

ESET NOD32 ANTIVIRUS 8

Guía para el usuario

(destinada para la versión 8.0 del producto y posteriores)

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

[Haga un clic aquí para descargar la versión más reciente de este documento.](#)

ESET NOD32 ANTIVIRUS

Copyright ©2014 por ESET, spol. s r. o.

ESET NOD32 Antivirus fue desarrollado por ESET, spol. s r. o.

Para obtener más información, visite www.eset-la.com.

Todos los derechos reservados. Ninguna parte de esta documentación podrá reproducirse, almacenarse en un sistema de recuperación o transmitirse en forma o modo alguno, ya sea por medios electrónicos, mecánicos, fotocopia, grabación, escaneo o cualquier otro medio sin la previa autorización por escrito del autor.

ESET, spol. s r. o. se reserva el derecho de modificar cualquier elemento del software de la aplicación sin previo aviso.

Soporte al cliente en todo el mundo: www.eset.com/support

REV. 9/30/2014

Contenido

1. ESET NOD32 Antivirus.....	5
1.1 Novedades de la versión 8.....	5
1.2 Requisitos del sistema.....	6
1.3 Prevención.....	6
2. Instalación.....	8
2.1 Instalador activo.....	8
2.2 Instalación fuera de línea.....	9
2.2.1 Configuración avanzada.....	10
2.3 Activación del producto.....	10
2.4 Ingreso del nombre de usuario y la contraseña.....	11
2.5 Reemplazo a una versión más reciente.....	11
2.6 Primera exploración después de la instalación.....	12
3. Guía para principiantes.....	13
3.1 La ventana principal del programa.....	13
3.2 Actualizaciones.....	15
4. Trabajar con ESET NOD32 Antivirus.....	17
4.1 Equipo.....	19
4.1.1 Antivirus y antispyware.....	19
4.1.1.1 Protección del sistema de archivos en tiempo real.....	20
4.1.1.1.1 Opciones avanzadas de exploración.....	21
4.1.1.1.2 Niveles de desinfección.....	22
4.1.1.1.3 Cuándo modificar la configuración de la protección en tiempo real.....	23
4.1.1.1.4 Verificación de la protección en tiempo real.....	23
4.1.1.1.5 Qué hacer si la protección en tiempo real no funciona.....	23
4.1.1.2 Exploración del equipo.....	23
4.1.1.2.1 Iniciador de la exploración personalizada.....	24
4.1.1.2.2 Progreso de la exploración.....	25
4.1.1.2.3 Perfiles de exploración.....	26
4.1.1.3 Exploración en el inicio.....	27
4.1.1.3.1 Verificación de archivos de inicio automática.....	27
4.1.1.4 Exploración en estado inactivo.....	27
4.1.1.5 Exclusiones.....	28
4.1.1.6 Configuración de los parámetros del motor ThreatSense.....	29
4.1.1.6.1 Objetos.....	29
4.1.1.6.2 Opciones.....	30
4.1.1.6.3 Desinfección.....	30
4.1.1.6.4 Extensiones.....	30
4.1.1.6.5 Límites.....	31
4.1.1.6.6 Otros.....	31
4.1.1.7 Detección de una infiltración.....	32
4.1.1.8 Protección de documentos.....	33
4.1.2 Medios extraíbles.....	34
4.1.3 Control del dispositivo.....	34
4.1.3.1 Reglas de control del dispositivo.....	35
4.1.3.2 Agregado de reglas del control del dispositivo.....	36
4.1.4 HIPS.....	37
4.1.5 Modo de juego.....	39
4.2 Internet y correo electrónico.....	40
4.2.1 Protección del cliente de correo electrónico.....	41
4.2.1.1 Integración con los clientes de correo electrónico.....	41
4.2.1.1.1 Configuración de la protección del cliente de correo electrónico.....	42
4.2.1.2 Módulo de exploración IMAP/IMAPS.....	42
4.2.1.3 Filtro para POP3, POP3S.....	43
4.2.2 Protección del acceso a la Web.....	44
4.2.2.1 HTTP, HTTPS.....	44
4.2.2.2 Administración de direcciones URL.....	45
4.2.3 Filtrado de protocolos.....	46
4.2.3.1 Clientes de Internet y correo electrónico.....	46
4.2.3.2 Aplicaciones excluidas.....	47
4.2.3.3 Direcciones IP excluidas.....	48
4.2.3.3.1 Agregar dirección IPv4.....	48
4.2.3.3.2 Agregar dirección IPv6.....	48
4.2.3.4 Verificación del protocolo SSL.....	49
4.2.3.4.1 Certificados.....	49
4.2.3.4.1.1 Certificados de confianza.....	50
4.2.3.4.1.2 Certificados excluidos.....	50
4.2.3.4.1.3 Comunicación cifrada SSL.....	50
4.2.4 Protección antiphishing.....	50
4.3 Actualización del programa.....	51
4.3.1 Configuraciones de actualización.....	54
4.3.1.1 Perfiles de actualización.....	55
4.3.1.2 Configuración avanzada de la actualización.....	55
4.3.1.2.1 Modo de actualización.....	55
4.3.1.2.2 Servidor proxy.....	56
4.3.1.2.3 Conexión a la red de área local.....	57
4.3.2 Actualizar reversión.....	57
4.3.3 Cómo crear tareas de actualización.....	58
4.4 Herramientas.....	59
4.4.1 Archivos de registro.....	60
4.4.1.1 Mantenimiento de registros.....	61
4.4.2 Tareas programadas.....	61
4.4.3 Estadísticas de protección.....	63
4.4.4 Observar la actividad.....	63
4.4.5 ESET SysInspector.....	64
4.4.6 ESET Live Grid.....	64
4.4.6.1 Archivos sospechosos.....	65
4.4.7 Procesos activos.....	66
4.4.8 Cuarentena.....	67
4.4.9 Configuración del servidor proxy.....	68
4.4.10 Alertas y notificaciones.....	69
4.4.10.1 Formato de mensajes.....	70
4.4.11 Envío de muestras para su análisis.....	70
4.4.12 Actualizaciones del sistema.....	71
4.5 Interfaz del usuario.....	71
4.5.1 Gráficos.....	71
4.5.2 Alertas y notificaciones.....	72
4.5.2.1 Configuración avanzada.....	72

4.5.3	Ventanas de notificación ocultas.....	73	6.1.9	Aplicaciones potencialmente no deseadas.....	98
4.5.4	Configuración del acceso.....	73	6.2 Tecnología ESET.....	99	
4.5.5	Menú del programa.....	73	6.2.1	Bloqueador de exploits.....	99
4.5.6	Menú contextual.....	74	6.2.2	Exploración de memoria avanzada.....	99
5. Usuario avanzado.....	75		6.2.3	ESET Live Grid.....	99
5.1	Administrador de perfiles.....	75	6.2.4	Bloqueador de exploits de Java.....	100
5.2	Accesos directos desde el teclado.....	75	6.3 Correo electrónico.....	100	
5.3	Diagnósticos.....	76	6.3.1	Anuncios.....	100
5.4	Importación y exportación de una configuración.....	76	6.3.2	Mensajes falsos.....	100
5.5	Detección en estado inactivo.....	77	6.3.3	Phishing.....	101
5.6	ESET SysInspector.....	77	6.3.4	Reconocimiento de fraudes de spam.....	101
5.6.1	Introducción a ESET SysInspector.....	77			
5.6.1.1	Inicio de ESET SysInspector.....	78			
5.6.2	Interfaz del usuario y uso de la aplicación.....	78			
5.6.2.1	Controles de programa.....	78			
5.6.2.2	Navegación por ESET SysInspector.....	80			
5.6.2.2.1	Accesos directos desde el teclado.....	81			
5.6.2.3	Comparación.....	82			
5.6.3	Parámetros de la línea de comandos.....	83			
5.6.4	Script de servicio.....	84			
5.6.4.1	Generación de scripts de servicio.....	84			
5.6.4.2	Estructura del script de servicio.....	84			
5.6.4.3	Ejecución de scripts de servicio.....	87			
5.6.5	Preguntas frecuentes.....	87			
5.6.6	ESET SysInspector como parte de ESET NOD32 Antivirus.....	89			
5.7 ESET SysRescue.....	89				
5.7.1	Requisitos mínimos.....	89			
5.7.2	Cómo crear un CD de recuperación.....	90			
5.7.3	Selección de objetos.....	90			
5.7.4	Configuración.....	91			
5.7.4.1	Carpetas.....	91			
5.7.4.2	ESET Antivirus.....	91			
5.7.4.3	Configuración avanzada.....	92			
5.7.4.4	Protocolo de Internet.....	92			
5.7.4.5	Dispositivo USB de inicio.....	92			
5.7.4.6	Grabación.....	92			
5.7.5	Trabajo con ESET SysRescue.....	93			
5.7.5.1	Utilización de ESET SysRescue.....	93			
5.8 Línea de comandos.....	93				
6. Glosario.....	96				
6.1 Tipos de infiltraciones.....	96				
6.1.1	Virus.....	96			
6.1.2	Gusanos.....	96			
6.1.3	Trojanos.....	97			
6.1.4	Rootkits.....	97			
6.1.5	Adware.....	97			
6.1.6	Spyware.....	98			
6.1.7	Empaquetadores.....	98			
6.1.8	Aplicaciones potencialmente no seguras.....	98			

1. ESET NOD32 Antivirus

ESET NOD32 Antivirus representa un nuevo enfoque para la seguridad del equipo plenamente integrada. La versión más reciente del motor de exploración ThreatSense® utiliza velocidad y precisión para mantener el equipo seguro. El resultado es un sistema inteligente constantemente alerta frente a los ataques y el software malicioso que podrían poner en peligro su equipo.

ESET NOD32 Antivirus es una completa solución de seguridad que combina la máxima protección con el mínimo impacto en el sistema. Nuestras tecnologías avanzadas usan la inteligencia artificial para prevenir infiltraciones de virus, spyware, troyanos, gusanos, adware, rootkits y otras amenazas sin entorpecer el rendimiento del sistema ni perturbar el equipo.

Características y beneficios

Antivirus y antispyware	Detecta en forma proactiva y desinfecta más cantidad de amenazas conocidas y desconocidas, tales como virus, gusanos, troyanos y rootkits. La tecnología de heurística avanzada identifica hasta al malware nunca antes visto. Lo protege de amenazas desconocidas, a las que neutraliza antes de que lleguen a causar daño. La protección del acceso a la web y Anti-Phishing funciona mediante el monitoreo de la comunicación entre navegadores Web y servidores remotos (incluido SSL). La protección del cliente de correo electrónico proporciona el control de las comunicaciones por correo electrónico recibidas a través de los protocolos POP3(S) e IMAP(S).
Actualizaciones de rutina	La actualización de rutina de la base de datos de firmas de virus y de los módulos del programa es el mejor método para asegurar el máximo nivel de seguridad en el equipo.
ESET Live Grid (Reputación basada en la nube)	Usted podrá verificar la reputación de los procesos en ejecución y de los archivos directamente desde ESET NOD32 Antivirus.
Control del dispositivo	Explora automáticamente todas las unidades flash USB, las tarjetas de memoria, los CD y los DVD. Bloquea los medios extraíbles en función del tipo de medio, el fabricante, el tamaño y otros atributos.
Funcionalidad del HIPS	Puede personalizar el comportamiento del sistema a un nivel superior: especificar reglas para el registro del sistema, activar procesos y programas, y ajustar su posición de seguridad.
Modo de juego	Pospone todas las ventanas emergentes, actualizaciones y demás actividades que consumen recursos del sistema a fin de conservarlos para los juegos y otras actividades de pantalla completa.

Es necesario tener una licencia activa para que las características de ESET NOD32 Antivirus sean funcionales. Se recomienda renovar la licencia varias semanas antes de que venza la licencia para ESET NOD32 Antivirus.

1.1 Novedades de la versión 8

ESET NOD32 Antivirus en la versión 8 presenta muchas mejoras pequeñas:

- **Un nuevo modo inteligente para HIPS:** se ubica entre los modos Automático e Interactivo. Capacidad para identificar actividades sospechosas y procesos maliciosos en el sistema.
- **Bloqueador de exploits mejorado:** diseñado para fortalecer diferentes tipos de aplicaciones comúnmente explotadas como los navegadores web, los lectores de PDF, los clientes de correo electrónico y los componentes de MS Office. El bloqueador de exploits ahora soporta Java y ayuda a mejorar la detección y protección de estos tipos de vulnerabilidad.
- **Control del dispositivo:** un reemplazo del control de los medios extraíbles usados en la versión 5 y 6: Le permite explorar, bloquear o ajustar los filtros o permisos extendidos y definir una habilidad de los usuarios para acceder a un dispositivo determinado.

- **Exploración avanzada de memoria** trabaja en conjunto con el bloqueador de exploits para fortalecer la protección contra malware diseñado para evadir la detección por los productos antimalware con el uso de ofuscación o cifrado.
- **Las mejoras antiphishing:** ESET NOD32 Antivirus ahora bloquean sitios fraudulentos y sitios phishing. Envío mejorado de sitios sospechosos y falsos positivos por parte de los usuarios.
- **Limpiador especializado:** inclusión de las 3-5 amenazas de malware crítico prevalente.
- **Instalación más rápida y más confiable** con la inclusión de una exploración inicial que se ejecuta a los 20 minutos de finalizada la instalación o reinicio.
- **Compatibilidad del complemento del correo electrónico:** nuestro complemento ahora está integrado dentro de la nueva versión de Office 2013 y Windows Live Mail.
- **Compatibilidad mejorada con Windows 8/8.1:** ESET SysRescue es ahora completamente funcional con Windows 8. Las notificaciones del sistema se muestran ahora en el entorno de Windows 8, que le notifican sobre detecciones de HIPS o detecciones de archivos que requieren una interacción del usuario o descargas de aplicaciones potencialmente no deseadas.

1.2 Requisitos del sistema

Para un funcionamiento óptimo de ESET NOD32 Antivirus, el sistema debería cumplir con 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+ 32-bit/XP SP2+ 64-bit/Home Server 2003 SP2 32-bit/Home Server 2011 64-bit

1.3 Prevención

Cuando trabaja con su equipo y, en particular, cuando navega por Internet, recuerde que ningún sistema antivirus del mundo puede eliminar completamente el riesgo de las [infiltraciones](#) y de los ataques. Para ofrecer la máxima protección y conveniencia, es imprescindible utilizar su solución antivirus correctamente y atenerse a varias reglas útiles:

Actualizaciones habituales

De acuerdo con las estadísticas de ESET Live Grid, cada día se crean miles de infiltraciones nuevas y únicas para evadir las medidas de seguridad existentes y generar ganancias para sus creadores (a costa de otros usuarios). Los especialistas del laboratorio de virus de ESET analizan dichas amenazas diariamente, y luego preparan y lanzan actualizaciones para mejorar en forma continua el nivel de protección de los usuarios. Para asegurar la máxima eficacia de estas actualizaciones, es importante configurarlas adecuadamente en el sistema. Para obtener más información sobre cómo configurar las actualizaciones, consulte el capítulo [Configuración de la actualización](#).

Descargas de revisiones de seguridad

Los creadores de software malicioso suelen aprovechar diversas vulnerabilidades del sistema para incrementar la eficacia de la propagación de los códigos maliciosos. Por eso, las empresas de software controlan cuidadosamente la aparición de vulnerabilidades en sus aplicaciones y lanzan actualizaciones de seguridad que eliminan amenazas potenciales en forma habitual. Es importante descargar estas actualizaciones de seguridad apenas se emiten. Microsoft Windows y los navegadores Web como Internet Explorer son ejemplos de los programas que publican actualizaciones de seguridad de manera periódica.

Copia de seguridad de datos importantes

A los creadores de malware en general no les importan las necesidades de los usuarios, y la actividad de los programas maliciosos suele generar un funcionamiento totalmente defectuoso de un sistema operativo, así como la pérdida de datos importantes. Es imprescindible realizar copias de seguridad habituales de los datos importantes y confidenciales en una fuente externa, como un DVD o un disco externo. Este tipo de precauciones facilitan y

aceleran la recuperación de datos en caso de una falla del sistema.

Exploración habitual del equipo en busca de virus

El módulo de protección del sistema de archivos en tiempo real maneja la detección de otros virus, gusanos, troyanos y rootkits conocidos y desconocidos. Esto significa que, cada vez que accede a un archivo o lo abre, se lo explora para evitar actividades de malware. No obstante, se recomienda realizar una exploración completa del equipo al menos una vez por mes, ya que las firmas de malware varía y la base de datos de firmas de virus se actualiza todos los días.

Seguimiento de reglas de seguridad básicas

Esta es la regla más útil y más efectiva de todas: siempre hay que tener cuidado. Hoy en día, muchas infiltraciones requieren la interacción del usuario para ejecutarse y propagarse. Si el usuario es precavido al abrir nuevos archivos, ahorrará un tiempo y esfuerzo considerables, que de otra forma se emplearían en desinfectar las infiltraciones. Estas son algunas pautas útiles:

- No visitar sitios Web sospechosos con muchas ventanas emergentes y anuncios intermitentes.
- Tener cuidado al instalar programas gratuitos, paquetes de códecs, etc. Solamente usar programas seguros y visitar sitios Web de Internet seguros.
- Tener cuidado al abrir los archivos adjuntos de los correos electrónicos, en especial los mensajes de envío masivo y los mensajes de remitentes desconocidos.
- No usar una cuenta de administrador para trabajar diariamente en el equipo.

2. Instalación

Existe varios métodos para la instalación de ESET NOD32 Antivirus en su equipo. Los métodos de instalación pueden variar dependiendo del país y los medios de distribución:

- [Instalador activo](#) se puede descargar del sitio Web ESET. El paquete de instalación es universal para todos los idiomas (escoja un idioma deseado). El Instalador activo en sí es un archivo pequeño, los archivos adicionales requeridos para instalar ESET NOD32 Antivirus se descargarán automáticamente.
- [Instalación fuera de línea](#): este tipo de instalación se usa cuando instala desde un CD/DVD del producto. Usa un archivo .msi que es más grande que el archivo Instalador activo y no necesita de una conexión de Internet o archivos adicionales para terminar la instalación.

Importante: Asegúrese de que no haya otros programas antivirus instalados en el equipo antes de instalar ESET NOD32 Antivirus. Si hay dos o más soluciones antivirus instaladas en el mismo equipo, pueden entrar en conflicto. Es recomendable desinstalar cualquier otro programa antivirus que haya en el sistema. Consulte nuestro [artículo de la base de conocimiento de ESET](#) para obtener una lista de herramientas del desinstalador para el software antivirus común (disponible en inglés y otros idiomas más).

2.1 Instalador activo

Una vez que descarga el paquete de instalación del *Instalador activo*, haga doble clic en el archivo de instalación y siga las instrucciones detalladas en la ventana del instalador.

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



Seleccione su idioma deseado desde el menú desplegable **Seleccionar idioma del producto** y haga clic en **Instalar**. Deje que pasen unos minutos para que se descarguen los archivos de instalación.

Después de aceptar el **Acuerdo de licencia del usuario final**, se le solicitará que configure **ESET Live Grid**. [ESET Live Grid](#) le ayuda a asegurar que ESET se informe inmediata y continuamente sobre las nuevas amenazas con el fin de proteger a nuestros clientes. El sistema le permite enviar las nuevas amenazas al laboratorio de virus de ESET, donde se analizan, procesan y agregan a la base de datos de firmas de virus.

Como valor predeterminado, está seleccionado **Sí, deseo participar**, el cual activará esta características.

El paso siguiente en el proceso de instalación consiste en configurar la detección de aplicaciones potencialmente no deseadas. Las aplicaciones potencialmente no deseadas no son necesariamente maliciosas, pero pueden afectar el comportamiento de su equipo en forma negativa. Vea el capítulo [Aplicaciones potencialmente no deseadas](#) para obtener más detalles.

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

2.2 Instalación fuera de línea

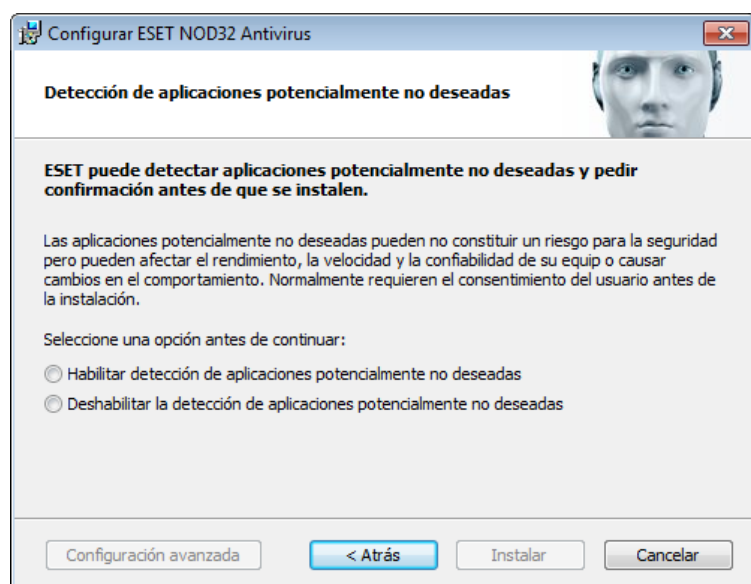
Una vez que haya iniciado el paquete de instalación fuera de línea (.msi), el asistente de instalación lo guiará a través del proceso de configuración.



En primer lugar, el programa verifica para ver si hay una nueva versión de ESET NOD32 Antivirus disponible. Si se encuentra una nueva versión, 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 continuará la instalación. Esta casilla de verificación es visible solamente cuando se encuentra disponible una versión más nueva que la versión que está instalando.

A continuación, se mostrará el Acuerdo de licencia de usuario final. Lea el acuerdo y haga clic en **Aceptar** para reconocer que acepta los términos del Acuerdo de licencia de usuario final. Luego de aceptar, la instalación continuará.

Para obtener información sobre los pasos de la instalación, **ESET Live Grid y Detección de aplicaciones potencialmente no deseadas**, siga las instrucciones de la sección anterior (consulte [“Instalador activo”](#)).



El modo de instalación proporciona las opciones de configuración apropiadas para la mayoría de los usuarios. Estas opciones brindan un excelente nivel de seguridad, una instalación sencilla y un alto rendimiento del sistema. Las **Configuraciones avanzadas** se diseñaron para usuarios con experiencia en el ajuste de programas y que desean modificar la configuración avanzada durante la instalación. Haga clic en **Instalar** para iniciar el proceso de instalación y para evadir las Configuraciones avanzadas.

2.2.1 Configuración avanzada

Luego de seleccionar **Configuraciones avanzadas**, 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 la ubicación (no recomendado).

Haga clic en **Siguiente** para configurar su conexión a Internet. Si usa un servidor proxy, debe estar bien configurado para que las actualizaciones de firmas de virus funcionen correctamente. Si no está seguro de usar un servidor proxy para conectarse a Internet, seleccione **Utilizar la misma configuración que Internet Explorer (recomendado)** y haga clic en **Siguiente**. Si no usa un servidor proxy, seleccione **No uso servidor proxy**.

Para configurar las opciones del servidor proxy, seleccione **Uso servidor proxy** y haga clic en **Siguiente**. Ingrese la dirección IP o el URL del servidor proxy en el campo **Dirección**. En el campo **Puerto**, especifique el puerto en el que el servidor proxy aceptará las conexiones (el predeterminado es 3128). En caso de que el servidor proxy requiera autenticación, ingrese un **Nombre de usuario** y una **Contraseña** válidos para tener acceso al servidor proxy. Si lo desea, también puede copiar la configuración del servidor proxy desde Internet Explorer. Para ello, haga clic en **Aplicar** y confirme la selección.

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

Si no desea que se actualicen los componentes del programa, seleccione **Nunca actualizar los componentes del programa**. Seleccione **Preguntar antes de descargar componentes del programa** para mostrar una ventana de confirmación cada vez que el sistema intente descargar componentes del programa. Para descargar los reemplazos de componentes del programa en forma automática, seleccione **Siempre actualizar los componentes del programa**.

NOTA: Luego de una actualización de componentes del programa, en general es necesario reiniciar el equipo. Es recomendable seleccionar **Si es necesario, reiniciar el equipo sin notificar**.

La siguiente ventana de instalación ofrece la opción de establecer una contraseña para proteger la configuración del programa. Seleccione la opción **Proteger las opciones de configuración mediante una contraseña** e ingrese su contraseña en los campos **Nueva contraseña** y **Confirmar la nueva contraseña**. Esta contraseña será necesaria para cambiar o acceder a la configuración del ESET NOD32 Antivirus. Cuando coincidan ambos campos de contraseña, haga clic en **Siguiente** para continuar.

Para realizar los siguientes pasos de la instalación, **ESET Live Grid** y **Detección de aplicaciones potencialmente no deseadas**, siga las instrucciones de la sección Instalador activo (consulte ["Instalador activo"](#)).

Para deshabilitar la [primera exploración después de la instalación](#) que se realiza normalmente cuando finaliza la instalación para revisar códigos maliciosos, quite la selección de la casilla de verificación junto a **Permitir exploración después de la instalación**. Para completar la instalación, haga clic en **Instalar** en la ventana **Preparado para instalar**.

2.3 Activación del producto

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

Hay varios métodos para activar su producto. La disponibilidad de un escenario de activación particular en la ventana de activación puede variar dependiendo del país así como de los medios de distribución (CD/DVD, página Web de ESET, etc.).

Si compró una versión comercial del producto en caja, seleccione **Activación mediante una clave de activación**. Por lo general, la clave de activación aparece en el interior o al dorso del paquete del producto. Para que la activación se realice correctamente, deberá ingresar la clave de activación tal como fue suministrada.


En caso de que haya recibido el nombre de usuario y la contraseña, seleccione **Activar mediante un nombre de usuario y una contraseña** e ingrese sus credenciales en los campos adecuados.

Si desea evaluar ESET NOD32 Antivirus antes de realizar una compra, seleccione **Activar la licencia de prueba**.

Ingrese su dirección de correo electrónico y su país para activar ESET NOD32 Antivirus durante un tiempo limitado. La licencia de prueba se enviará a su correo electrónico. Las licencias de prueba solo se pueden activar una vez por cliente.

Si no tiene licencia y desea comprar una, haga clic en **Adquirir licencia**. Será redirigido al sitio Web de su distribuidor local de ESET.

Seleccione **Activar luego** si quiere evaluar rápidamente el producto y no desea activarlo de inmediato o si le gustaría activarlo posteriormente.

También puede activar su copia de ESET NOD32 Antivirus directamente desde el programa. Haga clic en el icono [Menú del programa](#) ubicado en la esquina superior derecha o haga clic derecho en el icono ESET NOD32 Antivirus en la bandeja del sistema  y seleccione **Active su producto...** del menú.

2.4 Ingreso del nombre de usuario y la contraseña

Para un funcionamiento óptimo, es importante que el programa se actualice automáticamente. Esto solo será posible si se ingresaron el Nombre de usuario y la Contraseña correctos en la **Configuración de la actualización**.

Si no ingresó el Nombre de usuario y la Contraseña durante la instalación, puede hacerlo ahora. Desde la ventana principal del programa, haga clic en **Ayuda y soporte**, luego en **Activar la licencia** e ingrese los datos de la licencia que recibió con el producto de seguridad de ESET en la ventana de activación del producto.

Al ingresar el **Nombre de usuario** y la **Contraseña**, es importante escribirlos en forma exacta, sin errores:

- El nombre de usuario y la contraseña distinguen mayúsculas de minúsculas, y el guión en el nombre de usuario es necesario.
- La contraseña tiene diez caracteres de longitud, todos en minúscula.
- No se utiliza la letra “L” en las contraseñas (en su lugar, use el número uno “1”).
- Un “0” grande es el número cero (0), una “o” pequeña es la letra “o” en minúscula.

Es recomendable copiar y pegar los datos desde el correo electrónico de registro para garantizar la precisión.

2.5 Reemplazo a una versión más reciente

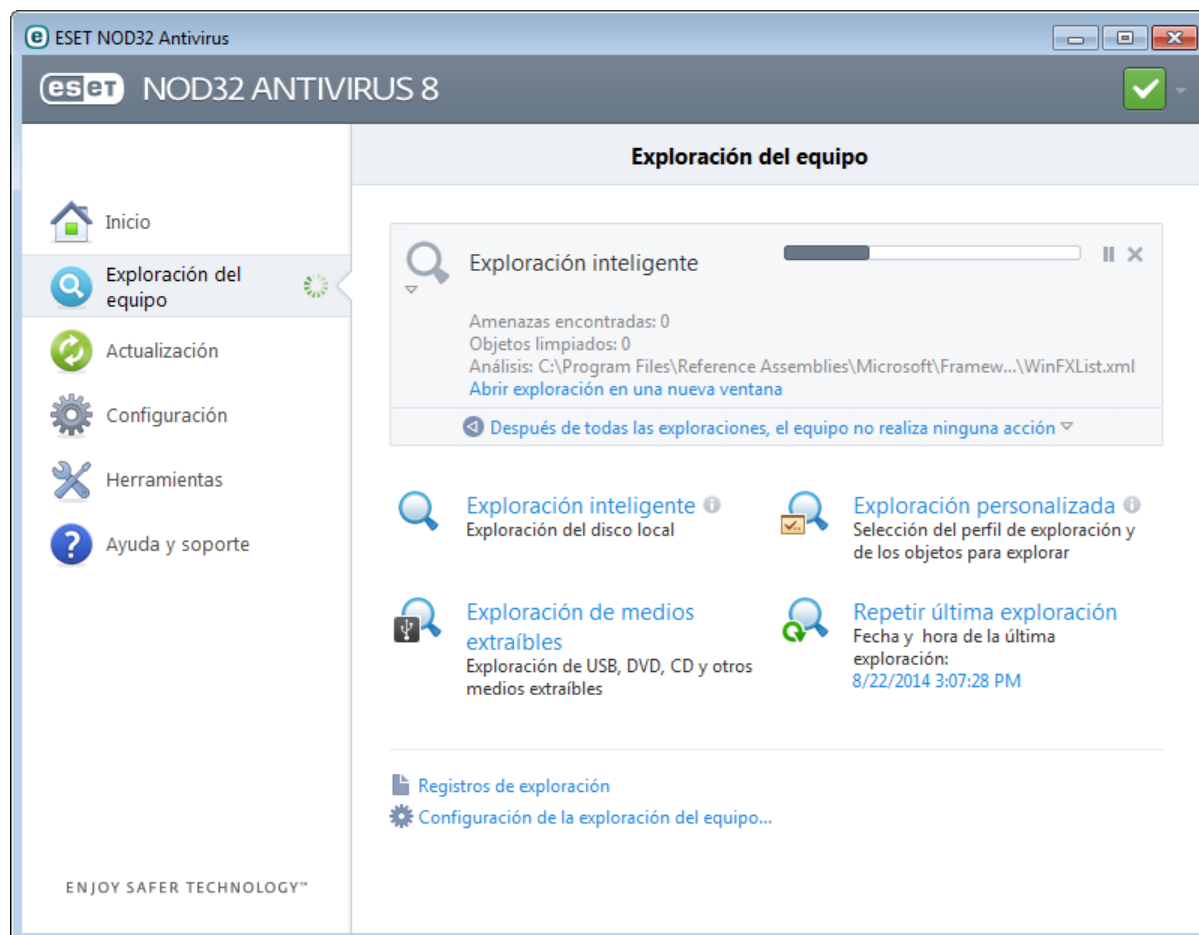
Las versiones nuevas de ESET NOD32 Antivirus se emiten para implementar mejoras del programa o para resolver problemas que no se pueden solucionar mediante la actualización automática de los módulos del programa. El reemplazo a una versión más reciente se puede realizar de varias maneras:

1. Reemplazar automáticamente mediante una actualización del programa.
Como el reemplazo de componentes del programa por una versión posterior se distribuye a todos los usuarios y puede afectar ciertas configuraciones del sistema, se emite luego de un largo período de prueba para asegurar la funcionalidad en todas las configuraciones posibles de sistema. Si necesita reemplazar el programa por una versión posterior inmediatamente después de su lanzamiento, use uno de los siguientes métodos.
2. Manualmente, en la ventana principal del programa haciendo clic en **Instalar/Verificar actualizaciones** en la sección **Actualización**.
3. En forma manual, mediante la descarga e instalación de la versión más reciente sobre la instalación previa.

2.6 Primera exploración después de la instalación

Luego de instalar ESET NOD32 Antivirus, se iniciará una exploración del equipo 20 minutos luego de la instalación o del reinicio del equipo para verificar códigos maliciosos.

También puede iniciar una exploración del equipo manualmente desde la ventana principal del programa mediante un clic en **Exploración del equipo** > **Exploración inteligente**. Para obtener más información sobre las exploraciones del equipo, consulte la sección [Exploración del equipo](#).



3. Guía para principiantes

Esta sección ofrece una visión general introductoria sobre ESET NOD32 Antivirus y su configuración básica.

3.1 La ventana principal del programa

La ventana principal de ESET NOD32 Antivirus se encuentra dividida en dos secciones principales. La ventana primaria que está a la derecha muestra información correspondiente a la opción seleccionada en el menú principal de la izquierda.

A continuación se describen las opciones del menú principal:

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

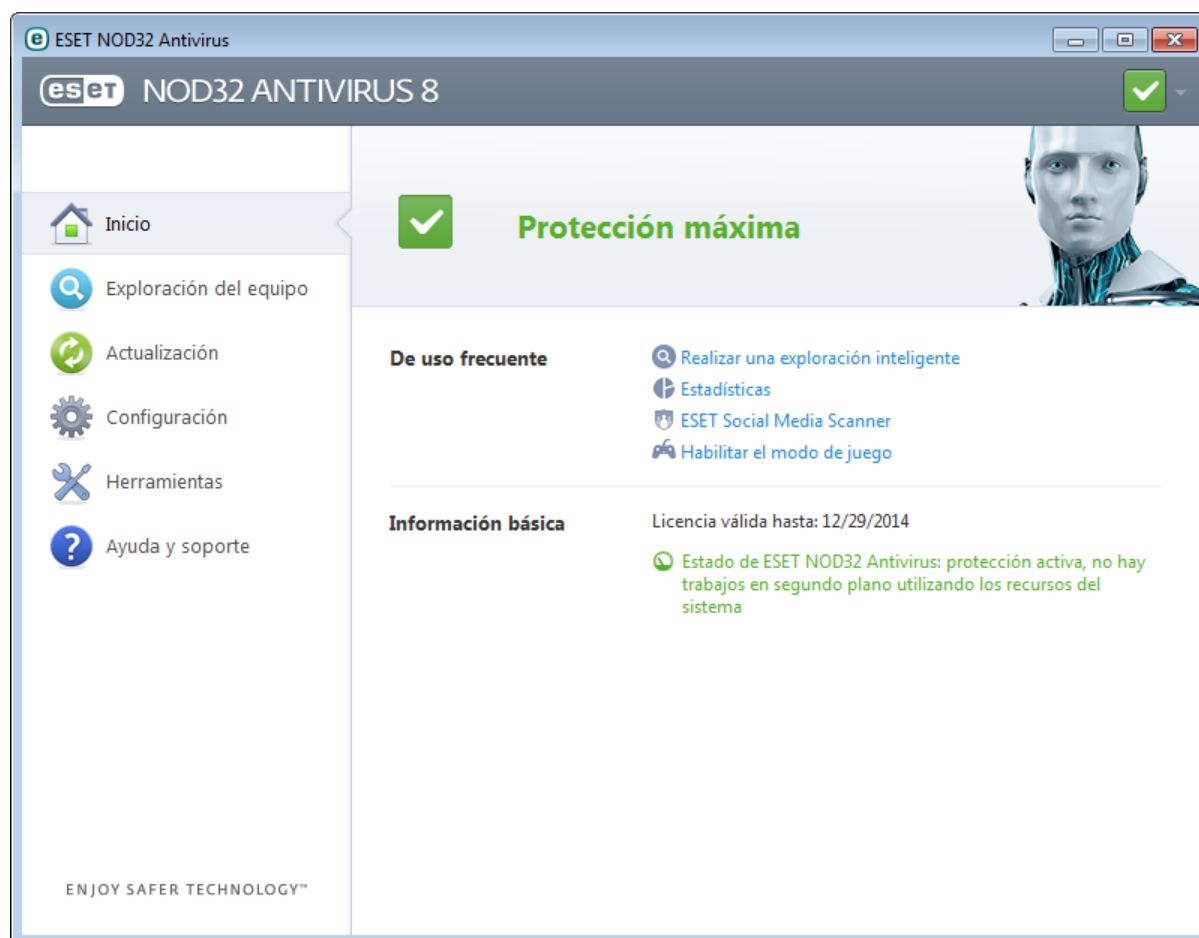
Exploración del equipo: esta opción permite configurar y ejecutar la Exploración inteligente o la Exploración personalizada.

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

Configuración: seleccione esta opción para ajustar el nivel de seguridad del equipo, de Internet y correo electrónico.

Herramientas: proporciona acceso a los archivos de registro, las estadísticas de protección, la visualización de la actividad, los procesos activos, las tareas programadas, ESET SysInspector y ESET SysRescue.

Ayuda y soporte: proporciona acceso a los archivos de ayuda, la [base de conocimiento de ESET](#), el sitio Web de ESET y los vínculos para abrir una solicitud de soporte a Atención al cliente.

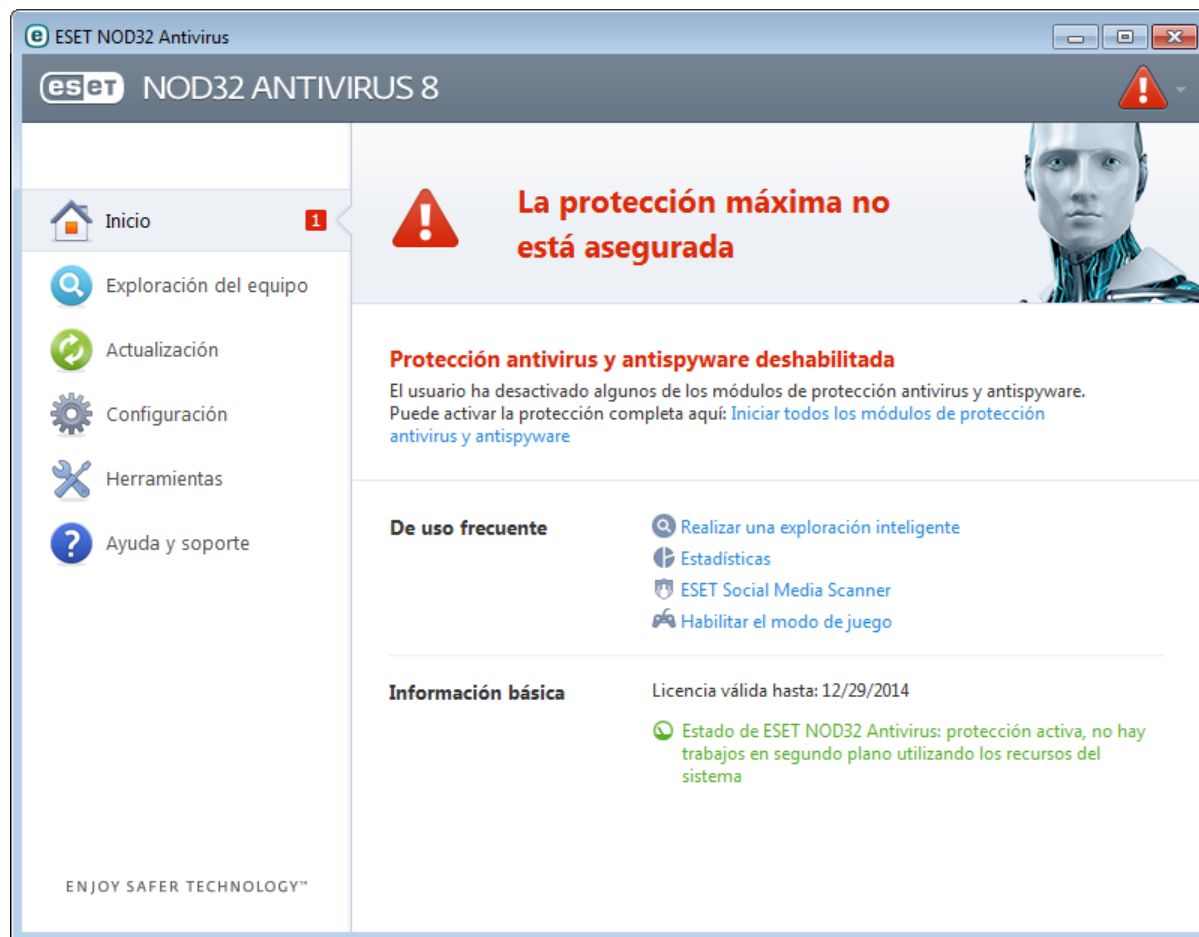



La pantalla **Inicio** le brinda información sobre el nivel de protección actual de su equipo y la seguridad. La ventana de estado también muestra las características de ESET NOD32 Antivirus utilizadas con mayor frecuencia. Aquí también se puede encontrar información sobre la fecha de vencimiento del programa en **Información básica**.

 El ícono verde y el estado de **Protección máxima** verde indican que la máxima protección está asegurada.


¿Qué hacer si el programa no funciona correctamente?

Si los módulos habilitados funcionan correctamente, el ícono de estado de protección será verde. Un signo de exclamación rojo o una notificación naranja indican que no se asegura el máximo nivel de protección. Visualizará información adicional sobre el estado de protección de cada módulo y soluciones sugeridas para restaurar la protección total en **Inicio**. Para cambiar el estado de un módulo individual, haga clic en **Configuración** y seleccione el módulo deseado.



