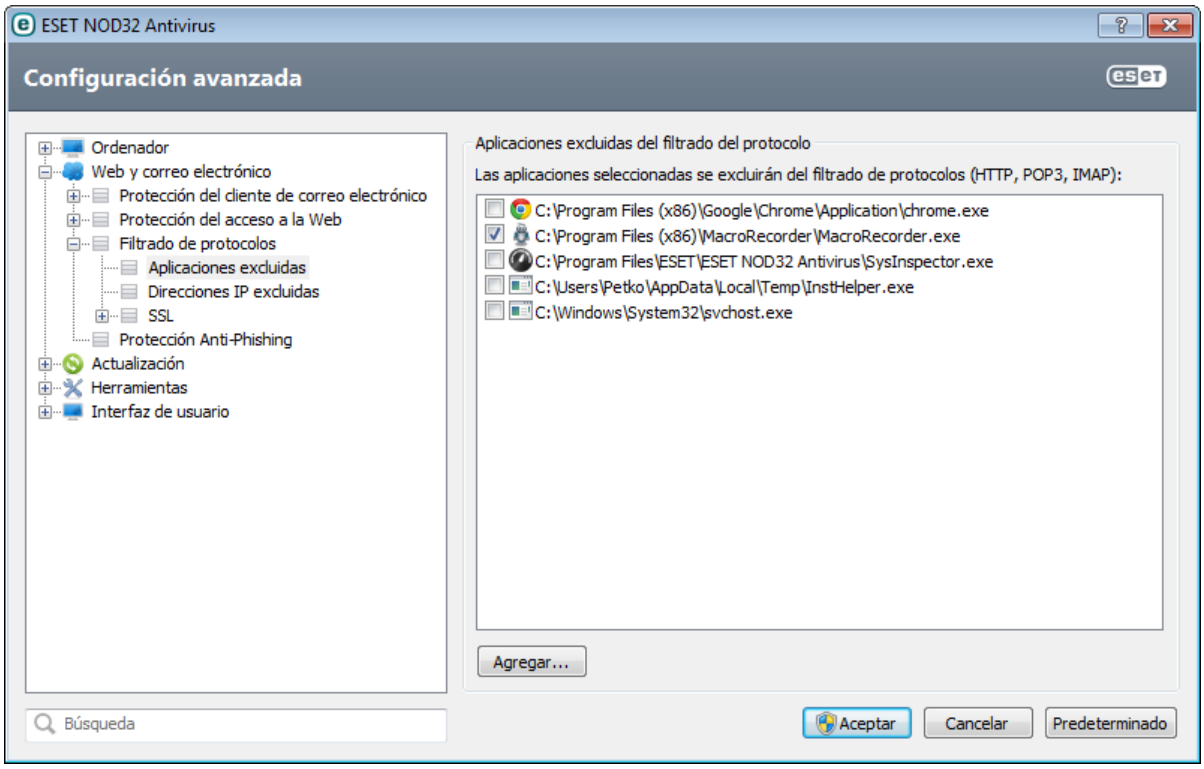
Dada la ingente cantidad de código malicioso que circula en Internet, la navegación segura es un aspecto crucial para la protección de los ordenadores. Las vulnerabilidades de los navegadores web y los vínculos fraudulentos sirven de ayuda a este tipo de código para introducirse en el sistema de incógnito; por este motivo, ESET NOD32 Antivirus se centra en la seguridad de los navegadores web. Cada aplicación que acceda a la red se puede marcar como un navegador de Internet. La casilla de verificación tiene dos estados:

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

4.2.3.2 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 **Agregar...** para seleccionar manualmente una aplicación que no se muestre en la lista del filtrado de protocolos.

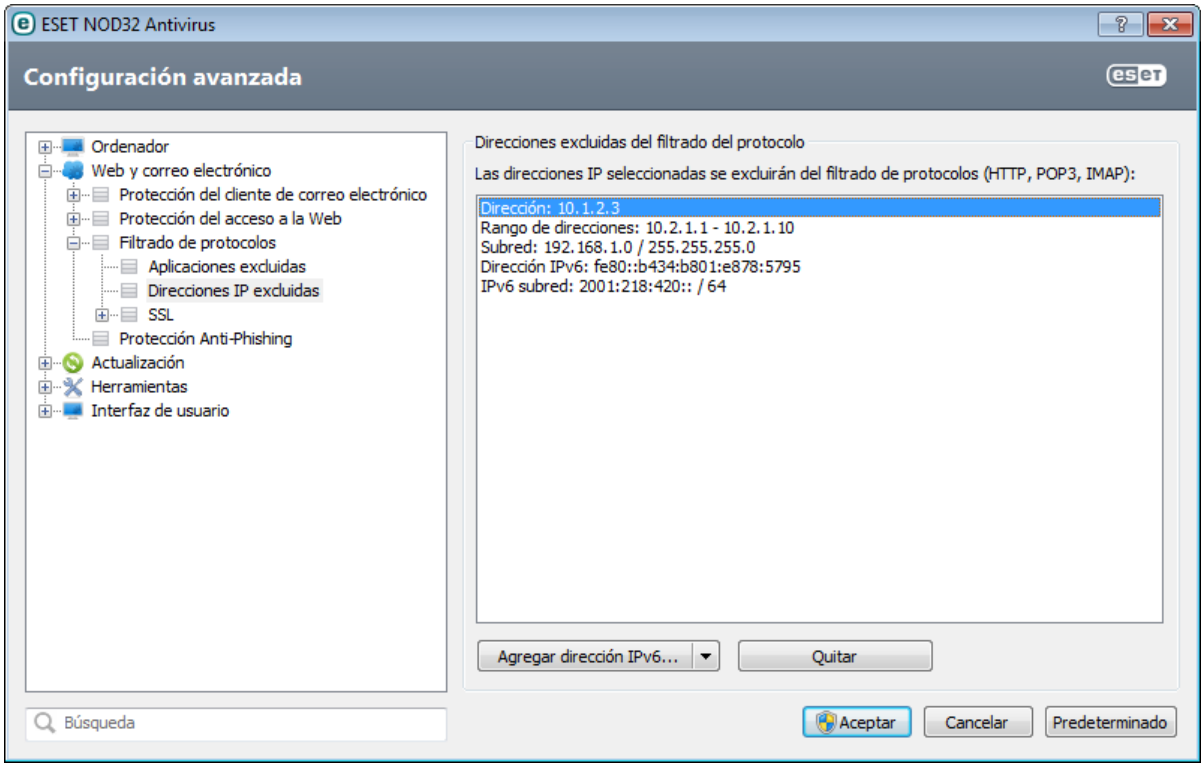


4.2.3.3 Direcciones IP excluidas

Las entradas de la lista se excluirán 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 que se sabe que son de confianza.

Agregar dirección IPv4/IPv6: haga clic para agregar una dirección IP, un intervalo de direcciones o una subred de un punto remoto al que aplicar una regla.

Quitar: elimina las entradas seleccionadas de la lista.



4.2.3.3.1 Agregar dirección IPv4

Esta opción le permite agregar una dirección IP, un intervalo de direcciones o una subred de un punto remoto al que se aplica la regla. El protocolo de Internet versión 4 es el más antiguo, pero sigue siendo el más utilizado.

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*).

4.2.3.3.2 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*).

4.2.3.4 Comprobación del protocolo SSL

ESET NOD32 Antivirus 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.

4.2.3.4.1 Certificados

Para que la comunicación SSL funcione correctamente en los navegadores y clientes de correo electrónico, es fundamental que el certificado raíz de ESET se agregue a la lista de certificados raíz conocidos (editores). **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 y Firefox) de forma automática. En los navegadores que utilicen el almacén de certificados del sistema, el certificado se agregará automáticamente (por ejemplo, en Internet Explorer). Para aplicar el certificado en navegadores no admitidos, haga clic en **Ver certificado** > **Detalles** > **Copiar en archivo** y, a continuación, impórtelo manualmente en el navegador.

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 se ha seleccionado **Preguntar sobre la validez del certificado** (predeterminada), se le pedirá al usuario que seleccione la acción que desea realizar cuando se establezca la comunicación cifrada. 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 lista, la ventana se mostrará en verde.

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.

4.2.3.4.1.1 Certificados de confianza

Además del archivo de autoridades certificadoras de confianza integrado, donde ESET NOD32 Antivirus 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 NOD32 Antivirus 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 **Quitar**. Haga clic en **Mostrar** (o haga doble clic en el certificado) para ver información sobre el certificado seleccionado.

4.2.3.4.1.2 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 **Quitar**. Haga clic en **Mostrar** (o haga doble clic en el certificado) para ver información sobre el certificado seleccionado.

4.2.3.4.1.3 Conexión SSL crifrada

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. No se mostrará la ventana de alerta en el siguiente intento de utilizar el certificado durante la sesión actual.

Sí, siempre: marca el certificado como de confianza y lo agrega a la lista de certificados de confianza. No se mostrará 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.

4.2.4 Protección Anti-Phishing

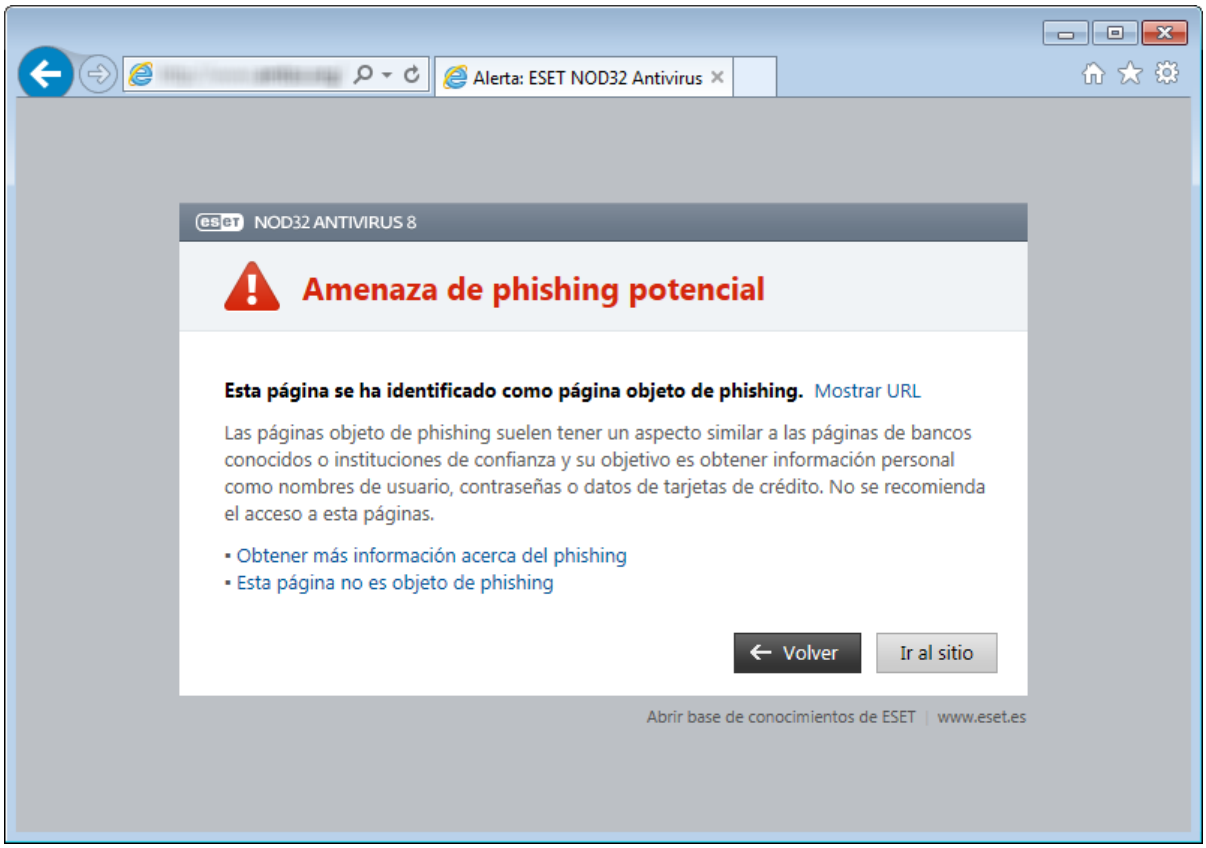
El término phishing, o suplantación de la identidad, define una actividad delictiva que usa técnicas de ingeniería social (manipulación de los usuarios para obtener información confidencial). Su objetivo con frecuencia es acceder a datos confidenciales como, por ejemplo, números de cuentas bancarias, códigos PIN, etc. Puede obtener más información sobre esta actividad en el glosario. ESET NOD32 Antivirus proporciona protección frente al phishing al bloquear páginas web conocidas por distribuir este tipo de contenido.