 El ícono rojo y el estado rojo No se asegura la máxima protección indican que hay problemas críticos. Existen varios motivos por los cuales se puede mostrar este estado, por ejemplo:

- **Producto no activado:** puede activar ESET NOD32 Antivirus desde **Inicio** mediante un clic en **Activar producto** o en **Comprar ahora** debajo del estado de protección.
- **La base de datos de firmas de virus está desactualizada:** este error aparecerá luego de varios intentos insatisfactorios de actualizar la base de datos de firmas de virus. Es recomendable verificar la configuración de la actualización. El motivo más común de este error es el ingreso incorrecto de los [datos de autenticación](#) o la configuración incorrecta de las [opciones de conexión](#).
- **Protección antivirus y antispyware deshabilitada:** puede volver a activar la protección antivirus y antispyware mediante un clic en **Iniciar todos los módulos de protección antivirus y antispyware**.
- **La licencia está vencida:** se indica mediante un ícono rojo de estado de protección. Una vez que se vence la licencia, el programa no se podrá actualizar. Es recomendable seguir las instrucciones en la ventana de alerta para renovar la licencia.

 El ícono naranja indica que la protección de su equipo es limitada. Por ejemplo, hay un problema con la actualización del programa o en poco tiempo se cumplirá la fecha de vencimiento de la licencia. Existen varios motivos posibles por los cuales se puede mostrar este estado, por ejemplo:

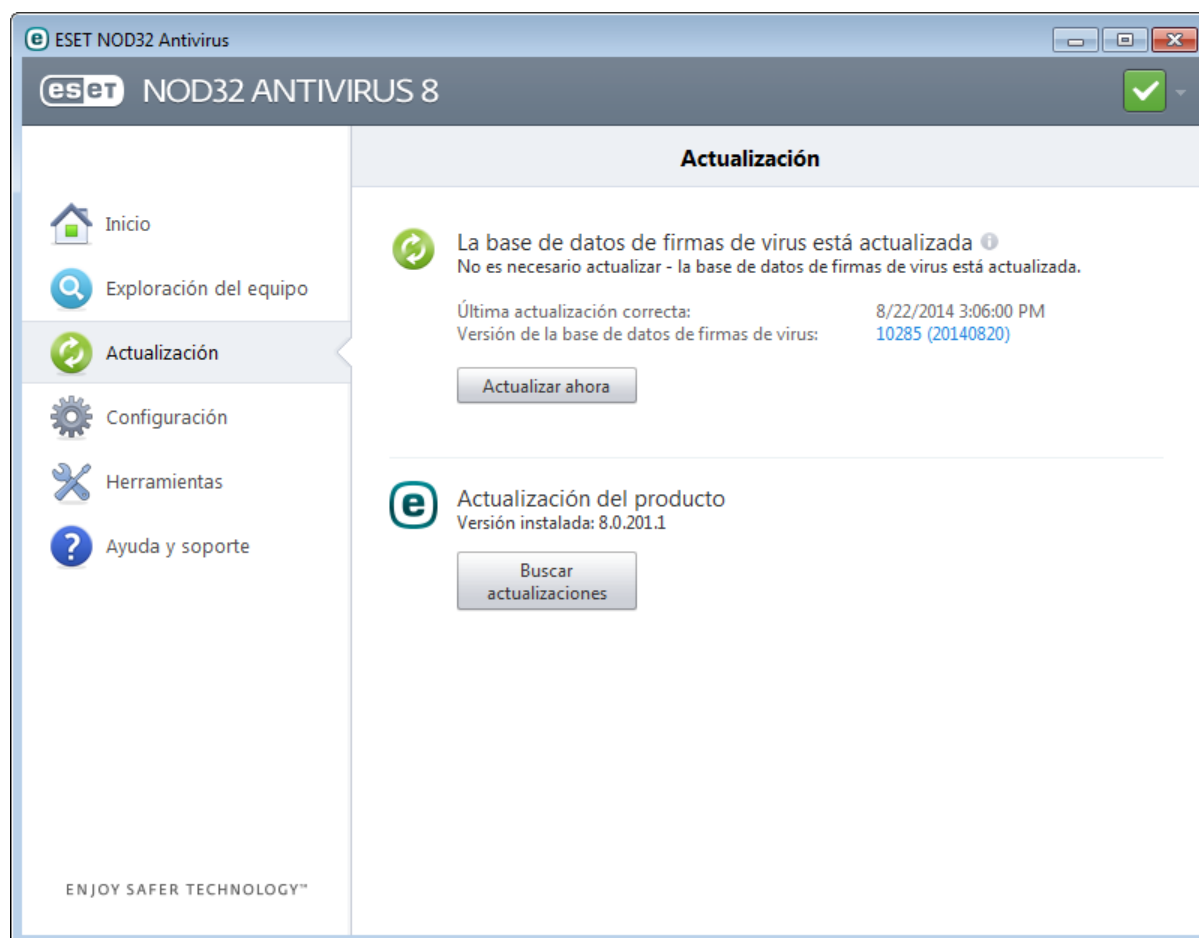
- **Advertencia de optimización de Anti-Theft:** este dispositivo no se encuentra optimizado para ESET Anti-Theft. Por ejemplo, una cuenta fantasma no existe inicialmente, pero es una característica de seguridad que se activa automáticamente cuando marca un dispositivo como perdido. Es posible que necesite crear una cuenta fantasma utilizando la característica [Optimización](#) en la interfaz web de ESET Anti-Theft.
- **Modo de juego habilitado:** activar el [Modo de juego](#) es un riesgo potencial en la seguridad. Al habilitar esta característica, todas las ventanas emergentes se deshabilitan y la actividad de las tareas programadas se detiene por completo.
- **La licencia se vencerá pronto:** se indica mediante un ícono de estado de protección y un signo de exclamación junto al reloj del sistema. Una vez que se vence la licencia, el programa no podrá actualizarse y el ícono de estado de protección se pondrá rojo.

Si no puede solucionar el problema mediante las sugerencias, haga clic en **Ayuda y soporte** para acceder a los archivos de ayuda o buscar en la [base de conocimiento de ESET](#). Si aún necesita asistencia, puede enviar una petición de soporte. El servicio de atención al cliente de ESET responderá rápidamente a sus preguntas y lo ayudará a encontrar una resolución.

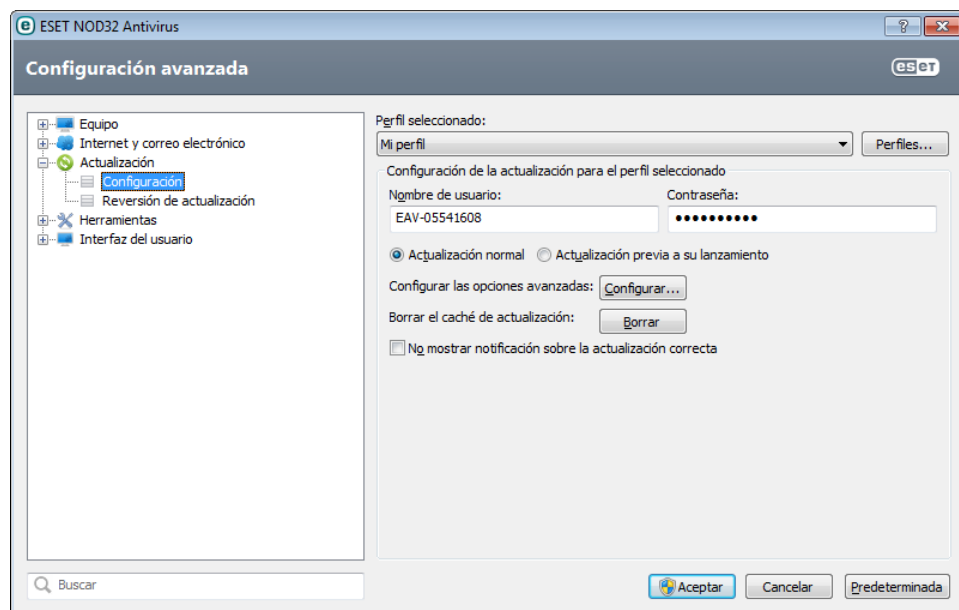
3.2 Actualizaciones

La actualización de la base de datos de firmas de virus, así como la actualización de componentes del programa, constituye una parte fundamental para proteger su sistema contra códigos maliciosos. Preste atención a su configuración y funcionamiento. Desde el menú principal, haga clic en **Actualización** y luego en **Actualizar ahora** para verificar si hay una actualización de la base de datos de firmas de virus.

Si el nombre de usuario y la contraseña no se ingresaron durante la activación de ESET NOD32 Antivirus, el programa se los pedirá en este momento.

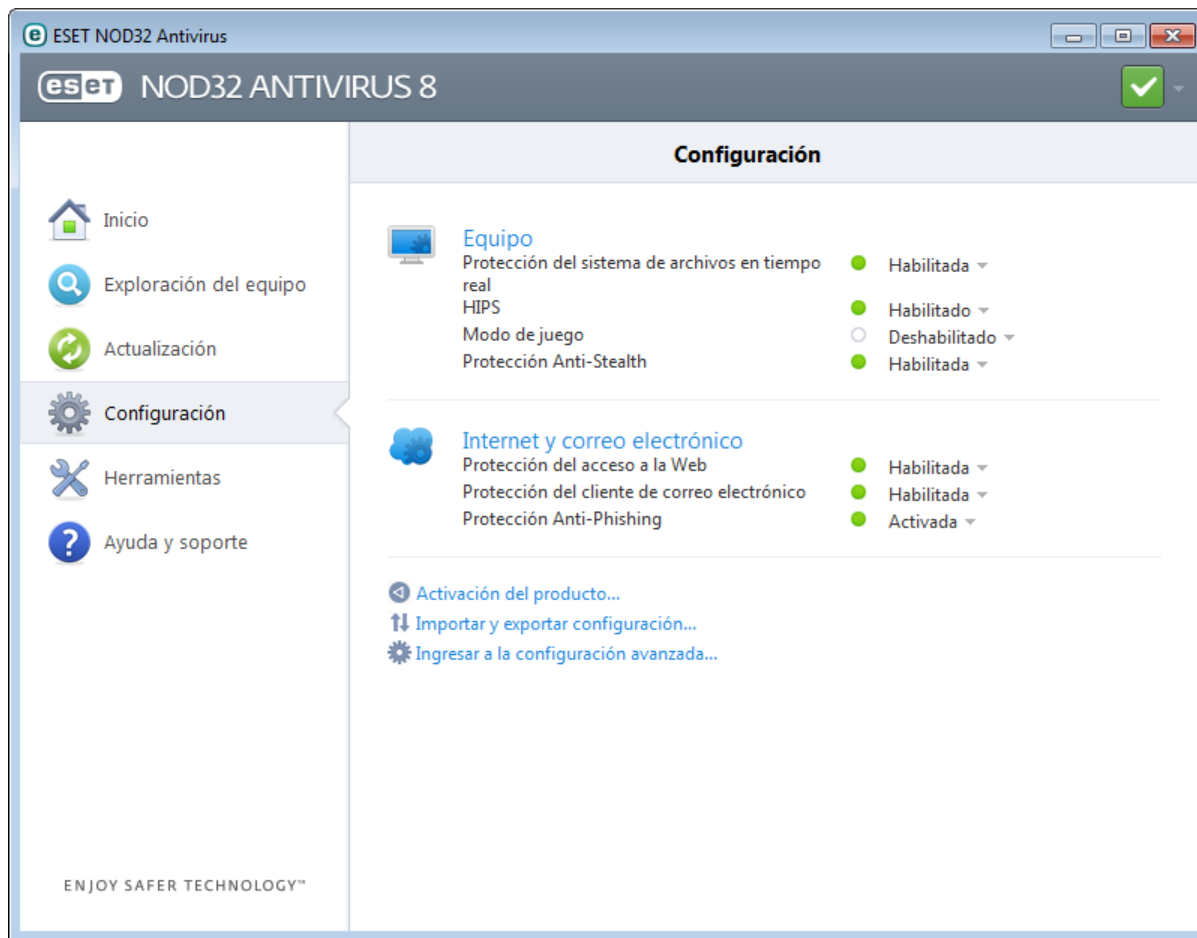


La ventana de configuración avanzada (haga clic en **Configuración** en el menú principal y luego en **Ingresar a la configuración avanzada...**, o presione la tecla **F5** del teclado) contiene opciones adicionales de actualización. Haga clic en **Actualización > Configuraciones** en el árbol de configuración avanzada a la izquierda. Para configurar las opciones avanzadas de actualización, como el modo de actualización, el acceso al servidor proxy y las conexiones de la LAN, haga clic en el botón **Configurar...** en la ventana **Actualizar**.



4. Trabajar con ESET NOD32 Antivirus

Las opciones de configuración de ESET NOD32 Antivirus permiten ajustar los niveles de protección de su equipo.



El menú **Configuración** contiene lo siguiente:

- **Equipo**
- **Internet y correo electrónico**

Haga clic en cualquiera de los componentes para ajustar la configuración avanzada del módulo de protección correspondiente.

La configuración de la protección del **Equipo** permite habilitar o deshabilitar los siguientes componentes:

- **Protección del sistema de archivos en tiempo real:** se exploran todos los archivos en busca de códigos maliciosos cuando se abren, crean o ejecutan en el equipo.
- **HIPS:** [HIPS](#) monitorea los sucesos dentro del sistema operativo y reacciona a ellos según un grupo de reglas personalizado.
- **Modo de juego:** habilita o deshabilita el [Modo de juego](#). Tras habilitar el modo de juego, recibirá un mensaje de advertencia (riesgo potencial en la seguridad) y la ventana principal se pondrá de color naranja.
- **Protección Anti-Stealth:** detecta programas peligrosos, como [rootkits](#), que tienen la capacidad de ocultarse del sistema operativo y de las técnicas de evaluación comunes.

La configuración de la protección de **Internet y correo electrónico** permite habilitar o deshabilitar los siguientes componentes:

- **Protección del acceso a la Web:** si se encuentra habilitada, todo el tráfico que pase a través de HTTP o HTTPS se explora en busca de software malicioso.
- **Protección del cliente de correo electrónico:** monitorea las comunicaciones recibidas a través de los protocolos POP3 e IMAP.
- **Protección antiphishing:** filtra los sitios Web sospechosos de distribuir contenido que manipulan a los usuarios para que envíen información confidencial.

Para volver a habilitar la protección del componente de seguridad deshabilitado, haga clic en **Deshabilitado** y luego en **Habilitar**.

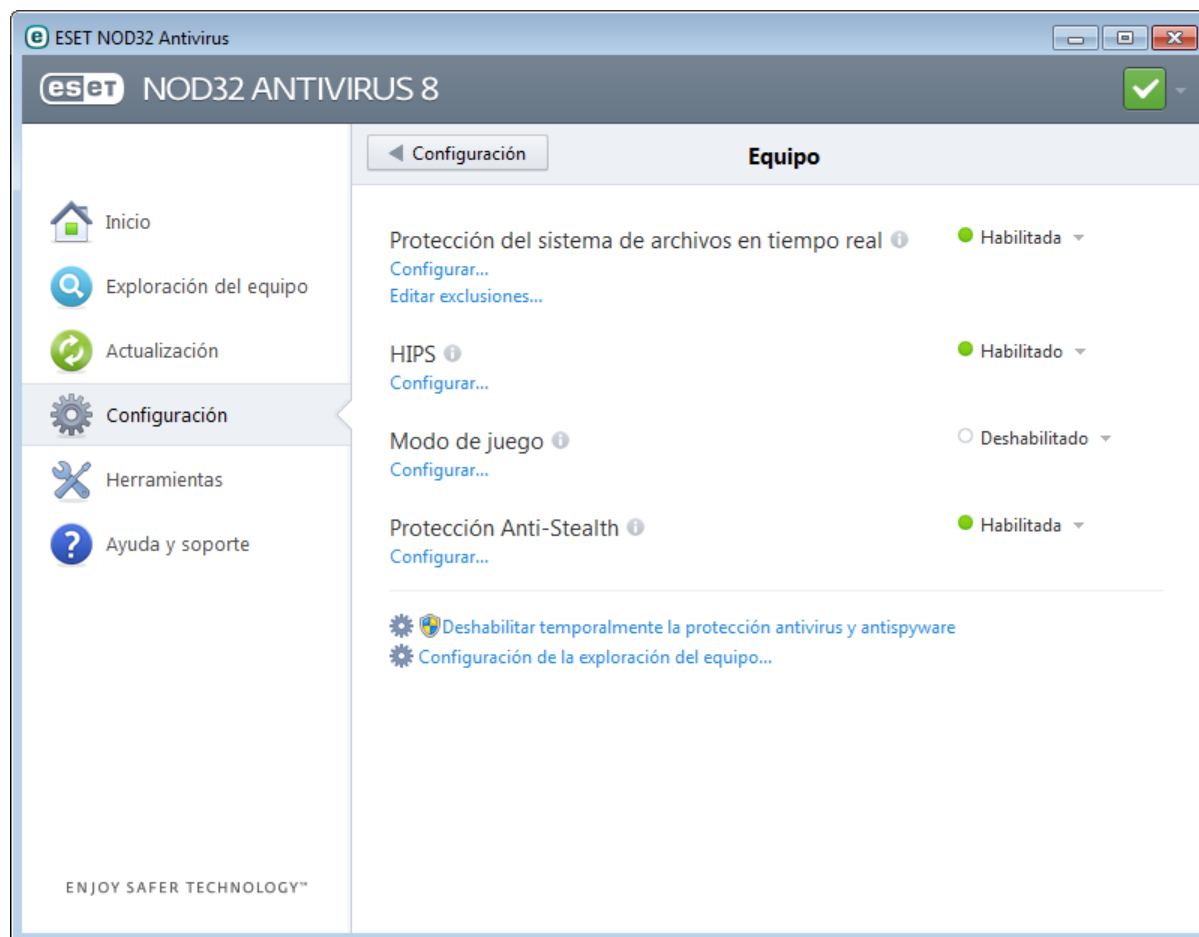
NOTA: Al deshabilitar la protección con este método, todas las partes de la protección deshabilitadas se volverán a habilitar tras reiniciar el equipo.

Hay opciones adicionales en la parte inferior de la ventana de configuración. Utilice el vínculo **Activación del producto...** para abrir un formulario de registro que activará su producto de seguridad de ESET y le enviará un correo electrónico con sus datos de autenticación (nombre de usuario y contraseña). Para cargar los parámetros de configuración desde un archivo de configuración *.xml* o para guardar los parámetros de configuración actuales en un archivo de configuración, utilice la opción **Importar y exportar una configuración...**

4.1 Equipo

El módulo del **Equipo** se encuentra en el panel **Configuración** al hacer clic en el título **Equipo**. Muestra información general de todos los módulos de protección. Para desactivar los módulos individuales temporalmente, haga clic en **Habilitado > Deshabilitar durante...** junto al módulo deseado. Tenga en cuenta que esto puede disminuir el nivel de protección del equipo. Para acceder a la configuración detallada de cada módulo, haga clic en **Configurar...**

Haga clic en **Editar exclusiones...** para abrir la ventana de configuración [Exclusión](#), que permite excluir archivos y carpetas de la exploración.



Deshabilitar temporalmente la protección antivirus y antispyware: deshabilita todos los módulos de protección antivirus y antispyware. Cuando deshabilita la protección, se abre la ventana **Deshabilitar temporalmente la protección** desde donde podrá determinar durante cuánto tiempo estará deshabilitada la protección al seleccionar un valor del menú desplegable **Intervalo de tiempo**. Haga clic en **Aceptar** para confirmar.

Configurar la exploración del equipo...: haga clic aquí para ajustar los parámetros del módulo de exploración bajo demanda (la exploración ejecutada en forma manual).

4.1.1 Antivirus y antispyware

La protección antivirus y antispyware defiende el sistema ante ataques maliciosos mediante el control de archivos, correos electrónicos y comunicaciones por Internet. Si se detecta una amenaza con códigos maliciosos, el módulo antivirus la puede eliminar en primer lugar bloqueándola y luego desinfectándola, eliminándola o enviándola a cuarentena.

Las opciones del módulo de exploración para todos los módulos de protección (por ej., la protección del sistema de archivos en tiempo real o la protección del acceso a la Web) permiten habilitar o deshabilitar la detección de lo siguiente:

- **Aplicaciones potencialmente no deseadas:** estas aplicaciones no tienen necesariamente la intención de ser maliciosas, pero pueden afectar el rendimiento de su equipo en forma negativa.

Lea más información sobre estos tipos de aplicaciones en el [glosario](#).

- **Aplicación potencialmente no segura:** hace referencia al software comercial y legítimo que puede utilizarse inadecuadamente para fines maliciosos. Algunos ejemplos de las aplicaciones potencialmente inseguras son las herramientas de acceso remoto, aplicaciones para adivinar contraseñas y registradores de pulsaciones (programas que registran cada tecla pulsada por el usuario). La opción se encuentra deshabilitada en forma predeterminada. Lea más información sobre estos tipos de aplicaciones en el [glosario](#).
- **Aplicaciones potencialmente sospechosas:** incluyen programas comprimidos con [empaquetadores](#) o protectores. Estos tipos de protectores por lo general son vulnerados por autores de malware para evadir la detección.

La tecnología Anti-Stealth es un sistema sofisticado que proporciona la detección de programas peligrosos como los [rootkits](#), que tienen la capacidad de ocultarse del sistema operativo. Esto significa que no es posible detectarlos mediante técnicas de evaluación comunes.

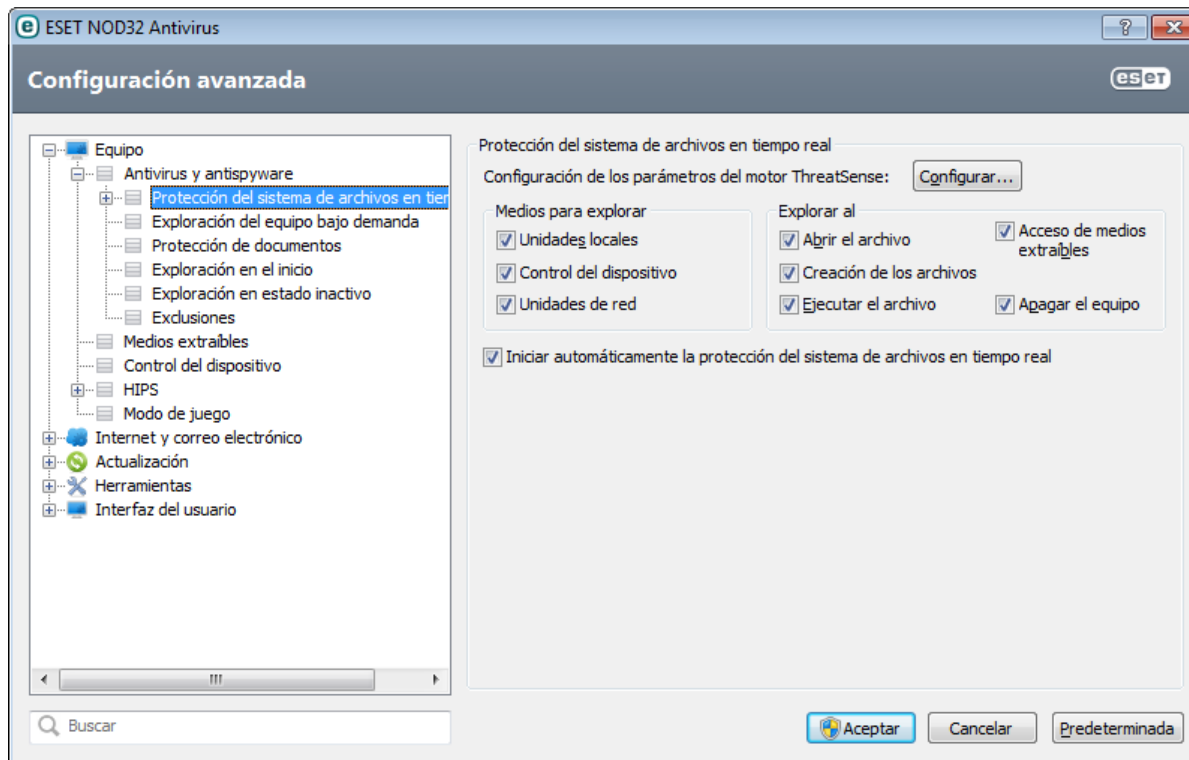
4.1.1.1 Protección del sistema de archivos en tiempo real

La protección del sistema de archivos en tiempo real controla todos los sucesos del sistema relacionados con el antivirus. Se exploran todos los archivos en busca de códigos maliciosos cuando se abren, crean o ejecutan en el equipo. La protección del sistema de archivos en tiempo real se activa junto con el inicio del sistema.

La protección del sistema de archivos en tiempo real verifica todos los tipos de medios y el control se acciona por diversos sucesos, como el acceso a un archivo. Al usar los métodos de detección de la tecnología ThreatSense (descritos en la sección titulada [Configuración de los parámetros del motor ThreatSense](#)), la protección del sistema de archivos en tiempo real puede configurarse para tratar nuevos archivos creados de modo diferente a los ya existentes. Por ejemplo, puede configurar la protección del sistema de archivos en tiempo real para controlar más de cerca a los nuevos archivos creados.

Para asegurar el mínimo impacto en el sistema al usar la protección en tiempo real, los archivos que ya se exploraron no se vuelven a explorar reiteradamente (a menos que se hayan modificado). Los archivos se vuelven a explorar de inmediato luego de cada actualización de la base de datos de firmas de virus. Este comportamiento se configura mediante el uso de la **Optimización inteligente**. Si esta característica está deshabilitada, se explorarán todos los archivos cada vez que se accede a ellos. Si desea modificar esta opción, presione la tecla **F5** para abrir la ventana Configuración avanzada y expanda **Equipo > Antivirus y antispyware > Protección del sistema de archivos en tiempo real**. Haga clic en **Configurar...** junto a la **Configuración de los parámetros del motor ThreatSense > Otros** y seleccione o anule la selección de la opción **Habilitar la optimización inteligente**.

En forma predeterminada, la protección del sistema de archivos en tiempo real se activa junto con el inicio del sistema y proporciona una exploración ininterrumpida. En casos especiales (por ejemplo, si existe un conflicto con otro explorador en tiempo real), se puede deshabilitar la protección en tiempo real anulando la selección **Iniciar automáticamente la protección del sistema de archivos en tiempo real** en la sección **Protección del sistema de archivos en tiempo real** de la Configuración avanzada.



Medios para explorar

En forma predeterminada, todos los tipos de medios se exploran en busca de amenazas potenciales:

Unidades locales: controla todos los discos rígidos del sistema.

Control del dispositivo: CD/DVD, dispositivos de almacenamiento USB, etc.

Unidades de red: explora todas las unidades asignadas.

Es recomendable conservar la configuración predeterminada y solo modificarla en casos específicos, por ej., si al explorar ciertos medios, se ralentizan significativamente las transferencias de archivos.

Exploración accionada por un suceso

En forma predeterminada, se exploran todos los archivos cuando se abren, crean o ejecutan. Se recomienda mantener estas configuraciones predeterminadas, ya que proveen el máximo nivel de protección en tiempo real del equipo:

- **Abrir el archivo:** habilita o deshabilita la exploración de los archivos abiertos.
- **Crear el archivo:** habilita o deshabilita la exploración de los nuevos archivos creados o modificados.
- **Ejecutar el archivo:** habilita o deshabilita la exploración de los archivos ejecutados.
- **Acceso de medios extraíbles:** habilita o deshabilita la exploración activada al acceder a medios extraíbles particulares con espacio de almacenamiento.
- **Apagar el equipo:** habilita o deshabilita la exploración accionada por el apagado del equipo.

4.1.1.1.1 Opciones avanzadas de exploración

Se pueden encontrar opciones de configuración más detalladas en **Equipo > Antivirus y antispyware > Protección del sistema de archivos en tiempo real > Configuración avanzada**.

Parámetros de ThreatSense adicionales para archivos creados o modificados recientemente.

La probabilidad de infección de archivos recientemente creados o modificados es comparativamente más alta que en archivos existentes. Por ese motivo, el programa verifica esos archivos con parámetros adicionales de exploración. Junto con los métodos de exploración basados en firmas, también se usa la heurística avanzada, que es capaz de detectar las nuevas amenazas antes del lanzamiento de la actualización de la base de datos de firmas de virus. Además de los archivos recientemente creados, también se exploran los **archivos de autoextracción** (.sfx) y los **empaquetadores de tiempo de ejecución** (archivos ejecutables comprimidos internamente). En forma predeterminada, los archivos comprimidos se exploran hasta el décimo nivel de anidado y se verifican

independientemente de su tamaño real. Para modificar la configuración de la exploración de archivos comprimidos, anule la selección de **Configuración predeterminada para la exploración de archivos comprimidos**.

Parámetros adicionales de ThreatSense para los archivos ejecutados

- **Heurística avanzada para la ejecución de archivos** de forma predeterminada, se utiliza [Heurística avanzada](#) cuando se ejecutan los archivos. Cuando está habilitada, recomendamos firmemente mantener la [Optimización inteligente](#) y el ESET Live Grid habilitados para mitigar el impacto en el rendimiento del sistema.
- **Heurística avanzada al ejecutar archivos de medios extraíbles** si desea excluir ciertos puertos de medios extraíbles (USB) de la exploración con heurística avanzada para los archivos ejecutados, haga clic en **Excepciones...** para abrir la ventana de exclusiones correspondiente a las unidades de medios extraíbles. Desde esta ventana, puede modificar la configuración mediante la selección o la anulación de la selección de las casillas de verificación que representan a cada puerto.

4.1.1.1.2 Niveles de desinfección

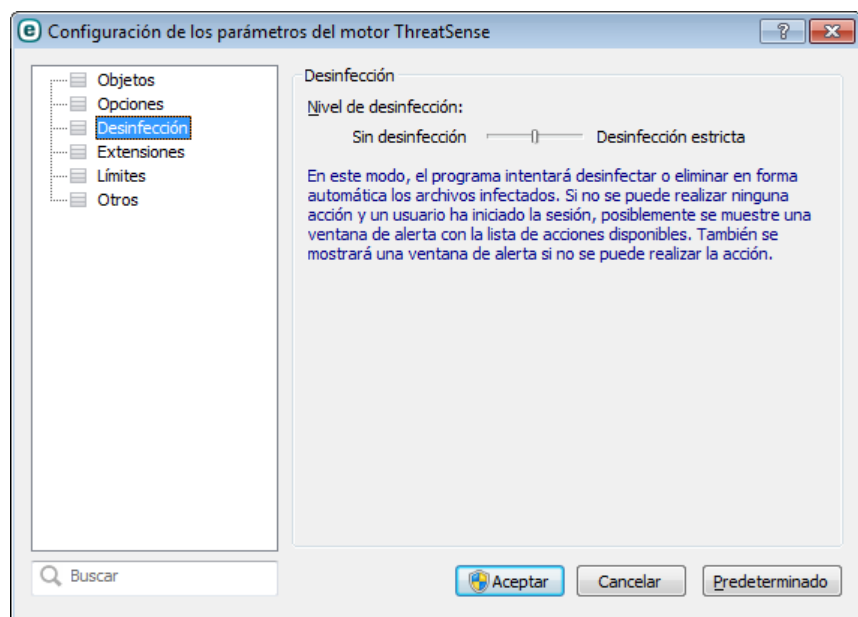
La protección en tiempo real tiene tres niveles de desinfección (para acceder, haga clic en **Configurar...** en la sección **Protección del sistema de archivos en tiempo real** y luego haga clic en la sección **Desinfección**).

Sin desinfección: los archivos infectados no se desinfectan automáticamente. El programa mostrará una ventana de advertencia y le permitirá al usuario que seleccione una acción. Este nivel está diseñado para los usuarios más avanzados que conocen los pasos a seguir en caso de detectar una infiltración.

Desinfección estándar: el programa intentará desinfectar o eliminar el archivo infectado automáticamente basándose en una acción predefinida (dependiendo del tipo de infiltración). La detección y eliminación de un archivo infectado se marca con una notificación en la esquina inferior derecha de la pantalla. Si no es posible seleccionar la acción correcta en forma automática, el programa ofrece otras acciones que se pueden realizar. Ocurre lo mismo cuando no es posible completar una acción predefinida.

Desinfección estricta: el programa desinfectará o eliminará todos los archivos infectados. Las únicas excepciones son los archivos del sistema. Si no es posible desinfectarlos, el programa le ofrecerá una acción al usuario en una ventana de advertencia.

Advertencia: Si un archivo comprimido contiene un archivo o varios archivos infectados, existen dos opciones para tratarlo. En el modo estándar (Desinfección estándar), se eliminará el archivo comprimido completo cuando todos los archivos que incluya estén infectados. En el modo de **Desinfección estricta**, el archivo comprimido se eliminará si al menos contiene un archivo infectado, sin importar el estado de los demás archivos que lo componen.



4.1.1.1.3 Cuándo modificar la configuración de la protección en tiempo real

La protección en tiempo real es el componente más imprescindible para mantener un sistema seguro. Siempre sea precavido al modificar sus parámetros. Recomendamos modificar los parámetros únicamente en casos específicos.

Luego de la instalación de ESET NOD32 Antivirus, todas las configuraciones se optimizan para proporcionar el máximo nivel de seguridad del sistema para los usuarios. Para restaurar la configuración predeterminada, haga clic en **Predeterminado** ubicado en el extremo inferior derecho de la ventana **Protección del sistema de archivos en tiempo real (Configuración avanzada > Equipo > Antivirus y antispyware > Protección del sistema de archivos en tiempo real)**.

4.1.1.1.4 Verificación de la protección en tiempo real

Para verificar que la protección en tiempo real se encuentra activa y es capaz de detectar virus, use un archivo de prueba de eicar.com. Este archivo de prueba es un archivo inofensivo, al que detectan todos los programas antivirus. El archivo fue creado por la empresa EICAR (Instituto Europeo para la Investigación de los Antivirus Informáticos, por sus siglas en inglés) para comprobar la eficacia de los programas antivirus. El archivo está disponible para su descarga desde <http://www.eicar.org/download/eicar.com>.

4.1.1.1.5 Qué hacer si la protección en tiempo real no funciona

En esta sección, se describirán problemas que se pueden presentar al utilizar la protección en tiempo real y se indicará cómo resolverlas.

La protección en tiempo real está deshabilitada

Si un usuario deshabilitó la protección en tiempo real sin darse cuenta, será necesario volver a activarla. Para reactivar 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 la protección en tiempo real no se activa durante el inicio del sistema, es posible que se deba a que **Iniciar automáticamente la protección del sistema de archivos en tiempo real** no está seleccionada. Para habilitar esta opción, vaya a Configuración avanzada (F5) y haga clic en **Equipo > Antivirus y antispyware > Protección del sistema de archivos en tiempo real** en el árbol de configuración avanzada. En la sección **Configuración avanzada** en la parte inferior de la ventana, asegúrese de que la casilla de verificación **Iniciar automáticamente la protección del sistema de archivos en tiempo real** esté seleccionada.

Si la protección en tiempo real no detecta ni desinfecta infiltraciones

Asegúrese de que no haya otros programas antivirus instalados en el equipo. Si están habilitados dos escudos de protección en tiempo real al mismo tiempo, es posible que entren en conflicto. Es recomendable desinstalar 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 durante el inicio del sistema (e **Iniciar automáticamente la protección del sistema de archivos en tiempo real** está habilitada), es posible que se deba a la existencia de conflictos con otros programas. Para obtener asistencia para resolver este problema, comuníquese con Atención al cliente de ESET.

4.1.1.2 Exploración del equipo

El módulo de exploración bajo demanda es una parte importante de la solución antivirus. Se usa para realizar la exploración de los archivos y las carpetas del equipo. Desde el punto de vista de la seguridad, es esencial que las exploraciones del equipo no se ejecuten solo cuando existen sospechas de una infección, sino en forma habitual como parte de una medida de seguridad de rutina. Es recomendable realizar habitualmente exploraciones profundas del sistema para detectar los virus que la **Protección del sistema de archivos en tiempo real** no capturó cuando se guardaron en el disco. Esta situación puede ocurrir si la protección del sistema de archivos en tiempo real no estaba habilitada en el momento, si la base de datos de virus no estaba actualizada o si el archivo no se detecta como un virus cuando se guarda en el disco.

Se encuentran disponibles dos tipos de **Exploración del equipo**. **Exploración inteligente** explora rápidamente el

sistema sin necesidad de realizar configuraciones adicionales de los parámetros de exploración. **Exploración personalizada** permite seleccionar perfiles de exploración predefinidos diseñados para determinadas ubicaciones de objetos, y también permite elegir objetos de exploración puntuales.

Exploración inteligente

La exploración inteligente permite iniciar rápidamente una exploración del equipo y desinfectar los archivos infectados sin necesidad de la intervención del usuario. La ventaja de la exploración inteligente es su facilidad de uso y que no requiere una configuración detallada de la exploración. La exploración inteligente verifica todos los archivos de las unidades locales y desinfecta o elimina en forma automática las infiltraciones detectadas. El nivel de desinfección está establecido automáticamente en el valor predeterminado. Para obtener información más detallada sobre los tipos de desinfección, consulte Desinfección.

Exploración personalizada

La exploración personalizada permite especificar parámetros de exploración, como los objetos o métodos de exploración. La ventaja de la exploración personalizada es la capacidad de configurar los parámetros detalladamente. Es posible guardar las configuraciones en perfiles de exploración definidos por el usuario, lo que resulta útil si la exploración se efectúa reiteradamente con los mismos parámetros.

Exploración de medios extraíbles

Es similar a la exploración inteligente: inicia rápidamente una exploración de los medios extraíbles (por ej., CD/DVD/USB) que estén conectados al equipo en ese momento. Puede ser útil cuando conecta al equipo una unidad flash USB y desea explorar sus contenidos en busca de posible malware y otras amenazas potenciales.

Este tipo de exploración también puede iniciarse al hacer clic en **Exploración personalizada**, luego en **Medios extraíbles** del menú desplegable de **Objetos para explorar** y por último en **Explorar**.

Para obtener más información sobre el proceso de la exploración, consulte [Progreso de la exploración](#).

Se recomienda ejecutar una exploración del equipo al menos una vez al mes. La exploración se puede configurar como una tarea programada en **Herramientas > Tareas programadas**. ¿Cómo programar una exploración semanal del equipo?

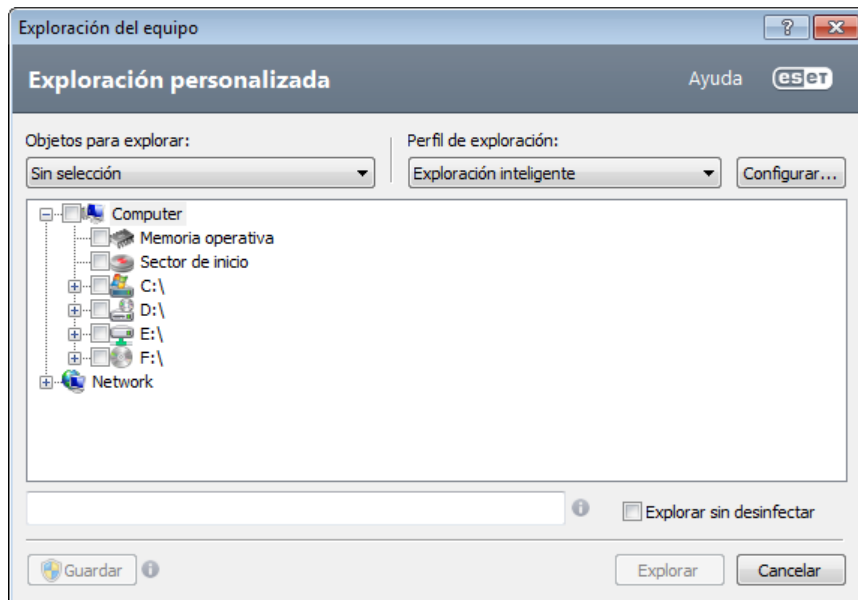
4.1.1.2.1 Iniciador de la exploración personalizada

Si no desea explorar todo el espacio en disco, sino solamente un objeto específico, puede usar la exploración personalizada haciendo clic en **Exploración del equipo > Exploración personalizada**. Luego elija una opción del menú desplegable **Objetos para explorar**, o bien seleccione los objetos específicos desde la estructura de árbol.

La ventana para explorar los objetos le permite definir los objetos (memoria, unidades, sectores, archivos y carpetas) que se explorarán en busca de infiltraciones. Seleccione los objetos desde la estructura con forma de árbol, que incluye la lista de todos los dispositivos disponibles en el equipo. El menú desplegable **Objetos para explorar** permite seleccionar los objetos predefinidos que se explorarán.

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

Para ir rápidamente hasta un objeto para explorar o para agregar en forma directa un objeto para explorar (carpeta o archivos), ingréselo en el campo vacío debajo de la lista de carpetas. Esta acción solo será posible si no se seleccionó ningún objeto para explorar en la estructura con forma de árbol y el menú **Objetos para explorar** está configurado en **Sin selección**.



Los elementos infectados no se desinfectan automáticamente. Puede usar la exploración sin desinfección cuando desee obtener una visión general del estado actual de la protección. Si solo le interesa explorar el sistema sin realizar acciones adicionales de desinfección, seleccione **Explorar sin desinfectar**. Además, puede elegir entre tres niveles de desinfección si hace un clic en **Configurar... > Desinfección**. La información sobre la exploración se guarda en un registro de exploración.

En el menú desplegable **Perfil de exploración**, puede elegir un perfil que podrá usar con los objetos para explorar seleccionados. El perfil predeterminado es **Exploración inteligente**. Hay otros dos perfiles de exploración predefinidos denominados **Exploración profunda** y **Exploración del menú contextual**. Estos perfiles de exploración usan diferentes [parámetros del motor ThreatSense](#). Haga clic en el botón **Configurar...** para establecer detalladamente el perfil de exploración seleccionado desde el menú de perfiles de exploración. Las opciones disponibles se describen en [Configuración del módulo de exploración](#).

Guardar: para guardar los cambios realizados en su selección de objetos, incluyendo las selecciones hechas dentro de la carpeta con estructura en forma de árbol.

Haga clic en **Explorar** para ejecutar la exploración con los parámetros personalizados establecidos.

Explorar como administrador permite ejecutar la exploración desde una cuenta de administrador. Haga clic en esta opción si el usuario actual no tiene los privilegios necesarios para acceder a los archivos apropiados que se van a explorar. Tenga en cuenta que este botón no está disponible si el usuario actual no puede realizar operaciones UAC como administrador.

4.1.1.2.2 Progreso de la exploración

La ventana de progreso de la exploración muestra el estado actual de la exploración junto con información sobre la cantidad detectada de archivos con códigos maliciosos.

NOTA: Es común que algunos archivos, como los archivos protegidos por contraseña o los que usa el sistema de manera exclusiva (habitualmente, archivos *pagefile.sys* y ciertos archivos de registro), no se puedan explorar.

La barra de progreso muestra el porcentaje de objetos ya explorados en comparación con los objetos que aún faltan explorar. Este valor proviene de la cantidad total de objetos incluidos en una exploración.

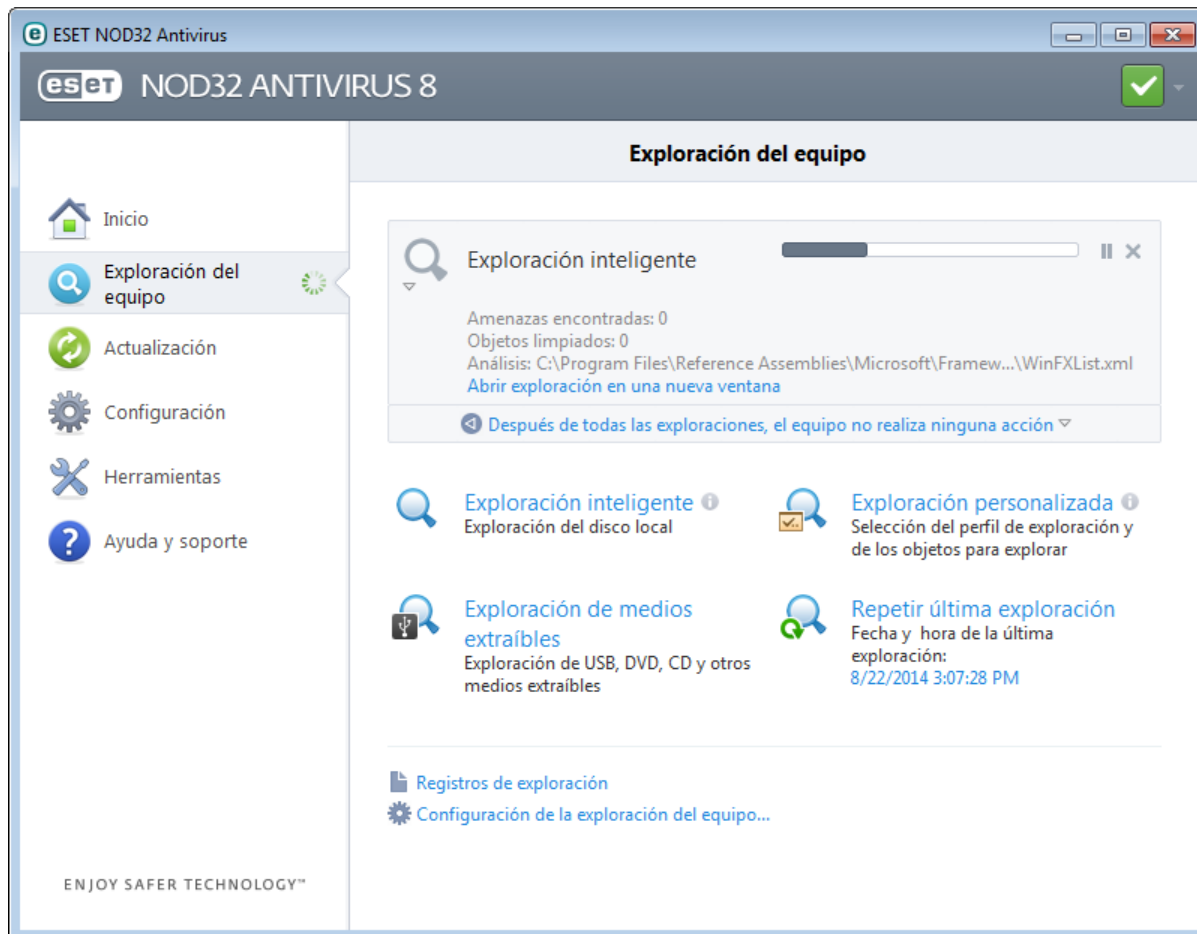
Sugerencias:

Haga clic en la lupa o flecha para mostrar los detalles sobre la exploración actualmente en ejecución.

Si desea ejecutar una exploración en paralelo, haga clic en **Exploración inteligente** o **Exploración personalizada...**

Objetos: muestra la cantidad total de archivos explorados, de amenazas encontradas y de amenazas eliminadas durante una exploración.

Destino: el nombre del objeto actualmente explorado.



El equipo no realiza ninguna acción al completarse todas las exploraciones: acciona un apagado o reinicio programado al finalizar la exploración del equipo. Al concluir la exploración, se abrirá una ventana de diálogo para confirmar el apagado con un tiempo de espera de 60 segundos. Haga clic en esta opción nuevamente para desactivar la acción seleccionada.

4.1.1.2.3 Perfiles de exploración

Es posible guardar los parámetros preferidos de exploración para usarlos en el futuro. Se recomienda crear un perfil distinto (con varios objetos para explorar, métodos de exploración y otros parámetros) para cada exploración utilizada regularmente.

Para crear un nuevo perfil, abra la ventana de configuración avanzada (F5) y haga clic en **Equipo > Antivirus y antispyware > Exploración del equipo bajo demanda > Perfiles...** La ventana **Perfiles de configuración** incluye el menú desplegable **Perfil seleccionado** que enumera los perfiles de exploración existentes así como la opción de crear uno nuevo. Para obtener ayuda sobre cómo crear un perfil de exploración acorde a sus necesidades, consulte la sección [Configuración de los parámetros del motor ThreatSense](#), donde obtendrá la descripción de cada parámetro de la configuración de la exploración.

Ejemplo: Suponga que desea crear su propio perfil de exploración y la configuración de la exploración inteligente es parcialmente adecuada, pero no desea explorar empaquetadores en tiempo real o aplicaciones potencialmente no seguras y además quiere aplicar una **Desinfección estricta**. En la ventana **Perfiles de configuración**, haga clic en el botón **Agregar...** Ingrese el nombre de su nuevo perfil en el campo **Nombre del perfil** y seleccione **Exploración inteligente** desde el menú desplegable **Copiar configuración desde el perfil**. Ajuste los parámetros restantes según sus necesidades y guarde su nuevo perfil.

4.1.1.3 Exploración en el inicio

En forma predeterminada, la exploración automática de archivos durante el inicio del sistema se realizará durante el inicio del sistema y durante la actualización de la base de datos de firmas de virus. Esta exploración depende de la [Configuración y de las tareas en Tareas programadas](#).

Las opciones de exploración en el inicio son parte de una tarea programada de **Verificación de archivos de inicio del sistema**. Para modificar sus configuraciones, navegue a **Herramientas > Tareas programadas**, haga clic en **Exploración automática de archivos durante el inicio del sistema** y en **Editar....** En el último paso, aparecerá la ventana [Exploración automática de archivos durante el inicio del sistema](#) (consulte el siguiente capítulo para obtener más detalles).

Para obtener instrucciones detalladas sobre la creación y administración de tareas programadas, consulte la Creación de tareas nuevas.

4.1.1.3.1 Verificación de archivos de inicio automática

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

El menú desplegable **Nivel de exploración** especifica la profundidad de la exploración para la ejecución de archivos al inicio del sistema. Los archivos se organizan en orden ascendente de acuerdo con el siguiente criterio:

- **Solo los archivos más frecuentemente utilizados** (los archivos menos explorados)
- **Archivos de uso frecuente**
- **Archivos comúnmente utilizados**
- **Archivos rara vez utilizados**
- **Todos los archivos registrados** (la mayoría de archivos explorados)

También se incluyen dos grupos específicos de **Nivel de exploración**:

- **Archivos que se ejecutan antes del registro del usuario:** contiene archivos de las ubicaciones a las que puede accederse sin que el usuario se registre (incluye casi todas las ubicaciones de inicio tales como servicios, objetos del ayudante de exploración, winlogon notify, entradas de las tareas programadas de ventanas, dlls conocidos, etc.).
- **Archivos que se ejecutan después del registro del usuario:** contiene archivos de las ubicaciones a las que puede accederse solo después de que un usuario se registre (incluye archivos que solo se ejecutan para un usuario específico, por lo general archivos en `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`).

Las listas de archivos a escanear son fijas para cada grupo antes mencionado.

Prioridad de exploración: el nivel de prioridad utilizado para determinar cuándo se iniciará una exploración:

- **Normal:** en una carga promedio del sistema
- **Inferior:** en una carga baja del sistema
- **Más baja:** cuando la carga del sistema es lo más baja posible
- **Cuando está inactivo:** la tarea se realizará solo cuando el sistema esté inactivo

4.1.1.4 Exploración en estado inactivo

La exploración en estado inactivo puede configurarse y habilitarse desde **Configuración avanzada en Equipo > Antivirus y antispyware > Exploración en estado inactivo**. Cuando el equipo está en estado inactivo, se realiza una exploración silenciosa en todas las unidades locales del equipo. Consulte [Detección en estado inactivo](#) para obtener una lista completa de condiciones que deben cumplirse para activar la exploración del estado inactivo.

De forma predeterminada, la exploración de estado inactivo no se accionará cuando el equipo (portátil) está funcionando con la energía de la batería. Puede anular esta configuración al seleccionar la casilla de verificación al lado de **Ejecutar incluso si el equipo recibe alimentación de la batería** en la Configuración avanzada.

Seleccione **Habilitar la creación de registros** en la Configuración avanzada para registrar el resultado de la

exploración del equipo en la sección [Archivos de registro](#) (desde la ventana principal del programa haga clic en **Herramientas > Archivos de registro** y seleccione **Exploración del equipo**, en el menú desplegable **Registro**).

El último ajuste aquí es la [configuración de los parámetros del motor de ThreatSense](#). Haga clic en **Configurar...** si desea modificar diversos parámetros de exploración (por ejemplo, los métodos de detección).

4.1.1.5 Exclusiones

Las exclusiones permiten excluir archivos y carpetas de la exploración. Para asegurarse de que todos los objetos se exploren en busca de amenazas, recomendamos únicamente crear exclusiones cuando sea absolutamente necesario. Sin embargo, existen situaciones donde es posible que necesite excluir un objeto, por ejemplo las entradas de una base de datos grande que podría reducir la velocidad de su equipo durante una búsqueda o software que entra en conflicto con la búsqueda.

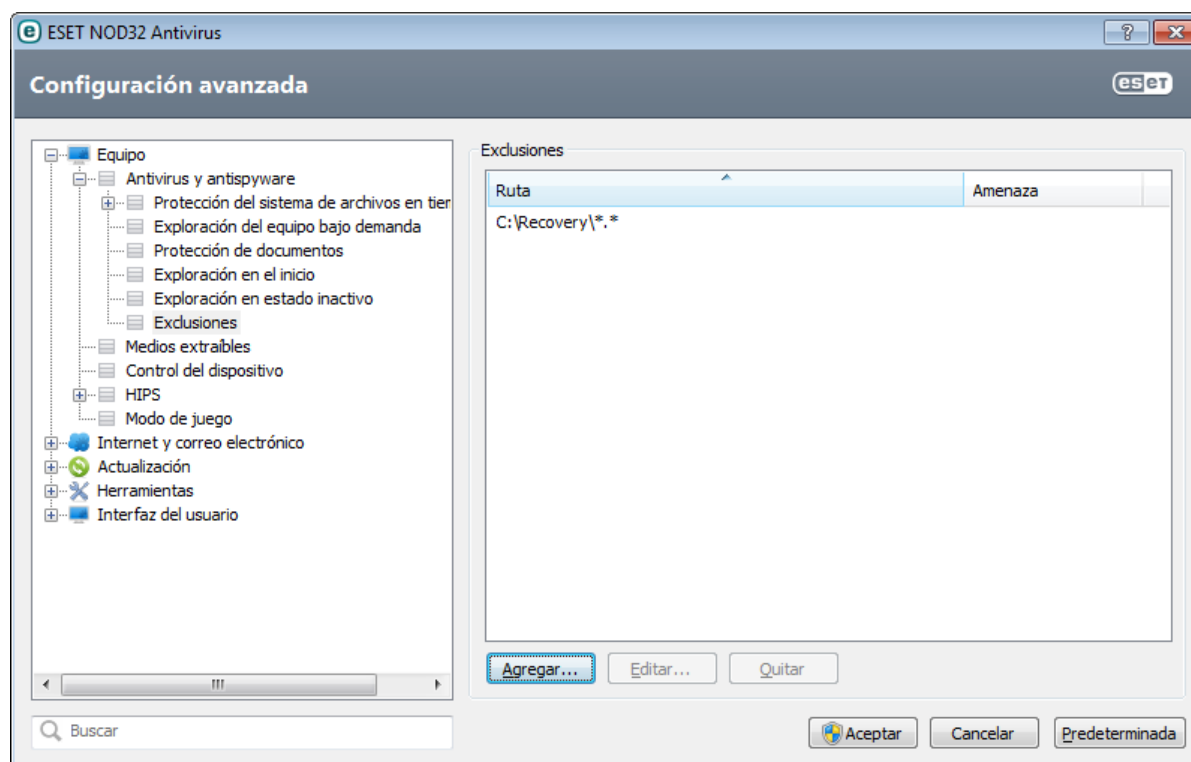
Para excluir un objeto de la exploración:

1. Haga clic en **Agregar...**,
2. Ingrese la ruta a un objeto o selecciónelo en la estructura con forma de árbol.

Puede utilizar caracteres globales para abarcar un grupo de archivos. Un signo de interrogación (?) representa un carácter único variable, mientras que un asterisco (*) representa una cadena variable de cero o más caracteres.

Ejemplos

- Si desea excluir todos los archivos en una carpeta, escriba la ruta a la carpeta y utilice la máscara `"*. *"`.
- Para excluir un disco completo incluyendo todos los archivos y subcarpetas, utilice la máscara `"D:*"`.
- Si solo desea excluir archivos doc, utilice la máscara `"*.doc"`.
- Si el nombre del archivo ejecutable tiene un número determinado de caracteres (que varían) y solo conoce el primero en forma segura (por ejemplo, "D"), utilice el siguiente formato: `"D?????.exe"`. Los símbolos de interrogación reemplazan a los caracteres faltantes (desconocidos).



Nota: Una amenaza dentro de un archivo no se detectará por el módulo de protección del sistema de archivos en tiempo real o módulo de exploración del equipo si un archivo cumple con los criterios para la exclusión de la exploración.

Ruta: ruta a los archivos y las carpetas excluidos.

Amenaza: si se pone el nombre de una amenaza al lado de un archivo excluido, significa que el archivo solo se excluirá de la exploración en lo que respecta a dicha amenaza, pero no se excluirá completamente. Si dicho archivo

más tarde se infecta con otro código malicioso, el módulo antivirus lo detectará. Este tipo de exclusión puede usarse solamente para ciertos tipos de infiltraciones y puede crearse ya sea en la ventana de alerta de amenazas que informa sobre la infiltración (haga clic en **Mostrar opciones avanzadas** y luego seleccione **Excluir de la detección**) o en **Configuración > Cuarentena**, mediante la opción del menú contextual **Restaurar y excluir de la detección** que aparece al hacer un clic derecho en el archivo puesto en cuarentena.

Agregar...: excluye objetos de la detección

Editar...: permite editar las entradas seleccionadas

Quitar: elimina las entradas seleccionadas.

4.1.1.6 Configuración de los parámetros del motor ThreatSense

ThreatSense es una tecnología conformada por muchos métodos complejos de detección de amenazas. Esta tecnología es proactiva, lo que significa que también brinda protección durante las primeras horas de propagación de una nueva amenaza. Utiliza una combinación la exploración del código, la emulación del código, las firmas genéricas, las firmas de virus que funcionan conjuntamente para mejorar en forma significativa la seguridad del sistema. El motor de exploración cuenta con la capacidad de controlar varios flujos de datos simultáneamente, lo que maximiza la eficiencia y la tasa de detección. La tecnología ThreatSense también elimina con éxito los rootkits.

Las opciones de configuración del motor ThreatSense permiten especificar varios parámetros de exploración:

- Los tipos de archivos y las extensiones que se van a explorar,
- La combinación de diversos métodos de detección,
- Los niveles de desinfección, etc.

Para ingresar a la ventana de configuración, haga clic en **Configurar...** ubicado en la ventana de Configuración avanzada de cualquier módulo que use la tecnología ThreatSense (ver abajo). Diferentes escenarios de seguridad pueden requerir distintas configuraciones. Por ese motivo, ThreatSense puede configurarse en forma individual para cada uno de los siguientes módulos de protección:

- Protección del sistema de archivos en tiempo real,
- Protección de documentos,
- Protección del cliente de correo electrónico,
- Protección del acceso a la Web,
- Exploración del equipo.

Los parámetros de ThreatSense están sumamente optimizados para cada módulo y su modificación puede afectar el funcionamiento del sistema en forma significativa. Por ejemplo, la modificación de los parámetros para que siempre se exploren los empaquetadores de tiempo de ejecución, o la habilitación de la heurística avanzada en el módulo de protección del sistema de archivos en tiempo real podrían ralentizar el sistema (normalmente, solo los nuevos archivos creados se exploran con estos métodos). En consecuencia, es recomendable mantener los parámetros predeterminados de ThreatSense sin modificaciones en todos los módulos excepto para la exploración del equipo.

4.1.1.6.1 Objetos

La sección **Objetos** permite definir qué componentes y archivos del equipo se explorarán en busca de infiltraciones.

Memoria operativa: explora en busca de amenazas que atacan la memoria operativa del sistema.

Sectores de inicio: explora los sectores de inicio para detectar la presencia de virus en el Master Boot Record.

Archivos de correo electrónico: el programa es compatible con las siguientes extensiones: DBX (Outlook Express) y EML.

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

Archivos comprimidos de autoextracción: los archivos comprimidos de autoextracción (SFX) son archivos comprimidos que no necesitan ningún programa de extracción especializado para descomprimirse.

Empaquetadores de tiempo de ejecución: tras su ejecución, los empaquetadores de tiempo de ejecución (a diferencia de los tipos de archivos comprimidos estándar) se descomprimen en la memoria. Además de los empaquetadores estáticos estándar (UPX, yoda, ASPack, FSG, etc.), gracias a la emulación de códigos, el módulo de exploración también es compatible con muchos otros tipos de empaquetadores.

4.1.1.6.2 Opciones

Use la sección **Opciones** para seleccionar los métodos utilizados al explorar el sistema en busca de infiltraciones. Se encuentran disponibles las siguientes opciones:

Heurística: la heurística es un algoritmo que analiza la actividad (maliciosa) de los programas. La ventaja principal radica en su capacidad de identificar software malicioso que antes no existía o que no fue identificado por las bases de datos de firmas de virus anteriores. La desventaja es la probabilidad reducida de identificar falsos positivos.

Heurística avanzada/ADN/Firmas inteligentes - La heurística avanzada es una de las tecnologías utilizadas por ESET NOD32 Antivirus para proporcionar una detección proactiva de amenazas. Proporciona la habilidad de detectar malware desconocido en base a su funcionalidad a través de la emulación. Este nuevo traductor binario ayuda a evadir los trucos antiemulación utilizados por los creadores de malware. Su última versión presenta una forma completamente nueva de la emulación de códigos en base a la traducción binaria. Este nuevo traductor binario ayuda a evadir los trucos antiemulación utilizados por los creadores de malware. Además de estas mejoras, la exploración basada en ADN se ha actualizado significativamente para permitir mejores detecciones genéricas y tratar el malware actual con más precisión.

ESET Live Grid: gracias a la tecnología de reputación de ESET, la información sobre los archivos explorados se contrasta con los datos de [ESET Live Grid](#) basado en la nube para mejorar la detección y la velocidad de exploración.

4.1.1.6.3 Desinfección

La configuración de la desinfección determina el comportamiento del módulo de exploración durante la desinfección de los archivos infectados. Existen [3 niveles de desinfección](#).

4.1.1.6.4 Extensiones

Una extensión es una parte delimitada por un punto en el nombre de un archivo. Una extensión define el tipo de archivo y su contenido. Esta sección de la configuración de los parámetros de ThreatSense permite definir los tipos de archivos que se van a explorar.

En forma predeterminada, se exploran todos los archivos independientemente de su extensión. Se puede agregar cualquier extensión a la lista de archivos excluidos de la exploración. Si **Explorar todos los archivos** no está seleccionada, la lista pasa a mostrar todas las extensiones de archivos actualmente explorados.

Para habilitar la exploración de archivos sin extensión, seleccione **Explorar los archivos sin extensión**. **No explorar los archivos sin extensión** está disponible mientras **Explorar todos los archivos** está habilitada.

A veces es necesario excluir ciertos tipos de archivos cuando su exploración impide el funcionamiento correcto del programa que está usando ciertas extensiones. Por ejemplo, puede ser recomendable excluir las extensiones .edb, .eml y .tmp al usar los servidores de Microsoft Exchange.

Mediante el uso de los botones **Agregar** y **Quitar**, puede permitir o prohibir la exploración de extensiones de archivos específicas. Al escribir una **Extensión** se activa el botón **Agregar**, por medio del cual se agrega la nueva extensión a la lista. Seleccione una extensión de la lista y luego haga clic en **Quitar** para eliminar esa extensión de la lista.

Pueden utilizarse los símbolos especiales * (asterisco) y ? (signo de interrogación). El asterisco sustituye a cualquier cadena de caracteres y el signo de interrogación, a cualquier símbolo. Tenga especial cuidado al especificar direcciones excluidas, ya que la lista solo debe contener direcciones seguras y de confianza. Del mismo modo, es necesario asegurarse de que los símbolos * y ? se utilizan correctamente en esta lista.

Para explorar únicamente el grupo de extensiones predeterminadas, haga clic en **Predeterminado** y luego en **Sí** cuando se le indique para confirmar la acción.

4.1.1.6.5 Límites

La sección Límites permite especificar el tamaño máximo de los objetos y los niveles de los archivos comprimidos anidados que se explorarán:

Tamaño máximo del objeto: define el tamaño máximo de los objetos que se van a explorar. El módulo antivirus determinado explorará solamente los objetos con un tamaño inferior al especificado. Los únicos que deberían modificar esta opción son los usuarios avanzados que tengan motivos específicos para excluir objetos de mayor tamaño de la exploración. Valor predeterminado: *ilimitado*.

Tiempo máximo de exploración del objeto (seg.): define el valor máximo de tiempo para explorar un objeto. Si en esta opción se ingresó un valor definido por el usuario, el módulo antivirus detendrá la exploración de un objeto cuando haya transcurrido dicho tiempo, sin importar si finalizó la exploración. Valor predeterminado: *ilimitado*.

Nivel de anidado de archivos comprimidos: especifica la profundidad máxima de la exploración de archivos comprimidos. Valor predeterminado: *10*.

Tamaño máximo del archivo incluido en el archivo comprimido: esta opción permite especificar el tamaño máximo de los archivos incluidos en archivos comprimidos (al extraerlos) que se explorarán. Valor predeterminado: *ilimitado*.

Si la exploración finaliza prematuramente por estas razones, la casilla de verificación del archivo comprimido quedará sin seleccionar.

Nota: No se recomienda cambiar los valores predeterminados: en circunstancias normales, no existe ninguna razón para modificarlos.

4.1.1.6.6 Otros

En la sección **Otros**, puede configurar las siguientes opciones:

Registrar todos los objetos: si se selecciona esta opción, el archivo de registro mostrará todos los archivos explorados, incluso los que no estén infectados. Por ejemplo, si se detecta una infiltración dentro de un archivo comprimido, el registro también incluirá en la lista los archivos no infectados del archivo comprimido.

Habilitar la optimización inteligente: cuando la opción para habilitar la optimización inteligente está seleccionada, se usa la configuración más favorable para garantizar el nivel de exploración más eficiente, al mismo tiempo que mantiene la mayor velocidad de exploración. Los diversos módulos de protección realizan exploraciones en forma inteligente; para ello emplean distintos métodos de exploración y los aplican a tipos de archivos específicos. Si se deshabilita la optimización inteligente, solo se aplica la configuración definida por el usuario en el núcleo ThreatSense de esos módulos específicos al efectuar una exploración.

Cuando se configuran los valores de los parámetros del motor ThreatSense para una exploración del equipo, las opciones siguientes también están disponibles:

Explorar secuencias de datos alternativas (ADS): las secuencias de datos alternativas usadas por el sistema de archivos NTFS constituyen asociaciones de archivos y carpetas que son invisibles para las técnicas comunes de exploración. Muchas infiltraciones intentan evitar la detección camuflándose como secuencias de datos alternativas.

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

Preservar el último acceso con su fecha y hora: seleccione esta opción para preservar la hora de acceso original a los archivos explorados en vez de actualizarla (por ejemplo, para usarlos con sistemas que realizan copias de seguridad de datos).

Desplazarse por el registro de exploración: esta opción permite habilitar o deshabilitar el desplazamiento del registro. Si está seleccionada, la información se desplaza hacia arriba dentro de la ventana de visualización.

4.1.1.7 Detección de una infiltración

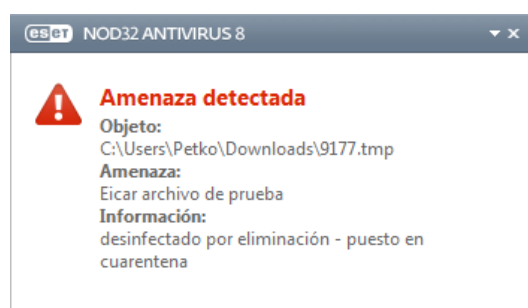
Las infiltraciones pueden llegar al sistema desde diversos puntos de entrada, como páginas Web, carpetas compartidas, correo electrónico o dispositivos extraíbles (USB, discos externos, CD, DVD, disquetes, etc.).

Conducta estándar

Como ejemplo general de la forma en que ESET NOD32 Antivirus maneja las infiltraciones, las infiltraciones se pueden detectar mediante:

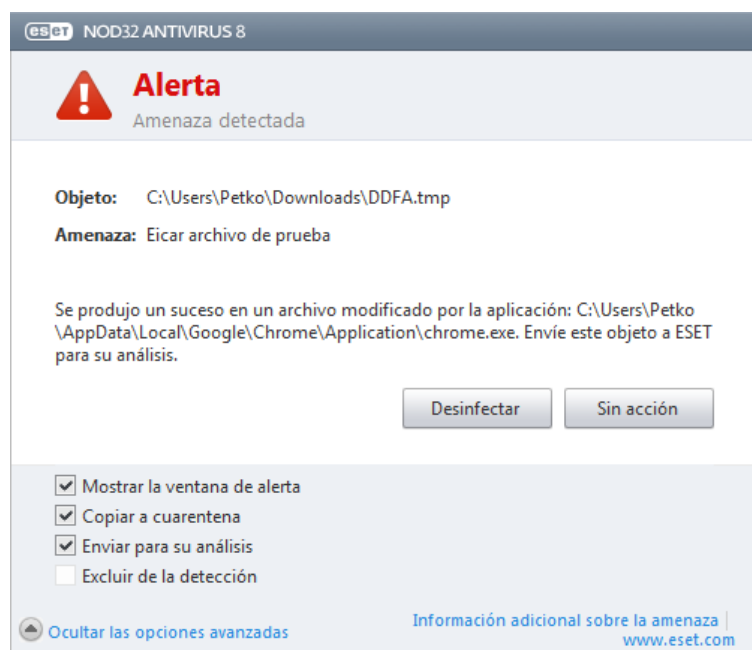
- Protección del sistema de archivos en tiempo real
- Protección del acceso a la Web
- Protección del cliente de correo electrónico
- Exploración del equipo bajo demanda

Cada uno utiliza el nivel de desinfección estándar e intentará desinfectar el archivo y moverlo a [Cuarentena](#) o finalizar la conexión. Una ventana de notificación se muestra en el área de notificaciones en la esquina inferior derecha de la pantalla. Para obtener más información sobre los niveles de desinfección y conducta, consulte en Desinfección.



Desinfección y eliminación

Si no hay ninguna acción predefinida para la protección del sistema de archivos en tiempo real, el programa le pedirá que seleccione una opción en una ventana de alerta. Por lo general están disponibles las opciones **Desinfectar**, **Eliminar** y **Sin acción**. No se recomienda seleccionar **Sin acción**, ya que esto dejará los archivos infectados sin desinfectar. La excepción a este consejo es cuando usted está seguro de que un archivo es inofensivo y fue detectado por error.



Aplique la opción de desinfección si un virus atacó un archivo y le adjuntó códigos maliciosos. En este caso, primero intente desinfectar el archivo infectado para restaurarlo a su estado original. Si el archivo está compuesto exclusivamente por códigos maliciosos, será eliminado.

Si un archivo infectado está “bloqueado” u otro proceso del sistema lo está usando, por lo general se elimina cuando es liberado (normalmente tras el reinicio del sistema).

Varias amenazas

Si algún archivo infectado no se desinfectó durante la exploración del equipo (o el Nivel de desinfección estaba configurado en **Sin desinfección**), se muestra una ventana de alerta que le solicitará seleccionar las acciones para dichos archivos. Seleccione las acciones para los archivos (las acciones se establecen en forma individual para cada archivo de la lista) y luego haga clic en **Finalizar**.

Eliminación de archivos en archivos comprimidos

En el modo de desinfección predeterminado, se eliminará el archivo comprimido completo solo si todos los archivos que lo componen están infectados. En otras palabras, los archivos comprimidos no se eliminan si también contienen archivos inofensivos no infectados. Tenga precaución al realizar una exploración con Desinfección estricta: si la Desinfección estricta está habilitada, un archivo se eliminará si al menos contiene un archivo infectado, sin importar el estado de los demás archivos que lo componen.

Si su equipo muestra signos de infección por malware, por ej., funciona más lento, con frecuencia no responde, etc., se recomienda hacer lo siguiente:

- abra ESET NOD32 Antivirus y haga clic en Exploración del equipo
- Haga clic en **Exploración inteligente** (para obtener más información, consulte en [Exploración del equipo](#)),
- una vez finalizada la exploración, consulte el registro para verificar la cantidad de archivos explorados, infectados y desinfectados

Si solo quiere explorar una parte determinada del disco, haga clic en **Exploración personalizada** y seleccione los objetos para explorar en busca de virus.

4.1.1.8 Protección de documentos

La característica de protección de documentos explora los documentos de Microsoft Office antes de que se abran, así como los archivos descargados automáticamente por Internet Explorer, por ej., los elementos ActiveX de Microsoft. La protección de documentos proporciona un nivel de protección adicional a la protección del sistema de archivos en tiempo real. Puede deshabilitarse para mejorar el rendimiento en los sistemas que no están expuestos a un alto volumen de documentos de Microsoft Office.

La opción **Integrar al sistema** activa el sistema de protección. Si desea modificar esta opción, presione la tecla F5 para abrir la ventana de configuración avanzada y haga clic en **Equipo > Antivirus y antispyware > Protección de documentos** en el árbol de configuración avanzada.

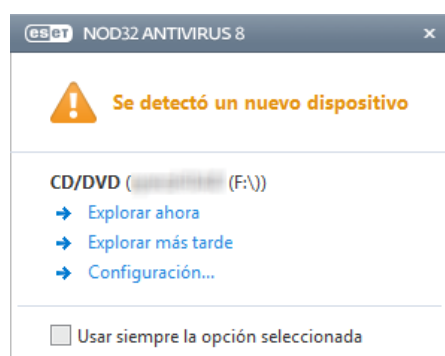
La característica se activa por medio de las aplicaciones que usan Antivirus API de Microsoft (por ej., Microsoft Office 2000 y posterior, o Microsoft Internet Explorer 5.0 y posterior).

4.1.2 Medios extraíbles

ESET NOD32 Antivirus proporciona la exploración automática de los medios extraíbles (CD/DVD/USB/...). Este módulo le permite explorar un medio insertado. Resulta útil si el administrador del equipo desea prevenir que los usuarios utilicen medios extraíbles con contenido no solicitado.

Para modificar el comportamiento de la acción que se realizará cuando se inserte un medio extraíble en el equipo (CD/DVD/USB/...), presione **F5** para abrir la ventana de Configuración avanzada y expanda **Equipo > Antivirus y antispyware > Medios extraíbles** y seleccione la acción predeterminada en el menú desplegable **Acción a realizar luego de insertar medios extraíbles**. Si se selecciona la opción **Mostrar las opciones de exploración**, se mostrará una notificación que permite elegir la acción deseada:

- **Explorar ahora:** se llevará a cabo una exploración del equipo bajo demanda en los dispositivos de medios extraíbles insertados.
- **Explorar más tarde:** no se realizará ninguna acción y se cerrará la ventana **Se detectó un nuevo dispositivo**.
- **Configurar...:** abre la sección de configuración de medios extraíbles.



4.1.3 Control del dispositivo

ESET NOD32 Antivirus proporciona el control del dispositivo automático (CD/DVD/USB/...). Este módulo permite explorar, bloquear o ajustar los filtros o permisos extendidos y definir la forma en que el usuario puede acceder y trabajar con un dispositivo determinado. Resulta útil si el administrador del equipo desea prevenir que los usuarios utilicen dispositivos con contenido no solicitado.

Dispositivos externos admitidos

- CD/DVD
- Almacenamiento en disco
- Almacenamiento FireWire

Nota: Control del dispositivo en ESET Endpoint Security o ESET Endpoint Antivirus utilizado en un entorno corporativo es compatible con más tipos de dispositivos externos.

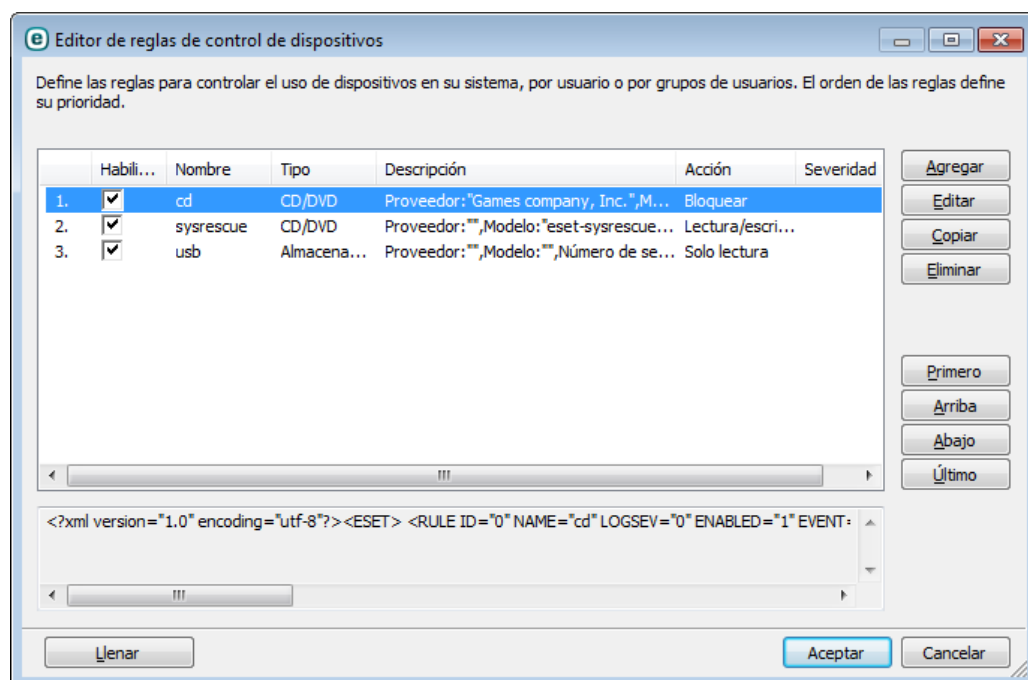
Las opciones de configuración del control del dispositivo se pueden modificar en **Configuración avanzada (F5) > Equipo > Control del dispositivo**.

Al seleccionar la casilla de verificación ubicada junto a **Integrar al sistema** activa la característica de Control del dispositivo en ESET NOD32 Antivirus; necesitará reiniciar su equipo para que este cambio se aplique. Una vez que se habilita el Control del dispositivo, **Configurar reglas...** se activará, lo cual le permite abrir la ventana [Editor de reglas control del dispositivo](#).

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 el acceso al dispositivo será denegado.

4.1.3.1 Reglas de control del dispositivo

La ventana **Editor de reglas de control del dispositivo** muestra las reglas existentes y permite el control preciso de dispositivos externos que los usuarios conectan al equipo.



Los dispositivos específicos se pueden permitir o bloquear por usuario o grupo de usuarios y con base en los parámetros adicionales del dispositivo que se pueden especificar en la configuración de reglas. La lista de reglas contiene varias descripciones de una regla como nombre, tipo de dispositivo externo, acción a realizar después de conectar un dispositivo externo en su equipo y la severidad del registro.

Haga clic en **Agregar** o **Editar** para administrar una regla. Haga clic en **Copiar** para crear una nueva regla con opciones predefinidas utilizadas para otra regla seleccionada. Las cadenas XML mostradas al hacer clic en una regla se pueden copiar en el portapapeles para ayudar a los administradores del sistema a exportar/importar estos datos y usarlos, por ejemplo en ESET Remote Administrator.

Al presionar CTRL y hacer clic, puede seleccionar varias reglas y aplicar acciones, tales como eliminarlas o moverlas hacia arriba o abajo de la lista, a todas las reglas seleccionadas. La casilla de verificación **Habilitada** deshabilita o habilita una regla; esto puede ser útil si no desea eliminar una regla permanentemente en caso de que desee utilizarla en el futuro.

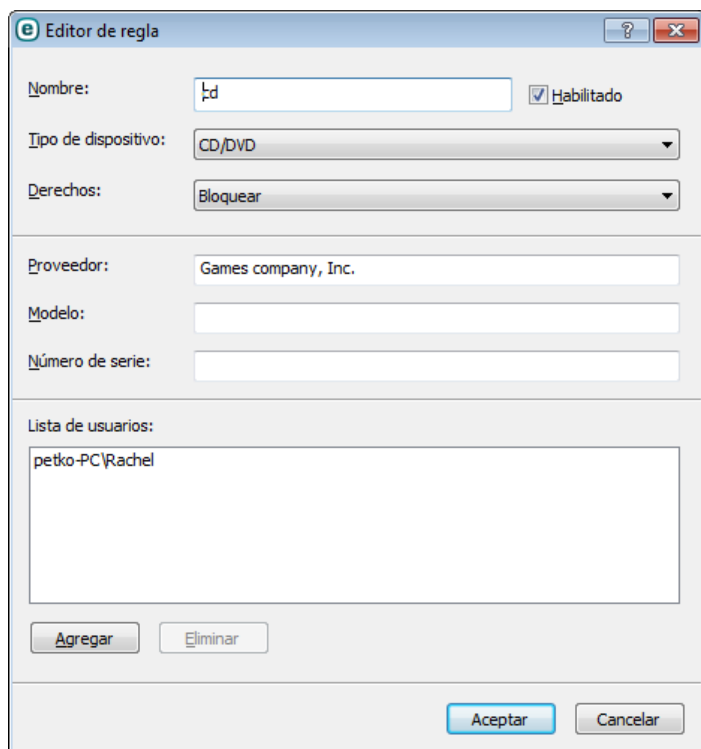
El control se logra por medio de las reglas que se clasifican en orden para determinar su prioridad, con las reglas de mayor prioridad hasta arriba.

Puede hacer clic derecho en una regla para mostrar el menú contextual. Aquí también puede establecer los detalles mínimos de entradas del registro (severidad) de una regla. Las entradas de registro se pueden ver desde la ventana principal del ESET NOD32 Antivirus en **Herramientas** > [Archivos de registro](#).

Haga clic en **Llenar** para completar automáticamente los parámetros de los dispositivos de medios extraíbles conectados al equipo.

4.1.3.2 Agregado de reglas del control del dispositivo

Una regla de control del dispositivo define la acción que se tomará cuando un dispositivo, que cumple con los criterios de las reglas, se conecte al equipo.



Ingrese una descripción de la regla en el campo **Nombre** para tener una mejor identificación. Seleccionar la casilla de verificación al lado de **Habilitado** deshabilita o habilita esta regla; esto puede ser útil si no desea eliminar la regla permanentemente.