Recomendamos encarecidamente que active la protección Anti-Phishing en ESET NOD32 Antivirus. Para ello vaya a **Configuración avanzada** (F5) en **Web y correo electrónico** > **Protección Anti-Phishing**.

Consulte también nuestro artículo de la base de conocimientos para ver una versión actualizada y más detallada de esta página de ayuda.

Acceso a un sitio web de phishing

Cuando entre en un sitio web de phishing verá el siguiente cuadro de diálogo en su navegador web. Al hacer clic en **Ir al sitio** (no recomendado), podrá tener acceso al sitio web sin ver un mensaje de advertencia.



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

Cómo informar de sitios de phishing

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

NOTA: antes de enviar un sitio web a ESET, asegúrese de que cumple uno o más de los siguientes criterios:
- El sitio web no se detecta en absoluto.
- El sitio web se detecta como una amenaza, pero no lo es. En este caso, consulte el enlace Eliminar sitio que suplanta la identidad.

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

4.3 Actualización del programa

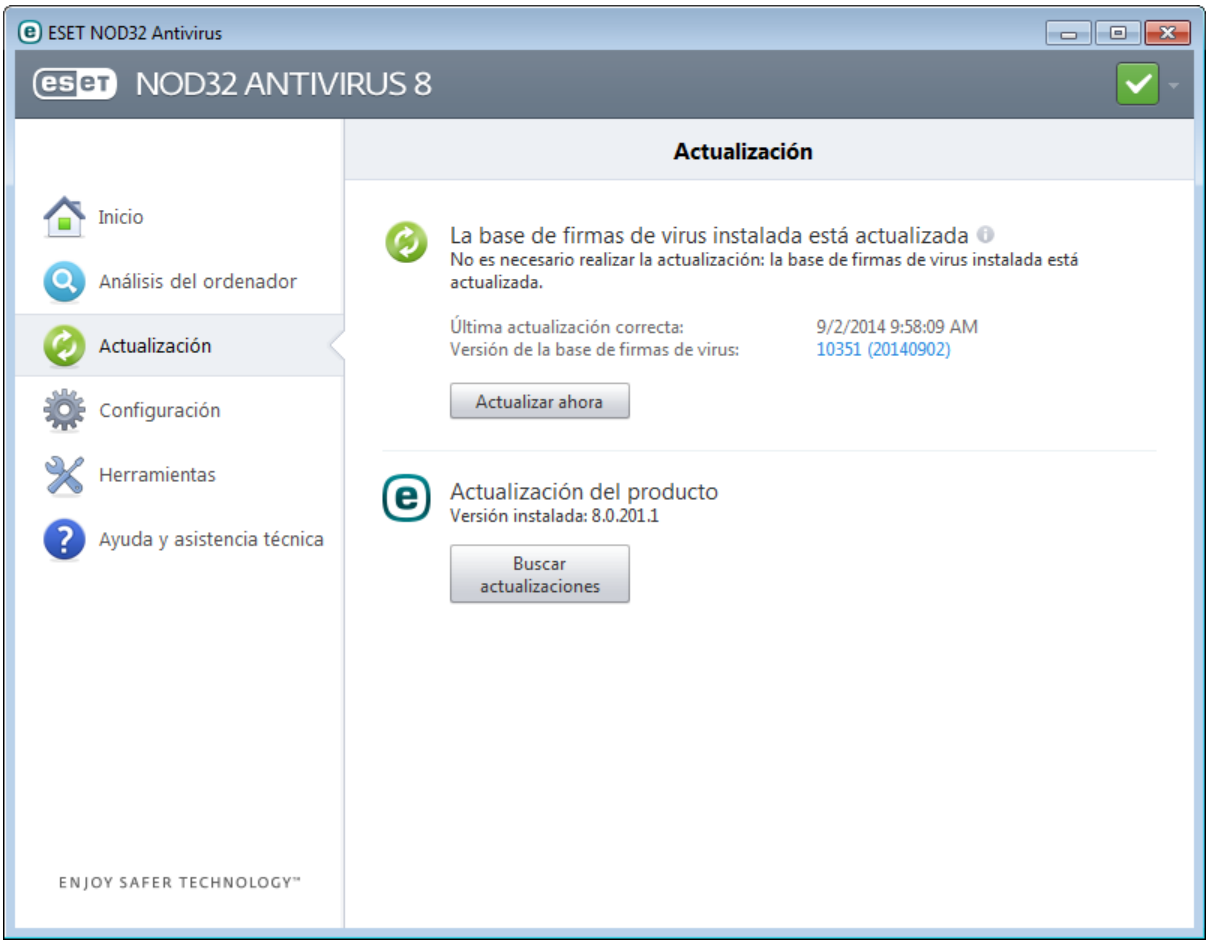
La mejor manera de disfrutar del máximo nivel de seguridad en el ordenador es actualizar ESET NOD32 Antivirus de forma periódica. El módulo Actualización garantiza que el programa está siempre actualizado de dos maneras: actualizando la base de firmas de virus y los componentes del sistema.

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.

Además de las actualizaciones automáticas, puede hacer clic en **Actualizar ahora** para activar una actualización manualmente. 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 NOD32 Antivirus.



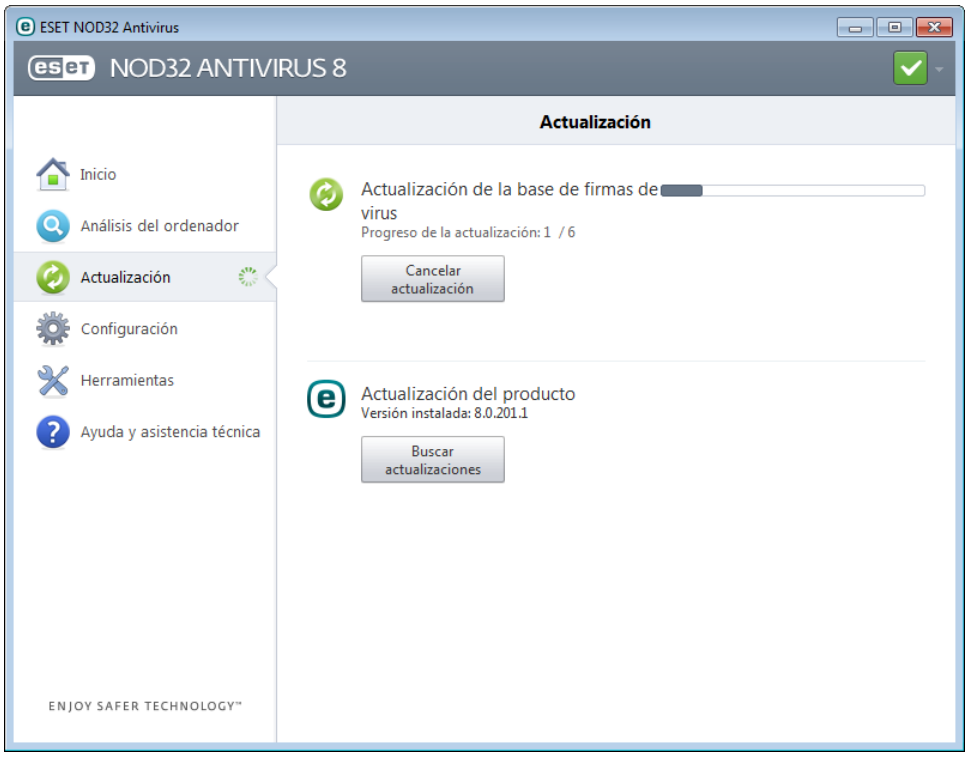
Última actualización correcta: fecha de la última actualización. Si no ve una fecha reciente, es posible que su base de firmas de virus no esté actualizada.

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

Haga clic en **Buscar actualizaciones** para detectar la versión disponible más reciente de ESET NOD32 Antivirus.

Proceso de actualización

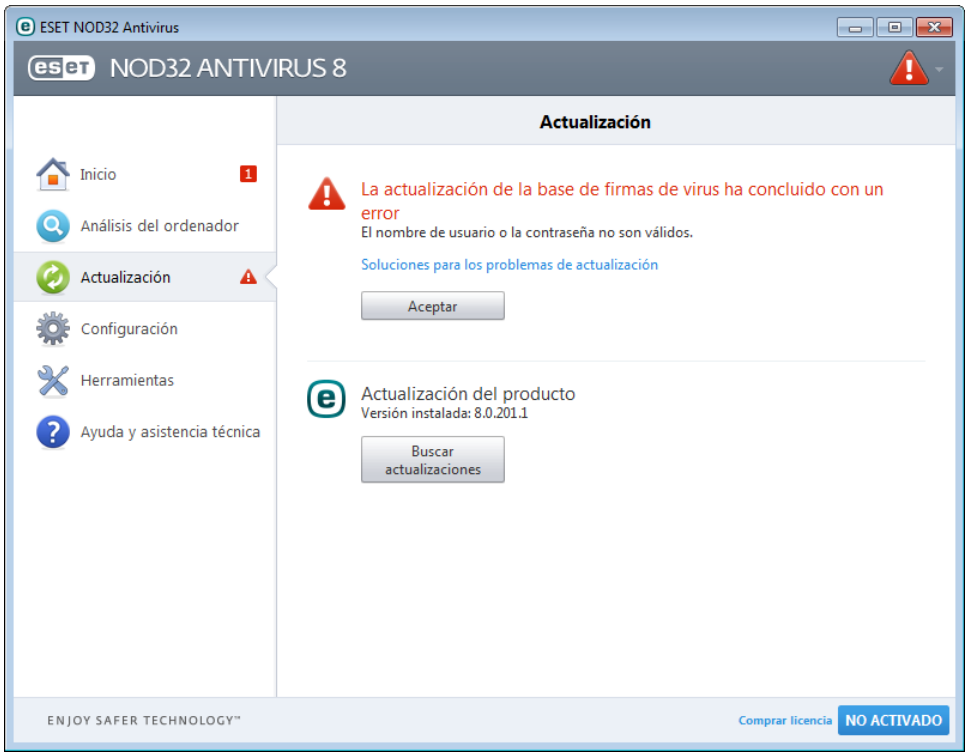
El proceso de descarga se inicia al hacer clic en **Actualizar ahora**. Se muestran una barra de progreso de la descarga y el tiempo que falta para que finalice la descarga. Para interrumpir la actualización, haga clic en **Cancelar actualización**.