Tipo de dispositivo

Elija el tipo de dispositivo externo desde 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 siempre y cuando un dispositivo esté conectado al equipo. El tipo de dispositivo de **Unidades ópticas** en el menú desplegable se refiere al almacenamiento de datos en un medio que se puede leer ópticamente (por ej., CD, DVD). Los dispositivos de almacenamiento cubren los discos externos o los lectores de tarjetas de memoria convencionales conectados vía USB o FireWire. Los lectores de tarjetas inteligentes incluyen los lectores de tarjetas inteligentes con un circuito integrado, tal como las tarjetas SIM o tarjetas de autenticación. Ejemplos de dispositivos de imagen son escáneres o cámaras, estos dispositivos no proporcionan información sobre usuarios, únicamente sobre sus acciones. Esto significa que los dispositivos de imagen solo se pueden bloquear globalmente.

Derechos

El acceso a los dispositivos no de almacenamiento se puede permitir o bloquear. En contraste, 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 la lectura de acceso al dispositivo.
- **Lectura/escritura:** se permitirá el acceso total al dispositivo.

Observe que no todos los derechos (acciones) están disponibles para todos los tipos de dispositivo. Si un dispositivo tiene espacio de almacenamiento, hay tres acciones disponibles. Para los dispositivos no de almacenamiento, solo existen dos (por ejemplo, la acción **Solo lectura** no está disponible para Bluetooth, entonces los dispositivos Bluetooth solo se pueden permitir o bloquear).

Otros parámetros que se pueden utilizar para ajustar las reglas y personalizarlas a dispositivos. Todos los parámetros no distinguen entre mayúsculas y minúsculas:

- **Proveedor:** filtrado por nombre o número de identificación del proveedor.
- **Modelo:** el nombre determinado del dispositivo.
- **Número de serie:** los dispositivos externos generalmente tienen sus propios números de serie. En caso de un CD/DVD, este es el número de serie que corresponde al medio determinado, no a la unidad de CD.

Nota: Si los tres descriptores anteriores están vacíos, la regla ignorará estos campos mientras realiza la coincidencia. Los parámetros de filtrado en todos los campos de texto distinguen mayúsculas de minúsculas y no se aceptan caracteres globales (*, ?). Deben escribirse tal como lo indica el fabricante.

Sugerencia: Con el fin de descifrar los parámetros de un dispositivo, cree una regla de permiso para el tipo adecuado de dispositivos, conecte el dispositivo a su equipo y luego revise los detalles del dispositivo en el [Registro de control del dispositivo](#).

Las reglas se pueden limitar a ciertos usuarios o grupos de usuarios al agregarlos a la **Lista de usuarios**:

- **Agregar:** abre el **Tipo de objeto: usuarios o grupos** que permite seleccionar los usuarios deseados.
- **Eliminar:** quita el usuario seleccionado del filtro.

Observe que no todos los dispositivos pueden ser limitados por reglas del usuario, (por ejemplo, los dispositivos de imagen no proporcionan información sobre usuarios, únicamente sobre acciones invocadas).

4.1.4 HIPS

El **Sistema de prevención de intrusiones basado en el host (HIPS)** protege su sistema de malware y actividades no deseadas que intentan perjudicar el equipo. El sistema HIPS utiliza el análisis avanzado de conducta combinado con las capacidades de detección del filtrado de red para monitorear los procesos activos, los archivos y las claves de registro. HIPS es aparte de la protección del sistema de archivos en tiempo real y no es un firewall; solo monitorea los procesos activos en el sistema operativo.

La configuración de HIPS se encuentra en **Configuración avanzada (F5)**. Para acceder a HIPS en el árbol de configuración avanzada, haga clic en **Equipo > HIPS**. El estado del HIPS (habilitado/deshabilitado) se muestra en la ventana principal de ESET NOD32 Antivirus, en el panel **Configuración**, del lado derecho de la sección Equipo.

Advertencia: Las modificaciones de la configuración del HIPS deben realizarse únicamente por un usuario experimentado.

ESET NOD32 Antivirus tiene la tecnología integrada *Autodefensa* que evita que el software malicioso dañe o desactive la protección antivirus y antispyware. *Autodefensa* protege los archivos y las claves de registro fundamentales para que ESET NOD32 Antivirus funcione, y asegura que el software potencialmente malicioso no pueda realizar modificaciones en estas ubicaciones.

Los cambios en la configuración **Habilitar HIPS** y **Habilitar la Autodefensa** se aplican luego del reinicio de Windows. La deshabilitación del sistema **HIPS** completo también requiere reiniciar el equipo para aplicar los cambios.

Bloqueador de exploits está diseñado para fortalecer diferentes tipos de aplicaciones comúnmente explotadas como los navegadores web, los lectores de PDF, los clientes de correo electrónico y los componentes de MS Office. Lea más información sobre este tipo de protección en el [glosario](#).

Exploración de memoria avanzada trabaja en conjunto con el bloqueador de exploits para fortalecer la protección contra malware diseñado para evadir la detección por los productos antimalware con el uso de ofuscación o cifrado. Lea más información sobre este tipo de protección en el [glosario](#).

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

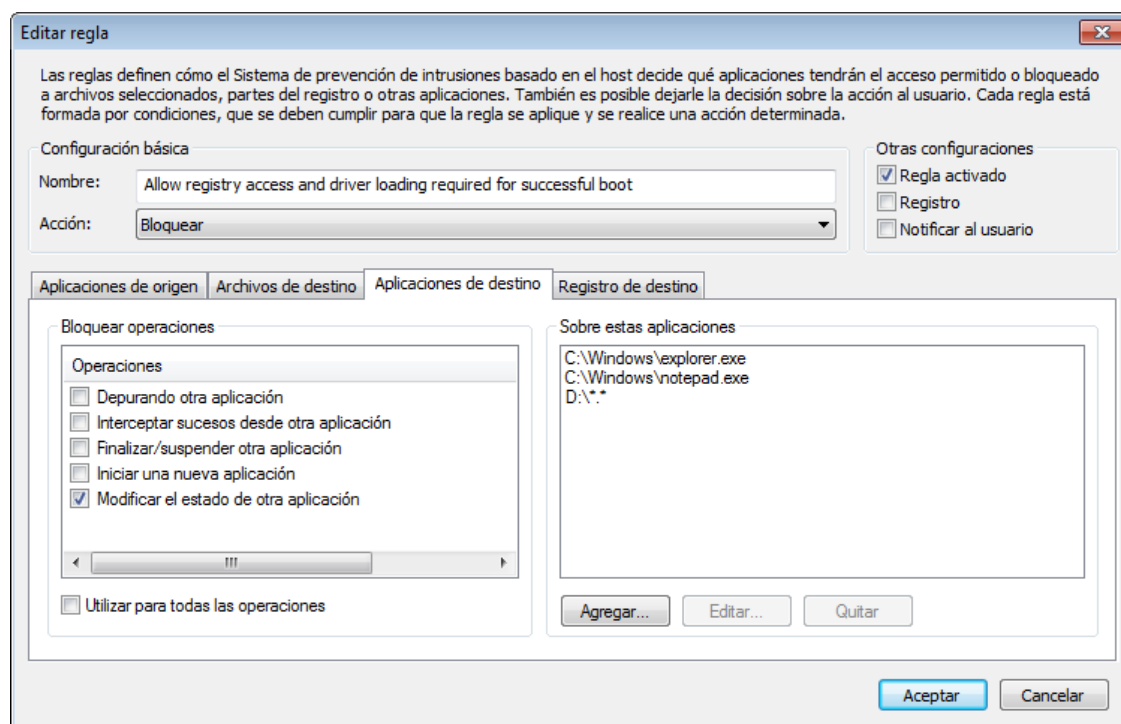
- **Modo automático con reglas:** las operaciones están habilitadas y se utiliza un conjunto de reglas predefinidas que protegen su sistema.
- **Modo inteligente:** Se notificará al usuario solo en caso de eventos muy sospechosos.
- **Modo interactivo:** el programa le solicitará al usuario que confirme las operaciones.
- **Modo basado en políticas:** las operaciones que no estén definidas por una regla pueden estar bloqueadas.
- **Modo de aprendizaje:** las operaciones están habilitadas y se crea una regla luego 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 creadas en el modo automático. Tras seleccionar **Modo de aprendizaje**, la opción **Notificar sobre**

el vencimiento del modo de aprendizaje en X días se vuelve activa. Luego de que termine el período de tiempo definido en **Notificar sobre el vencimiento del modo de aprendizaje en X días**, se deshabilita el modo de aprendizaje nuevamente. El período máximo es de 14 días. Cuando finaliza, se abrirá una ventana emergente que permite editar las reglas y seleccionar un modo de filtrado diferente.

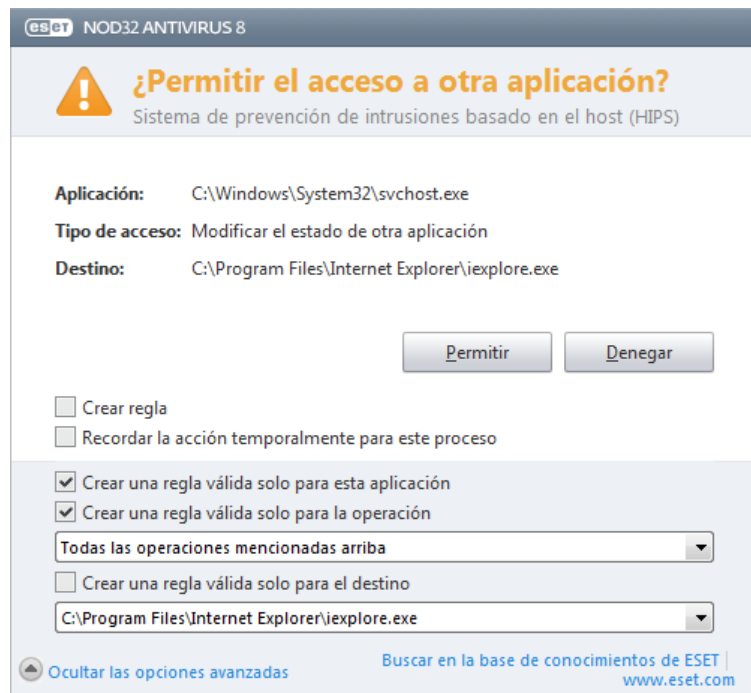
El sistema HIPS monitorea los sucesos dentro del sistema operativo y reacciona en conformidad según las reglas, que son similares a las reglas del firewall personal en ESET Smart Security. Haga clic en **Configurar reglas...** para abrir la ventana de administración de reglas del HIPS. Allí podrá seleccionar, crear, editar o eliminar reglas.

En el siguiente ejemplo, mostraremos cómo restringir la conducta no deseada de las aplicaciones:

1. Póngale un nombre a la regla y seleccione **Bloquear** del menú desplegable **Acción**.
2. Abra la pestaña **Aplicaciones de destino**. Deje la pestaña **Aplicaciones de origen** en blanco para aplicar la nueva regla a todas las aplicaciones que intentan llevar a cabo alguna de las operaciones seleccionadas en la lista **Operaciones** correspondientes a las aplicaciones incluidas en la lista **Sobre estas aplicaciones**.
3. Seleccionar **Modificar el estado de otra aplicación** (todas las operaciones están descritas en la ayuda del producto, a la que puede accederse presionando F1).
4. **Agregue** una o varias aplicaciones que desee proteger.
5. Seleccione la casilla de verificación **Notificar al usuario** para mostrar una notificación cada vez que se aplica una regla.
6. Haga clic en **Aceptar** para guardar la nueva regla.



Si selecciona **preguntar** como acción predeterminada, ESET NOD32 Antivirus mostrará una ventana de dialogo cada vez que se ejecute una operación. Puede elegir **Denegar** o **Permitir** la operación. Si no elige una acción, se seleccionará una acción en base a las reglas predeterminadas.



La ventana de diálogo **permitir acceso a otra aplicación** permite crear una regla basada en cualquier acción nueva que HIPS detecte, y definir luego las condiciones mediante las cuales se permitirá o denegará esa acción. Haga clic en **Mostrar las opciones avanzadas** para definir los parámetros exactos para su nueva regla. Las reglas creadas de esta forma se consideran equivalentes a las creadas manualmente. En consecuencia, la regla creada desde una ventana de diálogo puede ser menos específica que la que desencadena la ventana de diálogo. Esto significa que luego de crear dicha regla, la misma operación puede accionar otra ventana de diálogo si los parámetros que configuró su regla anterior no se aplica a la situación.

Recordar la acción temporalmente para este proceso hace usar una acción (**Permitir / Denegar**) hasta que se cambie una regla o modo de filtrado, se actualice un módulo de HIPS o se reinicie el sistema. Las reglas temporales se eliminarán tras cualquiera de estas acciones.

4.1.5 Modo de juego

El modo de juego es una característica para los usuarios que requieren utilizar el software en forma ininterrumpida, que no desean que las ventanas emergentes los molesten y que quieren minimizar el uso de la CPU. El modo de juego también se puede utilizar durante las presentaciones que la actividad del programa antivirus no puede interrumpir. Al habilitar esta característica, todas las ventanas emergentes se deshabilitan y la actividad de las tareas programadas se detiene por completo. La protección del sistema seguirá ejecutándose en segundo plano, pero no requerirá ninguna interacción por parte del usuario.

Para habilitar o deshabilitar el modo de juego, en la ventana principal del programa seleccione **Configuración > Equipo**, luego **Habilitar** desde **Modo de juego**. También puede habilitarlo desde el árbol de configuración avanzada (F5) al expandir la **Equipo**, hacer clic en **Modo de juego** y seleccionar la casilla de verificación junto a **Habilitar el modo de juego**. Habilitar el modo de juego constituye un riesgo potencial para la seguridad; por ese motivo, el ícono de estado de protección ubicado en la barra de tareas se pondrá naranja y mostrará una advertencia. Esta advertencia también aparecerá en la ventana principal del programa, donde el **Modo de juego habilitado** aparecerá en naranja.

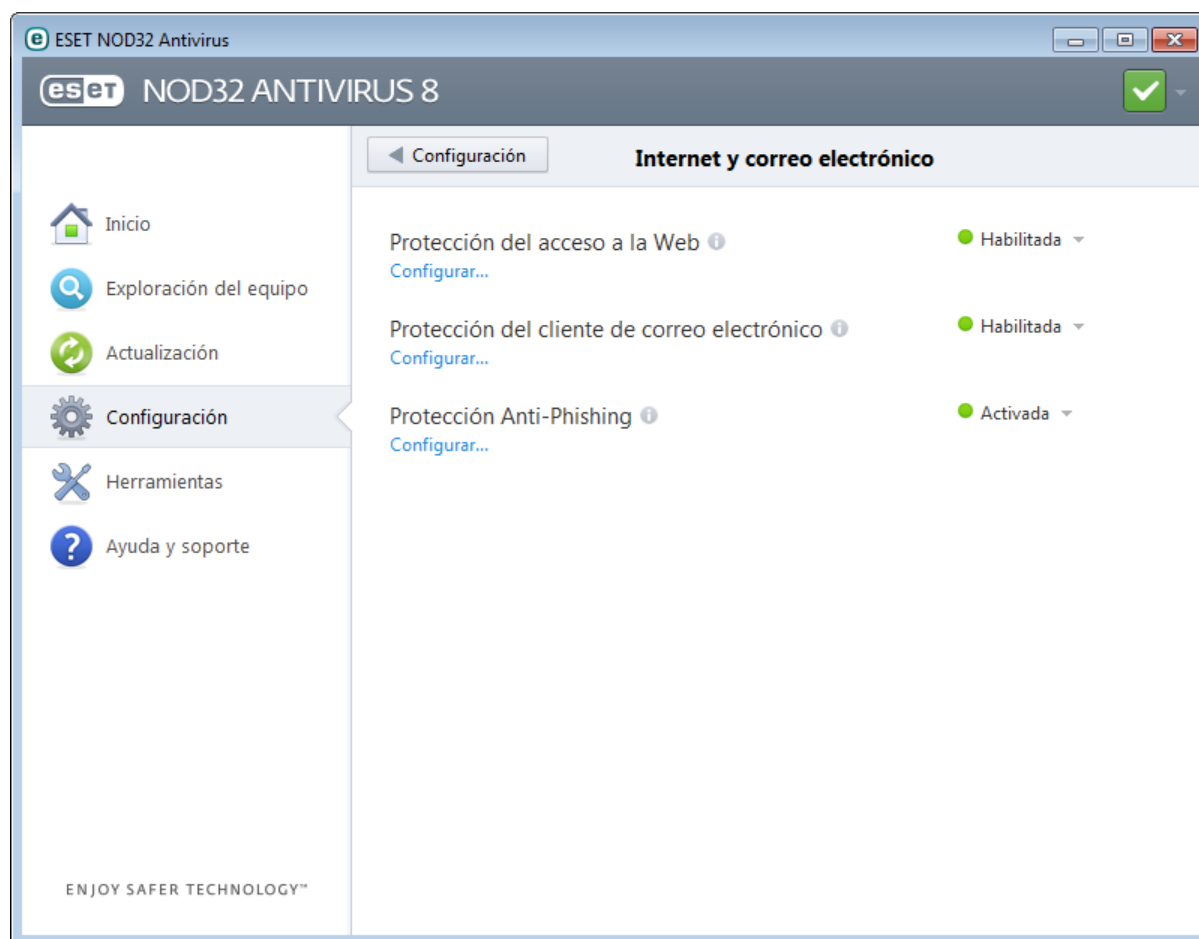
Al seleccionar **Habilitar el modo de juego automáticamente al ejecutar aplicaciones de pantalla completa**, el modo de juego se iniciará cuando se abra una aplicación de pantalla completa y se detendrá automáticamente al salir de dicha aplicación. Es útil en especial para iniciar el modo de juego inmediatamente tras empezar un juego, abrir una aplicación de pantalla completa o iniciar una presentación.

También puede seleccionar **Deshabilitar el modo de juego automáticamente después de X minutos** para definir el

tiempo que debe transcurrir para que el modo de juego quede deshabilitado automáticamente (el valor predeterminado es 1 minuto).

4.2 Internet y correo electrónico

La configuración de Internet y correo electrónico se encuentra en el panel **Configuración**, al hacer clic en el título **Internet y correo electrónico**. Desde aquí es posible acceder a la configuración detallada del programa.



La conectividad de Internet es una característica estándar de los equipos personales. Lamentablemente, Internet también se convirtió en el medio principal para la distribución de códigos maliciosos. Por ese motivo, es esencial que considere con mucho cuidado la configuración **Protección del acceso a la Web**.

Haga clic en **Configurar** para abrir las configuraciones de protección Web/correo electrónico/anti-phishing en la Configuración avanzada.

Protección del cliente de correo electrónico: proporciona el control de las comunicaciones por correo electrónico recibidas a través de los protocolos POP3 e IMAP. Mediante el complemento del programa para su cliente de correo electrónico, ESET NOD32 Antivirus proporciona el control de todas las comunicaciones entrantes y salientes del cliente de correo electrónico (POP3, MAPI, IMAP, HTTP).

Protección antiphishing le permite bloquear las páginas Web conocidas por distribuir contenido phishing. Se recomienda firmemente que deje Anti-Phishing habilitada.

Puede desactivar las configuraciones de protección Web/correo electrónico/anti-phishing temporalmente al hacer clic en **Habilitado**.

4.2.1 Protección del cliente de correo electrónico

La protección del correo electrónico proporciona el control de las comunicaciones por correo electrónico recibidas a través de los protocolos POP3 e IMAP. Mediante el complemento para Microsoft Outlook y otros clientes de correo electrónico, ESET NOD32 Antivirus proporciona el 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 avanzados de exploración incluidos en el motor de exploración ThreatSense. Esto significa que la detección de programas maliciosos se lleva a cabo incluso antes de verificar su coincidencia con la base de datos de firmas de virus. La exploración de las comunicaciones de los protocolos POP3 e IMAP es independiente del cliente de correo electrónico utilizado.

Las opciones para esta funcionalidad están disponibles en **Configuración avanzada > Internet y correo electrónico > Protección del cliente de correo electrónico**.

Configuración de los parámetros del motor ThreatSense: la configuración avanzada del módulo de exploración de virus permite configurar los objetos para explorar, los métodos de detección, etc. Haga clic en **Configurar...** para mostrar la ventana de configuración detallada del módulo de exploración de virus.

Luego de verificar el correo electrónico, se puede añadir al mensaje una notificación con el resultado de la exploración. Puede elegir **Añadir mensajes de etiqueta a los correos electrónicos recibidos y leídos**, o **Añadir mensajes de etiqueta a los correos electrónicos enviados**. Tenga en cuenta en ocasiones raras los mensajes de etiqueta pueden ser omitidos en mensajes HTML problemáticos o adulterados por algunos virus. Los mensajes de etiqueta se pueden añadir a los correos electrónicos recibidos y leídos, enviados o a ambas categorías. Las opciones disponibles son:

- **Nunca:** no se agregará ningún mensaje de etiqueta en absoluto.
- **Solo al correo electrónico infectado:** únicamente se marcarán como verificados los mensajes que contengan software malicioso (predeterminado).
- **A todos los correos electrónicos explorados:** el programa añadirá mensajes a todos los correos electrónicos explorados.

Añadir una nota al asunto de los correos electrónicos infectados que fueron recibidos y leídos/enviados: seleccione esta casilla de verificación si desea que la protección de correo electrónico incluya una advertencia sobre virus en el asunto de cada correo electrónico infectado. Esta característica hace posible realizar un filtrado simple del correo electrónico basado en el asunto (si es compatible con el programa de correo electrónico). También incrementa el nivel de credibilidad para el destinatario y si se detecta una amenaza, proporciona información valiosa sobre el grado de peligro de la amenaza de un correo electrónico o remitente específicos.

Plantilla añadida al asunto del correo electrónico infectado: si desea modificar el formato del prefijo en el asunto de un correo electrónico infectado, edite esta plantilla. Esta función reemplazará el asunto del mensaje "Hola" con un valor de prefijo dado "[virus]" por el siguiente formato: "[virus] Hola". La variable %VIRUSNAME% representa la amenaza detectada.

4.2.1.1 Integración con los clientes de correo electrónico

La integración de ESET NOD32 Antivirus con clientes de correo electrónico incrementa el nivel de protección activa frente a códigos maliciosos en los mensajes de correo electrónico. Si su cliente de correo electrónico es compatible, esta integración se puede habilitar en ESET NOD32 Antivirus. Cuando la integración está activada, la barra de herramientas de ESET NOD32 Antivirus se inserta directamente en el cliente de correo electrónico, lo que permite una protección más eficaz del correo electrónico. Las opciones de configuración de la integración están disponibles en **Configuración > Ingresar a la configuración avanzada... > Internet y correo electrónico > Protección del cliente de correo electrónico > Integración con el cliente de correo electrónico**.

Entre los clientes de correo electrónico actualmente compatibles, se incluyen Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail. Si desea obtener una lista completa de los clientes de correo electrónico compatibles y sus versiones, consulte el siguiente [artículo de base de conocimiento de ESET](#).

Seleccione la casilla de verificación al lado de **Deshabilitar la verificación en caso de cambios en el contenido del buzón de entrada** si nota que el sistema funciona con mayor lentitud mientras trabaja con el cliente de correo electrónico. Esto puede ocurrir cuando se recupera el correo electrónico desde Kerio Outlook Connector Store.

Incluso si la integración no está habilitada, la comunicación por correo electrónico todavía está 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 del cliente de correo electrónico es compatible con los siguientes clientes de correo electrónico: Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail. La protección de correo electrónico funciona como un complemento para estos programas. La ventaja principal de este complemento es su independencia respecto al protocolo utilizado. Cuando el cliente de correo electrónico recibe un mensaje cifrado, se descifra y se envía al módulo de exploración de virus.

Correo electrónico para explorar

Correo electrónico recibido: activa o desactiva la verificación de los mensajes recibidos.

Correo electrónico enviado: activa o desactiva la verificación de los mensajes enviados.

Correo electrónico leído: activa o desactiva la verificación de los mensajes leídos.

Acción para realizar en correos electrónicos infectados:

Sin acción: si se habilita esta opción, el programa identificará los archivos adjuntos infectados, pero dejará intactos los correos electrónicos, sin realizar ninguna acción.

Eliminar correo electrónico: el programa notificará al usuario sobre las infiltraciones y eliminará el mensaje.

Mover el correo electrónico a la carpeta de elementos eliminados: los correos electrónicos infectados se enviarán automáticamente a la carpeta **Elementos eliminados**.

Mover el correo electrónico a la carpeta: especifica la carpeta personalizada a la que desea enviar los correos electrónicos infectados cuando se detectan.

Otros

Repetir la exploración tras la actualización: activa o desactiva la exploración reiterada luego de actualizar la base de datos de firmas de virus.

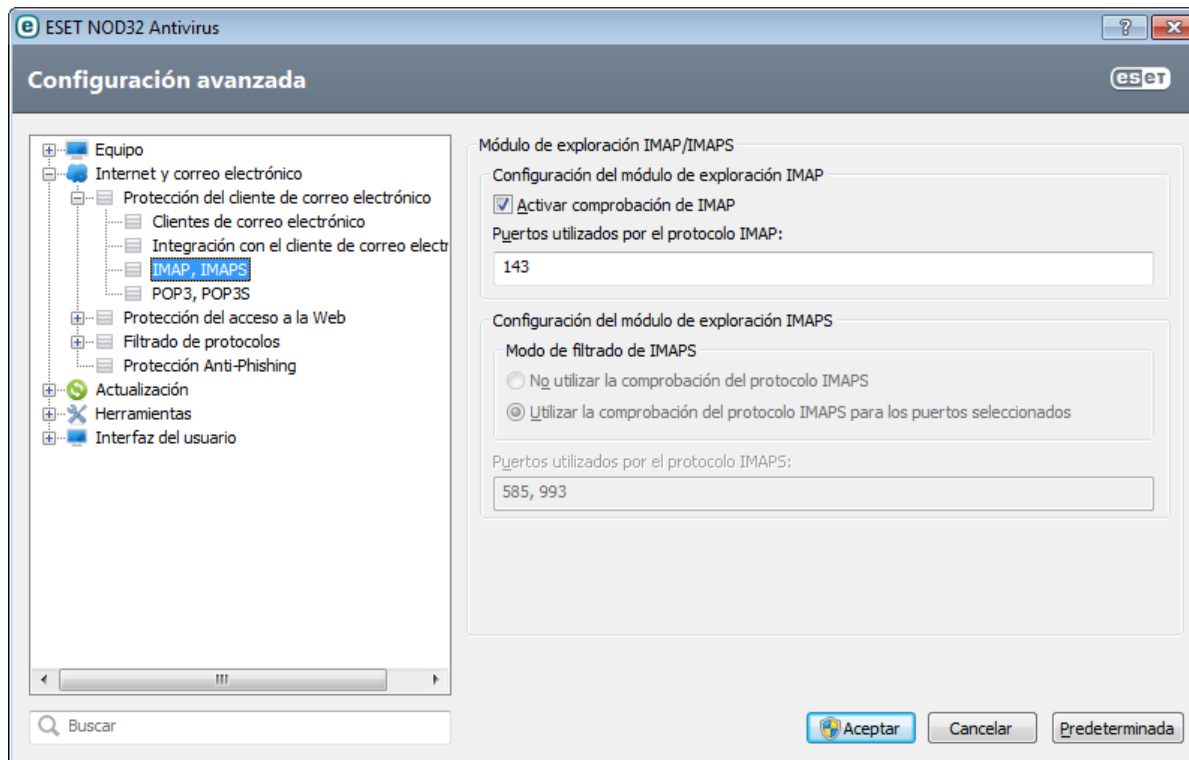
Aceptar los resultados de las exploraciones realizadas por otros módulos: si se selecciona, el módulo de protección de correo electrónico aceptará los resultados de la exploración de otros módulos de protección.

4.2.1.2 Módulo de exploración IMAP/IMAPS

El Protocolo de acceso a mensajes de Internet (IMAP, por sus siglas en inglés) es otro protocolo de Internet para la recuperación del correo electrónico. El protocolo IMAP tiene algunas ventajas sobre POP3, por ejemplo, se pueden conectar simultáneamente varios clientes al mismo buzón de correo y mantener información del estado de los mensajes: si se leyó, respondió o eliminó el mensaje, etc. ESET NOD32 Antivirus brinda protección para este protocolo independientemente del cliente de correo utilizado.

El módulo de protección que proporciona este control se inicia automáticamente al arrancar el sistema operativo y luego queda activo en la memoria. El control del protocolo IMAP se realiza automáticamente sin necesidad de reconfigurar el cliente de correo electrónico. En forma predeterminada, se exploran todas las comunicaciones en el puerto 143, pero se pueden agregar otros puertos de comunicación si es necesario. Los números de puerto múltiples deben delimitarse con una coma.

La comunicación cifrada no se explorará. Para habilitar la exploración de la comunicación cifrada y ver la configuración del módulo de exploración, vaya a [Verificación del protocolo SSL](#) en la sección de configuración avanzada, haga clic en **Internet y correo electrónico > Filtrado de protocolos > SSL** y habilite la opción **Explorar siempre el protocolo SSL**.



4.2.1.3 Filtro para POP3, POP3S

POP3 es el protocolo de uso más generalizado para recibir comunicaciones de correo electrónico en una aplicación de cliente de correo electrónico. ESET NOD32 Antivirus brinda protección para este protocolo independientemente del cliente de correo utilizado.

El módulo de protección que proporciona este control se inicia automáticamente al arrancar el sistema operativo y luego queda activo en la memoria. Para que el módulo funcione correctamente, asegúrese de que esté habilitado; la exploración POP3 se realiza automáticamente sin necesidad de reconfigurar el cliente de correo electrónico. En forma predeterminada, se exploran todas las comunicaciones en el puerto 110, pero se pueden agregar otros puertos de comunicación si es necesario. Los números de puerto múltiples deben delimitarse con una coma.

La comunicación cifrada no se explorará. Para habilitar la exploración de la comunicación cifrada y ver la configuración del módulo de exploración, vaya a [Verificación del protocolo SSL](#) en la sección de configuración avanzada, haga clic en **Internet y correo electrónico > Filtrado de protocolos > SSL** y habilite la opción **Explorar siempre el protocolo SSL**.

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

Habilitar la verificación del protocolo POP3: si esta opción se encuentra habilitada, todo el tráfico que pase a través de POP3 se monitorea en busca de software malicioso.

Puertos utilizados por el protocolo POP3: una lista de puertos utilizados por el protocolo POP3 (el predeterminado es 110).

ESET NOD32 Antivirus también admite la verificación del protocolo POP3S. Este tipo de comunicación utiliza un canal cifrado para transferir información entre el servidor y el cliente. ESET NOD32 Antivirus verifica las comunicaciones mediante los métodos de cifrado SSL (protocolo de capa de conexión segura) y TLS (seguridad de la capa de transporte).

No verificar el protocolo POP3S: no se verificarán las comunicaciones cifradas.

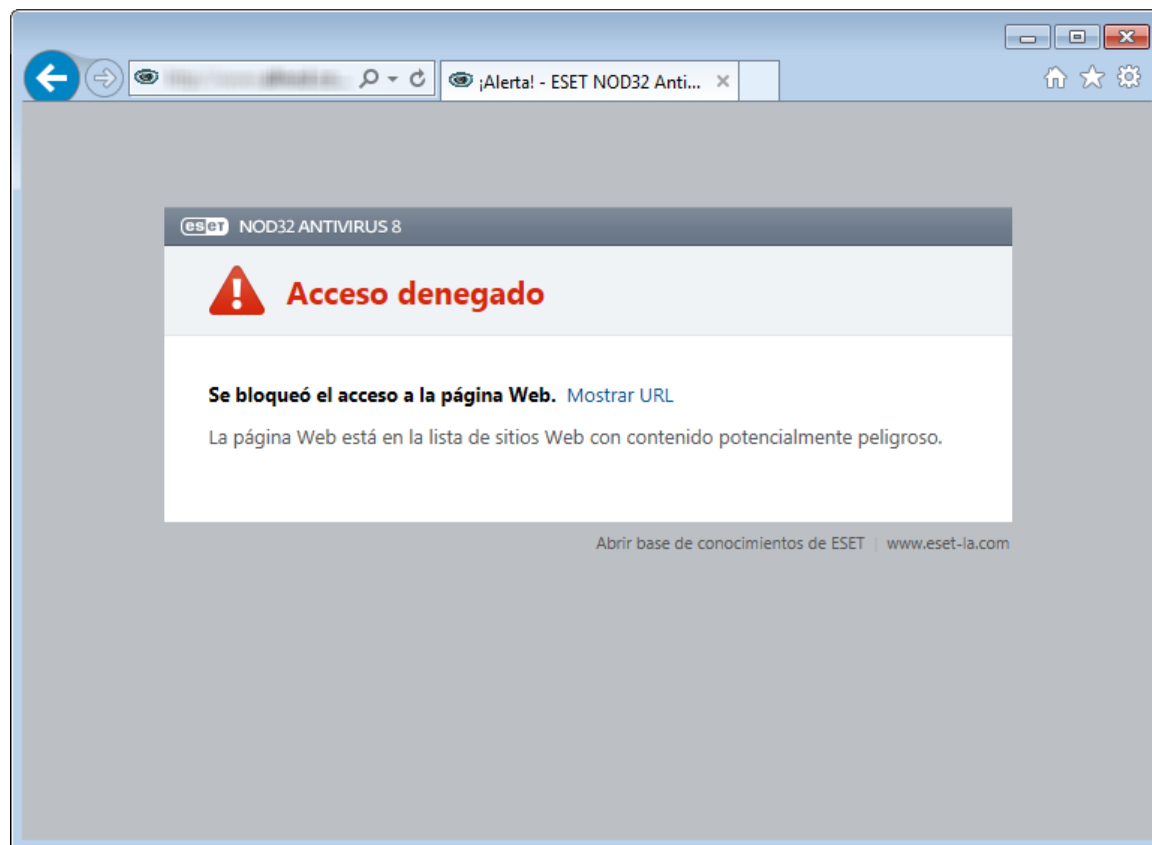
Verificar el protocolo POP3S para los puertos seleccionados: seleccione esta opción si desea habilitar la verificación POP3S únicamente para los puertos definidos en **Puertos utilizados por el protocolo POP3S**.

Puertos utilizados por el protocolo POP3S: una lista de puertos POP3S para verificar (el predeterminado es 995).

4.2.2 Protección del acceso a la Web

La conectividad a Internet es una función estándar del equipo personal. Lamentablemente, también se convirtió en el medio principal para transferir códigos maliciosos. La función de la protección del acceso a la Web es monitorear la comunicación entre los navegadores Web y los servidores remotos, según las disposiciones normativas de HTTP (protocolo de transferencia de hipertexto) y HTTPS (comunicación cifrada).

Se recomienda firmemente que la protección del acceso a la Web esté habilitada. Puede acceder a esta opción desde la ventana principal de ESET NOD32 Antivirus al ir a **Configuración > Internet y correo electrónico > Protección del acceso a la Web**. El acceso a las páginas Web conocidas con contenido malicioso siempre está bloqueado.



4.2.2.1 HTTP, HTTPS

En forma predeterminada, ESET NOD32 Antivirus está configurado para utilizar los estándares de la mayoría de los navegadores de Internet. No obstante, es posible modificar las opciones de configuración del módulo de exploración HTTP en **Configuración avanzada (F5) > Internet y correo electrónico > Protección del acceso a la Web > HTTP, HTTPS**. En la ventana principal **Módulo de exploración HTTP/HTTPS**, puede seleccionar o anular la selección de la opción **Habilitar la verificación de HTTP**. También puede definir los números del puerto usado para la comunicación HTTP. En forma predeterminada, se utilizan los números de puerto 80 (HTTP), 8080 y 3128 (para el servidor Proxy).

ESET NOD32 Antivirus admite la verificación del protocolo HTTPS. La comunicación de HTTPS utiliza un canal cifrado para transferir información entre el servidor y el cliente. ESET NOD32 Antivirus verifica las comunicaciones mediante los métodos de cifrado SSL (protocolo de capa de socket seguro) y TLS (seguridad de la capa de transporte). La verificación HTTPS puede realizarse en los siguientes modos:

No verificar el protocolo HTTPS: no se verificarán las comunicaciones cifradas.

Verificar el protocolo HTTPS para los puertos seleccionados: el programa solo verificará las aplicaciones especificadas en la sección [Clientes de Internet y correo electrónico](#) y que usen puertos definidos en **Puertos utilizados por el protocolo HTTPS**. El puerto establecido en forma predeterminada es 443.

La comunicación cifrada no se explorará. Para habilitar la exploración de la comunicación cifrada y ver la configuración del módulo de exploración, vaya a [Verificación del protocolo SSL](#) en la sección de configuración avanzada, haga clic en **Internet y correo electrónico > Filtrado de protocolos > SSL** y habilite la opción **Explorar**

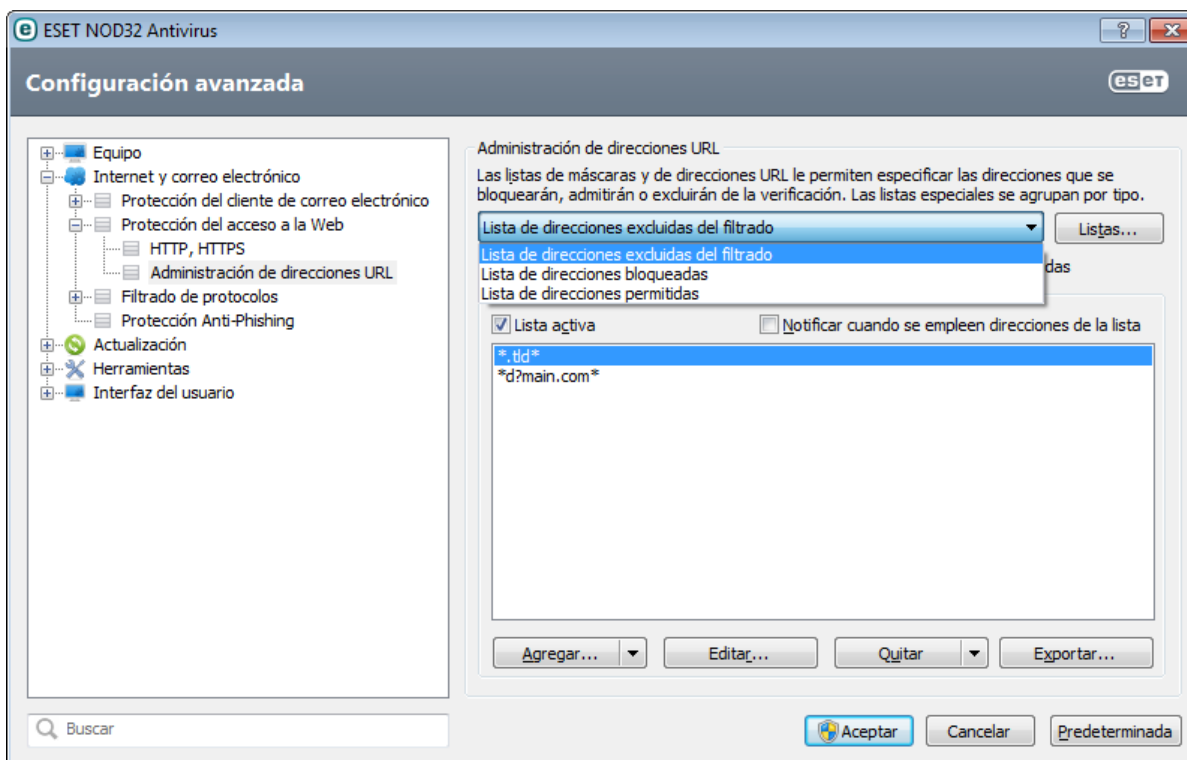
siempre el protocolo SSL.

4.2.2.2 Administración de direcciones URL

La sección sobre administración de direcciones URL permite especificar las direcciones HTTP que se desean bloquear, permitir o excluir de la verificación. **Agregar**, **Editar**, **Quitar** y **Exportar** se usan para administrar las listas de direcciones. No será posible acceder a los sitios Web incluidos en la lista de direcciones bloqueadas. Se otorgará acceso a los sitios Web presentes en la lista de direcciones excluidas sin explorarlos en busca de códigos maliciosos. Si selecciona **Solo permitir el acceso a las direcciones URL de la lista de direcciones permitidas**, únicamente se podrá acceder a las direcciones presentes en la lista de direcciones permitidas, mientras que las demás direcciones HTTP se bloquearán.

Si agrega una dirección URL a la **Lista de direcciones excluidas del filtrado**, la dirección quedará excluida de la exploración. También puede permitir o bloquear ciertas direcciones; para ello, agréguelas a la **Lista de direcciones permitidas** o a la **Lista de direcciones bloqueadas**. Haga clic en **Listas...**, para abrir la ventana **Listas de máscaras/direcciones HTTP** donde podrá **Agregar** o **Eliminar** listas de direcciones. Para agregar direcciones URL de protocolo HTTPS a la lista, **Explorar 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 Agregado de una máscara de dominio/dirección HTTP para conocer cómo todo un dominio, incluidos los subdominios, pueden hacerse coincidir de manera segura. Para activar una lista, seleccione la opción **Lista activa**. Si quiere recibir notificaciones al ingresar una dirección de la lista actual, seleccione **Notificar cuando se empleen direcciones de la lista**.



Agregar.../Del archivo: permite agregar una dirección de la lista, ya sea en forma manual (haga clic en **Agregar**) o desde un archivo de texto simple (haga clic en **Del archivo**). La opción **Del archivo** le permite agregar varias máscaras/direcciones URL desde el archivo de texto en el que están guardadas.

Editar... : Editar direcciones manualmente, por ejemplo, mediante el agregado de una máscara ("*" y "?").

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

Exportar...: guardar direcciones de la lista actual en un archivo de texto simple.

4.2.3 Filtrado de protocolos

El motor de exploración ThreatSense, que integra perfectamente todas las técnicas avanzadas para la exploración de malware, proporciona la protección antivirus para los protocolos de aplicación. El control funciona en forma automática, independientemente del navegador Web o del cliente de correo electrónico utilizado. Para comunicaciones cifradas (SSL), ingrese a **Filtrado de protocolos > SSL**.

Integrar al sistema : habilita el controlador para la funcionalidad de filtrado de protocolos de ESET NOD32 Antivirus.

Habilitar el filtrado del contenido de los protocolos de aplicación: si esta opción está habilitada, el módulo de exploración antivirus verificará todo el tráfico HTTP(S), POP3(S) e IMAP(S).

NOTA: desde Windows Vista Service Pack 1, Windows 7 y Windows Server 2008, la nueva arquitectura de Plataforma de filtrado de Windows (WFP) se usa para verificar la comunicación de red. La tecnología WFP utiliza técnicas de monitoreo especiales, por lo que las siguientes opciones no están disponibles:

- **Puertos HTTP, POP3 e IMAP**: limita el enrutamiento del tráfico al servidor proxy interno únicamente para los puertos correspondientes.
- **Las aplicaciones marcadas como navegadores Web y clientes de correo electrónico**: limita el enrutamiento del tráfico al servidor proxy interno únicamente para las aplicaciones marcadas como navegadores de Internet y clientes de correo electrónico (**Internet y correo electrónico > Filtrado de protocolos > Clientes de Internet y correo electrónico**).
- **Puertos y aplicaciones marcados como navegadores Web o clientes de correo electrónico**: habilita el enrutamiento de todo el tráfico de los puertos correspondientes así como todas las comunicaciones de las aplicaciones marcadas como navegadores de Internet y clientes de correo electrónico en el servidor proxy interno.

4.2.3.1 Clientes de Internet y correo electrónico

NOTA: desde Windows Vista Service Pack 1 y Windows Server 2008, la nueva arquitectura de Plataforma de filtrado de Windows (WFP) se usa para verificar la comunicación de red. La tecnología WFP utiliza técnicas de monitoreo especiales, por lo que la sección **Clientes de Internet y correo electrónico** no está disponible.

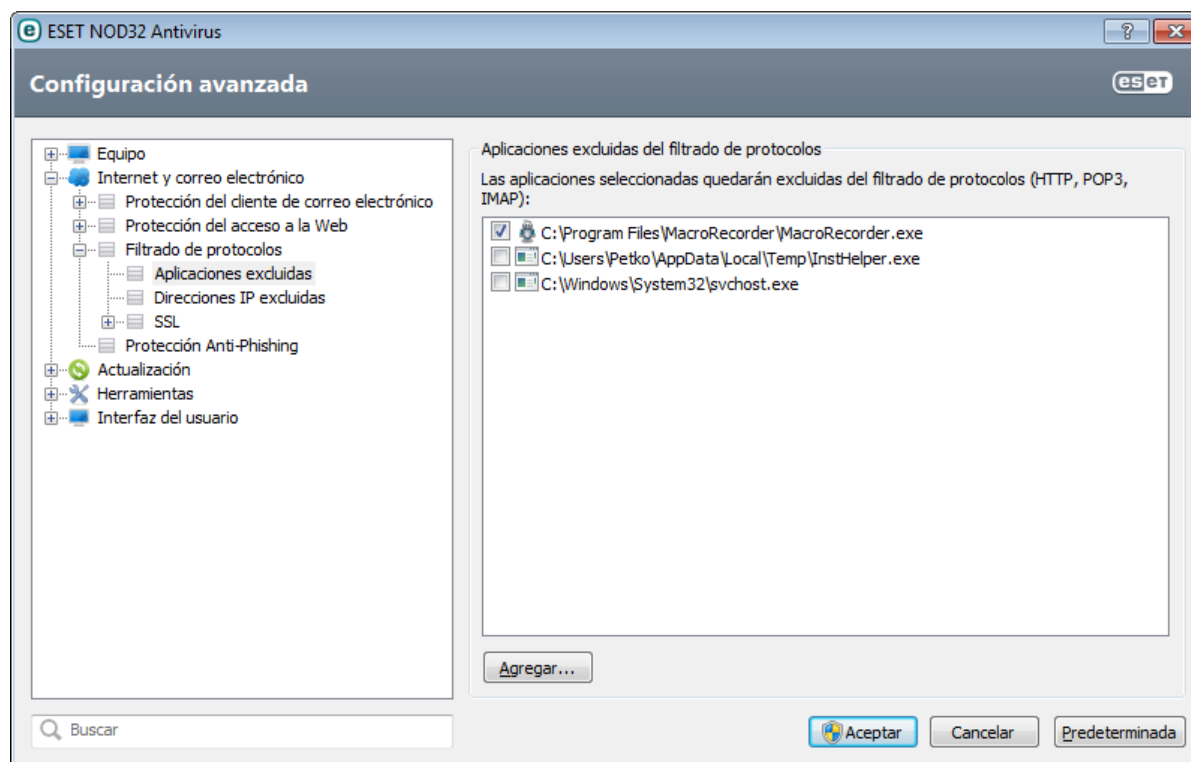
Dada la enorme cantidad de códigos maliciosos que circulan por Internet, la navegación segura es un aspecto crucial para la protección de los equipos. Las vulnerabilidades de los navegadores web y los vínculos fraudulentos sirven de ayuda a este tipo de código para introducirse en el sistema de incógnito; por este motivo, ESET NOD32 Antivirus se centra en la seguridad de los navegadores web. Todas las aplicaciones que accedan a la red se pueden marcar como navegadores de Internet. La casilla de verificación tiene dos estados posibles:

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

4.2.3.2 Aplicaciones excluidas

Para excluir del filtrado de contenido la comunicación de aplicaciones específicas con reconocimiento de redes, selecciónelas de la lista. La comunicación HTTP/POP3/IMAP de las aplicaciones seleccionadas no se verificará en busca de amenazas. Es recomendable usar esta opción solo para aplicaciones que no funcionen correctamente cuando se verifica su comunicación.

Las aplicaciones y los servicios activos se mostrarán automáticamente en esta ventana. Haga clic en el botón **Agregar...** para seleccionar manualmente una aplicación que no aparezca en la lista de filtrado de protocolos.

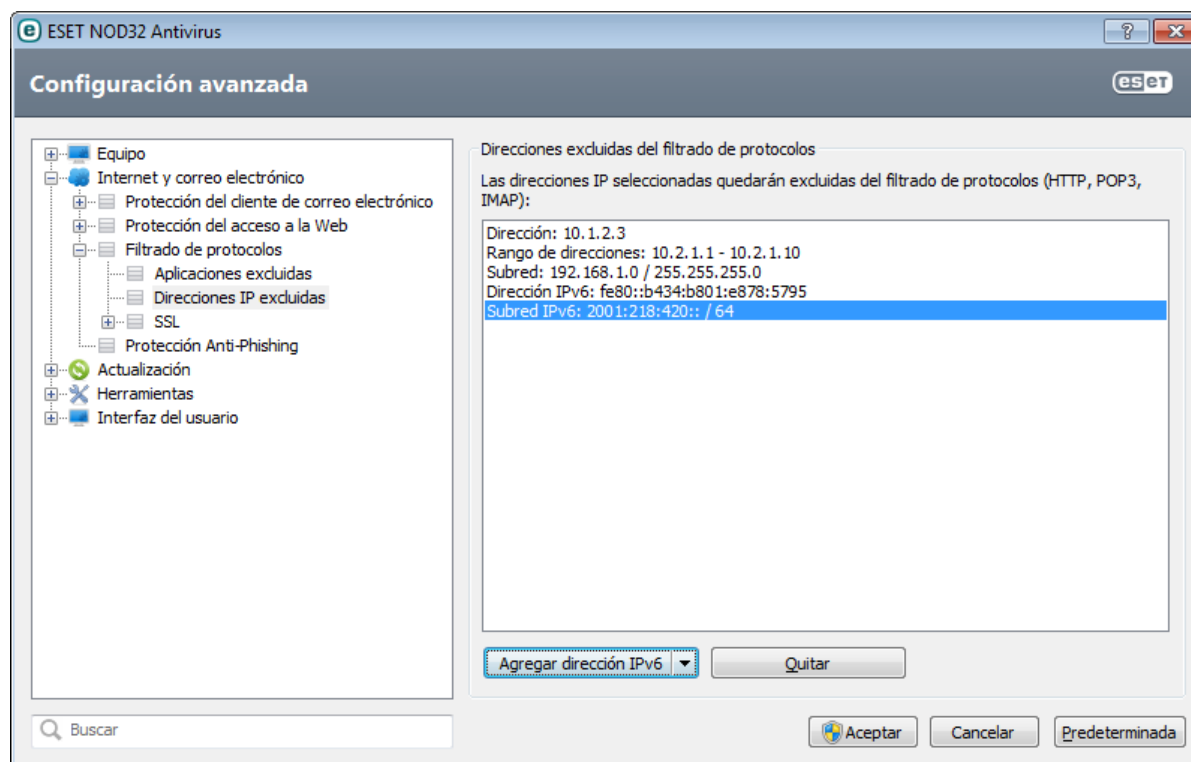


4.2.3.3 Direcciones IP excluidas

Las entradas de la lista quedarán excluidas del filtrado de contenido del protocolo. La comunicación HTTP/POP3/IMAP desde o hacia las aplicaciones seleccionadas no se verificará en busca de amenazas. Es recomendable que únicamente use esta opción para direcciones confiables conocidas.

Agregar dirección IPv4/IPv6: haga clic para agregar una dirección IP, un rango de direcciones o una subred de un punto remoto, al que se debe aplicar la 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 rango de direcciones o una subred de un punto remoto, al que se debe aplicar la regla. El protocolo de Internet versión 4 es la más antigua, pero sigue siendo la más utilizada.

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

Rango de direcciones: escriba la primera y la última dirección IP para especificar el rango de IP (de varios equipos) al que se debe aplicar la regla (por ejemplo, de *192.168.0.1* a *192.168.0.99*).

Subred: la subred (un grupo de equipos) está definida por una dirección IP y una máscara.

Por ejemplo, *255.255.255.0* es la máscara de red para el prefijo *192.168.1.0/24*, lo que implica un rango de direcciones de *192.168.1.1* a *192.168.1.254*.

4.2.3.3.2 Agregar dirección IPv6

Esto 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 y sustituirá a la versión 4 anterior.

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

Subred: la subred (un grupo de equipos) está definida por una dirección IP y una máscara (por ejemplo: *2002:c0a8:6301:1::1/64*).

4.2.3.4 Verificación del protocolo SSL

ESET NOD32 Antivirus permite verificar los protocolos encapsulados en el protocolo SSL. Puede utilizar varios modos de exploración para las comunicaciones protegidas por SSL: mediante certificados de confianza, certificados desconocidos o certificados excluidos de la verificación de comunicaciones protegidas por SSL.

Explorar siempre el protocolo SSL: seleccione esta opción para explorar todas las comunicaciones protegidas por SSL excepto las protegidas por certificados excluidos de la verificación. Si se establece una nueva comunicación que use un certificado firmado desconocido, no se notificará al usuario y se filtrará la comunicación en forma automática. Al acceder a un servidor con un certificado no confiable que fue marcado como de confianza (se agrega 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 los sitios no visitados (se pueden establecer exclusiones): si entra en un nuevo sitio protegido por SSL (con un certificado desconocido), se muestra un cuadro de diálogo con una selección de acciones posibles. Este modo le permite crear una lista de certificados SSL que se excluirán de la exploración.

No explorar el protocolo SSL: si esta opción está seleccionada, el programa no explorará las comunicaciones con el protocolo SSL.

Aplicar las excepciones creadas basándose en certificados: activa el uso de las exclusiones especificadas en los certificados excluidos y confiables para la exploración de comunicaciones SSL. Esta opción está disponible si selecciona **Explorar siempre el protocolo SSL**.

Bloquear las comunicaciones cifradas usando el protocolo obsoleto SSL v2: las comunicaciones que usen la versión anterior del protocolo SSL serán automáticamente bloqueadas.

4.2.3.4.1 Certificados

Para que la comunicación SSL funcione correctamente en los navegadores o clientes de correo electrónico, es imprescindible agregar el certificado raíz para ESET a la lista de certificados raíz conocidos (desarrolladores). **Agregar el certificado raíz a los navegadores conocidos** deberá estar habilitada. Seleccione esta opción para agregar automáticamente el certificado raíz de ESET a los navegadores conocidos (por ejemplo, Opera y Firefox). Para los navegadores que usan el almacén de certificaciones del sistema, el certificado se agrega en forma automática (por ej., Internet Explorer). Para aplicar el certificado en navegadores no compatibles, haga clic en **Ver el certificado > Detalles > Copiar en el archivo...** y luego impórtelo manualmente al navegador.

En algunos casos, el certificado no se puede verificar mediante el almacén de entidades de certificación raíz de confianza (por ej., VeriSign). Esto significa que alguien firma automáticamente el certificado (por ej., el administrador de un servidor de red o una empresa pequeña); por lo que considerar este certificado como confiable no siempre es un riesgo. La mayoría de los negocios (por ejemplo, los bancos) usan certificados firmados por TRCA (entidades de certificación raíz de confianza). Si **Preguntar sobre la validez del certificado** (predeterminado) está activada, el programa le indicará al usuario que seleccione la acción para realizar cuando se establezca una comunicación cifrada. Se mostrará un cuadro de diálogo para la selección de la acción donde puede decidir marcarlo como certificado de confianza o certificado excluido. En caso de que el certificado no esté presente en la lista de TRCA, la ventana es de color **rojo**. Si el certificado figura en la lista de TRCA, la ventana será de color **verde**.

Puede seleccionar **Bloquear las comunicaciones que usan el certificado** para que siempre se finalicen las conexiones cifradas al sitio que use el certificado sin verificar.

Si el certificado no es válido o está dañado, significa que el certificado está vencido o la firma automática no es correcta. En este caso, es recomendable bloquear la comunicación que usa el certificado.

4.2.3.4.1.1 Certificados de confianza

Además del almacén de entidades de certificación raíz de confianza donde ESET NOD32 Antivirus almacena los certificados de confianza, es posible crear una lista personalizada de certificados, que se puede ver en **Configuración avanzada (F5) > Internet y correo electrónico > Filtrado de protocolos > SSL > Certificados > Certificados de confianza**. ESET NOD32 Antivirus verificará el contenido de las comunicaciones cifradas mediante el uso de los certificados de esta lista.

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

4.2.3.4.1.2 Certificados excluidos

La sección Certificados excluidos contiene certificados que se consideran seguros. El contenido de las comunicaciones cifradas que utilicen los certificados de esta lista no se verificarán en busca de amenazas. Es recomendable excluir solo aquellos certificados Web con garantía de que son seguros y cuando la comunicación que use los certificados no necesite verificarse. Para eliminar elementos seleccionados de la lista, haga clic en **Quitar**. Haga clic en **Mostrar** (o haga doble clic en el certificado) para mostrar información sobre el certificado seleccionado.

4.2.3.4.1.3 Comunicación cifrada SSL

Si el equipo está configurado para la exploración del protocolo SSL, es posible que se abra una ventana de diálogo para elegir una acción cuando haya un intento de establecer una comunicación cifrada (mediante un certificado desconocido). La ventana de diálogo incluye la siguiente información: el nombre de la aplicación que inició la comunicación y nombre del certificado utilizado.

Si no se encuentra el certificado en el almacén de entidades de certificación raíz de confianza, será considerado no confiable.

Se encuentran disponibles las siguientes acciones para certificados:

Sí: el certificado se marcará temporalmente como de confianza; no se mostrará la ventana de alerta en el siguiente intento de utilizar el certificado.

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

No: marca el certificado como no confiable durante la sesión actual; no se mostrará la ventana de alerta en el siguiente intento de utilizar el certificado.

Excluir: agrega el certificado a la lista de certificados excluidos; los datos transferidos a través del canal cifrado dado no se verificarán en absoluto.

4.2.4 Protección antiphishing

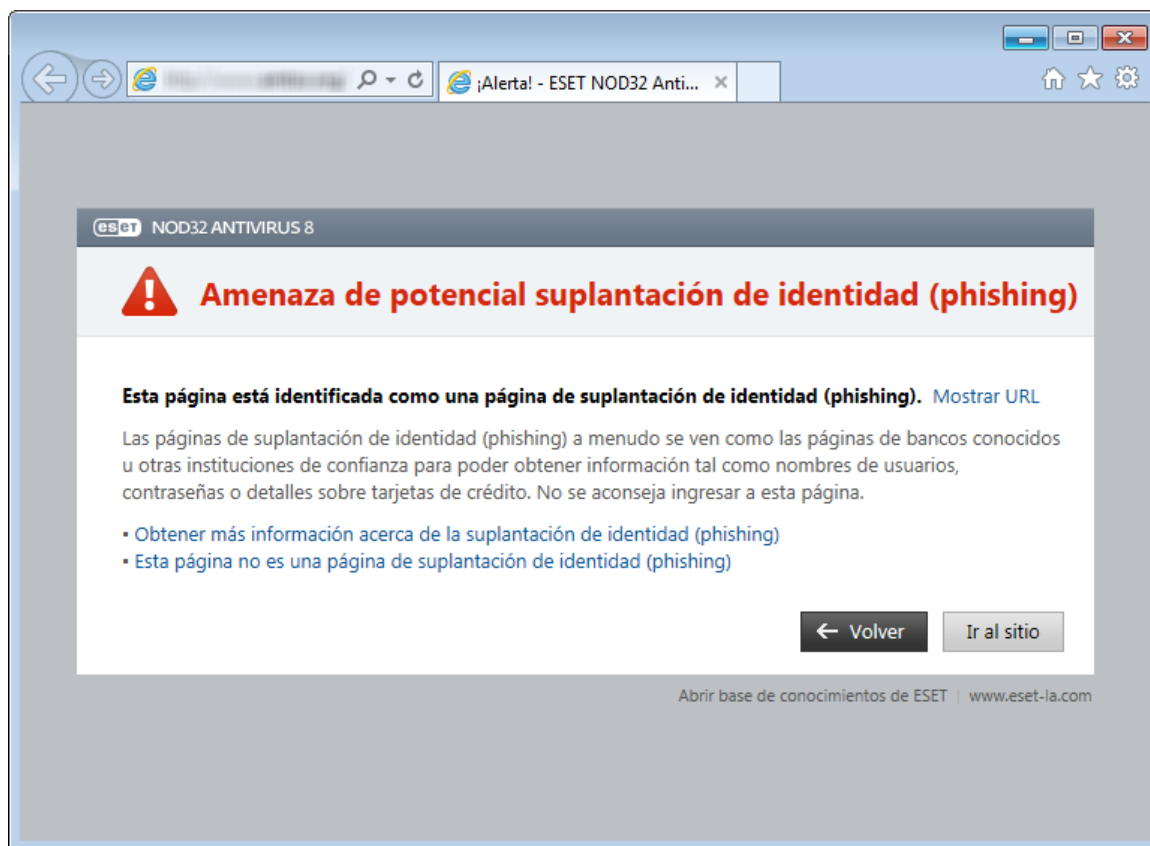
El término phishing define una actividad criminal que utiliza la ingeniería social (manipula a los usuarios para obtener información confidencial). El phishing suele utilizarse para obtener el acceso a datos confidenciales, como números de cuentas bancarias, códigos de identificación personal, etc. Lea más información sobre esta actividad en el [glosario](#). ESET NOD32 Antivirus brinda protección antiphishing: las páginas Web que se conocen con tal contenido siempre se bloquean.

Se recomienda firmemente habilitar Anti-Phishing en ESET NOD32 Antivirus. Puede acceder a esta opción desde **Configuración avanzada (F5)**. Vaya a **Internet y correo electrónico > Protección antiphishing**.

Consulte también nuestro [artículo de la base de conocimiento de ESET](#) para obtener una versión actualizada y más detallada de esta página de ayuda.

Acceso a un sitio Web de phishing

Cuando accede a un sitio Web de phishing, recibe el siguiente diálogo en su navegador Web. Al hacer clic en **Ir al sitio (no recomendado)**, podrá acceder al sitio Web sin un mensaje de advertencia.



NOTA: Los posibles sitios Web de phishing de la lista blanca se vencerán, de forma predeterminada, luego de algunas horas. Para permitir un sitio Web de manera permanente, puede usar la herramienta [Administración de direcciones URL](#). Desde **Configuración avanzada (F5)**, haga clic en **Internet y correo electrónico > Protección del acceso a la Web > Administración de direcciones URL**. Desde el menú desplegable de **Administración de direcciones URL**, seleccione **Lista de direcciones permitidas** y agregue su sitio Web a la lista.

Informe de un sitio de phishing

El vínculo [Informar un sitio de phishing](#) permite informar a ESET los sitios Web maliciosos o de phishing que deben analizarse.

NOTA: Antes de enviar un sitio Web a ESET, asegúrese de que cumpla con uno o más de los siguientes criterios:

- el programa directamente no detecta el sitio Web,
- el programa detecta erróneamente el sitio Web como una amenaza. En este caso, consulte el vínculo [Eliminar un sitio de phishing](#).

Como alternativa, puede enviar el sitio Web por correo electrónico. Envíe su correo electrónico a samples@eset.com. Recuerde agregar un asunto descriptivo y proporcionar la mayor cantidad de información posible sobre el sitio Web (por ej., el sitio Web que se lo recomendó, cómo escuchó hablar del sitio, etc.).

4.3 Actualización del programa

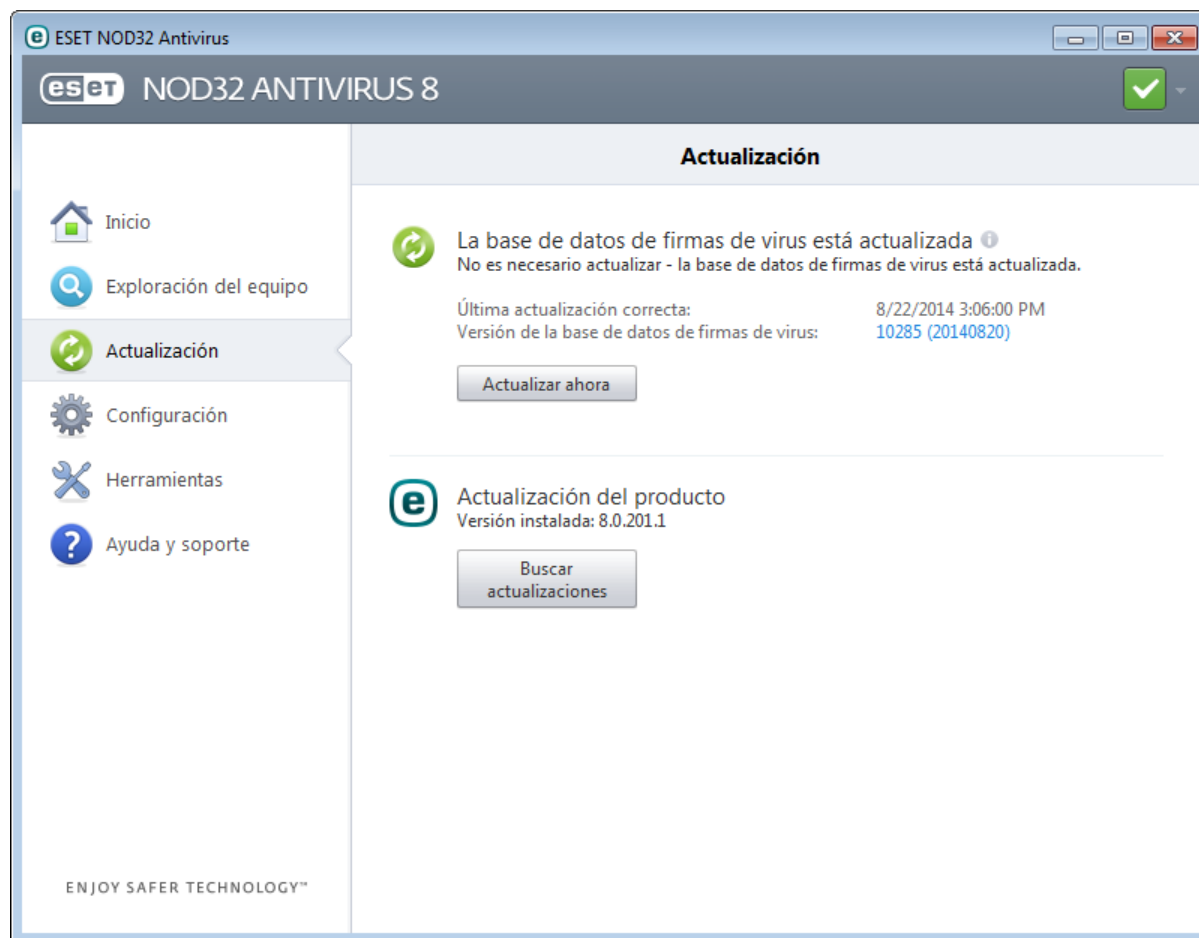
La actualización habitual de ESET NOD32 Antivirus es la mejor forma de asegurar el máximo nivel de seguridad en el equipo. El módulo de actualización garantiza que el programa esté siempre al día de dos maneras: actualizando la base de datos de firmas de virus y los componentes del sistema.

Al hacer clic en **Actualización** en la ventana principal del programa, puede visualizar el estado actual de la actualización, incluidas la fecha y la hora de la última actualización correcta, y si es necesario actualizar. La ventana principal también contiene la versión de la base de datos de firmas de virus. Este indicador numérico es un vínculo activo al sitio Web de ESET, donde aparece una lista de todas las firmas agregadas en esa actualización en particular.

Además de las actualizaciones automáticas, puede hacer clic en **Actualizar ahora** para accionar una actualización manual. La actualización de la base de datos de firmas de virus así como la actualización de componentes del programa constituyen una parte fundamental para mantener una protección completa contra códigos maliciosos. Preste atención a su configuración y funcionamiento. Si no ingresó los detalles de su licencia (Nombre de usuario y

Contraseña) durante la instalación, puede ingresar su Nombre de usuario y su Contraseña para acceder a los servidores de actualización de ESET cuando realiza una actualización.

NOTA: ESET proporciona el Nombre de usuario y la Contraseña tras la adquisición de ESET NOD32 Antivirus.



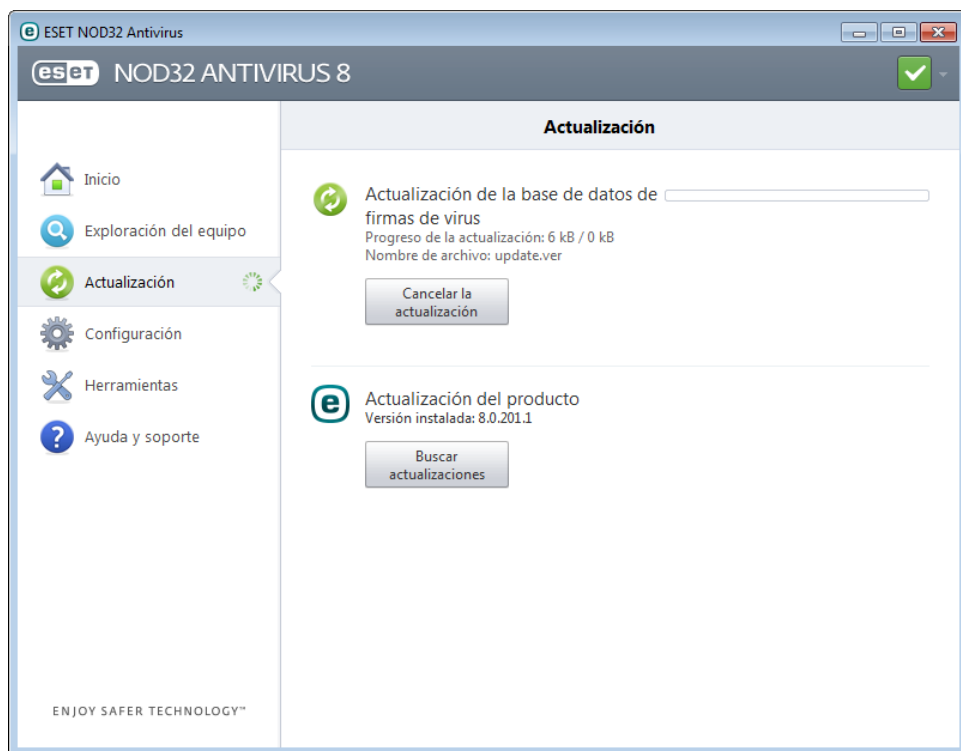
Última actualización correcta: es la fecha de la última actualización. Si no visualiza una fecha reciente, es posible que la base de datos de firmas de virus no esté actualizada.

Versión de la base de datos de firmas de virus: el número de la base de datos de firmas de virus, que además es un enlace activo al sitio Web de ESET. Haga clic en el número para ver una lista de todas las firmas agregadas en esa actualización en particular.

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

Proceso de actualización

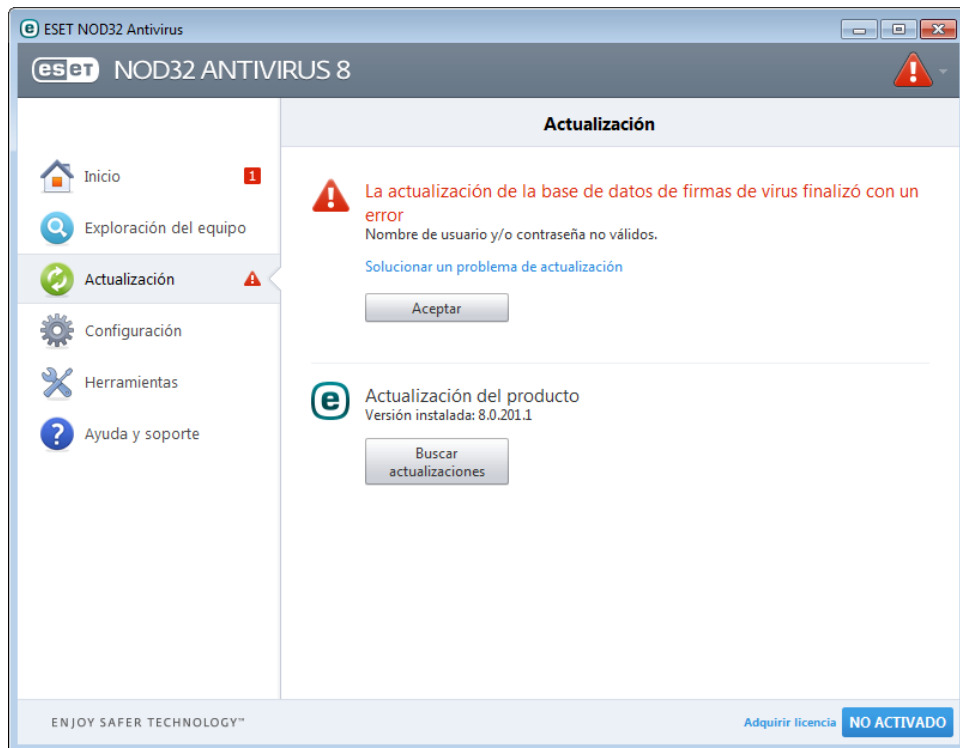
Luego de hacer clic en **Actualizar ahora**, comienza el proceso de descarga. Se mostrará una barra de progreso de la descarga y el tiempo restante para su finalización. Para interrumpir la actualización, haga clic en **Cancelar actualización**.



Importante: En circunstancias normales, cuando las actualizaciones se descargan correctamente, aparecerá el mensaje **No es necesario actualizar: la base de datos de firmas de virus está actualizada** en la ventana **Actualización**. Si este no es el caso, el programa está desactualizado y más vulnerable a una infección. Actualice la base de datos de firmas de virus lo antes posible. De lo contrario, se mostrará uno de los siguientes mensajes:

La notificación anterior está relacionada con los dos mensajes siguientes **La actualización de la base de datos de firmas de virus finalizó con un error** sobre actualizaciones insatisfactorias que se detallan a continuación:

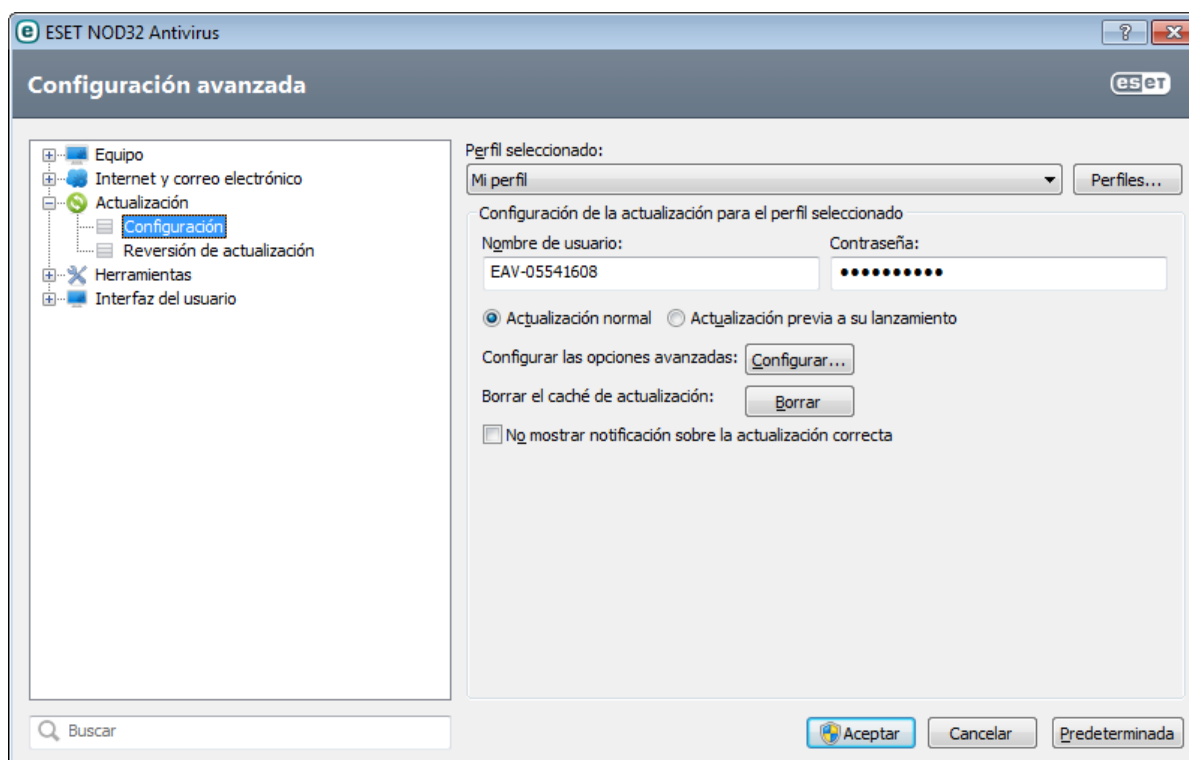
1. **Nombre de usuario y/o contraseña no válidos:** El Nombre de usuario y la Contraseña se ingresaron en forma incorrecta en la configuración de la actualización. Es recomendable verificar sus [datos de autenticación](#). La ventana de configuración avanzada (haga clic en **Configuración** desde el menú principal y luego en **Ingresar a la configuración avanzada...** o presione la tecla F5 del teclado) contiene opciones adicionales de actualización. Haga clic en **Actualización > Configuraciones** desde el árbol de configuración avanzada para ingresar un nombre de Usuario nuevo y Contraseña.
2. **Servidor no encontrado:** una posible causa del error es incorrecta [Ajustes de conexión a Internet](#). Es recomendable verificar su conectividad a Internet (para ello, abra cualquier sitio Web en su navegador Web). Si el sitio Web no se abre, es probable que la conexión a Internet no esté establecida o que haya problemas de conectividad en el equipo. Consulte el problema con su proveedor de servicios de Internet (ISP) si su conexión está inactiva.



4.3.1 Configuraciones de actualización

Las opciones de configuración de la actualización están disponibles desde el árbol de **Configuración avanzada** (tecla F5) al hacer clic en **Actualización > Configuración**. Esta sección especifica la información del origen de la actualización, como los servidores de actualización y sus datos de autenticación. En la versión local de los productos de ESET no puede elegir un servidor de actualizaciones propio. Se descargará Actualizar archivos automáticamente del servidor de ESET con el menor tráfico de red. El menú desplegable **Actualizar servidor** solo se encuentra disponible en ESET Endpoint Antivirus o ESET Endpoint Security.

Para que las actualizaciones se descarguen de manera adecuada, es fundamental ingresar correctamente toda la información de actualización. Si usa un firewall, asegúrese de que el programa tenga permiso para comunicarse con Internet (comunicación HTTP está habilitada).



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

crear un nuevo perfil.

La autenticación para los servidores de actualización está basada en el **Nombre de usuario** y la **Contraseña** generados y enviados al usuario tras la adquisición del producto. En forma predeterminada, no se requiere ninguna verificación y los campos **Nombre de usuario** y **Contraseña** quedan vacíos.

Las actualizaciones previas a su lanzamiento (la opción **Actualización previa a su lanzamiento**) son actualizaciones que fueron evaluadas en forma interna y que estarán disponibles al público en general en poco tiempo. Puede beneficiarse de la habilitación de las actualizaciones previas a la publicación al tener acceso a las soluciones y los métodos de detección más recientes. Sin embargo es posible que las actualizaciones previas a la publicación no sean lo suficientemente estables en todo momento y NO DEBEN utilizarse en estaciones de trabajo y servidores de producción donde se necesita de estabilidad y disponibilidad máximas. Puede encontrar la lista de los módulos actuales en **Ayuda y soporte > Acerca de ESET NOD32 Antivirus**. Se recomienda que los usuarios sin experiencia dejen la opción **Actualización normal** seleccionada, como aparece en forma predeterminada.

Haga clic en **Configurar...** al lado de **Configurar las opciones avanzadas** para mostrar una ventana con las opciones avanzadas de actualización.

En caso de que surjan problemas con una actualización, haga clic en **Borrar** para eliminar los archivos de actualización temporales.

No mostrar la notificación sobre actualizaciones correctas: desactiva la notificación de la bandeja del sistema en el sector inferior derecho de la pantalla. Resulta útil seleccionar esta opción si se está ejecutando una aplicación de pantalla completa o un juego. Tenga en cuenta que el [Modo de juego](#) desactivará todas las notificaciones.

4.3.1.1 Perfiles de actualización

Se pueden crear perfiles de actualización para diversas configuraciones y tareas de actualización. La creación de perfiles de actualización resulta útil en particular para usuarios móviles, que necesitan un perfil alternativo para las propiedades de conexión a Internet que cambian con frecuencia.

El menú desplegable **Perfil seleccionado** muestra el perfil seleccionado actualmente, que en forma predeterminada está configurado en **Mi perfil**. Para crear un nuevo perfil, haga clic en **Perfiles...**, luego en **Agregar...** e ingrese su propio **Nombre del perfil**. Al crear un nuevo perfil, puede copiar la configuración de uno existente seleccionándolo desde el menú desplegable **Copiar configuración desde el perfil**.

4.3.1.2 Configuración avanzada de la actualización

Para ver la configuración avanzada de la actualización, haga clic en **Configurar...** Entre las opciones de configuración avanzada de la actualización, se incluye la configuración del **Modo de actualización**, el **Proxy HTTP** y la **LAN**.

4.3.1.2.1 Modo de actualización

La pestaña **Modo de actualización** contiene las opciones relacionadas a la actualización de componentes del programa. El programa le permite al usuario predefinir su conducta cuando esté disponible un nuevo reemplazo de componentes del programa por una versión posterior.

Las actualizaciones de los componentes del programa (PCU) incluyen características nuevas o realizan cambios a características de versiones previas. Las PCU pueden realizarse automáticamente sin la intervención del usuario, pero también se puede elegir recibir una notificación cada vez que se realice una PCU. Luego de instalar la actualización de componentes del programa, es posible que se requiera reiniciar el equipo. En la sección **Actualización de componentes del programa** hay tres opciones disponibles:

- **Nunca actualizar los componentes del programa:** no se realizará ninguna actualización de componentes del programa en absoluto. Esta opción es adecuada para instalaciones en servidores, debido a que los servidores en general solo se pueden reiniciar durante su mantenimiento.
- **Siempre actualizar los componentes del programa:** la actualización de componentes del programa se descargará e instalará automáticamente. Recuerde que puede llegar a ser necesario reiniciar el equipo.
- **Preguntar antes de descargar componentes del programa:** es la opción predeterminada. El programa le solicitará que confirme o rechace las actualizaciones de componentes del programa cuando estén disponibles.