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 notificación anterior está relacionada con los dos mensajes siguientes **La actualización de la base de firmas de virus ha concluido con un error** sobre actualizaciones incorrectas:

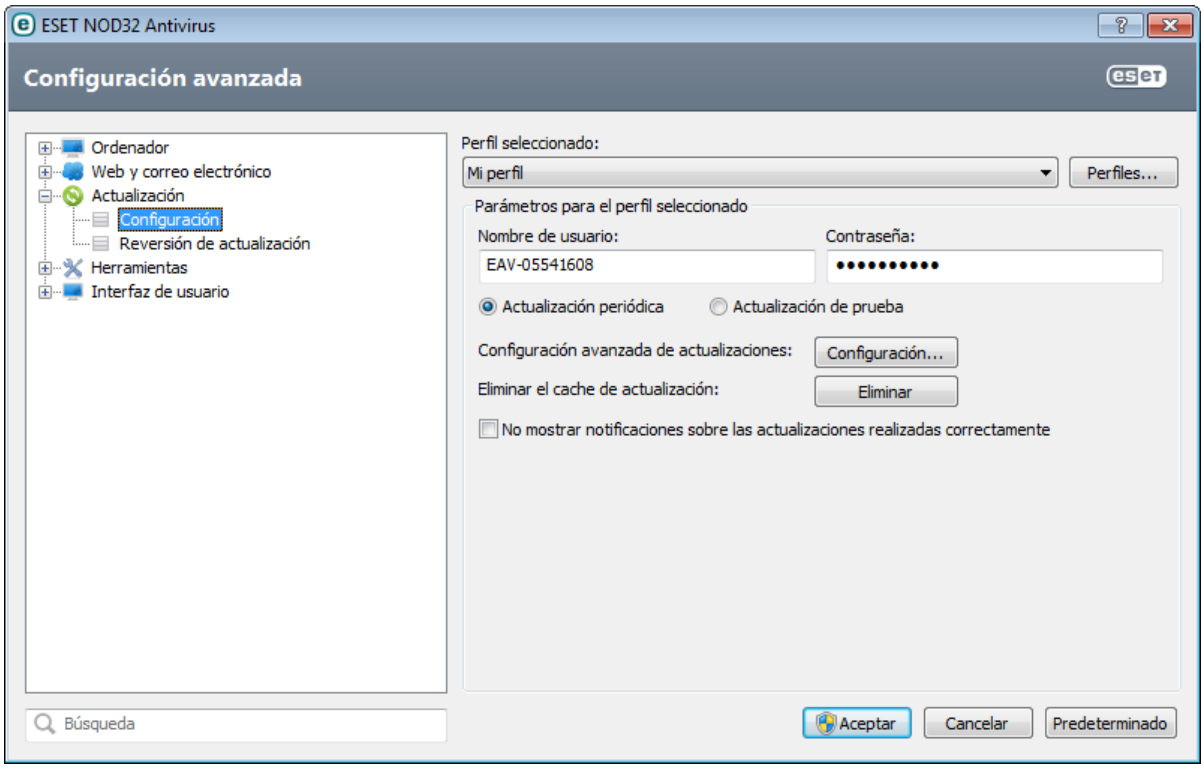
1. **El nombre de usuario o la contraseña no son válidos**: el nombre de usuario y la contraseña se han escrito incorrectamente en la configuración de actualización. Recomendamos que compruebe sus datos de autenticación. La ventana Configuración avanzada (haga clic en **Configuración** en el menú principal y, a continuación, en **Entrar a la configuración avanzada**, o pulse F5 en el teclado) ofrece opciones de actualización adicionales. Haga clic en **Actualizar** > **Configuración** en el árbol de configuración avanzada para escribir un nombre de usuario y una contraseña nuevos.
2. **No se ha encontrado el servidor**: este error podría deberse a una configuración de la conexión a Internet incorrecta. 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.



4.3.1 Configuración de actualización

Las opciones de configuración de actualización están disponibles en el árbol de **Configuración avanzada** (tecla F5) haciendo clic en **Actualizar** > **Configuración**. En esta sección se especifica la información del origen de la actualización, como los servidores de actualización y sus datos de autenticación. En la versión doméstica de los productos de ESET no puede elegir su propio servidor de actualización. Los archivos de actualización se descargarán automáticamente del servidor ESET con el menor tráfico de red. El menú desplegable **Servidor de actualización** solo está disponible en ESET Endpoint Antivirus o ESET Endpoint Security.

Para que las actualizaciones se descarguen correctamente, es esencial cumplimentar correctamente toda la información. Si utiliza un cortafuegos, asegúrese de que el programa goza de permiso para comunicarse con Internet (la comunicación HTTP está activada).



El perfil de actualización actual se muestra en el menú desplegable **Perfil seleccionado**. Haga clic en **Perfiles** para

crear un perfil nuevo.

La autenticación de los servidores de actualización se basa en el **nombre de usuario** y la **contraseña** generados y enviados tras la compra. De forma predeterminada, no se requiere ningún tipo de verificación y los campos **Nombre de usuario** y **Contraseña** se dejan en blanco.

Las actualizaciones de prueba (opción **Actualización de prueba**) son actualizaciones que han superado rigurosas pruebas internas y estarán pronto disponibles. Puede beneficiarse de activar las actualizaciones de prueba mediante el acceso a los métodos y soluciones de detección más recientes. No obstante, la actualización de prueba no siempre es estable, por lo que NO debe utilizarse en servidores de producción y estaciones de trabajo que requieran un elevado nivel de disponibilidad y estabilidad. La lista de módulos actuales está disponible en **Ayuda y asistencia técnica** > **Acerca de ESET NOD32 Antivirus**. Se recomienda que los usuarios básicos dejen la opción **Actualización periódica** seleccionada de forma predeterminada.

Haga clic en **Configuración...** 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 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 juego desactiva todas las notificaciones.

4.3.1.1 Perfiles de actualización

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

El menú desplegable **Perfil seleccionado** muestra el perfil seleccionado actualmente y está definido como **Mi perfil** de forma predeterminada. Para crear un perfil nuevo, haga clic en **Perfiles...** y, a continuación, en **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.

4.3.1.2 Configuración avanzada de actualizaciones

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

4.3.1.2.1 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 (PCU) incluyen nuevas características, o realizan cambios en las características de versiones anteriores. Las PCU se pueden realizar de manera automática, sin la intervención del usuario, o configurar de modo que este reciba una notificación cada vez que se realice una PCU. 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 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.

La opción **Buscar periódicamente la última versión del producto** activa la tarea programada **Búsqueda periódica de la última versión del producto** (consulte Planificador de tareas).

4.3.1.2.2 Servidor Proxy

Para acceder a las opciones de configuración del servidor Proxy de un perfil de actualización dado, haga clic en **Actualizar** en el árbol de configuración avanzada (F5) y, a continuación, en **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 **No usar servidor Proxy** para especificar que no se utilice ningún servidor Proxy para actualizar ESET NOD32 Antivirus.

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

- Para actualizar ESET NOD32 Antivirus, 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 NOD32 Antivirus 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 NOD32 Antivirus, que únicamente debe proporcionar si sabe que es necesaria una contraseña para acceder a Internet a través de un servidor Proxy.

4.3.1.2.3 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.

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 opción 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.

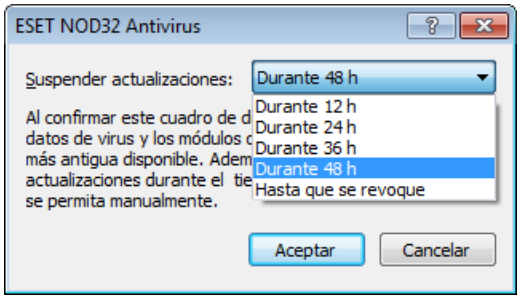
Seleccione **Desconectar del servidor después de actualizar** si la conexión al servidor permanece activa incluso después de haber descargado las actualizaciones.

4.3.2 Reversión de actualización

Si sospecha que una nueva actualización de la base de datos de virus o de los módulos del programa puede ser inestable o estar dañada, puede revertir a la versión anterior y desactivar las actualizaciones durante un período de tiempo definido. También puede activar actualizaciones desactivadas con anterioridad si las había pospuesto indefinidamente.

ESET NOD32 Antivirus registra instantáneas de la base de firmas de virus y los módulos del programa para usarlas con la función de *reversión*. Para crear instantáneas de bases de datos de virus, deje seleccionada la casilla de verificación **Crear instantáneas de archivos de actualización**. El campo **Número de instantáneas almacenadas localmente** define el número de instantáneas de la base de virus anteriores que se guardan.

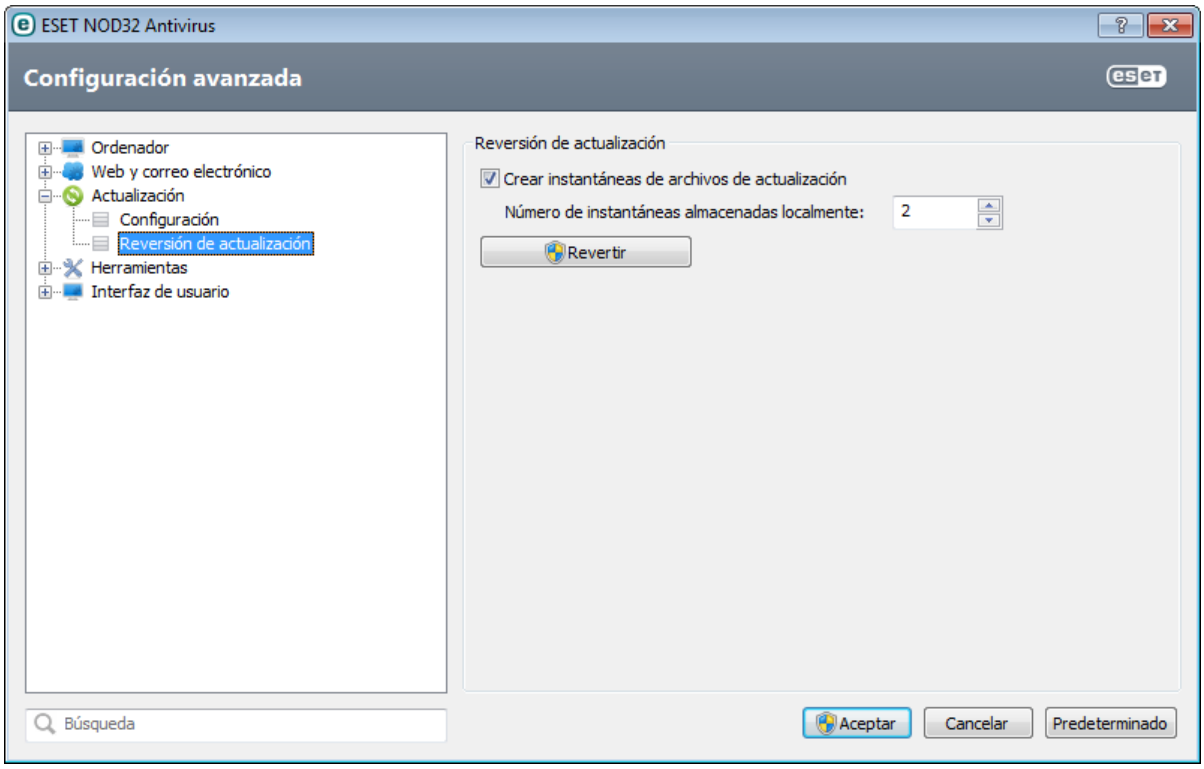
Si hace clic en **Revertir** (**Configuración avanzada** (F5) > **Actualizar** > **Reversión de actualización**), deberá seleccionar un intervalo de tiempo en el menú desplegable **Suspender actualizaciones** que representa el periodo de tiempo en el que estarán interrumpidas las actualizaciones de la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



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

Si se lleva a cabo una reversión, el botón **Revertir** cambia a **Permitir actualizaciones**. No se permitirán

actualizaciones para el intervalo de tiempo seleccionado en el menú desplegable **Suspender actualizaciones**. 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 y había disponible una actualización más reciente antes de que se descargara 6869. Si se ha definido 2 en el campo **Número de instantáneas almacenadas localmente** y hace clic en **Revertir**, la base de firmas de virus (incluidos los módulos del programa) se restaurará a la versión número 6868. Este proceso puede tardar un tiempo. Compruebe si la versión de base de datos de firmas de virus se ha degradado en la ventana principal del programa de ESET NOD32 Antivirus en la sección Actualizar.

4.3.3 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 NOD32 Antivirus:

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

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

4.4 Herramientas

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

Este menú incluye las herramientas siguientes:

- Archivos de registro
- Estadísticas de protección
- Observar actividad
- Procesos en ejecución (si ESET Live Grid se ha activado en ESET NOD32 Antivirus)
- Planificador de tareas
- Cuarentena
- ESET SysInspector

Enviar archivo para analizar: le permite enviar un archivo sospechoso para que lo analicen en el laboratorio 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.

Nota: puede que ESET SysRescue no esté disponible para Windows 8 en versiones más antiguas de productos de ESET. En tal caso, se recomienda que actualice su producto o que cree un disco de ESET SysRescue en otra versión de Microsoft Windows.

ESET Social Media Scanner: enlace a una aplicación de redes sociales (como Facebook) para proteger a los usuarios frente a posibles amenazas. Esta aplicación es independiente de otros productos de ESET y es totalmente gratuita.

4.4.1 Archivos de registro

Los archivos de registro contienen información relacionada con todos los sucesos importantes del programa y proporcionan información general acerca de las amenazas detectadas. 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 NOD32 Antivirus, donde también se pueden archivar registros.