Luego de una actualización de componentes del programa, es posible que sea necesario reiniciar el equipo para que todos los módulos funcionen con su capacidad plena. La sección **Reiniciar tras la actualización de componentes del programa** permite seleccionar una de las siguientes opciones:

- **Nunca reiniciar el equipo:** el programa no le solicitará reiniciar el equipo, por más que sea necesario. Tenga en cuenta que no se recomienda utilizar esta opción, ya que es posible que el equipo no funcione correctamente hasta el próximo reinicio.
- **Ofrecer reiniciar el equipo si es necesario:** es la opción predeterminada. Luego de una actualización de componentes del programa por una versión posterior, se abrirá una ventana de diálogo que le solicitará reiniciar el equipo.
- **Si es necesario, reiniciar el equipo sin notificar:** luego de realizar un reemplazo de componentes del programa, se reiniciará el equipo (en caso de que sea necesario).

NOTA: La selección de la opción más apropiada depende de la estación de trabajo donde se aplicará la configuración. Tenga en cuenta que existen diferencias entre estaciones de trabajo y servidores. Por ejemplo, reiniciar el servidor automáticamente luego de una actualización del programa puede causar daños graves.

Si la opción **Preguntar antes de descargar la actualización** está seleccionada, se mostrará una notificación cuando haya una nueva actualización disponible.

Si el tamaño del archivo de actualización es mayor que el valor especificado en el campo **Preguntar si un archivo de actualización es más grande que**, el programa mostrará una notificación.

La opción **Verificar la última versión del producto en forma habitual** habilitará la tarea programada **Verificación de rutina de la última versión del producto** (ver el capítulo [Tareas programadas](#)).

4.3.1.2.2 Servidor proxy

Si desea acceder a las opciones de configuración del servidor proxy para un perfil de actualización determinado, haga clic en **Actualización** en el árbol de configuración avanzada (F5) y luego en **Configurar...** a la derecha de **Configurar las opciones avanzadas**. Haga clic en la pestaña **Proxy HTTP** y seleccione una de las siguientes tres opciones:

- **Usar la configuración global del servidor proxy**
- **No usar servidor proxy**
- **Conexión a través de un servidor proxy**

Al seleccionar la opción **Usar la configuración global del servidor proxy**, se usarán 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 indicar que no se usará ningún servidor proxy para actualizar ESET NOD32 Antivirus.

La opción **Conexión a través de un servidor proxy** debe estar seleccionada si:

- Es necesario utilizar un servidor proxy para actualizar ESET NOD32 Antivirus y es un servidor proxy diferente al especificado en la configuración global (**Herramientas > Servidor proxy**). En ese caso, la configuración debe especificarse aquí: dirección del **Servidor proxy**, **Puerto** de comunicación, además del **Nombre de usuario** y **Contraseña** para el servidor proxy, de ser necesario.
- La configuración del servidor proxy no se estableció en forma global, pero ESET NOD32 Antivirus se conectará a un servidor proxy para descargar las actualizaciones.
- El equipo está conectado a Internet mediante un servidor proxy. Durante la instalación del programa, la configuración se copia de Internet Explorer, pero si posteriormente se cambia (por ej., cambia el ISP), verifique desde esta ventana que la configuración del proxy HTTP sea la correcta. De lo contrario, el programa no podrá conectarse a los servidores de actualización.

La configuración predeterminada para el servidor proxy es **Usar la configuración global del servidor proxy**.

NOTA: Los datos de autenticación como el **Nombre de usuario** y la **Contraseña** sirven para acceder al servidor proxy. Complete estos campos solo si el nombre de usuario y la contraseña son necesarios. Recuerde que estos campos no corresponden a su nombre de Usuario y Contraseña para ESET NOD32 Antivirus y solo deben suministrarse si tiene la certeza de que se requiere una contraseña para acceder a Internet a través de un servidor proxy.

4.3.1.2.3 Conexión a la red de área local

Cuando se lleva a cabo una actualización desde un servidor local basado en el sistema operativo Windows NT, se requiere autenticar cada conexión de red en forma predeterminada.

Para configurar dicha cuenta, haga clic en la pestaña **LAN**. La sección **Conectarse a la LAN como** ofrece las opciones **Cuenta del sistema (predeterminado)**, **Usuario actual** y **Usuario especificado**.

Seleccione la opción **Cuenta del sistema (predeterminado)** si desea utilizar la cuenta del sistema para la autenticación. Normalmente, no se lleva a cabo ningún proceso de autenticación si no se proporcionan los datos de autenticación en la sección principal correspondiente a la configuración de la actualización.

Para asegurar que el programa realice la autenticación mediante la cuenta de un usuario actualmente registrado, seleccione **Usuario actual**. La desventaja de esta opción es que el programa no podrá conectarse al servidor de actualización cuando no haya ningún usuario registrado.

Seleccione **Usuario especificado** si desea que el programa use la cuenta de un usuario específico para realizar la autenticación. Utilice este método cuando falle la conexión predeterminada de la cuenta del sistema. Recuerde que la cuenta de usuario especificada debe tener acceso al directorio de archivos de actualización en el servidor local. De lo contrario, el programa no podrá establecer una conexión y descargar las actualizaciones.

Advertencia: cuando esté seleccionado el **Usuario actual** o el **Usuario especificado**, puede aparecer un error al cambiar la identidad del programa según el usuario deseado. Es recomendable ingresar los datos de autenticación de la LAN en la sección principal correspondiente a la configuración de la actualización. En esta sección de configuración de la actualización, los datos de autenticación deben ingresarse de la siguiente forma: *nombre_de_dominio\usuario* (si es un grupo de trabajo, ingrese *nombre_del_grupo_de_trabajo\nombre*) y la contraseña. Cuando se actualiza desde la versión HTTP del servidor local, no se necesita realizar ninguna autenticación.

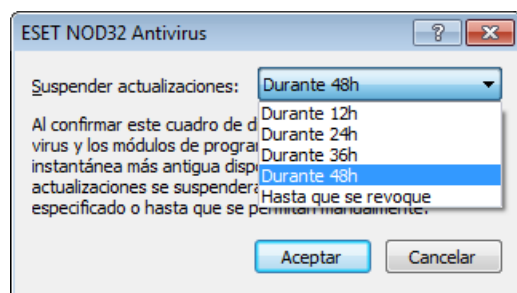
Seleccione **Desconectar del servidor tras la actualización** si la conexión al servidor permanece activa aunque las actualizaciones se hayan terminado de descargar.

4.3.2 Actualizar reversión

Si sospecha que la nueva actualización de la base de datos de virus o de los módulos de programas puede ser inestable o estar corrupta, puede hacer una reversión a la versión anterior y deshabilitar cualquier actualización para un período elegido. O bien puede habilitar las actualizaciones que se deshabilitaron anteriormente si las pospuso de manera indefinida.

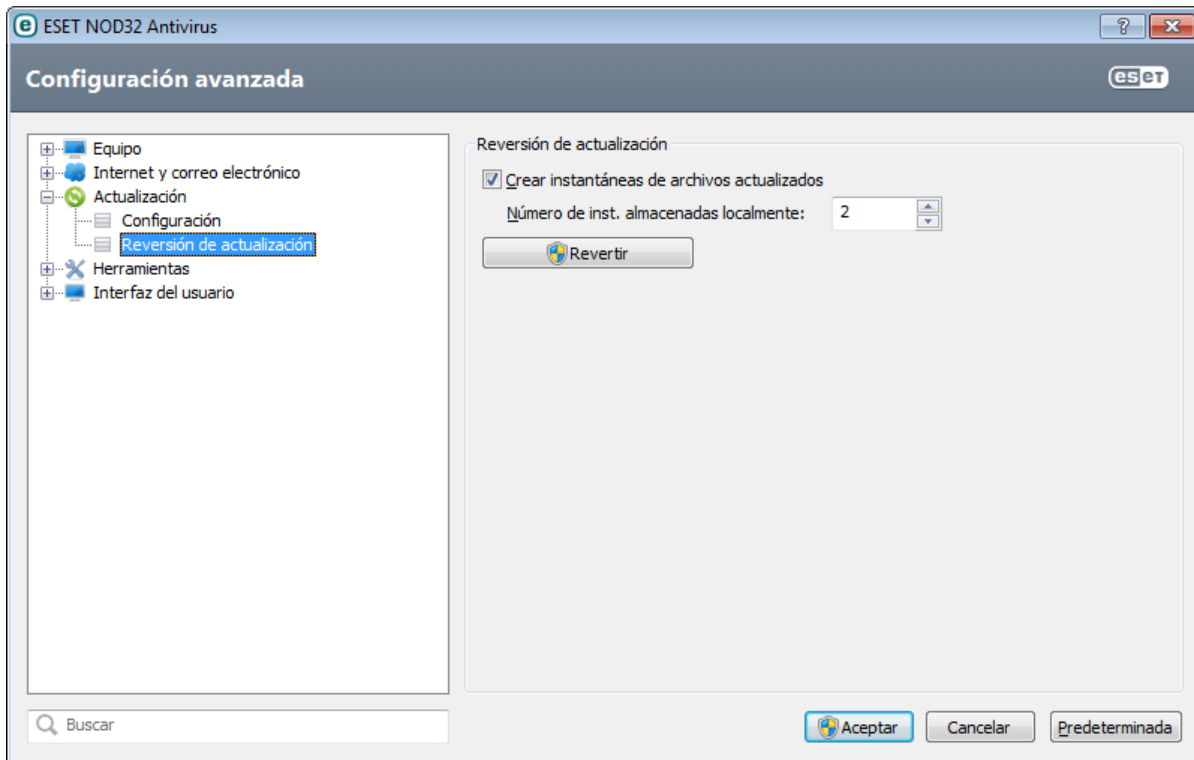
ESET NOD32 Antivirus registra instantáneas de la base de datos de firmas de virus y de los módulos de programa para usar con la característica de *reversión*. Para crear instantáneas de la base de datos de virus, deje la casilla de verificación **Crear instantáneas de los archivos de actualización** seleccionada. El campo **Cantidad de instantáneas almacenadas localmente** define la cantidad de instantáneas anteriores de la base de datos de virus que se almacenaron.

Si hace clic en **Revertir (Configuración avanzada (F5) > Actualización > Revertir actualización)**, debe seleccionar un intervalo de tiempo del menú desplegable **Suspender actualizaciones** que represente el período en que se hará una pausa en las actualizaciones de la base de datos de firmas de virus y del módulo del programa.



Seleccione **Hasta que se revoque** para posponer las actualizaciones regulares de manera indefinida hasta restaurar manualmente la funcionalidad de actualización. Debido a que esto representa un riesgo potencial para la seguridad, no recomendamos seleccionar esta opción.

Si se realiza una reversión, el botón **Revertir** cambia a **Permitir actualizaciones**. No se permitirán las actualizaciones durante el intervalo de tiempo seleccionado desde el menú desplegable **Suspender actualizaciones**. La versión de la base de datos de firmas de virus se degrada a la versión más antigua disponible y guardada como una instantánea en el sistema local de archivos del equipo.



Ejemplo: Deje que el número 6871 sea la versión más reciente de la base de datos de firmas de virus. 6870 y 6868 se guardan como instantáneas de la base de datos de firmas de virus. Tenga en cuenta que 6869 no está disponible porque, por ejemplo, el equipo estaba apagado y se ofreció una actualización más reciente antes de descargar 6869. Si ha ingresado 2 (dos) en el campo **Cantidad de instantáneas almacenadas localmente** y hace clic en **Revertir**, la base de datos de firmas de virus (incluidos los módulos de programa) se restaurará a la versión número 6868. Este proceso puede tardar un poco. Revise si la versión de la base de datos de firmas de virus se ha degradado desde la ventana principal del programa de ESET NOD32 Antivirus en la sección [Actualizar](#).

4.3.3 Cómo crear tareas de actualización

Las actualizaciones pueden accionarse manualmente con un clic en **Actualizar la base de datos de firmas de virus** en la ventana primaria que se muestra al hacer clic en **Actualización** en el menú principal.

Las actualizaciones también pueden ejecutarse como tareas programadas. Para configurar una tarea programada, haga clic en **Herramientas > Tareas programadas**. Las siguientes tareas se encuentran activas en forma predeterminada en ESET NOD32 Antivirus:

- **Actualización automática de rutina**
- **Actualización automática tras conexión de acceso telefónico**
- **Actualización automática tras el registro del usuario**

Cada tarea de actualización puede modificarse acorde a sus necesidades. Además de las tareas de actualización predeterminadas, puede crear nuevas tareas de actualización con una configuración definida por el usuario. Para obtener más detalles sobre la creación y la configuración de tareas de actualización, consulte la sección [Tareas programadas](#).

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 siguientes herramientas:

- [Archivos de registro](#)
- [Estadísticas de protección](#)
- [Observar la actividad](#)
- [Procesos activos](#) (si ESET Live Grid está habilitado en ESET NOD32 Antivirus)
- [Tareas programadas](#)
- [Cuarentena](#)
- [ESET SysInspector](#)

Enviar el archivo para su análisis: permite enviar un archivo sospechoso al laboratorio de virus de ESET para su análisis. La ventana de diálogo que se muestra tras hacer clic en esta opción se describe en la sección [Envío de archivos para su análisis](#).

ESET SysRescue: inicia el asistente para la creación de ESET SysRescue.

Nota: ESET SysRescue puede no estar disponible para Windows 8 en versiones más antiguas de los productos de seguridad de ESET. En este caso recomendamos que actualice su producto o cree un ESET SysRescue disco en otra versión de Microsoft Windows.

ESET Social Media Scanner: vínculo a la aplicación de medios sociales (es decir, Facebook) para proteger a los usuarios de medios sociales contra amenazas. Esta aplicación es independiente de otros productos de ESET y es completamente gratis.

4.4.1 Archivos de registro

Los archivos de registro contienen información sobre todos los sucesos importantes del programa que se llevaron a cabo y proporcionan una visión general de las amenazas detectadas. La emisión de registros es un componente esencial para el análisis del sistema, la detección de amenazas y la solución de problemas. La emisión de registros se mantiene activa en segundo plano sin necesidad de la interacción del usuario. La información se registra de acuerdo con el nivel de detalle actualmente configurado. Se pueden ver los mensajes de texto y los registros directamente desde el entorno de ESET NOD32 Antivirus, donde además se pueden comprimir registros.

Para acceder a los archivos de registro, diríjase a la ventana principal del programa y haga clic en **Herramientas > Archivos de registro**. Seleccione el tipo de registro deseado del menú desplegable **Registro**. Se encuentran disponibles los siguientes registros:

- **Amenazas detectadas:** el registro de amenazas ofrece información detallada sobre las infiltraciones detectadas por ESET NOD32 Antivirus. Esta información incluye la hora de la detección, el nombre de la infiltración, la ubicación, la acción realizada y el nombre del usuario registrado cuando se detectó la infiltración. Haga doble clic en la entrada de cualquier registro para mostrar sus detalles en una ventana separada.
- **Sucesos:** todas las acciones importantes que ESET NOD32 Antivirus lleva a cabo se registran en el registro de sucesos. El registro de sucesos contiene información sobre los sucesos y errores que se produjeron en el programa. Se diseñó para que los administradores de sistemas y los usuarios puedan solucionar problemas. Con frecuencia, la información aquí incluida puede ayudarlo a encontrar una solución a un problema que ocurra en el programa.
- **Exploración del equipo:** en esta ventana se muestran los resultados de todas las exploraciones completadas, tanto las ejecutadas manualmente como las planificadas. Cada línea corresponde a un único control del equipo. Haga doble clic en cualquier entrada para visualizar los detalles de la exploración respectiva.
- **HIPS:** contiene historiales de las reglas [HIPS](#) específicas que se marcaron para incluirse en el registro. El protocolo muestra la aplicación que desencadenó la operación, el resultado (si la regla se permitió o prohibió) y el nombre de la regla creada.
- **Sitios Web filtrados:** Esta lista es útil si quiere consultar los sitios Web bloqueados por la [Protección del acceso a la Web](#). En estos registros puede ver la hora, la dirección URL, el usuario y la aplicación de creación de conexión con el sitio Web en particular.
- **Control del dispositivo:** contiene registros de medios o dispositivos extraíbles que se conectaron al equipo. Solo los dispositivos con reglas de control del dispositivo respectivo se registrarán en el archivo de registro. Si la regla no coincide con un dispositivo conectado, se creará una entrada del registro para un dispositivo conectado. Aquí también puede ver detalles tales como el tipo de dispositivo, número de serie, nombre del proveedor y tamaño del medio (si está disponible).

En cada una de las secciones, la información mostrada se puede copiar directamente en el portapapeles; para ello, seleccione la entrada y presione las teclas de acceso directo Ctrl+C desde el teclado o haga clic en el botón **Copiar**. Para seleccionar varias entradas, puede utilizar las teclas CTRL y MAYÚS.

Puede hacer un clic derecho en una entrada específica para mostrar el menú contextual. Las siguientes opciones se encuentran disponibles en el menú contextual:

- **Filtrar historiales del mismo tipo:** luego de activar este filtro, solo verá los historiales del mismo tipo (diagnósticos, advertencias, etc.).
- **Filtrar.../Buscar...:** cuando esta habilitado, aparecerá una ventana emergente **Filtrado de registros** donde podrá definir los criterios del filtrado.
- **Limpiar el filtro:** borra todas las configuraciones del filtro (descritas arriba).
- **Copiar todo:** copia la información sobre todos los historiales que aparecen en la ventana.
- **Eliminar/Eliminar todo:** elimina los historiales seleccionados o todos los historiales mostrados (esta acción requiere privilegios de administrador).
- **Exportar:** exporta información sobre los historiales en formato XML.
- **Desplazar registro:** deje esta opción habilitada para desplazarse automáticamente desde los registros viejos a los activos en la ventana **Archivos de registro**.

4.4.1.1 Mantenimiento de registros

Se puede acceder a la configuración de la emisión de registros de ESET NOD32 Antivirus desde la ventana principal del programa. Haga clic en **Configuración > Ingresar a la configuración avanzada... > > Herramientas > Archivos de registro**. La sección Archivos de registros se usa para definir cómo se administrarán los registros. El programa elimina en forma automática los registros más antiguos para ahorrar espacio en el disco rígido. Especifique las siguientes opciones para los archivos de registro:

Nivel de detalle mínimo para los registros: especifica el nivel mínimo de detalle de los sucesos que se registrarán.

- **Diagnóstico:** registra la información necesaria para ajustar el programa y todos los historiales mencionados arriba.
- **Informativo:** registra los mensajes de información, incluyendo los mensajes de actualizaciones correctas, y todos los historiales mencionados arriba.
- **Advertencias:** registra errores críticos y mensajes de advertencia.
- **Errores:** Se registrarán los errores tales como *“Error al descargar el archivo”* y errores críticos.
- **Crítico:** registra solo los errores críticos (como por ej., un error al iniciar la protección antivirus, etc.)

Se eliminarán automáticamente las entradas de registro anteriores a la cantidad de días especificada en el campo **Eliminar automáticamente historiales anteriores a X días**.

Optimizar archivos de registro automáticamente: si se selecciona esta opción, se desfragmentarán automáticamente los archivos de registro si el porcentaje es mayor al valor especificado en el campo **Si la cantidad de historiales no utilizados excede X (%)**.

Haga clic en **Optimizar ahora** para comenzar la desfragmentación de los archivos de registro. Durante este proceso, se eliminan todas las entradas de registro vacías, lo que mejora el rendimiento y la velocidad de procesamiento de los registros. Esta mejora se observa más claramente cuanto mayor es el número de entradas de los registros.

4.4.2 Tareas programadas

Desde la sección de tareas programadas, se gestionan y ejecutan tareas programadas según la configuración y las propiedades predefinidas.

Puede acceder a las tareas programadas desde la ventana principal del programa ESET NOD32 Antivirus, al hacer clic en **Herramientas > Tareas programadas**. La sección **Tareas programadas** contiene una lista de todas las tareas programadas y propiedades de configuración, como la fecha y la hora predefinidas y el perfil de exploración utilizado.

Esta sección sirve para programar las siguientes tareas: la actualización de la base de datos de firmas de virus, la exploración, la verificación de archivos de inicio del sistema y el mantenimiento de registros. Puede agregar o eliminar tareas directamente desde la ventana principal de tareas programadas (haga clic en **Agregar...** o **Eliminar** en el sector inferior). Haga un clic derecho en cualquier parte de la ventana Tareas programadas para realizar una de las siguientes acciones: mostrar información detallada, ejecutar la tarea de inmediato, agregar una nueva tarea y eliminar una tarea existente. Utilice las casillas de verificación al comienzo de cada entrada para activar o desactivar las tareas.

En forma predeterminada, se muestran las siguientes **tareas programadas**:

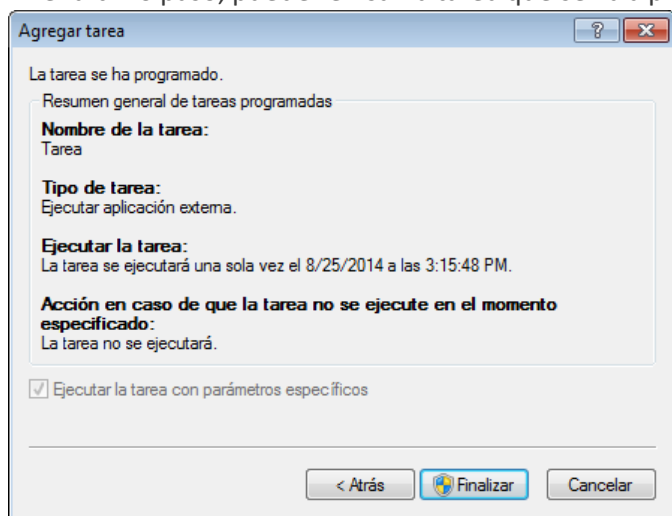
- **Mantenimiento de registros**
- **Actualización automática de rutina**
- **Actualización automática tras conexión de acceso telefónico**
- **Actualización automática tras el registro del usuario**
- **Verificación de rutina de la última versión del producto** (consulte el [Modo de actualización](#))
- **Exploración automática de archivos durante el inicio del sistema** (tras el registro del usuario)
- **Exploración automática de archivos durante el inicio del sistema** (tras la actualización correcta de la base de datos de firmas de virus)
- **Primera exploración automática**

Para editar la configuración de una tarea programada existente (ya sea predeterminada o definida por el usuario), haga un clic derecho en la tarea y luego en **Editar...** o seleccione la tarea que quiera modificar y haga clic en el botón

Editar....

Agregar una nueva tarea

1. Haga clic en **Agregar...** en el sector inferior de la ventana.
2. Seleccione la tarea deseada en el menú desplegable.
3. Introduzca un nombre de la tarea y seleccione una de las opciones de programación:
 - **Una vez:** la tarea se realizará una sola vez, en la fecha y a la hora predefinidas.
 - **Reiteradamente:** la tarea se realizará con el intervalo de tiempo especificado (en horas).
 - **Diariamente:** la tarea se ejecutará todos los días a la hora especificada.
 - **Semanalmente:** la tarea se ejecutará una o varias veces a la semana, en los días y a la hora especificados.
 - **Cuando se cumpla la condición:** la tarea se ejecutará tras un suceso especificado.
4. Según la opción de programación elegida en el paso anterior, se mostrará una de las siguientes ventanas de diálogo:
 - **Una vez:** la tarea se realizará en la fecha y a la hora predefinidas.
 - **Reiteradamente:** la tarea se realizará con el intervalo de tiempo especificado.
 - **Diariamente:** la tarea se ejecutará reiteradamente todos los días a la hora especificada.
 - **Semanalmente:** la tarea se ejecutará el día y a la hora especificados.
5. Si la tarea no se pudo ejecutar en el momento predefinido, puede especificar cuándo se realizará nuevamente:
 - Esperar hasta la próxima hora programada
 - Ejecutar la tarea lo antes 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 se va a 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 del menú desplegable **Estadísticas** para ver el gráfico y la leyenda correspondientes. Si pasa el mouse sobre un elemento de la leyenda, el gráfico únicamente mostrará los datos de ese elemento.

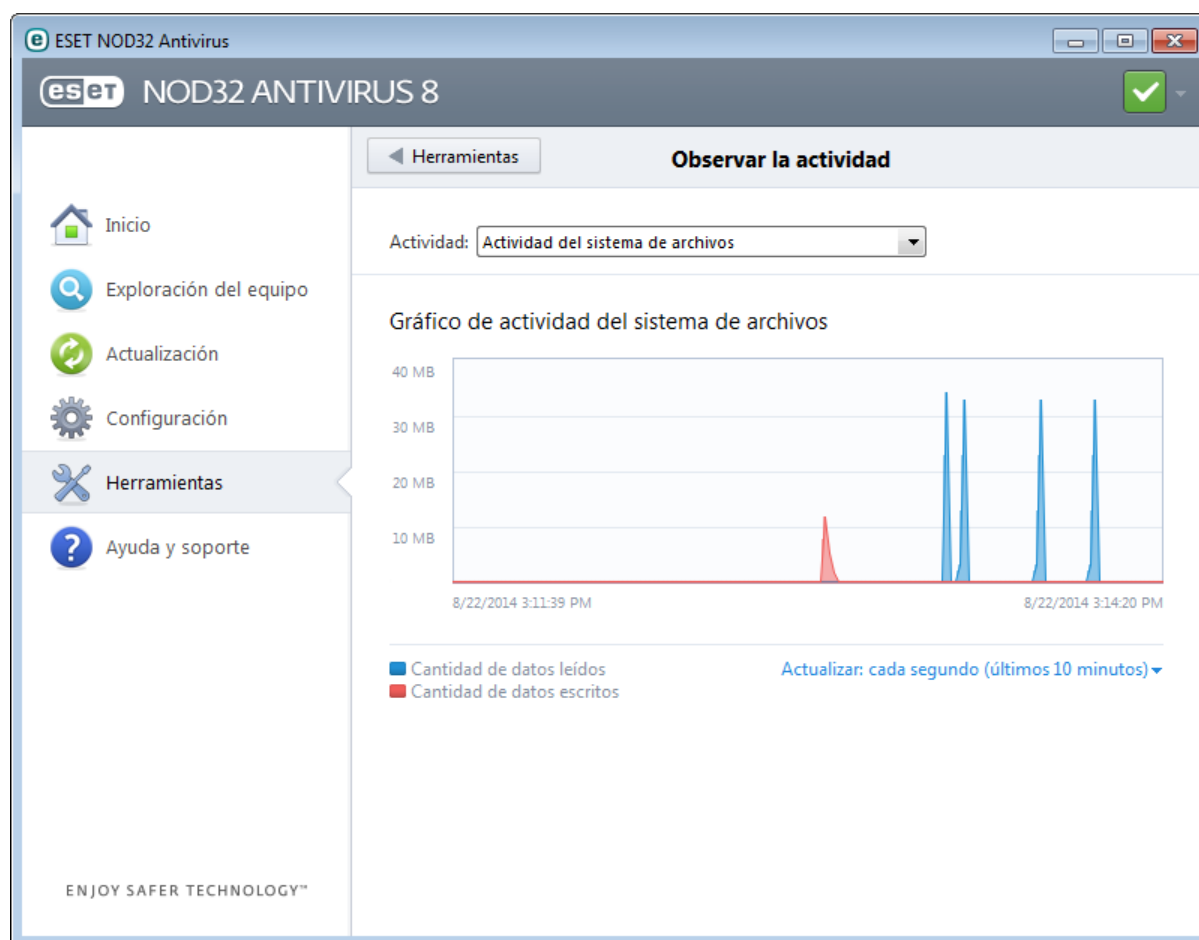
Están disponibles los siguientes gráficos de estadísticas:

- **Protección antivirus y antispyware:** muestra la cantidad de objetos infectados y desinfectados.
- **Protección del sistema de archivos:** solo muestra los objetos que fueron leídos o escritos en el sistema de archivos.
- **Protección del cliente de correo electrónico:** solo muestra los objetos que fueron enviados o recibidos por clientes de correo electrónico.
- **Acceso Web y protección antiphishing:** solo muestra los objetos descargados por los navegadores Web.

Debajo de los gráficos de estadísticas, podrá ver la cantidad total de objetos explorados, el último objeto explorado, y la fecha y hora de la creación de las estadísticas. Haga clic en **Restablecer** para borrar toda la información estadística.

4.4.4 Observar la actividad

Para observar la **Actividad del sistema de archivos** actual en forma de gráfico, haga clic en **Herramientas > Observar la actividad**. En el sector inferior del gráfico hay una línea de tiempo que registra la actividad del sistema de archivos en tiempo real conforme al intervalo de tiempo seleccionado. Para modificar el intervalo de tiempo, haga clic en la opción **Actualizar: 1...** en la parte inferior derecha de la ventana.



Se encuentran disponibles las siguientes opciones:

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

El eje vertical del **Gráfico de actividad del sistema de archivos** representa los datos leídos (en azul) y los escritos (en rojo). Los dos valores están representados en KB (kilobytes)/MB/GB. Al pasar el mouse sobre los datos leídos o escritos en la leyenda que se encuentra abajo del gráfico, el gráfico solo mostrará los datos correspondientes a ese tipo de actividad.

4.4.5 ESET SysInspector

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

La ventana SysInspector muestra la siguiente información sobre los registros creados:

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

Están disponibles las siguientes opciones:

- **Comparar:** compara dos registros existentes.
- **Crear...:** crea un nuevo registro. Espere hasta que el registro de ESET SysInspector se haya completado (cuando su **Estado** sea Creado).
- **Eliminar:** elimina los registros seleccionados de la lista.

Al hacer un clic derecho en uno o varios registros seleccionados, se ofrecen las siguientes opciones desde el menú contextual:

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

4.4.6 ESET Live Grid

ESET Live Grid (creada en el sistema avanzado de alerta temprana de ThreatSense.Net ESET) utiliza datos que los usuarios de ESET enviaron de todo el mundo y lo envía al laboratorio de virus de ESET. Al proporcionar muestras sospechosas y metadatos from the wild, ESET Live Grid nos permite reaccionar inmediatamente ante las necesidades de nuestros clientes y mantener a ESET receptivo a las últimas amenazas. Lea más acerca de ESET Live Grid en el [glosario](#).

Un usuario puede verificar la reputación de [los procesos activos](#) y de los archivos directamente desde la interfaz del programa o desde el menú contextual, con información adicional disponible desde ESET Live Grid. Hay dos opciones:

1. Puede decidir no habilitar ESET Live Grid. No perderá funcionalidad alguna en el software, pero, en algunos casos, ESET NOD32 Antivirus puede responder más rápido a las nuevas amenazas que una actualización de la base de datos de firmas de virus.
2. Puede configurar ESET Live Grid para enviar información anónima sobre nuevas amenazas y sobre el contexto donde se encuentra dicho código. Es posible enviar este archivo a ESET para su análisis detallado. El estudio de estos códigos ayudará a ESET a actualizar su capacidad de detección de amenazas.

ESET Live Grid recopilará información sobre el equipo en relación con las nuevas amenazas detectadas. Dicha información puede incluir una muestra o copia del archivo donde apareció la amenaza, la ruta a ese archivo, el nombre del archivo, la fecha y la hora, el proceso mediante el cual apareció la amenaza e información sobre el sistema operativo del equipo.

En forma predeterminada, ESET NOD32 Antivirus está configurado para enviar archivos sospechosos al laboratorio de virus de ESET para su análisis detallado. Los archivos con ciertas extensiones, como *.doc* o *.xls*, siempre se excluyen. También puede agregar otras extensiones si hay archivos específicos que usted o su empresa prefieren no enviar.

El menú de configuración de ESET Live Grid proporciona varias opciones para habilitar o deshabilitar ESET Live Grid, que sirve para enviar archivos sospechosos e información estadística anónima a los laboratorios de ESET. Puede acceder al sistema desde el Árbol de configuración avanzada, al hacer clic en **Herramientas > ESET Live Grid**.

Participar en ESET Live Grid (recomendado): habilita o deshabilita ESET Live Grid, que sirve para enviar archivos sospechosos e información estadística anónima a los laboratorios de ESET.

No enviar las estadísticas: seleccione esta opción si no quiere enviar información anónima sobre su equipo recopilada por ESET Live Grid. Esta información guarda relación con las nuevas amenazas detectadas, que pueden incluir el nombre de la infiltración, información sobre la fecha y la hora de la detección, la versión de ESET NOD32 Antivirus, información sobre la versión del sistema operativo del equipo y la configuración de la ubicación. En general, las estadísticas se envían a los servidores de ESET una o dos veces por día.

No enviar los archivos: los archivos sospechosos, que se asemejan a infiltraciones por su contenido o conducta, no se envían a ESET para su análisis mediante la tecnología ESET Live Grid.

Configuración avanzada...: abre una ventana con opciones adicionales para la configuración de ESET Live Grid.

Si usted ya utilizó antes ESET Live Grid y lo deshabilitó, es posible que hayan quedado paquetes de datos para enviar. Aunque lo haya desactivado, esos paquetes se enviarán a ESET en la próxima oportunidad. Posteriormente, no se seguirán creando paquetes.

4.4.6.1 Archivos sospechosos

La pestaña **Archivos** en la configuración avanzada de ESET Live Grid permite configurar la manera en que las amenazas se envían a los laboratorios de virus de ESET para su análisis.

Si encuentra un archivo sospechoso, puede enviarlo a nuestro laboratorio de amenazas para su análisis. Si se trata de una aplicación maliciosa, se agregará su detección en la siguiente actualización de firmas de virus.

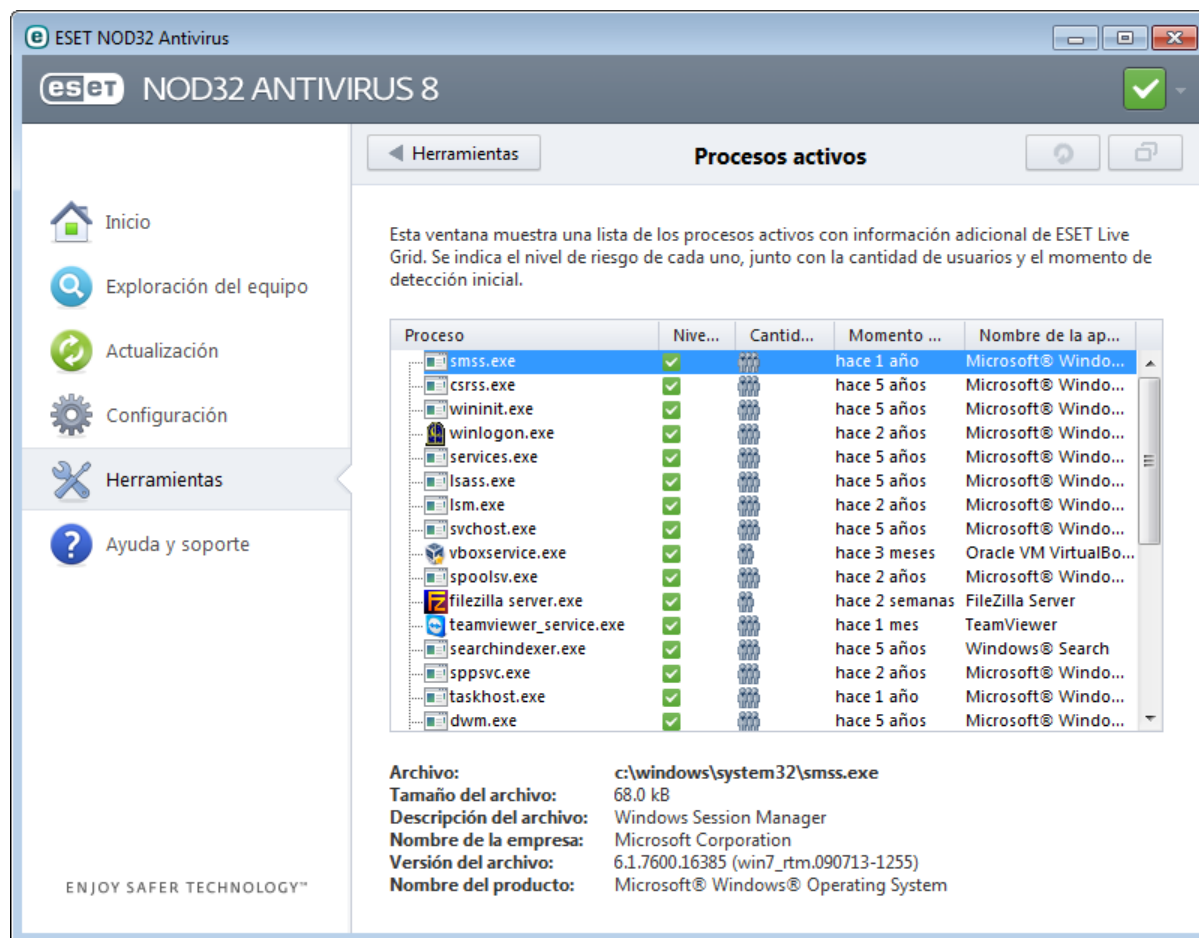
Filtro de exclusión: el filtro de exclusión permite excluir ciertos archivos o carpetas del envío. Los archivos incluidos en la lista nunca se enviarán a los laboratorios de ESET para su análisis, aunque contengan un código sospechoso. Por ejemplo, quizá resulte útil excluir archivos que puedan contener información confidencial, como documentos u hojas de cálculo. Los tipos de archivos más comunes se excluyen en forma predeterminada (*.doc*, etc.). Si lo desea, puede agregar archivos a la lista de archivos excluidos.

Correo electrónico de contacto (opcional): puede incluir su correo electrónico junto con los archivos sospechosos, así podrá utilizarse para contactarlo en caso de que se requiera información adicional para el análisis. Recuerde que no recibirá ninguna respuesta de ESET a menos que se necesite información adicional.

Seleccione **Habilitar la creación de registros** para crear un registro de sucesos que recopile información sobre los archivos y los datos estadísticos enviados. Esto permite la creación de registros en el [Registro de sucesos](#) cuando los archivos o datos estadísticos se envían.

4.4.7 Procesos activos

Los procesos activos muestran los programas o procesos activos en su equipo y mantiene a ESET informado de manera instantánea y continua sobre las nuevas infiltraciones. ESET NOD32 Antivirus proporciona información detallada sobre los procesos activos para proteger a los usuarios con la tecnología [ESET Live Grid](#).



Proceso: la imagen y el nombre del programa o proceso que se está ejecutando actualmente en el equipo. También puede usar el Administrador de tareas de Windows para ver todos los procesos activos en el equipo. Para abrir el Administrador de tareas, haga un clic derecho en un área vacía de la barra de tareas y luego seleccione el **Administrador de tareas**, o presione las teclas Ctrl+Mayús+Esc en el teclado.

Nivel de riesgo: en la mayoría de los casos, la tecnología ESET NOD32 Antivirus y ESET Live Grid les asigna niveles de riesgo a los objetos (archivos, procesos, claves de registro, etc.). Para ello, utiliza una serie de reglas heurísticas que examinan las características de cada uno objeto y después estima su 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)**.

NOTA: Las aplicaciones conocidas marcadas como **seguro (en verde)** indudablemente no están infectadas (figuran en la lista blanca) y se excluyen de la exploración, ya que de esta forma se mejora la velocidad de exploración correspondiente a la exploración del equipo bajo demanda o la protección del sistema de archivos en tiempo real en el equipo.

Cantidad de usuarios: la cantidad de usuarios que utilizan una aplicación específica. Estos datos se recopilan con la tecnología ESET Live Grid.

Momento de detección: período transcurrido desde que la tecnología ESET Live Grid descubrió la aplicación.

NOTA: Cuando una aplicación se marca como **Desconocida (naranja)**, quizá no sea necesariamente un software malicioso. Por lo general, solo se trata de una aplicación nueva. Si no está seguro con respecto al archivo, puede [enviar el archivo para su análisis](#) al laboratorio de virus de ESET. Si el archivo resulta ser una aplicación maliciosa, se agregará su detección en una de las próximas actualizaciones.

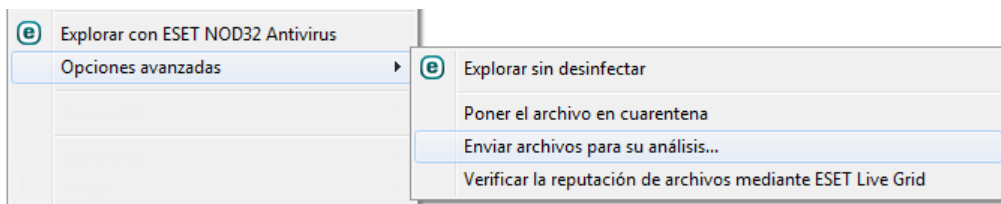
Nombre de la aplicación: el nombre dado a un programa o proceso.

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

Al hacer clic en una aplicación determinada que se encuentra abajo, aparecerá la siguiente información en el sector inferior de la ventana:

- **Archivo:** ubicación de una aplicación en el equipo.
- **Tamaño del archivo:** tamaño del archivo en B (bytes).
- **Descripción del archivo:** características del archivo según la descripción proporcionada por el sistema operativo.
- **Nombre de la empresa:** nombre del fabricante o el proceso de la aplicación.
- **Versión del archivo:** información proporcionada por el desarrollador de la aplicación.
- **Nombre del producto:** nombre de la aplicación y/o nombre comercial.

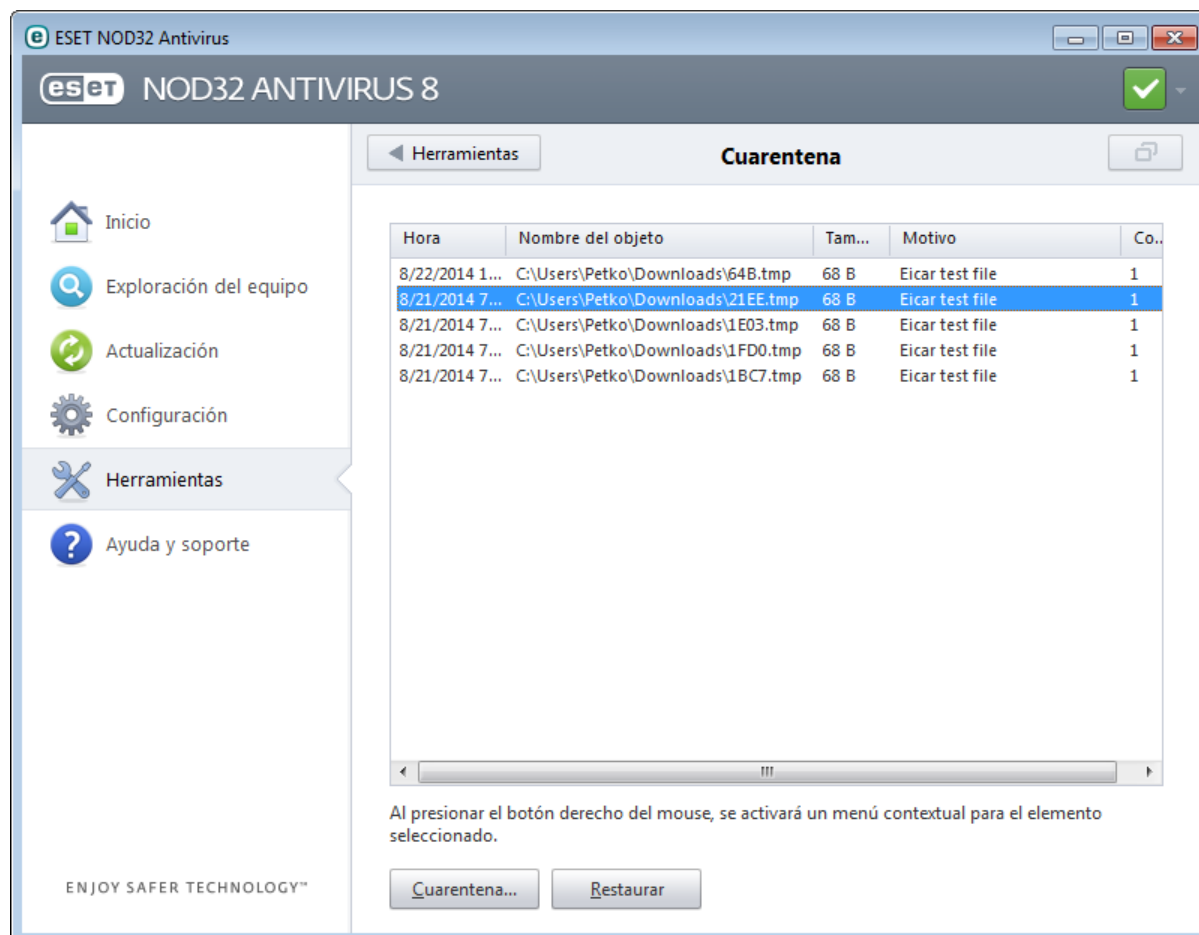
NOTA: La reputación también se puede revisar en archivos que no sean programas o procesos activos; - para ello, marque los archivos que desea verificar, haga un clic derecho en ellos y seleccione **Opciones avanzadas > Verificar la reputación de archivos mediante ESET Live Grid**.



4.4.8 Cuarentena

La función principal de la cuarentena consiste en almacenar los archivos infectados en forma segura. Los archivos deben ponerse en cuarentena cuando no se pueden limpiar, cuando no es seguro o recomendable eliminarlos o en caso de que ESET NOD32 Antivirus los esté detectado erróneamente.

Puede elegir poner cualquier archivo en cuarentena. Esta acción es recomendable cuando un archivo se comporta de manera sospechosa pero la exploración antivirus no lo detecta. Los archivos en cuarentena se pueden enviar para su análisis al laboratorio de virus de ESET.



Los archivos almacenados en la carpeta de cuarentena pueden visualizarse en una tabla que muestra la fecha y la hora en que se pusieron en cuarentena, la ruta a la ubicación original de los archivos infectados, su tamaño en bytes, el motivo (por ejemplo, objeto agregado por el usuario) y la cantidad de amenazas (por ejemplo, si se trata de un archivo comprimido que contiene varias infiltraciones).

Envío de archivos a cuarentena

ESET NOD32 Antivirus envía automáticamente a cuarentena los archivos eliminados (a menos que se haya cancelado esta opción desde la ventana de alerta). Si lo desea es posible enviar a cuarentena cualquier archivo sospechoso en forma manual mediante un clic en el botón **Cuarentena...** En este caso, el archivo original no se quita de su ubicación inicial. También se puede usar el menú contextual con este propósito. Para ello, haga un clic derecho en la ventana **Cuarentena** y luego seleccione el botón **Cuarentena...**

Restauración desde cuarentena

Los archivos puestos en cuarentena también pueden restaurarse a su ubicación original. Para ello, use la función **Restaurar**, que también está disponible en el menú contextual al hacer un clic derecho en el archivo correspondiente en la ventana Cuarentena. Si un archivo está marcado como aplicación potencialmente no deseada, la opción **Restaurar y excluir de la exploración** está habilitada. Lea más información sobre este tipo de aplicación en el [glosario](#). Asimismo, el menú contextual ofrece la opción **Restaurar a...**, que permite restaurar un archivo en una ubicación diferente a la que tenía cuando fue eliminado.

NOTA: Si el programa puso en cuarentena un archivo no infectado por error, restáurelo, [exclúyalo de la exploración](#) y envíelo a atención al cliente de ESET.

Envío de un archivo desde cuarentena

Si puso en cuarentena un archivo sospechoso que el programa no detectó o si un archivo se determinó erróneamente como infectado (por ejemplo, tras la exploración heurística del código) y luego se puso en cuarentena, envíe el archivo al laboratorio de amenazas de ESET. Para enviar un archivo desde cuarentena, haga un clic derecho en el archivo y seleccione **Enviar para su análisis** desde el menú contextual.

4.4.9 Configuración del servidor proxy

En redes de área local muy extensas, la conexión del equipo a Internet puede tener como intermediario un servidor proxy. En tal caso, será necesario definir las siguientes opciones de configuración. De lo contrario, el programa no podrá actualizarse en forma automática. En ESET NOD32 Antivirus, la configuración del servidor proxy está disponible en dos secciones diferentes del árbol de configuración avanzada.

Primero, la configuración del servidor proxy puede establecerse en **Configuración avanzada** en **Herramientas > Servidor proxy**. La especificación del servidor proxy en esta etapa define la configuración global del servidor proxy para todo ESET NOD32 Antivirus. Todos los módulos que requieran una conexión a Internet usarán los parámetros aquí ingresados.

Para especificar la configuración del servidor proxy en esta etapa, seleccione la casilla de verificación **Usar servidor proxy** y luego ingrese la dirección del servidor proxy en el campo **Servidor proxy**, junto con el número de **Puerto** correspondiente.

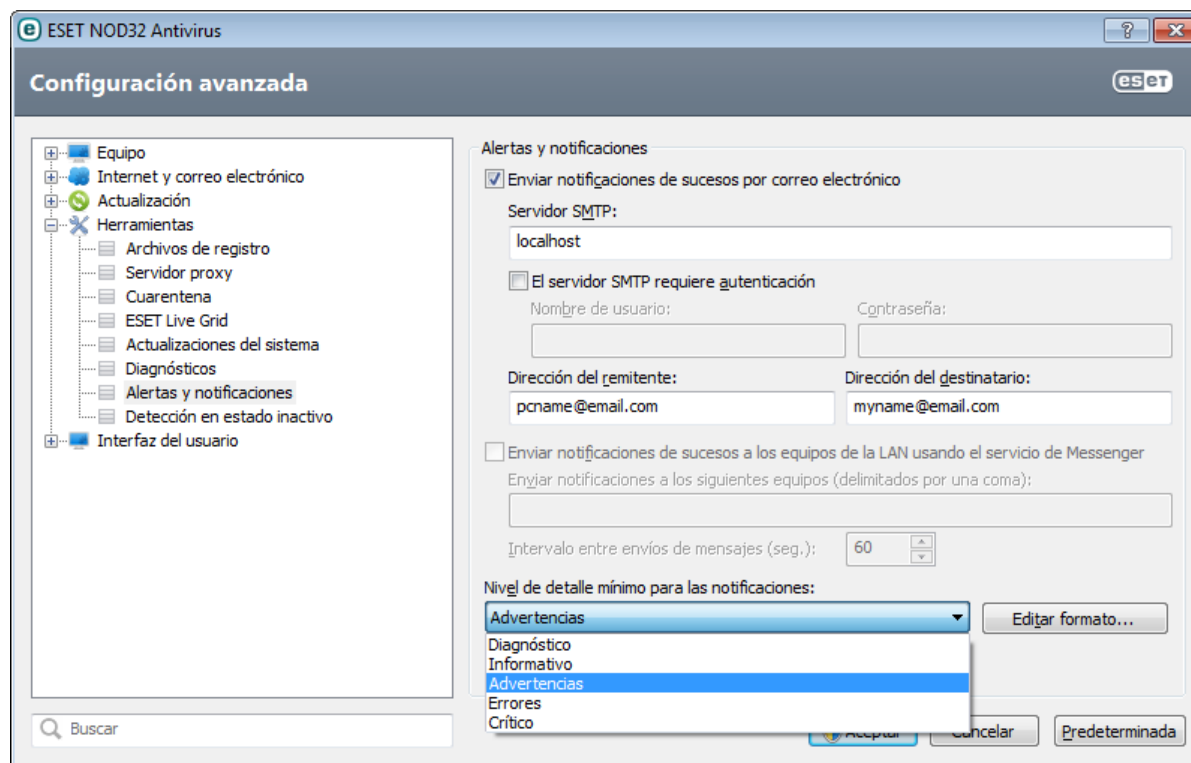
Si la comunicación con el servidor proxy requiere autenticación, seleccione la casilla de verificación **El servidor proxy requiere autenticación** e ingrese un **Nombre de usuario** y una **Contraseña** válidos en los campos respectivos. Haga clic en **Detectar el servidor proxy** para detectar y llenar la configuración del servidor proxy en forma automática. Se copiarán los parámetros especificados en Internet Explorer.

NOTA: Esta característica no recupera los datos de autenticación (nombre de usuario y contraseña); debe ingresarlos usted.

La configuración del servidor proxy también se puede establecer en la configuración de las opciones avanzadas (en la sección **Actualización** del árbol de **Configuración avanzada**). Esta configuración se aplica al perfil de actualización determinado y es recomendado para equipos portátiles, ya que suelen recibir las actualizaciones de firmas de virus desde distintas ubicaciones. Para obtener más información sobre esta configuración, consulte la sección [Configuración avanzada de la actualización](#).

4.4.10 Alertas y notificaciones

ESET NOD32 Antivirus admite el envío de correos electrónicos si ocurre un suceso con el nivel de detalle de los sucesos seleccionado. Haga clic en la casilla de verificación **Enviar notificaciones de sucesos por correo electrónico** para habilitar esta característica y activar las notificaciones por correo electrónico.



Servidor SMTP: el servidor SMTP que se usa para enviar notificaciones.

Nota: Los servidores SMTP con cifrado SSL/TLS no son admitidos por ESET NOD32 Antivirus.

El servidor SMTP requiere autenticación: si el servidor SMTP requiere autenticación, estos campos deben completarse con un nombre de usuario y una contraseña válidos, lo que otorgará el acceso al servidor SMTP.

Dirección del remitente: este campo especifica la dirección del remitente que se mostrará en el encabezado de los correos electrónicos de notificación.

Dirección del destinatario: este campo especifica la dirección del destinatario que se mostrará en el encabezado de los correos electrónicos de notificación.

Enviar notificaciones de sucesos a los equipos de la LAN usando el servicio de Messenger: seleccione esta casilla de verificación para enviar mensajes a equipos de la red de área local mediante el servicio de mensajería de Windows®.

Enviar notificaciones a los siguientes equipos (delimitados por una coma): ingrese el nombre de los equipos que recibirán notificaciones mediante el servicio de mensajería de Windows®.

Intervalo entre envíos de mensajes (seg.): para cambiar la longitud del intervalo entre notificaciones enviadas por la LAN, ingrese el intervalo de tiempo deseado en segundos.

Nivel de detalle mínimo para las notificaciones: especifica el nivel mínimo de detalle de las notificaciones que se enviarán.

Editar formato...: las comunicaciones entre el programa y el usuario remoto o el administrador del sistema se llevan a cabo por medio de los correos electrónicos o los mensajes de la LAN (mediante el servicio de mensajería de Windows®). El formato predeterminado de las notificaciones y los mensajes de alerta será óptimo para la mayoría de las situaciones. En ciertas circunstancias, es posible que necesite cambiar el formato de los mensajes: haga clic en [Editar formato...](#)

4.4.10.1 Formato de mensajes

Aquí puede configurar el formato de los mensajes de sucesos que se muestran en los equipos remotos.

Los mensajes de notificación y de alerta sobre amenazas tienen un formato predefinido por defecto. No es recomendable modificar dicho formato. No obstante, en ciertas circunstancias (por ejemplo, si tiene un sistema automatizado de procesamiento de correo electrónico), es posible que necesite modificar el formato de los mensajes.

Las palabras clave (cadenas separadas por signos %) son reemplazadas en el mensaje por la información real especificada. Se encuentran disponibles las siguientes palabras clave:

- **%TimeStamp%**: fecha y la hora del suceso
- **%Scanner%**: módulo pertinente
- **%ComputerName%**: nombre del equipo 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 no causado por un virus

Las palabras clave **%InfectedObject%** y **%VirusName%** no solo se utilizan en mensajes de alerta de amenazas, y **%ErrorDescription%** solo se utiliza en mensajes de sucesos.

Usar caracteres del alfabeto local: convierte un mensaje de correo electrónico a la codificación de caracteres de ANSI con base en la configuración regional de Windows (por ejemplo, windows-1250). Si deja esta opción sin seleccionar, un mensaje se convertirá y codificará en ACSII de 7 bits (por ejemplo, “á” cambiará a “a” y un símbolo desconocido a “?”).

Usar la codificación local de caracteres: el origen del mensaje de correo electrónico se codificará en el formato Entrecomillado imprimible (QP) que utiliza los caracteres de ASCII y puede transmitir correctamente los caracteres nacionales especiales por correo electrónico en el formato de 8 bits (áéíóú).

4.4.11 Envío de muestras para su análisis

El cuadro de diálogo para envío de archivos permite enviar un archivo a ESET para su análisis y puede encontrarse en **Herramientas > Enviar muestra para su análisis**. Si encuentra un archivo de conducta sospechosa en su equipo o un sitio sospechoso en Internet, puede enviarlo al laboratorio de virus de ESET para su análisis. Si el archivo resulta ser una aplicación maliciosa o sitio malicioso, se agregará su detección a una de las próximas actualizaciones.

Como alternativa, puede enviar el archivo por correo electrónico. Si prefiere esta opción, comprima el archivo o los archivos con WinRAR o WinZIP, proteja el archivo comprimido con la contraseña “infected” y envíelo a samples@eset.com. Recuerde utilizar un tema descriptivo e incluir la mayor cantidad de información posible sobre el archivo (por ejemplo, el sitio Web desde donde realizó la descarga).

NOTA: Antes de enviar un archivo a ESET, asegúrese de que cumpla con uno o más de los siguientes criterios:

- el programa directamente no detecta el archivo
 - el programa detecta erróneamente el archivo como una amenaza
- No recibirá una respuesta a menos que se requiera más información para el análisis.

Seleccione la descripción del menú desplegable **Motivo por el cual se envía el archivo** que mejor se adapte a su mensaje:

- **Archivo sospechoso**
- **Sitio sospechosos** (un sitio web que se encuentra infectado por algún malware),
- **Archivo falso positivo** (un archivo que se detecta como una infección pero no está infectado),
- **Sitio falso positivo**
- **Otros**

Archivo/sitio: la ruta al archivo o sitio web que desea enviar.

Correo electrónico de contacto: el correo electrónico de contacto se envía junto con los archivos sospechosos a ESET y puede utilizarse para contactarlo en caso de que se requiera información adicional para el análisis. El ingreso del

correo electrónico de contacto es opcional. No obtendrá una respuesta de ESET a menos que se requiera más información, ya que nuestros servidores reciben decenas de miles de archivos por día, lo que hace imposible responder a todos los envíos.

4.4.12 Actualizaciones del sistema

La funcionalidad Windows Update es un componente importante para proteger a los usuarios ante software malicioso. Por ese motivo, es imprescindible instalar las actualizaciones de Microsoft Windows en cuanto estén disponibles. ESET NOD32 Antivirus lo mantendrá notificado sobre las actualizaciones faltantes según el nivel que haya especificado. Se encuentran disponibles los siguientes niveles:

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

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

4.5 Interfaz del usuario

La sección **Interfaz del usuario** permite configurar la conducta de la interfaz gráfica del usuario (GUI) del programa.

Con la herramienta [Gráficos](#), es posible ajustar el aspecto visual del programa y los efectos utilizados.

En la configuración de las [Alertas y notificaciones](#), puede cambiar el comportamiento de las alertas sobre amenazas detectadas y las notificaciones del sistema. Dichos mensajes se pueden personalizar acorde a sus necesidades.

Si elige no mostrar algunas notificaciones, aparecerán en el área [Ventanas de notificación ocultas](#). Aquí puede verificar su estado, ver más detalles o quitarlas de esta ventana.

Para que el software de seguridad proporcione la máxima protección, puede impedir cualquier cambio no autorizado mediante la protección de la configuración con una contraseña; para ello, utilice la herramienta [Configuración del acceso](#).

El [menú contextual](#) aparece cuando se hace un clic derecho en un objeto. Use esta herramienta para integrar los elementos de control de ESET NOD32 Antivirus al menú contextual.

4.5.1 Gráficos

Las opciones de configuración de la interfaz del usuario en ESET NOD32 Antivirus permiten ajustar el entorno de trabajo conforme a sus necesidades. Puede acceder a estas opciones de configuración desde el árbol de configuración avanzada al expandir **Interfaz del usuario** y hacer clic en **Gráficos**.

En la sección **Elementos de la interfaz del usuario**, la opción **Interfaz gráfica del usuario** debe deshabilitarse si los elementos gráficos disminuyen el rendimiento del equipo o provocan otros problemas. También es posible que sea necesario desactivar la interfaz gráfica para usuarios con discapacidades visuales, ya que podría entrar en conflicto con aplicaciones especiales utilizadas para leer el texto que aparece en pantalla.

Si desea desactivar la pantalla de bienvenida de ESET NOD32 Antivirus, quite la selección **Mostrar la pantalla de bienvenida al iniciar el programa**.

Habilite **Seleccionar el elemento de control activo** para que el sistema resalte el elemento que se encuentra actualmente bajo el área activa del cursor del mouse. El elemento resaltado se activará con un clic del mouse.

Si desea habilitar el uso de íconos animados para mostrar el progreso de diversas operaciones, seleccione **Usar**

íconos animados para indicar el progreso.

Si desea que ESET NOD32 Antivirus reproduzca un sonido cuando ocurren eventos importantes durante una exploración, por ejemplo cuando se descubre una amenaza o cuando finaliza la exploración, seleccione **Usar señal sonora**.

4.5.2 Alertas y notificaciones

La sección **Alertas y notificaciones** en **Interfaz del usuario** permite configurar cómo ESET NOD32 Antivirus gestionará las alertas ante amenazas y las notificaciones del sistema (por ej., mensajes sobre actualizaciones correctas). También puede establecer el tiempo de visualización y el grado de transparencia de las notificaciones en la bandeja del sistema (solo se aplica a los sistemas que son compatibles con las notificaciones en la bandeja del sistema).

Anule la selección de la casilla de verificación junto a **Mostrar alertas** para cancelar toda ventana de alerta. Esto solo es apropiado en ciertas situaciones. Para la mayoría de los usuarios, se recomienda dejar esta opción habilitada (predeterminada).

Las notificaciones en el escritorio y los globos de sugerencias son solo informativos y no necesitan ni ofrecen interacción con el usuario. Se muestran en el área de notificaciones en la esquina inferior derecha de la pantalla. Para activar las notificaciones en el escritorio, seleccione la opción **Mostrar notificaciones en el escritorio**. Se pueden modificar opciones más detalladas (como el tiempo de visualización de las notificaciones y la transparencia de la ventana) con un clic en el botón **Configurar notificaciones**. Para obtener una vista previa de los criterios de filtrado, haga clic en el botón **Vista previa**. Para quitar las notificaciones cuando ejecute una aplicación en la pantalla completa, seleccione **No mostrar las notificaciones al ejecutar aplicaciones en modo de pantalla completa**.

Para cerrar las ventanas emergentes automáticamente después de un período de tiempo determinado, seleccione **Cerrar las casillas de mensajes automáticamente después de (seg.)**. Si no se cierran manualmente, las ventanas de alerta se cerrarán en forma automática una vez que transcurra el período especificado.

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

4.5.2.1 Configuración avanzada

Desde el menú desplegable **Cantidad mínima de detalle de sucesos para mostrar**, puede seleccionar el nivel de gravedad a partir del cual se mostrarán las alertas y notificaciones.

- **Diagnóstico:** registra la información necesaria para ajustar el programa y todos los historiales mencionados arriba.
- **Informativo:** registra los mensajes de información, incluyendo los mensajes de actualizaciones correctas, y todos los historiales mencionados arriba.
- **Advertencias:** registra errores críticos y mensajes de advertencia.
- **Errores:** Se registrarán los errores tales como *"Error al descargar el archivo"* y errores críticos.
- **Crítico:** registra solo los errores críticos (como por ej., un error al iniciar la protección antivirus, etc.)

La última característica de esta sección permite configurar el destino de las notificaciones en un entorno con varios usuarios. El campo **En sistemas con varios usuarios, mostrar notificaciones en la pantalla del siguiente usuario** permite definir quién recibirá las notificaciones del sistema y otros tipos de notificaciones en sistemas a los que se conectan múltiples usuarios al mismo tiempo. Normalmente, se tratará de un administrador del sistema o de la red. Esta opción resulta especialmente útil para servidores de terminal, siempre y cuando todas las notificaciones del sistema se envíen al administrador.

4.5.3 Ventanas de notificación ocultas

Si se seleccionó la opción **No volver a mostrar este mensaje** para cualquier ventana de notificación (o de alerta) mostrada anteriormente, aparecerá en la lista de ventanas de notificación ocultas. Las acciones que ahora se ejecutan en forma automática se muestran en la columna **Confirmar**.

Mostrar: muestra una vista previa de las ventanas de notificación actualmente ocultas y que cuentan con una acción automática preestablecida.

Quitar: quita elementos de la lista **Casillas de mensajes ocultas**. Se mostrarán nuevamente todas las ventanas de notificación que haya quitado de la lista.

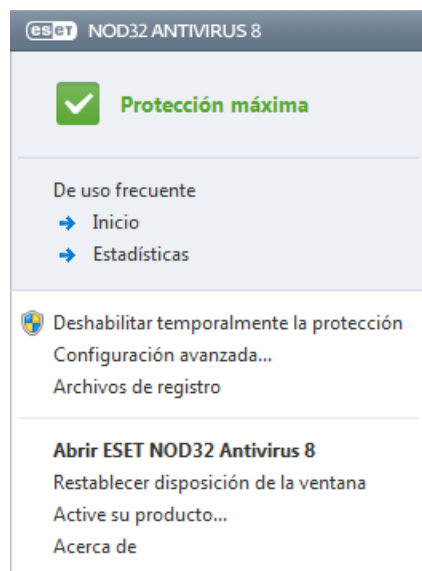
4.5.4 Configuración del acceso

ESET NOD32 Antivirus las configuraciones son una parte crucial de su política de seguridad. Las modificaciones no autorizadas pueden poner potencialmente en peligro la estabilidad y la protección del sistema. Para proteger los parámetros de configuración con una contraseña, desde el menú principal, haga clic en **Configuración > Ingresar a la configuración avanzada... > Interfaz del usuario > Configuración del acceso**, seleccione la opción **Configuración de la protección por contraseña** y haga clic en el botón **Establecer contraseña**. Observe que su contraseña distingue entre mayúsculas y minúsculas.

Exigir derechos completos de administrador para cuentas de administrador limitadas: selecciónela para solicitarle al usuario actual (si no dispone de derechos de administrador) que introduzca el nombre de usuario y la contraseña de administrador cuando modifique determinados parámetros del sistema (similar al Control de cuentas de usuario, UAC, de Windows Vista y Windows 7). Las modificaciones incluyen la deshabilitación de los módulos de protección. En los sistemas con Windows XP que no tienen UAC, los usuarios contarán con la opción **Exigir derechos de administrador (sistema sin soporte UAC)**.

4.5.5 Menú del programa

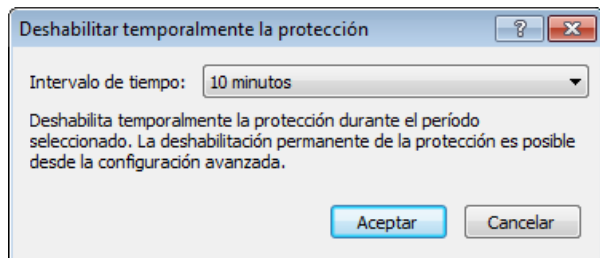
Algunas de las características y opciones de configuración más importantes están disponibles en el menú principal del programa.



De uso frecuente: muestra las partes de ESET NOD32 Antivirus usadas con mayor frecuencia. Puede acceder rápidamente a ellas desde el menú del programa.

Deshabilitar temporalmente la protección: muestra el cuadro de diálogo de confirmación que deshabilita la [Protección antivirus y antispyware](#), que protege ante ataques maliciosos contra el sistema mediante el control de los archivos, las comunicaciones por Internet y correo electrónico. Seleccione **No preguntar de nuevo** para no volver a mostrar este mensaje en el futuro.

El menú desplegable **Intervalo de tiempo** representa el período durante el cual la protección antivirus y antispyware permanecerá deshabilitada.



Configuración avanzada...: seleccione esta opción para ingresar el árbol de **Configuración avanzada** . También hay otras formas de abrir la configuración avanzada, como presionar la tecla F5 o ir a **Configuración > Ingresar a la configuración avanzada...**

Archivos de registro: los [archivos de registro](#) contienen información sobre los sucesos importantes del programa que se llevaron a cabo y proporcionan una visión general de las amenazas detectadas.

Restablecer disposición de la ventana: restablece la ventana de ESET NOD32 Antivirus a su tamaño y posición predeterminados en la pantalla.

Active su producto... - Seleccione esta opción si todavía no está activado su producto de seguridad ESET o para volver a ingresar las credenciales de activación del producto después de renovar su licencia.

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

4.5.6 Menú contextual

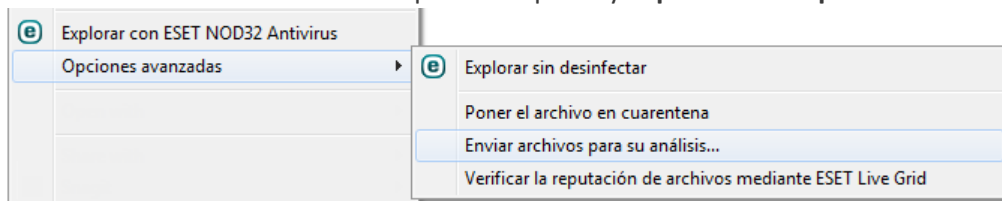
El menú contextual aparece cuando se hace un clic derecho en un objeto. El menú muestra una lista de todas las acciones que puede realizar en un objeto.

Es posible integrar los elementos de control de ESET NOD32 Antivirus al menú contextual. Las opciones más detalladas de configuración para esta función están disponibles en el árbol de configuración avanzada, en **Interfaz del usuario > Menú contextual**.

Integrar en el menú contextual: integrar los elementos de control de ESET NOD32 Antivirus al menú contextual.

Las siguientes opciones se encuentran disponibles en el menú desplegable **Tipo de menú:**

- **Completo (primero explorar):** Activa todas las opciones del menú contextual, el menú principal mostrará **Explorar sin limpieza con ESET NOD32 Antivirus** como primera opción y **Explorar y limpiar** como el elemento de segundo nivel.
- **Completo (primero desinfectar):** Activa todas las opciones del menú contextual, el menú principal mostrará **Explorar con ESET NOD32 Antivirus** como primera opción y **Explorar sin limpieza** como el elemento del segundo nivel.



- **Solo explorar:** solo la opción **Explorar sin limpieza con ESET NOD32 Antivirus** se mostrará en el menú contextual.
- **Solo desinfectar:** solo **Explorar con ESET NOD32 Antivirus** se mostrará en el menú contextual.

5. Usuario avanzado

5.1 Administrador de perfiles

El administrador de perfiles se usa en dos partes de ESET NOD32 Antivirus: en la sección **Exploración del equipo bajo demanda** y en **Actualización**.

Exploración del equipo

Es posible guardar los parámetros preferidos de exploración para usarlos en el futuro. Se recomienda crear un perfil distinto (con varios objetos para explorar, métodos de exploración y otros parámetros) para cada exploración utilizada regularmente.

Para crear un nuevo perfil, abra la ventana de configuración avanzada (F5) y haga clic en **Equipo > Antivirus y antispyware > Exploración del equipo bajo demanda > Perfiles...** La ventana **Perfiles de configuración** incluye el menú desplegable **Perfil seleccionado** que enumera los perfiles de exploración existentes así como la opción de crear uno nuevo. Para obtener ayuda sobre cómo crear un perfil de exploración acorde a sus necesidades, consulte la sección [Configuración de los parámetros del motor ThreatSense](#), donde obtendrá la descripción de cada parámetro de la configuración de la exploración.

Ejemplo: Suponga que desea crear su propio perfil de exploración y la configuración de la exploración inteligente es parcialmente adecuada, pero no desea explorar empaquetadores en tiempo real o aplicaciones potencialmente no seguras y además quiere aplicar una **Desinfección estricta**. En la ventana **Perfiles de configuración**, haga clic en el botón **Agregar...** Ingrese el nombre de su nuevo perfil en el campo **Nombre del perfil** y seleccione **Exploración inteligente** desde el menú desplegable **Copiar configuración desde el perfil**. Ajuste los parámetros restantes según sus necesidades y guarde su nuevo perfil.

Actualización

El editor de perfiles en la sección de configuración de la actualización permite a los usuarios crear nuevos perfiles de actualización. Cree y utilice sus propios perfiles personalizados (distintos al perfil predeterminado: **Mi perfil**) únicamente si su equipo se conecta a los servidores de actualización de varias formas.

Un ejemplo es un equipo portátil que normalmente se conecta a un servidor local (mirror) desde la red local, pero que descarga las actualizaciones directamente desde los servidores de actualización de ESET cuando se desconecta de la red local (durante un viaje de negocios) puede utilizar dos perfiles: el primero para conectarse al servidor local; el otro para conectarse a los servidores de ESET. Una vez configurados estos perfiles, navegue a **Herramientas > Tareas programadas** y edite los parámetros de las tareas de actualización. Designe un perfil como principal y el otro como secundario.

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

Agregar...: crear nuevos perfiles de actualización.

La parte inferior de la ventana enumera los perfiles existentes.

5.2 Accesos directos desde el teclado

Los accesos directos que se pueden utilizar al trabajar con ESET NOD32 Antivirus incluyen:

Ctrl+G	deshabilita la interfaz gráfica del usuario en el producto
Ctrl+I	abre la página ESET SysInspector
Ctrl+L	abre la página Archivos de registro
Ctrl+S	abre la página Tareas programadas
Ctrl+Q	abre la página Cuarentena
Ctrl+U	abre la configuración del nombre de usuario y la contraseña
Ctrl+R	restablece la ventana a su tamaño y posición predeterminados en la pantalla

Para una mejor navegación en su producto de ESET, se pueden usar los siguientes accesos directos desde el teclado:

F1	abre las páginas de ayuda
F5	abre la configuración avanzada
Arriba/Abajo	permite la navegación en el producto por los elementos
*	expande el nodo del árbol de configuración avanzada
-	contrae los nodos del árbol de configuración avanzada
TAB	mueve el cursor en una ventana
Esc	cierra la ventana de diálogo activa

5.3 Diagnósticos

Los diagnósticos proporcionan el volcado de memoria de los procesos de ESET en caso de que se bloquee una aplicación (por ejemplo, *ekrn*). Si una aplicación se bloquea, se generará un volcado de memoria. Esto es de utilidad para que los desarrolladores depuren y reparen diversos problemas de ESET NOD32 Antivirus. Hay dos tipos de volcado disponibles:

- **Volcado de memoria completa:** registra todo el contenido de la memoria del sistema cuando una aplicación se detiene inesperadamente. Un volcado de memoria completa puede incluir datos de los procesos que estaban activos cuando se recopiló la memoria de volcado.
- **Minivolcado:** registra el grupo de datos útiles más reducido posible que pueda ayudar a identificar por qué se bloqueó la aplicación en forma inesperada. Este tipo de archivo de volcado puede resultar útil cuando el espacio es limitado. Sin embargo, debido a la cantidad limitada de información incluida, es posible que los errores que no se provocaron directamente por el subproceso activo en el momento del problema no se descubran al analizar este archivo.
- Seleccione **No generar una volcado de memoria** (predeterminado) para deshabilitar esta característica.

Directorio de destino: ubicación donde se va a generar la volcado de memoria durante el bloqueo. Haga clic en ... para abrir este directorio dentro de una nueva ventana de *Windows Explorer*.

5.4 Importación y exportación de una configuración

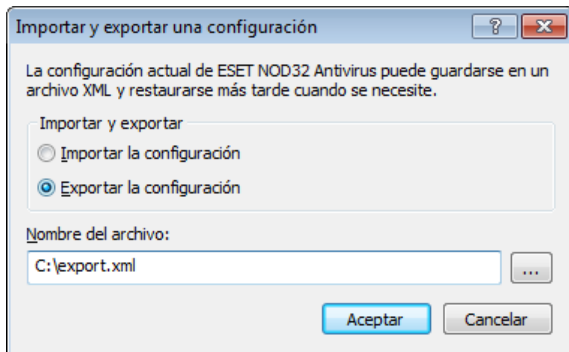
Puede importar o exportar su archivo de configuración personalizado ESET NOD32 Antivirus .xml desde el menú **Configuración**.

La importación y exportación de los archivos de configuración es útil si necesita hacer una copia de seguridad de la configuración actual de ESET NOD32 Antivirus para usarla más adelante. La opción para exportar la configuración también es conveniente para usuarios que desean usar su configuración preferida en varios sistemas: pueden importar fácilmente un archivo .xml para transferir estas configuraciones.

Es muy fácil importar una configuración. En la ventana principal del programa, haga clic en **Configuración > Importar y exportar las configuraciones...**, luego seleccione la **Importar la configuración**. Ingrese el nombre del archivo 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 una configuración....** Seleccione **Exportar configuraciones** e ingrese el nombre del archivo de la configuración (es decir *export.xml*). Use el botón de exploración para elegir la ubicación en el equipo donde desea guardar el archivo de configuración.

Nota: Es probable que encuentre un error mientras exporta las configuraciones, si no tiene suficientes derechos para escribir el archivo exportado en el directorio especificado.



5.5 Detección en estado inactivo

La configuración de la detección en estado inactivo puede establecerse desde **Configuración avanzada** en **Herramientas > Detección en estado inactivo**. Esta configuración especifica un desencadenante para la [exploración en estado inactivo](#) cuando:

- el protector de pantalla está activo,
- el equipo está bloqueado,
- un usuario se desconecta.

Use las casillas de verificación para habilitar o deshabilitar los desencadenantes de la detección en estado inactivo.

5.6 ESET SysInspector

5.6.1 Introducción a ESET SysInspector

ESET SysInspector es una aplicación que examina el equipo a fondo y muestra los datos recopilados en forma exhaustiva. La información sobre los controladores y aplicaciones instalados, las conexiones de red o las entradas de registro importantes, por ejemplo, puede ayudarle en la investigación de un comportamiento sospechoso del sistema, ya sea debido a incompatibilidades del software o hardware o a una infección por malware.

Puede acceder a ESET SysInspector de dos maneras: Desde la versión integrada en las soluciones ESET Security o mediante la descarga de la versión autosostenible (SysInspector.exe) sin cargo desde el sitio Web de ESET. Ambas versiones tienen una función idéntica y cuentan con los mismos controles del programa. La única diferencia radica en el manejo de los resultados. Tanto la versión autosostenible como la integrada permiten exportar instantáneas del sistema a un archivo *.xml* y guardarlas en el disco. Sin embargo, la versión integrada también permite almacenar las instantáneas del sistema directamente en **Herramientas > ESET SysInspector** (excepto ESET Remote Administrator). Para obtener más información, consulte la sección [ESET SysInspector como parte de ESET NOD32 Antivirus](#).

Aguarde un momento mientras ESET SysInspector explora el equipo. Puede tardar de 10 segundos a unos minutos según la configuración del hardware, el sistema operativo y la cantidad de aplicaciones instaladas en el equipo.

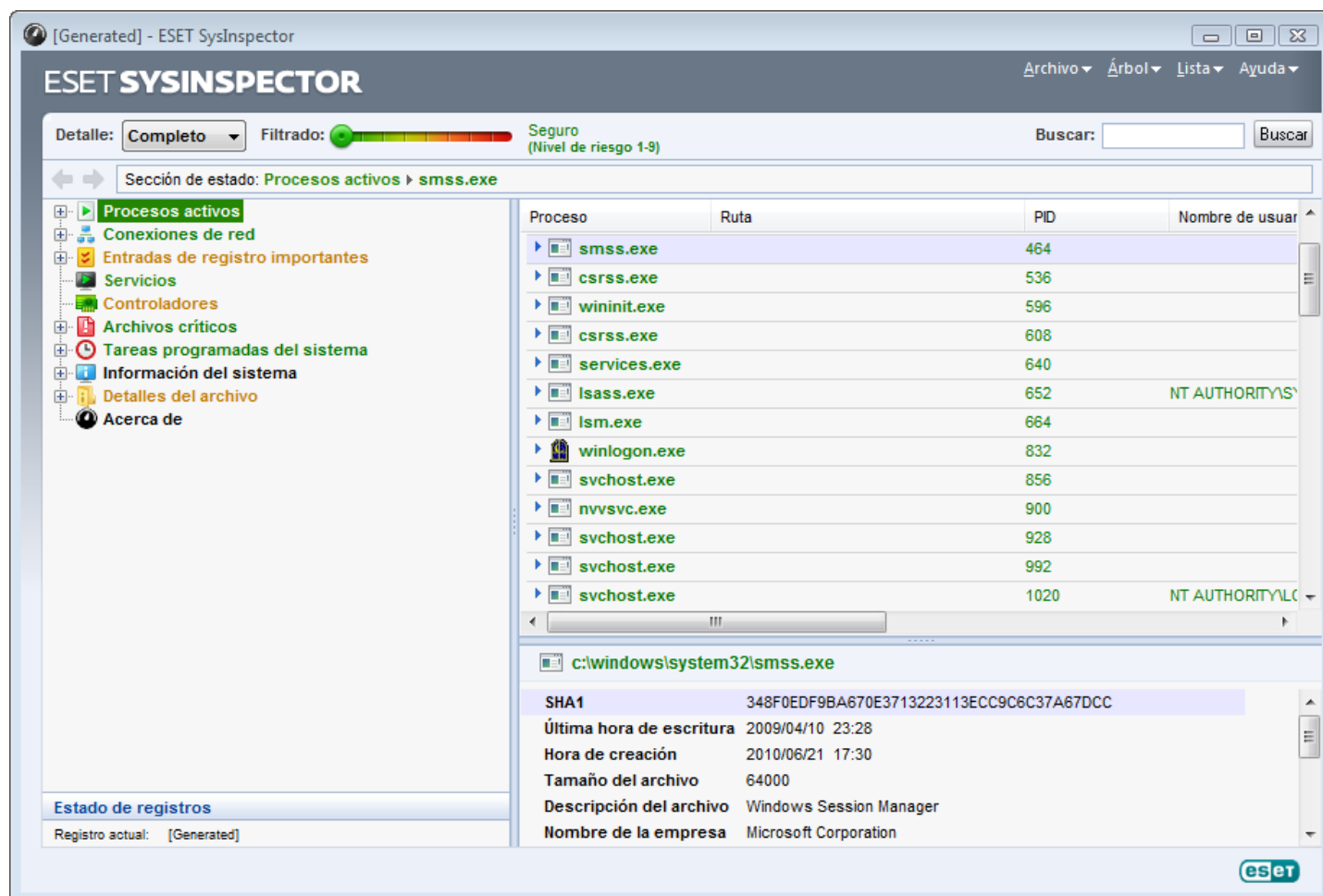
5.6.1.1 Inicio de ESET SysInspector

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 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. Puede tardar varios minutos.

5.6.2 Interfaz del usuario y uso de la aplicación

Para lograr una mayor claridad, la ventana principal del programa se divide en cuatro secciones principales: la sección de controles del programa, situada en la parte superior de la ventana principal del programa; la ventana de navegación, situada a la izquierda; la ventana de descripción, situada a la derecha; y la ventana de detalles, situada en la parte inferior de la ventana principal del programa. La sección Estado de registros muestra una lista de los parámetros básicos de un registro (filtro utilizado, tipo de filtro, si el registro es el 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 generar un registro **Adecuado para enviar**. De esta forma, el registro omite la información confidencial (nombre del usuario actual, nombre del equipo, nombre del dominio, privilegios del usuario actual, variables de entorno, etc.).