Se puede acceder a los archivos de registro desde la 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 ESET NOD32 Antivirus. La información incluye el momento de la detección, el nombre de la amenaza, la ubicación, la acción ejecutada y el nombre del usuario registrado en el momento en que se detectó la amenaza. Haga doble clic en la entrada del registro para ver los detalles en una ventana independiente.
- **Sucesos**: todas las acciones importantes realizadas por ESET NOD32 Antivirus 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 de HIPS que se marcaron para su registro. El protocolo muestra la aplicación que activó la operación, el resultado (si la regla se admitió o no) y el nombre de la regla creada.
- **Sitios web filtrados**: esta lista es útil si desea ver una lista de sitios web que la Protección del tráfico de Internet ha bloqueado. En estos registros puede ver la hora, la dirección URL, el usuario y la aplicación que creó una conexión con el sitio web en cuestión.
- **Control de dispositivos**: contiene registros de los dispositivos o medios extraíbles conectados al ordenador. Solo los dispositivos con reglas de control de dispositivos correspondientes se registrarán 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 una entrada determinada 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**: si está activada, se abre la ventana **Filtrado de registros**, donde puede definir los criterios de filtrado.
- **Borrar 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**.

4.4.1.1 Mantenimiento de registros

La configuración de registros de ESET NOD32 Antivirus está disponible en la ventana principal del programa. Haga clic en **Configuración** > **Entrar a la configuración avanzada** > **Herramientas** > **Archivos de registro**. La sección 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:

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, etc.).

Las entradas de registro anteriores al número de días especificado en el campo **Eliminar automáticamente los registros con una antigüedad de más de X días** 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 empezar 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 del proceso de registro. Esta mejora es especialmente notable cuando los registros contienen muchas entradas.

4.4.2 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 NOD32 Antivirus haciendo clic en **Herramientas** > **Planificador de tareas**. El **Planificador de tareas** contiene una lista de todas las tareas programadas y sus propiedades de configuración, como la fecha, la hora y el perfil de análisis predefinidos utilizados.

El Planificador de tareas sirve para programar las siguientes tareas: actualización 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:

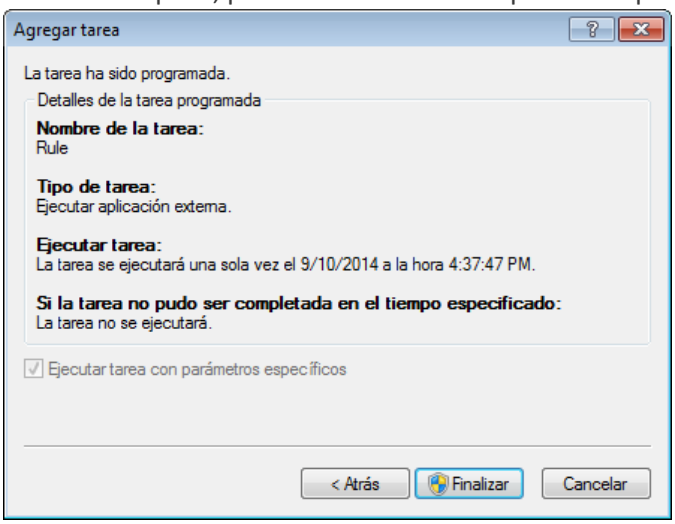
- **Mantenimiento de registros**
- **Actualización automática de rutina**
- **Actualización automática al detectar la conexión por módem**
- **Actualización automática después del registro del usuario**
- **Búsqueda periódica de la última versión del producto** (consulte Tipo de actualización)
- **Verificación automática de archivos en el inicio** (tras inicio de sesión del usuario)
- **Comprobación de la ejecución de archivos en el inicio** (después de actualizar correctamente la base de firmas de virus)
- **Primer análisis automático**

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 **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.



4.4.3 Estadísticas de protección

Para ver un gráfico de datos estadísticos relacionados con los módulos de protección de ESET NOD32 Antivirus, haga clic en **Herramientas** > **Estadísticas de protección**. Seleccione el módulo de protección deseado en el menú desplegable **Estadísticas** para ver el gráfico y la leyenda correspondientes. Si pasa el ratón por encima de un elemento de la leyenda, solo aparecerán en el gráfico los datos de ese elemento.

Están disponibles los siguientes gráficos de estadísticas:

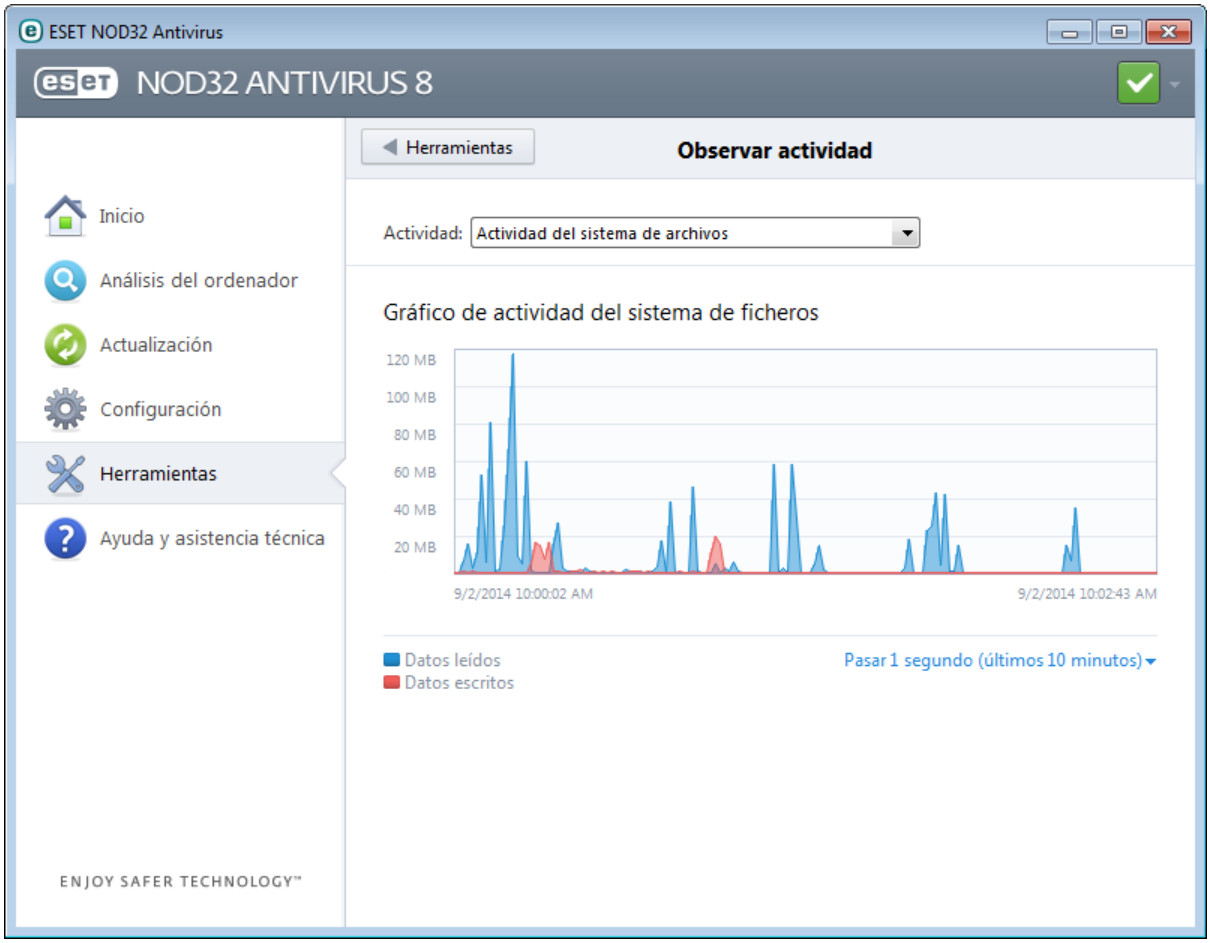
- **Protección antivirus y antiespía**: muestra el número de objetos infectados y no infectados
- **Protección del sistema de archivos**: solo muestra objetos que se leyeron o escribieron en el sistema de archivos.
- **La protección del cliente de correo electrónico**: solo muestra objetos que fueron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

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.

4.4.4 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 **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.

4.4.5 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.

4.4.6 ESET Live Grid

ESET Live Grid (que se basa en el sistema avanzado de alerta temprana ThreatSense.Net) utiliza los datos enviados por usuarios de ESET de todo el mundo y los envía al laboratorio de virus de ESET. ESET Live Grid proporciona metadatos y muestras sospechosas en estado salvaje, lo cual nos permite reaccionar de forma inmediata a las necesidades de nuestros clientes y hace posible la respuesta de ESET a las amenazas más recientes. Puede obtener más información sobre ESET Live Grid en el glosario.

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, pero puede que ESET NOD32 Antivirus responda más rápido a las nuevas amenazas que solo con la actualización de la base de firmas de virus.
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 NOD32 Antivirus está configurado para enviar archivos sospechosos al laboratorio de virus de ESET para su análisis detallado. 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 (recomendado): 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 recopilada por ESET Live Grid acerca de su ordenador. 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 NOD32 Antivirus, la versión del sistema operativo del ordenador y la configuración regional. Normalmente, las estadísticas se envían a los servidores 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 opciones adicionales 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.

4.4.6.1 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.

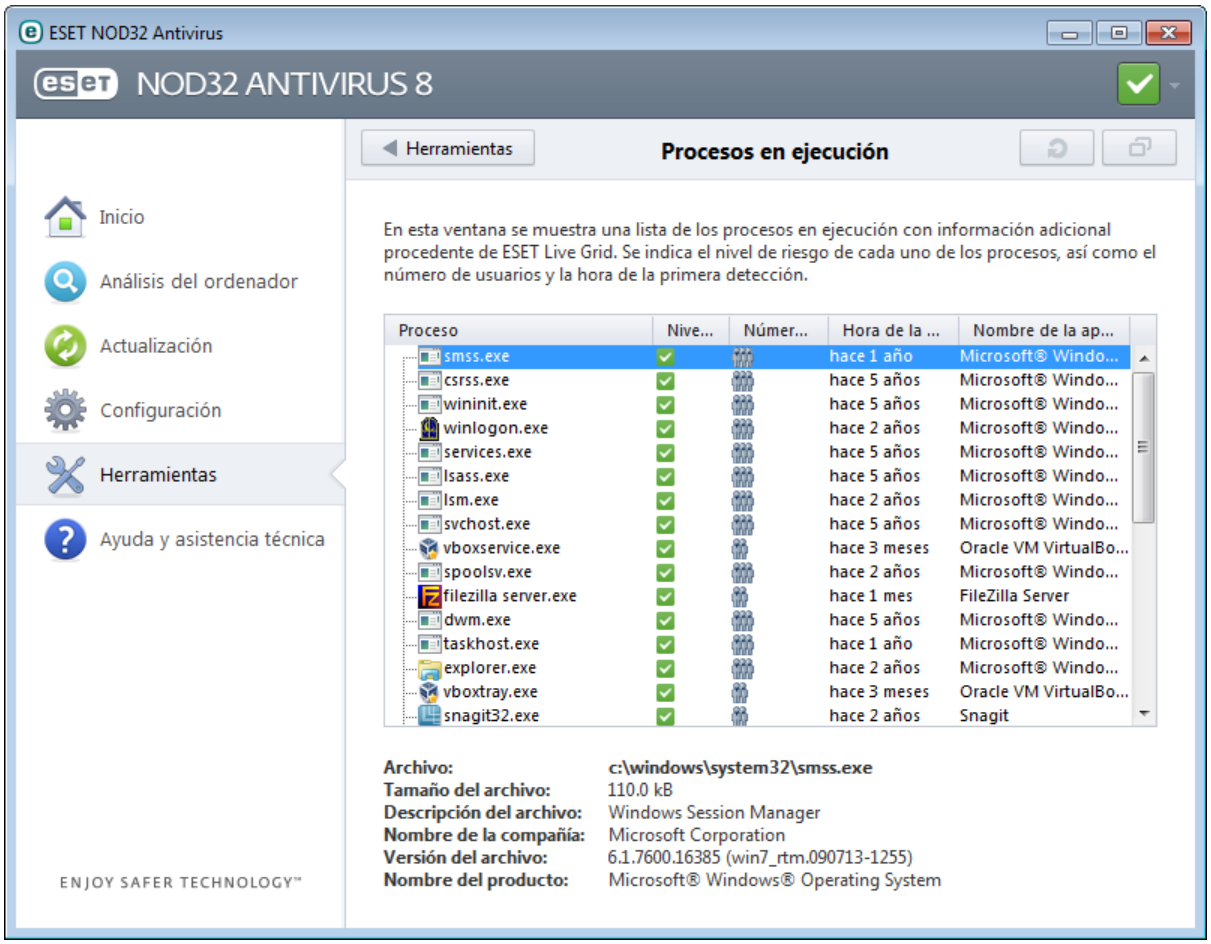
Filtro de exclusión: esta opción le permite excluir del envío determinados archivos o carpetas. Los archivos mostrados en la lista nunca se enviarán al laboratorio de ESET para su análisis, aunque contengan código sospechoso. Esta opción puede ser útil, por ejemplo, para excluir archivos que puedan contener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

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

4.4.7 Procesos en ejecución

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 NOD32 Antivirus 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 NOD32 Antivirus 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 la 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.

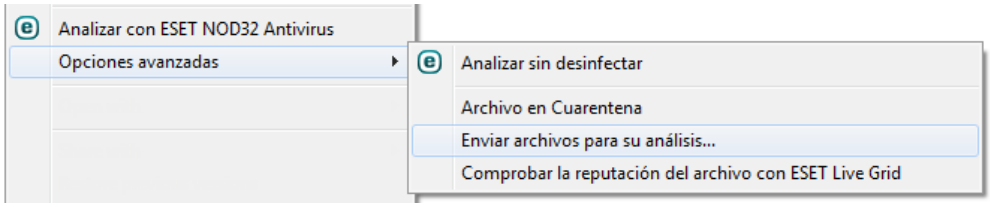
Nombre de aplicación: nombre de un programa o un proceso.

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 B (bytes).
- **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.

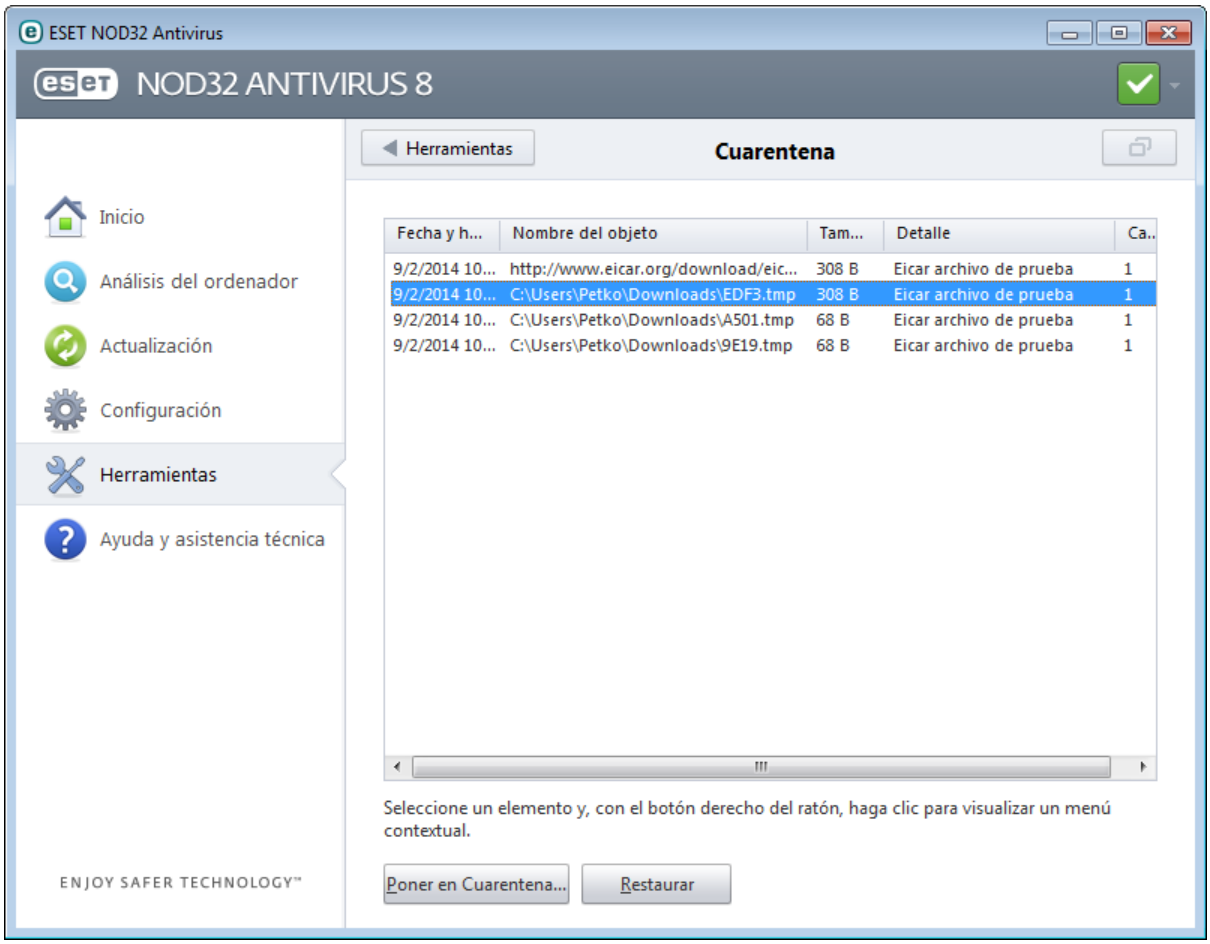
NOTA: la reputación también se puede comprobar en los archivos que no actúan como programas o procesos en ejecución. Seleccione los archivos que desea comprobar, haga clic con el botón derecho del ratón en ellos y seleccione **Opciones avanzadas** > **Comprobar la reputación del archivo con ESET Live Grid**.



4.4.8 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 NOD32 Antivirus los detecta incorrectamente como infectados.

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



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

Puesta de archivos en cuarentena

ESET NOD32 Antivirus 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 **Poner en 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. Para realizar esta tarea, utilice la opción **Restaurar**, disponible en el menú contextual que se abre al hacer clic con el botón derecho del ratón en un archivo en la ventana de cuarentena. Si 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, exclúyalo del análisis después de restaurarlo y enviarlo al servicio de atención al cliente de ESET.

Envío de un archivo de cuarentena

Si ha copiado en cuarentena un archivo sospechoso que el programa no ha detectado o si se ha 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.

4.4.9 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 NOD32 Antivirus, el servidor Proxy se puede configurar en dos secciones diferentes del árbol de configuración avanzada.

En primer lugar, se puede configurar en **Configuración avanzada**, bajo **Herramientas** > **Servidor Proxy**. Al especificar el servidor Proxy en este nivel, se define la configuración global del servidor Proxy para ESET NOD32 Antivirus. 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**.

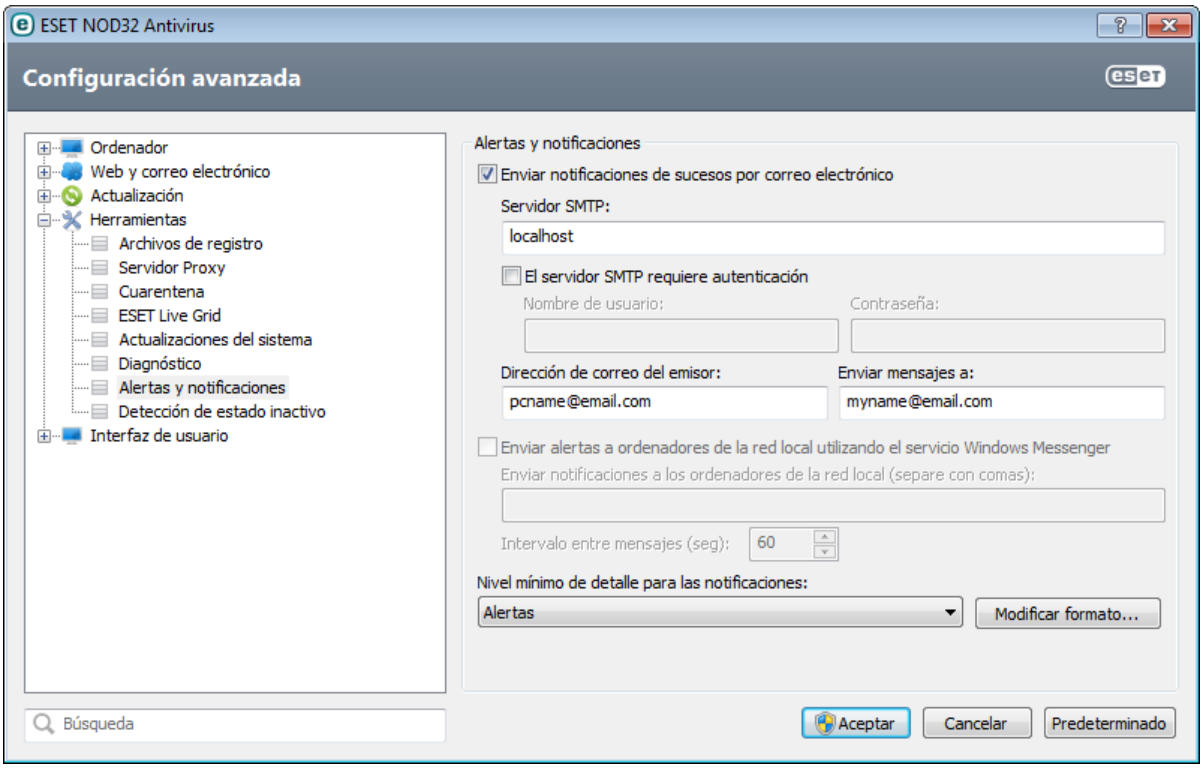
Si la comunicación con el servidor Proxy requiere autenticación, seleccione la casilla de verificación **El servidor Proxy requiere autenticación** e introduzca un **nombre de usuario** y una **contraseña** válidos en los campos correspondientes. Haga clic en **Detectar servidor Proxy** para detectar 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.

4.4.10 Alertas y notificaciones

ESET NOD32 Antivirus 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 NOD32 Antivirus.

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 Messenger: 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....

4.4.10.1 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 ordenador en el que se produjo la alerta.
- **%ProgramName%**: programa que generó la alerta.
- **%InfectedObject%**: nombre del archivo, mensaje, etc., infectado.
- **%VirusName%**: identificación de la infección.
- **%ErrorDescription%**: descripción de un suceso que no está relacionado con un virus.

Las palabras clave **%InfectedObject%** y **%VirusName%** solo se utilizan 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 (por ejemplo, "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 (áéíóú).

4.4.11 Envío de muestras para el análisis

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

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

NOTA: antes de enviar 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**
- **Sitio sospechoso** (sitio web que está infectado por código malicioso)
- **Archivo de falso positivo** (archivo que se detecta como amenaza pero no está infectado)
- **Sitio de falso positivo**
- **Otros**

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

Correo electrónico de contacto: la dirección de correo de contacto se envía a ESET junto con los archivos sospechosos y se puede utilizar para el contacto con usted en caso de que sea necesario enviar más información para poder realizar el análisis. No es obligatorio introducir una dirección de correo electrónico de contacto. No obtendrá

ninguna respuesta de ESET a menos que sea necesario enviar información adicional, ya que cada día nuestros servidores reciben decenas de miles de archivos, lo que hace imposible responder a todos los envíos.

4.4.12 Actualizaciones del sistema

La característica Windows Update es un componente importante de protección de los usuarios de software malicioso, por eso es fundamental que instale las actualizaciones de Microsoft Windows en cuanto se publiquen. ESET NOD32 Antivirus le informa sobre las actualizaciones que le faltan, según el nivel que haya especificado. Están disponibles los siguientes niveles:

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

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

4.5 Interfaz de usuario

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

La herramienta 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 un objeto. Utilice esta herramienta para integrar elementos de control de ESET NOD32 Antivirus en el menú contextual.

4.5.1 Gráficos

Las opciones de configuración de la interfaz de usuario de ESET NOD32 Antivirus le permiten ajustar el entorno de trabajo según sus necesidades. Estas opciones de configuración se encuentran en el árbol de configuración avanzada al expandir **Interfaz de usuario** y hacer clic en **Gráficos**.

En la sección **Elementos de la interfaz del 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 NOD32 Antivirus, anule la selección de **Mostrar pantalla inicial con la carga del sistema**.

Active **Resaltar elemento al seleccionar** para que el sistema resalte 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 activar el uso de iconos animados que muestran el progreso de varias operaciones, seleccione **Usar iconos animados para mostrar el progreso**.

Si desea que ESET NOD32 Antivirus reproduzca un sonido cuando se produzcan sucesos importantes durante un análisis, por ejemplo al detectar una amenaza o al finalizar el análisis, seleccione **Usar efectos de sonido**.

4.5.2 Alertas y notificaciones

La sección de **Alertas y notificaciones** de **Interfaz de usuario** le permite configurar cómo gestiona ESET NOD32 Antivirus las notificaciones del sistema (por ejemplo, mensajes de actualización correcta) y las alertas de amenaza. También puede definir si se muestra la hora y 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).

Anule la selección de la casilla de verificación situada junto a **Mostrar alertas** para cancelar todas las ventanas de alerta. Esto solo es adecuado en ciertas situaciones. Para la mayoría de los usuarios, se recomienda mantener esta opción activada (predeterminada).

Las notificaciones del escritorio son meramente informativas y 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 **Mostrar alertas como notificaciones en el escritorio**. Haga clic en el botón **Configurar notificaciones** para acceder a opciones avanzadas como 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 **Vista previa**. Para suprimir notificaciones durante la ejecución de una aplicación a pantalla completa, seleccione **No mostrar notificaciones durante la ejecución de aplicaciones a pantalla completa**.

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.

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

4.5.2.1 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, 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.

4.5.3 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.

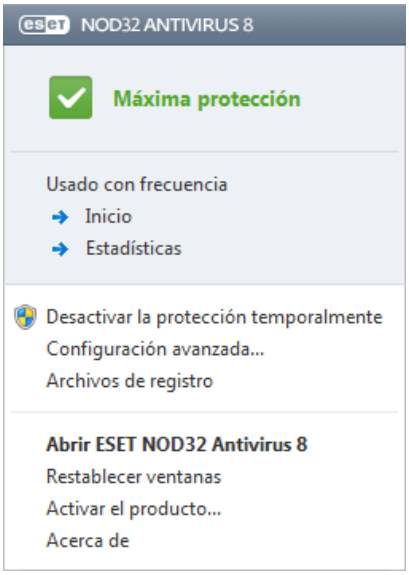
4.5.4 Configuración de acceso

La configuración de ESET NOD32 Antivirus es una parte crucial de la política 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** > **Entrar a la configuración avanzada** > **Interfaz de usuario** > **Configuración de acceso** en el menú principal, seleccione la opción **Protección de la configuración** y haga clic en **Introduzca la contraseña**. Recuerde que la contraseña distingue entre mayúsculas y minúsculas.

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 control de cuentas de usuario (UAC) en Windows Vista y Windows 7). Estas modificaciones incluyen la desactivación de los módulos de protección. En sistemas con Windows XP en los que no se ejecuta el UAC, los usuarios tendrán disponible la opción **Exigir derechos de administrador (sistema sin soporte UAC)**.

4.5.5 Menú del programa

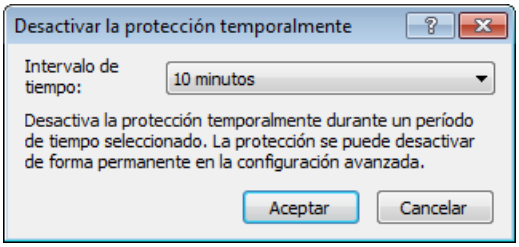
En el menú del programa principal están disponibles algunas de las opciones de configuración y características más importantes.



Usado con frecuencia: muestra las partes de ESET NOD32 Antivirus que se utilizan con mayor frecuencia. Puede acceder a estas secciones rápidamente desde el menú del programa.

Desactivar la protección temporalmente: muestra el cuadro de diálogo de confirmación que desactiva la Protección antivirus y antispyware, 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.



Configuración avanzada: seleccione esta opción para ver el árbol de **Configuración avanzada**. La configuración avanzada también se puede abrir pulsando la tecla F5 o desde **Configuración** > **Entrar a la 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 NOD32 Antivirus.

Activar el producto...: seleccione esta opción si todavía no ha activado su producto de seguridad ESET o para volver a introducir las credenciales de activación del producto después de renovar su licencia.

Acerca de: proporciona información del sistema y detalles acerca de la versión instalada de ESET NOD32 Antivirus, así como de los módulos del programa instalados. Aquí también puede encontrar la fecha de expiración de la licencia e información sobre el sistema operativo y los recursos del sistema.

4.5.6 Menú contextual

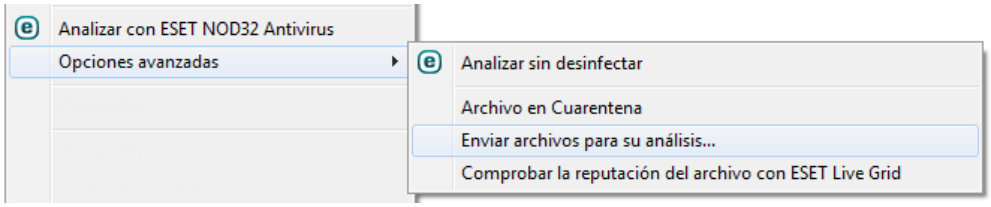
El menú contextual aparece al hacer clic con el botón derecho en un objeto. En el menú se muestra una lista de todas las acciones que se pueden realizar en un objeto.

Es posible integrar elementos de control de ESET NOD32 Antivirus 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 NOD32 Antivirus 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 primero la opción **Analizar sin desinfectar con ESET NOD32 Antivirus** y, después, la opción **Analizar y desinfectar**.
- **Completo (primero desinfectar)**: activa todas las opciones del menú contextual; el menú principal mostrará primero la opción **Analizar con ESET NOD32 Antivirus** y, después, la opción **Analizar sin desinfectar**.



- **Sólo analizar**: solo aparecerá **Analizar sin desinfectar con ESET NOD32 Antivirus** en el menú contextual.
- **Sólo desinfectar**: solo aparecerá **Analizar con ESET NOD32 Antivirus** en el menú contextual.

5. Usuario avanzado

5.1 Administrador de perfiles

El administrador de perfiles se utiliza en dos secciones de ESET NOD32 Antivirus: en **Análisis de estado inactivo** y en **Actualización**.

Análisis del ordenador

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 de estado inactivo** > **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 **Administración de perfiles**, haga clic en **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**. Ajuste los parámetros restantes a sus requisitos y guarde el nuevo perfil.

Actualización

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

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

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

Agregar: cree nuevos perfiles de actualización.

En la parte inferior de la ventana se enumeran los perfiles existentes.

5.2 Accesos directos del teclado

Los accesos directos que se pueden utilizar en ESET NOD32 Antivirus 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 la configuración del Nombre de usuario y 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 su producto 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 los nodos del árbol de configuración avanzada
TABULADOR	mueve el cursor en una ventana
Esc	cierra el cuadro de diálogo activo

5.3 Diagnóstico

El diagnóstico proporciona volcados de memoria de los procesos de ESET (por ejemplo, *ekrn*). Cuando una aplicación se bloquea, se genera un volcado de memoria que puede ayudar a los desarrolladores a depurar y arreglar varios problemas de ESET NOD32 Antivirus. Están disponibles dos tipos de volcados:

- **Volcado de memoria completo**: registra todo el contenido de la memoria del sistema cuando la aplicación se detiene de forma inesperada. Los volcados de memoria completos pueden contener datos de procesos que se estaban ejecutando cuando se generó el volcado.
- **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 **...** para abrir este directorio en una ventana nueva del *Explorador de Windows*.

5.4 Importar y exportar configuración

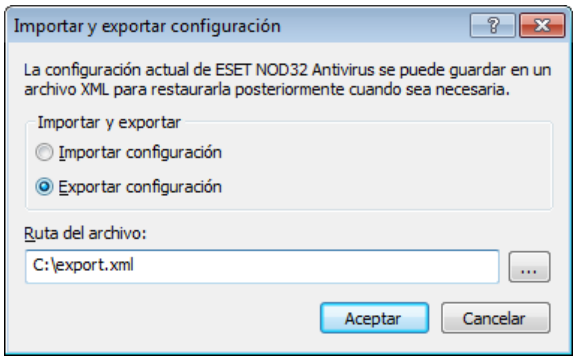
Puede importar o exportar el archivo de configuración .xml de ESET NOD32 Antivirus del menú **Configuración**.

La importación y la exportación de un archivo de configuración son útiles cuando necesita realizar una copia de seguridad de la configuración actual de ESET NOD32 Antivirus para utilizarla en otro momento. La opción de exportación de configuración también es de utilidad para los usuarios que desean utilizar su configuración preferida en varios sistemas, ya que les permite importar fácilmente el archivo *.xml* para transferir estos ajustes.

Importar la configuración es muy fácil. En la ventana principal del programa, haga clic en **Configuración** > **Importar y exportar configuración** y, a continuación, seleccione la opción **Importar configuración**. Introduzca el nombre del archivo de configuración o haga clic en el botón **...** para buscar el archivo de configuración que desea importar.

Los pasos para exportar una configuración son muy similares. En la ventana principal del programa, haga clic en **Configuración** > **Importar y exportar configuración...**. Seleccione **Exportar configuración** e introduzca el nombre del archivo de configuración (por ejemplo, *export.xml*). Utilice el navegador para seleccionar la ubicación del ordenador donde desee guardar el archivo de configuración.

Nota: puede encontrarse con un error al exportar la configuración si no dispone de derechos suficientes para escribir el archivo exportado en el directorio especificado.



5.5 Detección de estado inactivo

La detección de estado inactivo se puede configurar en **Configuración avanzada**, bajo **Herramientas** > **Detección de estado inactivo**. Esta configuración especifica un activador para el Análisis de estado inactivo cuando:

- el salvapantallas se está ejecutando,
- el ordenador está bloqueado,
- un usuario cierra sesión.

Utilice las casillas de verificación de cada estado correspondiente para activar o desactivar los distintos activadores de la detección del estado inactivo.

5.6 ESET SysInspector

5.6.1 Introducción a ESET SysInspector

ESET SysInspector es una aplicación que examina el ordenador a fondo y muestra los datos recopilados de forma exhaustiva. 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). Para obtener más información, consulte la sección ESET SysInspector como parte de ESET NOD32 Antivirus.

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.

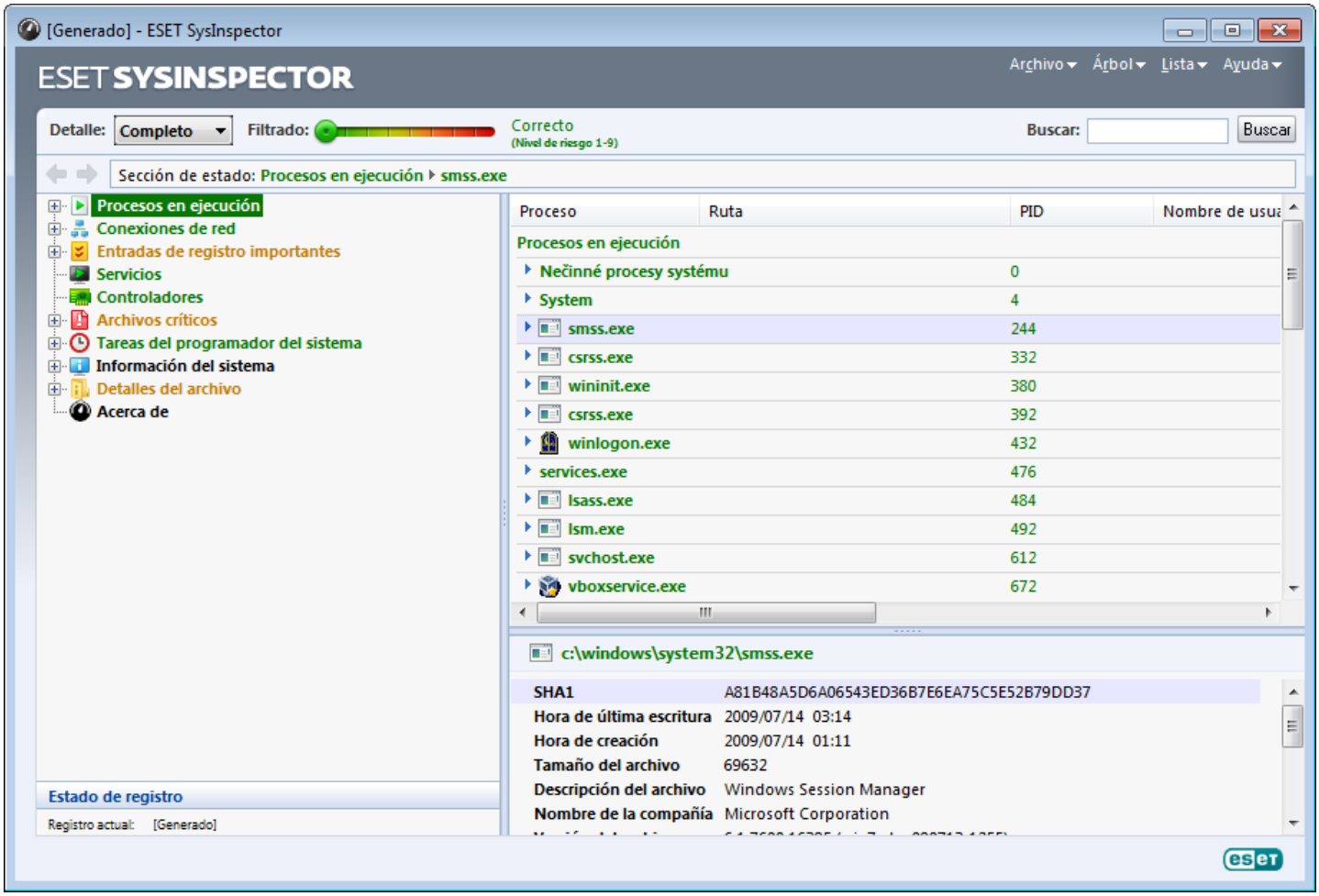
5.6.1.1 Inicio de ESET SysInspector

Para iniciar ESET SysInspector simplemente tiene que ejecutar el archivo *SysInspector.exe* que descargó del sitio web de ESET. Si ya tiene instalada alguna de las soluciones de ESET Security, puede ejecutar ESET SysInspector directamente desde el menú Inicio (haga clic en **Programas** > **ESET** > **ESET NOD32 Antivirus**).

Espere mientras la aplicación examina el sistema. El proceso de inspección puede tardar varios minutos.

5.6.2 Interfaz de usuario y uso de la aplicación

Para un uso sencillo, la ventana principal del programa se divide en cuatro secciones: Controles de programa, en la parte superior de la ventana principal del programa; la ventana de navegación, situada a la izquierda; la ventana Descripción, situada a la derecha; y la ventana Detalles, situada en la parte inferior de la ventana principal. 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.).



5.6.2.1 Controles de programa

Esta sección contiene la descripción de todos los controles de programa disponibles en ESET SysInspector.

Archivo

Al hacer clic en **Archivo**, puede guardar el estado actual del sistema para examinarlo más tarde o abrir un registro guardado anteriormente. Para la publicación, es recomendable que genere un registro **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 del programa.

Árbol

Le permite expandir o cerrar todos los nodos, y exportar las secciones seleccionadas al script de servicio.

Lista

Contiene funciones para una navegación más sencilla por el programa y otras funciones como, por ejemplo, la búsqueda de información en línea.

Ayuda

Contiene información sobre la aplicación y sus funciones.

Detalle

Este ajuste modifica la información mostrada en la ventana principal del programa para que pueda trabajar con ella más fácilmente. 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

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 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.

Comparar

Cuando se comparan dos registros, puede elegir que se visualicen todos los elementos, solo los elementos agregados, solo los elementos eliminados y solo los elementos sustituidos.

Buscar

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

Retorno

Al hacer clic en las flechas hacia atrás o hacia delante, puede volver a la información mostrada previamente en la ventana Descripción. Puede utilizar la tecla Retroceso y la tecla de espacio, en lugar de hacer clic en las flechas atrás y adelante.

Sección de estado

Muestra el nodo actual en la ventana de navegación.

Importante: los elementos destacados en rojo son elementos desconocidos, 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.

5.6.2.2 Navegación por ESET SysInspector

ESET SysInspector divide los tipos de información en distintas secciones básicas denominadas nodos. Si está disponible, puede encontrar información adicional expandiendo 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 constantemente 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.

5.6.2.2.1 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 + 0	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

5.6.2.3 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 herramienta permite realizar un seguimiento de los cambios introducidos en el sistema, una característica muy útil para la detección de código malicioso.

Una vez iniciada, la aplicación crea un registro nuevo, que aparecerá en una ventana nueva. Haga clic en **Archivo** > **Guardar registro** para guardar un registro en un archivo. Los archivos de registro se pueden abrir y ver posteriormente. Para abrir un registro existente, haga clic en **Archivo** > **Abrir registro**. En la ventana principal del programa, ESET SysInspector muestra siempre un registro 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, haga clic en **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.

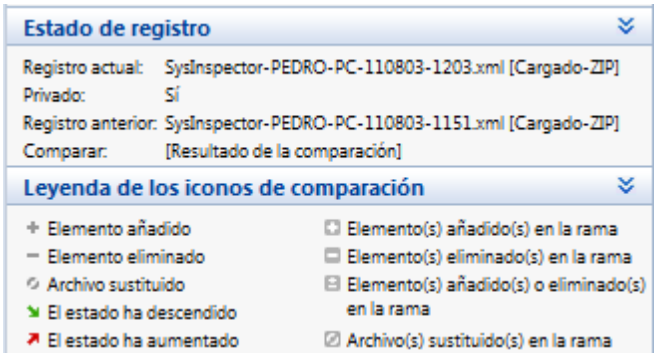
NOTA: si compara dos archivos de registro, haga clic en **Archivo** > **Guardar registro** para guardarlo como archivo ZIP. Se guardarán ambos archivos. Si abre posteriormente dicho archivo, los registros contenidos en el mismo se compararán automáticamente.

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

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, haga clic en **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

5.6.3 Parámetros de la línea de comandos

ESET SysInspector admite la generación de informes desde la línea de comandos con estos parámetros:

/gen	genera un registro directamente desde la línea de comandos, sin ejecutar la interfaz gráfica.
/privacy	genera un registro omitiendo la información personal.
/zip	guarda el registro obtenido en un archivo comprimido zip.
/silent	cancela la ventana de progreso cuando se genera un registro desde la línea de comandos.
/blank	inicia ESET SysInspector sin generar o cargar un registro.

Ejemplos

Uso:

```
Sysinspector.exe [load.xml] [/gen=save.xml] [/privacy] [/zip] [compareto.xml]
```

Para cargar un registro determinado directamente en el navegador, utilice: *SysInspector.exe .\clientlog.xml*
Para generar un registro desde la línea de comandos, utilice: *SysInspector.exe /gen=.\mynewlog.xml*
Para generar un registro que no incluya la información confidencial directamente como archivo comprimido, utilice: *SysInspector.exe /gen=.\mynewlog.zip /privacy /zip*
Para comparar dos archivos de registro y examinar las diferencias, utilice: *SysInspector.exe new.xml old.xml*

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

5.6.4 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 sospecha que el ordenador está infectado por un virus que el antivirus no detecta, siga estas instrucciones:

1. Ejecute ESET SysInspector para generar una nueva instantánea del sistema.
2. Seleccione el primero y el último elemento de la sección de la izquierda (en la estructura de árbol) mientras mantiene pulsada la tecla Mayús.
3. Haga clic con el botón secundario en los objetos seleccionados y elija la opción **Exportar las secciones seleccionadas al script de servicio**.
4. Los objetos seleccionados se exportarán a un nuevo registro.
5. Este es el paso más importante de todo el procedimiento: abra el registro nuevo y cambie el atributo - a + para todos los objetos que desee eliminar. Asegúrese de que no ha marcado ningún archivo u objeto importante del sistema operativo.
6. Abra ESET SysInspector, haga clic en **Archivo** > **Ejecutar script de servicio** e introduzca la ruta del script.
7. Haga clic en **Aceptar** para ejecutar el script.

5.6.4.1 Generación de scripts de servicio

Para generar un script de servicio, haga clic con el botón derecho del ratón en cualquier elemento del árbol de menús (en el panel izquierdo) de la ventana principal de ESET SysInspector. En el menú contextual, seleccione **Exportar todas las secciones al script de servicio** o **Exportar secciones seleccionadas al script de servicio**.

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

5.6.4.2 Estructura del script de servicio

En la primera línea del encabezado del script encontrará información sobre la versión del motor (ev), la versión de la interfaz gráfica de usuario (gv) y la versión del registro (lv). Puede utilizar estos datos para realizar un seguimiento de los posibles cambios del archivo .xml que genere el script y evitar las incoherencias durante la ejecución. Esta parte del script no se debe modificar.

El resto del archivo se divide en secciones, donde los elementos se pueden modificar (indique los que procesará el script). Para marcar los elementos que desea procesar, sustituya el carácter “-” situado delante de un elemento por el carácter “+”. En el script, las secciones se separan mediante una línea vacía. Cada sección tiene un número y un título.

01) Running processes (Procesos en ejecución)

En esta sección se incluye una lista de todos los procesos que se están ejecutando en el sistema. Cada proceso se identifica mediante su ruta UNC y, posteriormente, su código hash CRC16 representado mediante asteriscos (*).

Ejemplo:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

En este ejemplo se ha seleccionado (marcado con el carácter "+") el proceso module32.exe, que finalizará al ejecutar el script.

02) Loaded modules (Módulos cargados)

En esta sección se 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.

5.6.4.3 Ejecución de scripts de servicio

Seleccione todos los elementos que desee y, a continuación, guarde y cierre el script. Ejecute el script modificado directamente desde la ventana principal de ESET SysInspector, con la opción **Ejecutar script de servicio** del menú Archivo. Cuando abra un script, el programa mostrará el mensaje siguiente: **¿Está seguro de que desea ejecutar el script de servicio "%Scriptname%"?** Una vez que haya confirmado la selección, es posible que se muestre otra advertencia para informarle de que el script de servicio que intenta ejecutar no está firmado. Haga clic en **Ejecutar** para iniciar el script.

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.

5.6.5 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, haga clic en **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 haga clic en **Archivo** > **Abrir registro** en el menú principal del programa. También puede arrastrar y soltar los archivos de registro en la aplicación ESET SysInspector. Si necesita ver los archivos de registro de ESET SysInspector con frecuencia, le recomendamos que cree un acceso directo al archivo SYSINSPECTOR.EXE en su escritorio. Para ver los archivos de registro, arrástrelos y suéltelos en ese acceso directo. Por razones de seguridad, es posible que Windows Vista/7 no

permita la 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.

5.6.6 ESET SysInspector como parte de ESET NOD32 Antivirus

Para abrir la sección ESET SysInspector en ESET NOD32 Antivirus, haga clic en **Herramientas** > **ESET SysInspector**. El sistema de administración de la ventana de ESET SysInspector es parecido al de los registros de análisis del 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, seleccione **Mostrar** en el menú contextual. Para exportar la instantánea seleccionada a un archivo, haga clic con el botón derecho del ratón en ella y seleccione **Exportar**.

A continuación, se muestra una descripción detallada de las opciones disponibles:

- **Comparar**: le permite comparar dos registros existentes. Esta opción es ideal para realizar un seguimiento de los cambios entre el registro actual y el anterior. Para poder aplicar esta opción, debe seleccionar dos instantáneas con el fin de compararlas.
- **Crear**: 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).

5.7 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.

5.7.1 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) o Windows Assessment and Deployment Kit (WADK) y, por tanto, Windows AIK o WADK debe estar instalado antes de crear ESET SysRescue (http://go.eset.eu/AIK, http://www.microsoft.com/en-us/download/details.aspx?id=30652). La elección de uno de estos kits depende de la versión del sistema operativo. 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 así como con WADK 1.0 y versiones posteriores.

Al instalar Windows ADK, elija únicamente los paquetes Herramientas de implementación y Windows Preinstallation Enviroment (Windows PE) para la instalación. Como el tamaño de estos paquetes es superior a 3,0 GB, se recomienda una conexión a Internet de alta velocidad para realizar la descarga.

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

Windows ADK es compatible con:

- Windows 8
- Windows 7
- Windows Vista
- Windows Vista Service Pack 1
- Windows Vista Service Pack 2

Nota: puede que ESET SysRescue no esté disponible para Windows 8 en versiones más antiguas de productos de ESET. En tal caso, se recomienda que actualice su producto o que cree un disco de ESET SysRescue en otra versión de Microsoft Windows.

Windows AIK es compatible con:

- Windows 7
- Windows Vista
- Windows XP Service Pack 2 con KB926044
- Windows XP Service Pack 3

5.7.2 Cómo crear un CD de recuperación

Para iniciar el asistente de ESET SysRescue, haga clic en **Inicio** > **Programas** > **ESET** > **ESET NOD32 Antivirus** > **ESET SysRescue**.

En primer lugar, el asistente comprueba si está instalado Windows AIK o ADK y un dispositivo adecuado para la creación de medios de arranque. Si Windows AIK o ADK 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, http://www.microsoft.com/en-us/download/details.aspx?id=30652).

NOTA: como el tamaño de Windows AIK es superior a 1 GB, se requiere una conexión a Internet de alta velocidad.

Al instalar Windows ADK, elija únicamente los paquetes Herramientas de implementación y Windows Preinstallation Enviroment (Windows PE) para la instalación. Como el tamaño de estos paquetes es superior a 3,0 GB, se requiere una conexión a Internet de alta velocidad para realizar la descarga.

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

5.7.3 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.

5.7.4 Configuración

Antes de empezar a crear ESET SysRescue, el asistente de instalación muestra los parámetros de compilación. 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)

La opción **Crear** no está activa 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 **Cambiar** y vaya a la ficha **ESET Antivirus**. Además, si no rellena el nombre de usuario y la contraseña (**Cambiar** > **ESET Antivirus**), la opción **Crear** aparecerá atenuada.

5.7.4.1 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.

5.7.4.2 ESET Antivirus

Para crear un CD de ESET SysRescue, puede elegir entre 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, la opción predeterminada **Carpeta ESS/EAV/Archivo MSI** debe estar seleccionada. 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 campos 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.

5.7.4.3 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. automática**). 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.

5.7.4.4 Protocolo de Internet

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

5.7.4.5 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 **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.

5.7.4.6 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.

5.7.5 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** y **Herramientas**. 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.

5.7.5.1 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.

5.8 Línea de comandos

El módulo antivirus de ESET NOD32 Antivirus se puede iniciar manualmente a través de la línea de comandos, con el comando "ecls", o con un archivo por lotes ("bat"). Uso del análisis de línea de comandos ESET:

```
ecls [OPTIONS..] FILES..
```

Los siguientes parámetros y modificadores se pueden utilizar al ejecutar el análisis a petición desde la línea de comandos:

Opciones

/base-dir=CARPETA	cargar módulos desde una CARPETA
/quar-dir=CARPETA	CARPETA de cuarentena
/exclude=MÁSCARA	excluir del análisis los archivos que cumplan MÁSCARA
/subdir	analizar subcarpetas (predeterminado)
/no-subdir	no analizar subcarpetas
/max-subdir-level=NIVEL	máximo nivel de anidamiento para subcarpetas a analizar
/symlink	seguir enlaces simbólicos (predeterminado)
/no-symlink	omitir enlaces simbólicos
/ads	analizar ADS (predeterminado)
/no-ads	no analizar ADS
/log-file=ARCHIVO	registrar salida en ARCHIVO
/log-rewrite	sobrescribir el archivo de salida (predeterminado - agregar)
/log-console	enviar registro a la consola (predeterminado)
/no-log-console	no enviar registro a la consola
/log-all	registrar también los archivos sin infectar
/no-log-all	no registrar archivos sin infectar (predeterminado)
/aind	mostrar indicador de actividad
/auto	analizar y desinfectar automáticamente todos los discos locales

Opciones de análisis

/files	analizar archivos (predeterminado)
/no-files	no analizar archivos
/memory	analizar memoria
/boots	analizar sectores de inicio
/no-boots	no analizar sectores de inicio (predeterminado)
/arch	analizar archivos comprimidos (predeterminado)
/no-arch	no analizar archivos
/max-obj-size=TAMAÑO	analizar solo archivos menores de TAMAÑO megabytes (predeterminado 0 = ilimitado)
/max-arch-level=NIVEL	máxima profundidad de anidamiento para archivos comprimidos (archivos anidados) a analizar
/scan-timeout=LÍMITE	analizar archivos comprimidos durante LÍMITE segundos como máximo
/max-arch-size=TAMAÑO	analizar los archivos dentro de un archivo comprimido solo si su tamaño es inferior a TAMAÑO (predeterminado 0 = ilimitado)
/max-sfx-size=TAMAÑO	analizar solo los archivos en un archivo comprimido de autoextracción si su tamaño es inferior a TAMAÑO megabytes (predeterminado 0 = ilimitado)
/mail	analizar archivos de correo (predeterminado)
/no-mail	no analizar archivos de correo
/mailbox	analizar buzones de correo (predeterminado)
/no-mailbox	no analizar buzones de correo
/sfx	analizar archivos comprimidos de autoextracción (predeterminado)
/no-sfx	no analizar archivos comprimidos de autoextracción
/rtp	analizar empaquetadores en tiempo real (predeterminado)
/no-rtp	no analizar empaquetadores en tiempo real
/unsafe	analizar en busca de aplicaciones potencialmente peligrosas
/no-unsafe	no analizar en busca de aplicaciones potencialmente peligrosas
/unwanted	analizar en busca de aplicaciones potencialmente indeseables
/no-unwanted	no analizar en busca de aplicaciones potencialmente indeseables (predeterminado)
/suspicious	analizar en busca de aplicaciones sospechosas (predeterminado)
/no-suspicious	no analizar en busca de aplicaciones sospechosas
/pattern	usar firmas (predeterminado)
/no-pattern	no usar firmas
/heur	activar heurística (predeterminado)
/no-heur	desactivar heurística
/adv-heur	activar heurística avanzada (predeterminado)
/no-adv-heur	desactivar heurística avanzada
/ext=EXTENSIONES	analizar solo EXTENSIONES separadas por dos puntos
/ext-exclude=EXTENSIONES	excluir EXTENSIONES del análisis, separándolas por el signo ":" (dos puntos)
/clean-mode=MODO	utilizar el MODO desinfección para objetos infectados Están disponibles las opciones siguientes: • **none** (ninguno): no se realiza la desinfección automática. • **standard** (estándar, predeterminado): ecls.exe intenta desinfectar o eliminar automáticamente los archivos infectados. • **strict** (estricto): ecls.exe intenta desinfectar o eliminar automáticamente los archivos infectados sin la intervención del usuario (no verá una notificación antes de que se eliminen los archivos). • **rigorous** (riguroso): ecls.exe elimina los archivos sin intentar desinfectarlos, sea cual sea el archivo. • **delete** (eliminar): ecls.exe elimina los archivos sin intentar desinfectarlos, pero no elimina archivos delicados como los archivos del sistema de Windows.
/quarantine	copiar archivos infectados (si se han desinfectado) a la carpeta Cuarentena (complementa la acción realizada durante la desinfección)
/no-quarantine	no copiar archivos infectados a cuarentena

Opciones generales

/help	mostrar ayuda y salir

/version	mostrar información sobre la versión y salir
/preserve-time	conservar hora del último acceso

Códigos de salida

0	no se ha detectado ninguna amenaza
1	amenaza detectada y eliminada
10	no se han podido analizar todos los archivos (podrían ser amenazas)
50	amenaza detectada
100	error

NOTA: los códigos de salida superiores a 100 significan que no se ha analizado el archivo y que, por lo tanto, puede estar infectado.

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 de los análisis habituales. Los usuarios de ESET NOD32 Antivirus tienen la ventaja de la tecnología Anti-Stealth que también detecta y elimina 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 Empaquetadores

Un empaquetador es un archivo ejecutable autoextraíble en tiempo de ejecución que implementa varios tipos de código malicioso en un solo paquete.

Los más comunes son UPX, PE_Compact, PKLite y ASPack. El mismo código malicioso se puede detectar de forma diferente cuando se comprime con un empaquetador diferente. Los empaquetadores también tienen la capacidad de hacer que sus "firmas" muten con el tiempo, haciendo que el código malicioso sea más difícil de detectar y eliminar.

6.1.8 Aplicaciones potencialmente peligrosas

Existen muchos programas legítimos que sirven para simplificar la administración de ordenadores en red. Sin embargo, si caen en las manos equivocadas, podrían utilizarse con fines maliciosos. ESET NOD32 Antivirus proporciona una opción para detectar estas amenazas.

Aplicaciones potencialmente peligrosas es la clasificación utilizada para el software comercial legítimo. Esta clasificación incluye programas como herramientas de acceso remoto, aplicaciones para detectar contraseñas y registradores de pulsaciones (programas que graban todas las teclas pulsadas por un usuario).

Si detecta la presencia de una aplicación potencialmente peligrosa que esté en ejecución en su ordenador (y no la ha instalado usted), consulte con el administrador de la red o elimine la aplicación.

6.1.9 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 el consentimiento del usuario para 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 Tecnología de ESET

6.2.1 Bloqueo de exploits

El Bloqueo de exploits se ha diseñado para fortificar aquellas aplicaciones que sufren más ataques, como los navegadores de Internet, los lectores de archivos pdf, los clientes de correo electrónico y los componentes de MS Office. Este producto supervisa el comportamiento de los procesos en busca de actividad sospechosa que pueda indicar la presencia de un exploit.

Cuando detecta un proceso sospechoso, el Bloqueador de exploits lo detiene inmediatamente y registra los datos de la amenaza; después los envía al sistema de nube de ESET Live Grid. El laboratorio de amenazas de ESET procesa estos datos y los utiliza para mejorar la protección que ofrece a los usuarios frente a amenazas desconocidas y ataques 0-day (código malicioso reciente para el que no hay ninguna solución preconfigurada).

6.2.2 Análisis de memoria avanzado

El Análisis de memoria avanzado trabaja conjuntamente con el Bloqueao de exploits para aumentar la protección contra código malicioso que utiliza los métodos de ofuscación y cifrado para evitar su detección por productos de protección antivirus. En aquellos casos en los que la emulación o la heurística normales no detectan una amenaza, el Análisis de memoria avanzado consigue identificar comportamientos sospechosos y analiza las amenazas que se presentan en la memoria del sistema. Esta solución es eficaz incluso para código malicioso muy ofuscado.

A diferencia del Bloqueador de exploits, el Análisis de memoria avanzado es un método posterior a la ejecución, lo cual significa que existe la posibilidad de que haya habido actividad maliciosa antes de la detección de una amenaza. No obstante, ofrece una capa de seguridad adicional cuando las otras técnicas de detección fallan.

6.2.3 ESET Live Grid

ESET Live Grid, que se basa en el sistema avanzado de alerta temprana ThreatSense.Net®, utiliza los datos enviados por usuarios de ESET de todo el mundo y los envía al laboratorio de virus de ESET. ESET Live Grid proporciona metadatos y muestras sospechosas en estado salvaje, lo cual nos permite reaccionar de forma inmediata a las necesidades de nuestros clientes y hace posible la respuesta de ESET a las amenazas más recientes. Los investigadores de código malicioso de ESET utilizan la información para crear una instantánea precisa de la naturaleza y el alcance de las amenazas globales, de modo que podemos centrarnos en los objetos adecuados. Los datos de ESET Live Grid son fundamentales a la hora de establecer las prioridades en nuestro procesamiento automatizado.

Además implementa un sistema de reputación que contribuye a la mayor eficacia de nuestras soluciones de protección contra código malicioso. Cuando se inspecciona un archivo ejecutable en el sistema de algún usuario, primero se contrasta su etiqueta hash con una base de datos de elementos incluidos en las listas blanca y negra. Si el elemento se encuentra en la lista blanca, el archivo inspeccionado se marca para su exclusión en próximos análisis. Si está en la lista negra, se emprenden las acciones necesarias de acuerdo con la naturaleza de la amenaza. Si no se encuentra ninguna coincidencia, el archivo se analiza a fondo. Los archivos se clasifican como amenazas o no en función de los resultados de este análisis. Este enfoque tiene un gran impacto positivo en el rendimiento del análisis.

Este sistema de reputación permite detectar eficazmente muestras de código malicioso, incluso antes de que sus firmas lleguen al ordenador del usuario mediante una base de datos de virus actualizada (lo cual sucede varias veces al día).

6.2.4 Bloqueor de exploits de Java

El Bloqueor de exploits de Java es una extensión de la protección actual del Bloqueo de exploits. Esta extensión busca comportamientos de tipo exploit en Java. Puede informar de las muestras bloqueadas a los analistas de código malicioso, a fin de que puedan crean firmas para bloquearlas en diferentes capas (bloqueo de URL, descarga de archivos, etc.).

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.