NOTA: Para abrir los informes de ESET SysInspector almacenados previamente, simplemente arrástrelos y suéltelos 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

Esta configuración afecta la información mostrada en la ventana principal del programa para que resulte más sencillo trabajar con dicha información. En el modo "Básico", el usuario tiene acceso a información utilizada para buscar soluciones a problemas comunes del sistema. En el modo "Medio", el programa muestra detalles menos usados. En el modo "Completo", ESET SysInspector muestra toda la información necesaria para solucionar problemas muy específicos.

Filtrado

Es la mejor opción para buscar entradas de registro o archivos sospechosos en el sistema. Mediante el ajuste del control deslizante, puede filtrar elementos por su nivel de riesgo. Si el control deslizante se encuentra en el extremo izquierdo (nivel de riesgo 1), se muestran todos los elementos. Al mover el control deslizante a la derecha, el programa filtra todos los elementos menos peligrosos que el nivel de riesgo actual y muestra solo los elementos con un nivel de sospecha superior al mostrado. Si el control deslizante se encuentra en el extremo derecho, el programa muestra únicamente los elementos dañinos conocidos.

Todos los elementos cuyo riesgo designado está entre 6 y 9 pueden suponer un riesgo para la seguridad. Si no está utilizando una solución de seguridad de ESET, es recomendable explorar 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 si se compara el color del elemento con el color del control deslizante del nivel de riesgo.

Comparación

Cuando compara dos registros, puede seleccionar mostrar todos los elementos, mostrar solo elementos agregados, mostrar solo elementos eliminados o mostrar solo elementos reemplazados.

Buscar

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

Volver


Al hacer clic en las flechas hacia atrás o hacia delante, puede volver a la información mostrada previamente en la ventana de descripción. Puede utilizar la tecla Retroceso y la tecla Barra espaciadora, 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 varios tipos de información en distintas secciones básicas denominadas nodos. Si está disponible, puede encontrar información adicional al expandir los subnodos de cada nodo. Para abrir o contraer un nodo, solo tiene que hacer doble clic en el nombre del nodo o en , que se encuentran junto al nombre del nodo. Cuando examine la estructura con forma de árbol de nodos y subnodos en la ventana de navegación, puede encontrar información variada de cada nodo en la ventana de descripción. Si examina los elementos en la ventana 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 Navegación e información relacionada en las ventanas Descripción y Detalles.

Procesos activos

Este nodo contiene información sobre aplicaciones y 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 y el nivel de riesgo del archivo.

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 importantes del núcleo que se ejecutan de forma ininterrumpida y que proporcionan funciones básicas y esenciales para otras aplicaciones de usuario. En determinados casos, dichos procesos aparecen en la herramienta ESET SysInspector con una ruta de archivo que comienza por `\\??\`. Estos símbolos optimizan el inicio previo de dichos procesos; 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 mediante el protocolo seleccionado en la ventana 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 del ayudante de exploración (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 Servicios de Windows. En la ventana Detalles, puede consultar la forma de inicio establecida 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 programadas del sistema

Contiene una lista de tareas accionadas por las Tareas programadas de Windows en un tiempo/intervalo especificado.

Información del sistema

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

Detalles del archivo

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

Acerca de

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

5.6.2.2.1 Accesos directos desde el teclado

Los accesos directos que se pueden utilizar al trabajar con ESET SysInspector incluyen:

Archivo

Ctrl+O	Abrir el registro existente
Ctrl+S	Guardar los registros creados

Generar

Ctrl+G	Genera una instantánea de estado del equipo estándar
Ctrl+H	Genera una instantánea de estado del equipo que también puede registrar información confidencial

Filtrado de elementos

1, O	Seguro, se muestran los elementos que tienen un nivel de riesgo de 1 a 9
2	Seguro, se muestran los elementos que tienen un nivel de riesgo de 2 a 9
3	Seguro, se muestran los elementos que tienen un nivel de riesgo de 3 a 9
4, U	Desconocido, se muestran los elementos que tienen un nivel de riesgo de 4 a 9
5	Desconocido, se muestran los elementos que tienen un nivel de riesgo de 5 a 9
6	Desconocido, se muestran los elementos que tienen un nivel de riesgo de 6 a 9
7, B	Peligroso, se muestran los elementos que tienen un nivel de riesgo de 7 a 9
8	Peligroso, se muestran los elementos que tienen un nivel de riesgo de 8 a 9
9	Peligroso, se muestran los elementos que tienen un nivel de riesgo de 9
-	Disminuir el nivel de riesgo
+	Aumentar el nivel de riesgo
Ctrl+9	Modo de filtrado, mismo nivel o superior
Ctrl+0	Modo de filtrado, solo mismo nivel

Ver

Ctrl+5	Ver por proveedor, todos los proveedores
Ctrl+6	Ver por proveedor, solo Microsoft
Ctrl+7	Ver por proveedor, resto de proveedores
Ctrl+3	Mostrar todos los detalles
Ctrl+2	Mostrar la mitad de los detalles
Ctrl+1	Visualización básica
Retroceso	Volver un paso atrás
Espacio	Continuar con el paso siguiente
Ctrl+W	Expandir el árbol
Ctrl+Q	Contraer el árbol

Otros controles

Ctrl+T	Ir a la ubicación original del elemento tras seleccionarlo en los resultados de búsqueda
Ctrl+P	Mostrar la información básica de un elemento
Ctrl+A	Mostrar la información completa de un elemento

Ctrl+C	Copiar el árbol del elemento actual
Ctrl+X	Copiar elementos
Ctrl+B	Buscar información en Internet acerca de los archivos seleccionados
Ctrl+L	Abrir la carpeta en la que se encuentra el archivo seleccionado
Ctrl+R	Abrir la entrada correspondiente en el editor de registros
Ctrl+Z	Copiar una ruta de acceso a un archivo (si el elemento está asociado a un archivo)
Ctrl+F	Activar el campo de búsqueda
Ctrl+D	Cerrar los resultados de búsqueda
Ctrl+E	Ejecutar el script de servicio

Comparación

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

Varios

F1	Ver la Ayuda
Alt+F4	Cerrar el programa
Alt+Mayús+F4	Cerrar el programa sin preguntar
Ctrl+I	Estadísticas del registro

5.6.2.3 Comparación

La característica Comparar le permite al usuario comparar dos registros existentes. El resultado es un conjunto de elementos no comunes a ambos registros. Esta opción es adecuada para realizar un seguimiento de los cambios realizados en el sistema; constituye una herramienta útil para detectar códigos maliciosos.

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

La ventaja de comparar dos registros es que permite ver un registro actualmente activo y un registro guardado en un archivo. Para comparar registros, haga clic en **Archivo > Comparar registros** y elija **Seleccionar archivo**. El registro seleccionado se comparará con el registro activo en la ventana principal del programa. El registro resultante solo mostrará las diferencias entre esos dos registros.

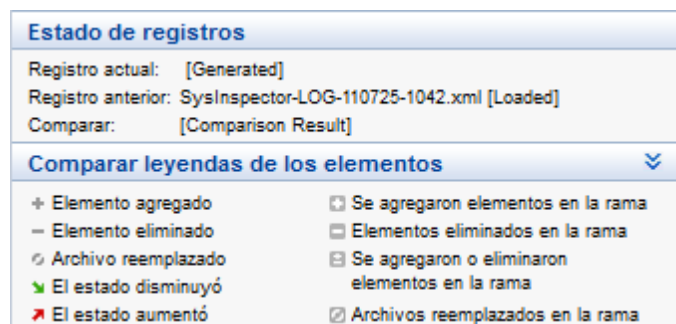
NOTA: Si compara dos archivos de registro, haga clic en **Archivo > Guardar registro** y guárdelo como un archivo ZIP. Se guardarán ambos archivos. Si abre posteriormente dicho archivo, se compararán automáticamente los registros que contiene.

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

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

- + nuevo valor que no se encuentra en el registro anterior
- □ la sección de estructura con forma de árbol contiene nuevos valores
- - valor eliminado que solo se encuentra en el registro anterior
- □ la sección de estructura con forma de árbol contiene valores eliminados
- ↻ se cambió un valor o archivo
- □ la sección de estructura con forma de árbol contiene valores o archivos modificados
- ▼ disminuyó el nivel de riesgo o era superior en el registro anterior
- ▲ aumentó el nivel de riesgo o era inferior en el registro anterior

La explicación que aparece en la esquina inferior izquierda describe todos los símbolos y muestra los nombres de los registros que se están comparando.



Se puede guardar cualquier registro comparativo en un archivo y abrirlo posteriormente.

Ejemplo

Genere y guarde un registro, en el que se recopile información original sobre el sistema, en un archivo con el nombre anterior.xml. Después de que se hagan los cambios en el sistema, abra ESET SysInspector y permítale generar un nuevo registro. Guárdelo en un archivo con el nombre *actual.xml*.

Para realizar un seguimiento de los cambios entre estos dos registros, haga clic en **Archivo > Comparar registros**. El programa creará un registro comparativo con las diferencias entre ambos registros.

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

SysInspector.exe actual.xml anterior.xml

5.6.3 Parámetros de la línea de comandos

ESET SysInspector es compatible con la generación de informes desde la línea de comandos mediante el uso de estos parámetros:

/gen	generar registro directamente desde la línea de comandos sin iniciar la interfaz gráfica de usuario
/privacy	generar registro omitiendo la información confidencial
/zip	guardar registro resultante en un archivo comprimido zip
/silent	quitar la ventana de progreso al generar el registro desde la línea de comandos
/blank	iniciar SysInspector sin generar o cargar el 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 en el que se excluya 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 ofrece asistencia a los clientes que utilizan ESET SysInspector mediante la eliminación de objetos no deseados del sistema.

El script de servicio le permite al usuario exportar el registro completo de ESET SysInspector o únicamente las partes seleccionadas. Tras la exportación, puede marcar los objetos que desee eliminar. A continuación, puede ejecutar el registro modificado para eliminar los objetos marcados.

El script de servicio es útil para usuarios avanzados con experiencia previa en el diagnóstico de problemas del sistema. Las modificaciones realizadas por usuarios sin experiencia pueden provocar daños en el sistema operativo.

Ejemplo

Si tiene la sospecha de que el equipo está infectado por un virus que el antivirus no detecta, siga estas instrucciones detalladas:

1. Ejecute ESET SysInspector para generar una nueva instantánea del sistema.
2. Seleccione el primer elemento de la sección que se encuentra a la izquierda (en la estructura con forma de árbol), presione Shift y seleccione el último elemento para marcarlos todos.
3. Haga un clic derecho en los objetos seleccionados y elija **Exportar las secciones seleccionadas a un script de servicio**.
4. Los objetos seleccionados se exportarán a un nuevo registro.
5. Este es el paso más importante de todo el procedimiento: abra el registro nuevo y cambie el atributo - a + para todos los objetos que desee eliminar. Asegúrese de no marcar ningún archivo u objeto importante del sistema operativo.
6. Abra ESET SysInspector, haga clic en **Archivo > Ejecutar el script de servicio** e ingrese la ruta en su 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 un clic derecho en cualquier elemento del árbol de menús (en el panel izquierdo) de la ventana principal de ESET SysInspector. En el menú contextual, seleccione la opción **Exportar todas las secciones al script de servicio** o la opción **Exportar las 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 activos)

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 seleccionó (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\khbexb.dll
- c:\windows\system32\advapi32.dll
[...]
```

En este ejemplo, se marcó el módulo khbexb.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: ekrm.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, lo que libera recursos del sistema.

04) UDP endpoints (Terminales UDP)

En esta sección se incluye información sobre las terminales 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 las terminales UDP marcadas 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
[...]
```

Cuando se ejecuta el script, se detienen los controladores seleccionados. Observe que algunos controladores no se permitirán detenerse.

09) Critical files (Archivos críticos)

En esta sección se proporciona información sobre los archivos que son críticos para el correcto funcionamiento del sistema operativo.

Ejemplo:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Los elementos seleccionados se eliminarán o restablecerán en sus valores originales.

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 el script de servicio** del menú Archivo. Cuando abra un script, el programa mostrará el siguiente mensaje: **¿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 mostrará una ventana de diálogo para confirmar que el script se ejecutó correctamente.

Si el script no se puede procesar por completo, se mostrará una ventana de diálogo con el siguiente mensaje: **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, aparecerá una ventana de diálogo con el siguiente mensaje: **El script de servicio seleccionado no está firmado. La ejecución de scripts desconocidos y sin firmar podría dañar seriamente los datos del equipo. ¿Está seguro de que desea ejecutar el script y llevar a cabo las acciones?** Esto podría deberse a que el script presenta inconsistencias (encabezado dañado, título de sección dañado, falta línea vacía entre secciones, etc.). Vuelva a abrir el archivo del script y corrija los errores o cree un script de servicio nueva.

5.6.5 Preguntas frecuentes

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

Aunque ESET SysInspector no requiere privilegios de administrador para su ejecución, sí es necesario utilizar una cuenta de administrador para acceder a parte de la información que recopila. Si lo ejecuta como usuario normal o restringido, se recopilará menor cantidad de información acerca de su entorno operativo.

¿ESET SysInspector crea archivos de registro?

ESET SysInspector puede crear un archivo de registro de la configuración de su equipo. Para guardar uno, haga clic en **Archivo > Guardar registro** desde la ventana principal del programa. Los registros se guardan con formato XML. De forma predeterminada, los archivos se guardan en el directorio *%USERPROFILE%\My Documents* con una convención de nomenclatura del tipo de "SysInspector-%COMPUTERNAME%-YYMMDD-HHMM.XML". Si lo desea, puede modificar tanto la ubicación como el nombre del archivo de registro antes de guardarlo.

¿Cómo puedo ver el contenido del archivo de registro de ESET SysInspector?

Para visualizar un archivo de registro creado por ESET SysInspector, ejecute la aplicación y haga clic en **Archivo > Abrir registro** en la ventana principal del programa. También puede arrastrar y soltar los archivos de registro en la aplicación ESET SysInspector. Si necesita ver los archivos de registro de ESET SysInspector con frecuencia, es recomendable crear 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 o 7

no permita la acción de arrastrar y soltar entre ventanas que cuentan con permisos de seguridad diferentes.

¿Existe alguna especificación disponible para el formato del archivo de registro? ¿Y algún conjunto de herramientas para el desarrollo de aplicaciones (SDK)?

Actualmente, no se encuentra disponible ninguna especificación para el formato del archivo de registro, ni un conjunto de herramientas 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 en particular?

Generalmente, ESET SysInspector asigna un nivel de riesgo a los objetos (archivos, procesos, claves de registro, etc.). Para ello, utiliza una serie de reglas heurísticas que examinan las características de cada uno de los objetos y luego estiman 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 riesgo 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 proporcionarles a dichos expertos una evaluación rápida, 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 desarrolló la aplicación y que no se alteró. Para verificar la autenticidad del certificado, el sistema operativo debe contactar con la autoridad certificadora, que verificará la identidad del desarrollador de la aplicación. Este es un comportamiento normal para todos los programas firmados digitalmente que se ejecutan en Microsoft Windows.

¿En qué consiste la tecnología Anti Stealth?

La tecnología Anti Stealth proporciona un método efectivo de detección de rootkits.

Si códigos maliciosos que se comportan como un rootkit atacan el sistema, el usuario se puede exponer a la pérdida o robo de información. Si no se dispone de una herramienta anti-rootkit especial, es prácticamente imposible detectar los rootkits.

¿Por qué a veces hay archivos con la marca "Firmado por MS" que, al mismo tiempo, tienen una entrada de "Nombre de compañía" diferente?

Al intentar identificar la firma digital de un archivo ejecutable, ESET SysInspector revisa en primer lugar si el archivo contiene una firma digital integrada. Si se encuentra una firma digital, el archivo se validará con esa información. Si no se encuentra una firma digital, ESI comienza a buscar el archivo CAT correspondiente (Catálogo de seguridad: %systemroot%\system32\catroot), que contiene información sobre el archivo ejecutable procesado. Si se encuentra el archivo CAT relevante, la firma digital de dicho archivo CAT será la que se aplique en el proceso de validación del archivo ejecutable.

Esa es la razón por la cual a veces hay archivos marcados como "Firmado por MS", pero que tienen una entrada "Nombre de compañía" diferente.

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 exploración del equipo o las tareas programadas. Se puede obtener acceso a todas las operaciones con instantáneas del sistema (como crear, ver, comparar, eliminar y exportar) con tan solo un par de clics.

La ventana 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 creó la instantánea y el estado de la misma.

Para comparar, crear o eliminar instantáneas, utilice los botones correspondientes ubicados debajo de la lista de instantáneas de la ventana ESET SysInspector. Estas opciones también están disponibles en el menú contextual. Para ver la instantánea del sistema seleccionada, utilice la opción del menú contextual **Mostrar**. Para exportar la instantánea seleccionada a un archivo, haga clic con el botón secundario en ella y seleccione **Exportar....**

Abajo 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 nuevo registro. Antes debe ingresar un breve comentario acerca del registro. Para obtener información sobre el progreso de la creación de la instantánea (que se está generando en ese momento), consulte la columna **Estado**. Todas las instantáneas completadas aparecen marcadas con el estado **Creado**.
- **Eliminar/Eliminar todos:** 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 inicio que contenga una de las soluciones de ESET Security: puede ser ESET NOD32 Antivirus, ESET Smart Security o incluso algunos de los productos orientados al servidor. La ventaja principal de ESET SysRescue es que la solución ESET Security se ejecuta en forma independiente del sistema operativo del host, a la vez que cuenta con acceso directo al disco y al sistema de archivos completo. De esta forma, es posible quitar infiltraciones que normalmente no se podían eliminar, por ej., mientras el sistema operativo está activo, etc.

5.7.1 Requisitos mínimos

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

Windows PE es parte del Kit de instalación automatizada de Windows (AIK de Windows) o Kit de despliegue y evaluación de Windows (WADK) y por lo tanto AIK de Windows o WADK debe ser instalado antes de crear ESET SysRescue (<http://go.eset.eu/AIK>, <http://www.microsoft.com/en-us/download/details.aspx?id=30652>). La elección entre estos kits depende de la versión del sistema operativo. Para que el programa sea compatible con la versión de 32 bits de Windows PE, es necesario usar un paquete de instalación de la solución ESET Security de 32 bits al crear ESET SysRescue en sistemas de 64 bits. ESET SysRescue es compatible con la versión 1.1 del AIK de Windows y versiones posteriores como también con WADK 1.0 o posterior.

Cuando instale ADK de Windows elija únicamente los paquetes Herramientas de despliegue y Entorno de preinstalación de Windows (Windows PE) para instalar. Debido a que estos paquetes son mayores a 3,0 GB en tamaño, se recomienda una conexión a Internet de alta velocidad para la descarga.

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

ADK de Windows es compatible con:

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

Nota: ESET SysRescue puede no estar disponible para Windows 8 en versiones más antiguas de los productos de seguridad de ESET. En este caso recomendamos que actualice su producto o cree un disco ESET SysRescue en otra versión de Microsoft Windows.

AIK de Windows 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**.

Primero, el asistente verifica la presencia del AIK o ADK de Windows y que haya un dispositivo adecuado para la creación de un medio de inicio. Si AIK o ADK de Windows no está instalado en el equipo (o si está dañado o no se instaló correctamente), el asistente le ofrecerá la opción de instalarlo o ingresar la ruta a la carpeta AIK de Windows (<http://go.eset.eu/AIK>, <http://www.microsoft.com/en-us/download/details.aspx?id=30652>).

NOTA: Debido a que el AIK de Windows es mayor de 1 GB en tamaño, se requiere una conexión a Internet de alta velocidad para la descarga.

Cuando instale ADK de Windows elija únicamente los paquetes Herramientas de despliegue y Entorno de preinstalación de Windows (Windows PE) para instalar. Debido a que estos paquetes son mayores a 3,0 GB en tamaño, se requiere una conexión a Internet de alta velocidad para la descarga.

En el [paso siguiente](#), seleccione el medio de destino donde se ubicará ESET SysRescue.

5.7.3 Selección de objetos

Además de un CD, DVD y USB, puede elegir guardar ESET SysRescue en un archivo ISO. Más tarde, puede grabar la imagen ISO en un CD o DVD, o usarla de alguna otra forma (por ej., en un entorno virtual como VMWare o Virtualbox).

Si selecciona USB como medio de destino, el inicio no funcionará en algunos equipos. Algunas versiones del BIOS pueden informar que hay problemas con el BIOS; se comunica con el administrador del inicio (por ej., en Windows Vista) y sale del proceso de inicio con el siguiente mensaje de error:

```
archivo: \boot\bcd
estado: 0xc000000e
Información: se produjo un error al intentar leer los datos de configuración del inicio
```

Si encuentra este mensaje, se recomienda seleccionar como medio una unidad de CD en vez de USB.

5.7.4 Configuración

Antes de iniciar la creación de ESET SysRescue, el asistente de instalación muestra los parámetros de la compilación. Se pueden modificar con un clic en el botón **Cambiar....** Entre las opciones disponibles están:

- [Carpetas](#)
- [ESET Antivirus](#)
- [Avanzado](#)
- [Protocolo de Internet](#)
- [Dispositivo USB de inicio](#) (cuando se selecciona el dispositivo USB de destino)
- [Grabación](#) (cuando se selecciona la unidad CD/DVD de destino)

La opción **Crear** aparece inactiva si no se especificó ningún paquete de instalación MSI o si no hay ninguna solución de ESET Security instalada en el equipo. Para seleccionar un paquete de instalación, haga clic en **Cambiar** y vaya a la pestaña **ESET Antivirus**. Asimismo, si no completa el nombre de usuario y la contraseña (**Cambiar > ESET Antivirus**), la opción **Crear** aparecerá inactiva, sombreada en gris.

5.7.4.1 Carpetas

Carpeta temporal: es un directorio activo que se usa para los archivos requeridos durante la compilación de ESET SysRescue.

Carpeta ISO: es la carpeta donde se guarda el archivo ISO resultante tras completar la compilación.

La lista de esta pestaña muestra todas las unidades de red asignadas junto con el espacio libre disponible. Si algunas de estas carpetas están ubicadas en una unidad con espacio en disco insuficiente, es recomendable seleccionar otra unidad con más espacio disponible. De lo contrario, es posible que la compilación finalice antes de tiempo debido a espacio libre en disco insuficiente.

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

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

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

5.7.4.2 ESET Antivirus

Cuando crea el CD de ESET SysRescue, puede seleccionar dos fuentes de archivos ESET para que se usen en la compilación:

Carpeta ESS/EAV: archivos ya incluidos en la carpeta donde se instaló la solución ESET Security en el equipo.

Archivo MSI: se usan los archivos incluidos en el programa de instalación MSI

A continuación, puede elegir actualizar la ubicación de los archivos de actualización (.nup). Normalmente, debería estar seleccionada la opción predeterminada **carpeta ESS/EAV/archivo MSI**. En ciertos casos, se puede elegir una **Carpeta de actualización** personalizada, por ej., para usar una base de datos de firmas de virus anterior o posterior.

Puede utilizar una de las siguientes dos fuentes de nombre de usuario y contraseña:

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

Del usuario: se utilizan el nombre de usuario y la contraseña ingresados en los campos correspondientes.

NOTA: La solución ESET Security presente en el CD de ESET SysRescue se actualiza por Internet o mediante la solución ESET Security instalada en el equipo donde se ejecuta el CD de ESET SysRescue.

5.7.4.3 Configuración avanzada

La pestaña **Avanzado** permite optimizar el CD de ESET SysRescue según la cantidad de memoria de su equipo. Seleccione **576 MB o más** para escribir el contenido del CD en la memoria operativa (RAM). Si selecciona **menor que 576 MB**, se accederá en forma permanente al CD de recuperación cuando WinPE se esté ejecutando.

En la sección **Controladores externos**, puede insertar controladores para hardware específico (generalmente adaptadores de red). Aunque WinPE se basa en Windows Vista SP1, que es compatible con una amplia variedad de hardware, el hardware a veces no se reconoce. En este caso, es necesario agregar el controlador en forma manual. Hay dos formas de introducir un controlador en la compilación de ESET SysRescue: manual (con el botón **Agregar**) y automática (con el botón **Búsqueda automática**). En el caso de la introducción manual, debe seleccionar la ruta al archivo .inf correspondiente (en esta carpeta también debe estar presente el archivo *.sys aplicable). En el caso de la introducción automática, el controlador se busca automáticamente en el sistema operativo del equipo dado. Es recomendable usar la introducción automática solo si ESET SysRescue se usa en un equipo que tiene el mismo adaptador de red que el equipo donde se creó el CD de ESET SysRescue. Durante la creación, el controlador de ESET SysRescue se introduce en la compilación, por lo que el usuario no necesitará buscarlo más tarde.

5.7.4.4 Protocolo de Internet

Esta sección permite configurar la información de red básica y establecer las conexiones predefinidas tras ejecutar ESET SysRescue.

Seleccione **Dirección IP privada automática** para obtener la dirección IP en forma automática desde el servidor DHCP (Protocolo de configuración dinámica de host, por sus siglas en inglés).

Como alternativa, esta conexión de red puede usar una dirección IP especificada manualmente (también conocida como dirección IP estática). Seleccione **Personalizado** para configurar los valores IP apropiados. Si selecciona esta opción, debe especificar una **Dirección IP** y, para las conexiones de la LAN y las de Internet de alta velocidad, una **Máscara de subred**. En **Servidor DNS preferido** y **Servidor DNS secundario**, escriba las direcciones del servidor DNS primario y alternativo.

5.7.4.5 Dispositivo USB de inicio

Si seleccionó los dispositivos USB como medio de destino, puede elegir uno de los dispositivos USB disponibles en la pestaña **Dispositivo USB de inicio** (en caso de que haya más de uno).

Seleccione el **Dispositivo** de destino apropiado donde se instalará ESET SysRescue.

Advertencia: El dispositivo USB seleccionado se formateará durante el proceso de creación de ESET SysRescue. Como consecuencia, se eliminarán todos los datos del dispositivo.

Si elige la opción **Formato rápido**, se eliminarán todos los archivos de la partición formateada, pero no se explorará el disco en busca de sectores defectuosos. Utilice esta opción si el dispositivo USB ya se formateó anteriormente y usted está seguro de que no se encuentra dañado.

5.7.4.6 Grabación

Si seleccionó como medio de destino un CD o DVD, puede especificar parámetros adicionales de grabación en la pestaña **Grabar**.

Eliminar archivo ISO: seleccione esta opción para eliminar el archivo temporal ISO luego de la creación del CD de ESET SysRescue.

Eliminación habilitada: permite seleccionar entre el borrado rápido y el borrado completo.

Dispositivo de grabación: seleccione la unidad que usará para grabar.

Advertencia: Esta opción es la predeterminada. Si se usa un CD o DVD regrabable, se eliminarán todos los datos del CD o DVD.

La sección Medio contiene información sobre el medio que se encuentra insertado en el dispositivo de CD o DVD.

Velocidad de grabación: seleccione la velocidad deseada en el menú desplegable. A la hora de seleccionar la

velocidad de grabación, deben tenerse en cuenta las capacidades de su dispositivo de grabación y el tipo de CD o DVD utilizado.

5.7.5 Trabajo con ESET SysRescue

Para que el CD/DVD/USB de recuperación sea eficaz, debe iniciar el equipo desde el medio de arranque de ESET SysRescue. Se puede modificar la prioridad de arranque desde el BIOS. Alternativamente, puede usar el menú de arranque durante el inicio del equipo (en general, mediante una de las teclas entre F9 y F12, dependiendo de la versión de la placa base o del BIOS).

Una vez efectuado el arranque desde el medio de inicio, 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 la **Exploración del equipo**, la **Actualización** y algunas secciones de la **Configuración** y **Herramientas**. La capacidad de actualizar la base de datos de firmas de virus es la característica más importante de ESET SysRescue; por lo tanto, se recomienda actualizar el programa antes de iniciar una exploración del equipo.

5.7.5.1 Utilización de ESET SysRescue

Imagine que los equipos de la red se infectaron con un virus que modifica los archivos ejecutables (.exe). La solución ESET Security es capaz de limpiar todos los archivos infectados excepto *explorer.exe*, el cual no se puede limpiar, incluso en el modo Guardar. Esto se debe a que *explorer.exe*, por ser uno de los procesos esenciales de Windows, también se ejecuta en el Modo seguro. La solución ESET Security no tendría la posibilidad de realizar ninguna acción con el archivo, por lo que permanecería infectado.

En un escenario de este tipo, existe la opción de usar ESET SysRescue para resolver el problema. ESET SysRescue no requiere ningún componente del sistema operativo del host y por lo tanto es capaz de procesar (limpieza, eliminación) cualquier archivo en el disco.

5.8 Línea de comandos

El módulo antivirus de ESET NOD32 Antivirus se puede iniciar mediante una línea de comandos; ya sea en forma manual (con el comando "ecls") o con un archivo de procesamiento por lotes ("bat"). Uso del Módulo de exploración por línea de comandos de ESET:

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

Se pueden usar los siguientes parámetros y modificadores desde la línea de comandos durante la ejecución del módulo de exploración bajo demanda:

Opciones

/base-dir=FOLDER	cargar módulos desde FOLDER
/quar-dir=FOLDER	FOLDER de cuarentena
/exclude=MASK	excluir de la exploración los archivos que coinciden con MASK
/subdir	explorar las subcarpetas (predeterminado)
/no-subdir	no explorar las subcarpetas
/max-subdir-level=LEVEL	subnivel máximo de carpetas dentro de las carpetas que se van a explorar
/symlink	seguir los vínculos simbólicos (predeterminado)
/no-symlink	saltar los vínculos simbólicos
/ads	explorar ADS (predeterminado)
/no-ads	no explorar ADS
/log-file=FILE	registrar salida en FILE
/log-rewrite	sobrescribir archivo de salida (predeterminado: añadir)
/log-console	registrar resultados en la consola (predeterminado)
/no-log-console	no registrar resultados en la consola
/log-all	también incluir en el registro los archivos no infectados
/no-log-all	no registrar los archivos no infectados (predeterminado)
/aind	mostrar indicador de actividad
/auto	explorar y desinfectar todos los discos locales automáticamente

Opciones del módulo de exploración

/files	explorar los archivos (predeterminado)
/no-files	no explorar los archivos
/memory	explorar la memoria
/boots	explorar los sectores de inicio
/no-boots	no explorar los sectores de inicio (predeterminado)
/arch	explorar los archivos comprimidos (predeterminado)
/no-arch	no explorar los archivos comprimidos
/max-obj-size=SIZE	solo explorar los archivos menores que SIZE megabytes (predeterminado 0 = ilimitado)
/max-arch-level=LEVEL	subnivel máximo de archivos comprimidos dentro de los archivos comprimidos (anidados) que se van a explorar
/scan-timeout=LIMIT	explorar los archivos comprimidos durante LIMIT segundos como máximo
/max-arch-size=SIZE	solo explorar los archivos en un archivo comprimido si son menores que SIZE (predeterminado 0 = ilimitado)
/max-sfx-size=SIZE	solo explorar archivos dentro de un archivo comprimido de autoextracción si son menores que SIZE megabytes (predeterminado 0 = ilimitado)
/mail	explorar los archivos de correo electrónico (predeterminado)
/no-mail	no explorar los archivos de correo electrónico
/mailbox	explorar los buzones de correo (predeterminado)
/no-mailbox	no explorar los buzones de correo
/sfx	explorar los archivos comprimidos de autoextracción (predeterminado)
/no-sfx	no explorar los archivos comprimidos de autoextracción
/rtp	explorar los empaquetadores de tiempo de ejecución (predeterminado)
/no-rtp	no explorar los empaquetadores de tiempo de ejecución
/unsafe	explorar en búsqueda de aplicaciones potencialmente no seguras
/no-unsafe	no explorar en búsqueda de aplicaciones potencialmente no seguras (predeterminado)
/unwanted	explorar en búsqueda de aplicaciones potencialmente no deseadas
/no-unwanted	no explorar en búsqueda de aplicaciones potencialmente no deseadas (predeterminado)
/suspicious	explorar en busca de aplicaciones sospechosas (predeterminado)
/no-suspicious	no explorar en busca de aplicaciones sospechosas
/pattern	usar firmas (predeterminado)
/no-pattern	no usar firmas
/heur	habilitar la heurística (predeterminado)
/no-heur	deshabilitar la heurística
/adv-heur	habilitar la heurística avanzada (predeterminado)
/no-adv-heur	deshabilitar la heurística avanzada
/ext=EXTENSIONS	explorar solo las EXTENSIONS delimitadas por dos puntos
/ext-exclude=EXTENSIONS	excluir de la exploración las EXTENSIONS delimitadas por dos puntos
/clean-mode=MODE	usar el MODO de desinfección para objetos infectados

Se encuentran disponibles las siguientes opciones:

- **ninguna:** no se realizará desinfección automática alguna.
- **estándar** (predeterminado): ecls.exe intentará desinfectar o eliminar en forma automática los archivos infectados.
- **estricta:** ecls.exe intentará desinfectar o eliminar en forma automática los archivos infectados sin la intervención del usuario (no se le notificará antes de que se eliminen los archivos).
- **rigurosa:** ecls.exe eliminará los archivos sin intentar desinfectarlos, independientemente de qué archivo sea.
- **eliminar:** ecls.exe eliminará los archivos sin intentar desinfectarlos, pero se abstendrá de eliminar los archivos importantes, como los archivos del sistema de Windows.

/quarantine	copiar los archivos infectados (si fueron desinfectados) a cuarentena (complementa la acción realizada durante la desinfección)
/no-quarantine	no copiar los archivos infectados a cuarentena

Opciones generales

/help	mostrar la ayuda y salir
/version	mostrar información de la versión y salir
/preserve-time	preservar el último acceso con su fecha y hora

Códigos de salida

0	no se detectó ninguna amenaza
1	se detectó una amenaza y se desinfectó
10	algunos archivos no se pudieron explorar (pueden ser amenazas)
50	amenaza detectada
100	error

NOTA: Los códigos de salida mayores que 100 significan que el archivo no se exploró, por lo que puede estar infectado.

6. Glosario

6.1 Tipos de infiltraciones

Una infiltración es un programa con códigos maliciosos que intenta ingresar al equipo del usuario y/o dañarlo.

6.1.1 Virus

Un virus del equipo es un programa con códigos maliciosos que está adjunto o añadido a los archivos existentes de su equipo. Se denominaron así por los virus biológicos, ya que utilizan técnicas similares para propagarse desde un equipo a otro. El término “virus” se suele utilizar de manera incorrecta para referirse a cualquier tipo de amenaza. El uso indebido del término se está superando gradualmente y se lo está reemplazando por un término más apropiado, “malware” (software malicioso).

Los virus informáticos atacan principalmente a los archivos ejecutables y los documentos. En resumen, el virus informático funciona de esta forma: una vez que se ejecuta el archivo infectado, se llama al código malicioso y se ejecuta antes que la ejecución de la aplicación original. Un virus puede infectar cualquier archivo para el cual el usuario actual tenga permisos escritos.

Los virus informáticos pueden variar en su objetivo y gravedad. Algunos son extremadamente peligrosos debido a su capacidad de eliminar archivos del disco duro en forma deliberada. Por otra parte, algunos virus no provocan ningún daño: solo sirven para molestar al usuario y demostrar las habilidades técnicas de sus creadores.

Si su equipo está infectado con un virus y no es posible realizar la desinfección, envíelo al laboratorio de ESET para examinarlo. En determinados casos, los archivos infectados se pueden modificar hasta tal punto que la limpieza no es posible y los archivos se deben reemplazar por una copia limpia.

6.1.2 Gusanos

Un gusano informático es un programa que contiene códigos maliciosos que atacan a los equipos host y se propagan a través de la red. La diferencia básica entre un virus y un gusano es que los gusanos tienen la capacidad de propagarse por sí mismos; no dependen de archivos host (o de sectores de inicio). Los gusanos se propagan a las direcciones de correo electrónico de la lista de contactos del usuario o aprovechan vulnerabilidades de seguridad en aplicaciones de red.

Como consecuencia, los gusanos son mucho más viables que los virus informáticos. Debido a la alta disponibilidad de Internet, pueden propagarse alrededor del mundo en cuestión de horas e incluso minutos después de su lanzamiento. Esta capacidad de replicarse en forma independiente y rápida los hace más peligrosos que otros tipos de malware.

Un gusano activado en un sistema puede provocar una serie de inconvenientes: eliminar archivos, afectar perjudicialmente el rendimiento del sistema o incluso desactivar programas. La naturaleza del gusano informático le permite servir de “medio de transporte” para otros tipos de infiltraciones.

Si su equipo está infectado con un gusano, se recomienda eliminar los archivos infectados, ya que probablemente contengan códigos maliciosos.

6.1.3 Troyanos

Históricamente, los troyanos (caballos de Troya) informáticos se definieron como una clase de amenazas que intenta pasar por programas útiles y engañar a los usuarios para que los ejecuten.

Debido a que los troyanos son una categoría muy amplia, a menudo se divide en varias subcategorías:

- **Descargador:** Programas maliciosos con capacidad de descargar otras amenazas desde Internet.
- **Lanzador:** Programas maliciosos con capacidad de lanzar otros tipos de malware a equipos expuestos.
- **Programa de puerta trasera:** Programas maliciosos que se comunican con atacantes remotos, permitiéndoles obtener acceso al equipo y controlarlo.
- **Registrador de pulsaciones :** es un programa que registra cada pulsación que el usuario hace en el teclado y envía la información a atacantes remotos.
- **Marcador :** programas maliciosos diseñados para conectar el equipo a números con tarifas más elevadas de lo normal en lugar de hacerlo con el proveedor de servicios de Internet del usuario. Resulta casi imposible que el usuario advierta que se creó una nueva conexión. Los marcadores solo pueden perjudicar a los usuarios que se conectan a Internet a través de un módem de discado telefónico, lo que está dejando de ser habitual.

Si un archivo de su equipo es identificado como un Troyano, se aconseja eliminarlo, ya que lo más probable es que no contenga más que códigos maliciosos.

6.1.4 Rootkits

Los rootkits son programas maliciosos que les garantizan a los atacantes por Internet acceso ilimitado a un sistema, a la vez que ocultan su presencia. Después de acceder a un sistema (en general luego de aprovecharse de una vulnerabilidad de un sistema), los rootkits utilizan funciones del sistema operativo para evitar ser detectados por el software antivirus: ocultan procesos, archivos y datos del registro de Windows. Por esa razón, es casi imposible detectarlos por medio de técnicas comunes de evaluación.

Existen dos niveles de detección para prevenir rootkits:

1. Cuando intentan acceder al sistema: Todavía no están presentes, por lo tanto están inactivos. La mayoría de los sistemas antivirus pueden eliminar rootkits en este nivel (asumiendo que realmente detectan dichos archivos como infectados).
2. Cuando se ocultan de la evaluación común: ESET NOD32 Antivirus tienen la ventaja de contar con la tecnología AntiStealth, que también es capaz de detectar y eliminar rootkits activos.

6.1.5 Adware

Adware es el término abreviado correspondiente a un programa relacionado con la publicidad. Los programas que muestran material publicitario se incluyen en esta categoría. Las aplicaciones de adware suelen abrir automáticamente una nueva ventana emergente con avisos publicitarios en un navegador de Internet o cambian la página de inicio del navegador. Con frecuencia, el adware forma parte de un paquete junto con programas de distribución gratuita, lo que les permite a sus creadores cubrir los gastos del desarrollo de las aplicaciones (normalmente útiles).

El adware no constituye un peligro en sí mismo: solo puede llegar a molestar a los usuarios con las publicidades. El peligro reside en el hecho de que el adware también puede realizar funciones de seguimiento (al igual que el spyware).

Si decide utilizar un producto de distribución gratuita, preste especial atención durante su instalación. Lo más probable es que el programa de instalación le informe acerca de la instalación de un programa de adware adicional. En muchas ocasiones se le permitirá cancelar esa opción e instalar el programa sin el adware.

Sin embargo, otros programas no se instalarán sin el adware o sus funciones serán limitadas. Esto significa que el adware a menudo puede obtener acceso al sistema en forma “legal”, ya que los usuarios dieron su consentimiento para instalarlo. En este caso, es mejor prevenir que lamentarse luego. Si se detecta un archivo como adware en el equipo, se recomienda eliminarlo, ya que existe una gran probabilidad de que contenga códigos maliciosos.

6.1.6 Spyware

Esta categoría abarca todas las aplicaciones que envían información privada sin el consentimiento o el conocimiento del usuario. El spyware utiliza funciones de seguimiento para enviar diversos datos estadísticos, tales como una lista de sitios Web visitados, direcciones de correo electrónico de la lista de contactos del usuario o una lista del registro de las pulsaciones del teclado.

Los creadores del spyware afirman que el propósito de estas técnicas es averiguar más sobre las necesidades y los intereses de los usuarios y mejorar la orientación de las publicidades. El problema es que no existe una clara distinción entre las aplicaciones útiles y las maliciosas, y nadie puede asegurar que la información recuperada no se usará inadecuadamente. Los datos obtenidos por las aplicaciones spyware pueden contener códigos de seguridad, números de identificación PIN, números de cuentas bancarias, etc. El spyware suele estar incluido en un paquete junto a versiones gratuitas de programas del mismo creador con el objetivo de generar ingresos o como un incentivo para que el usuario luego adquiera el programa. Con frecuencia, se les informa a los usuarios sobre la presencia del spyware durante la instalación del programa para incentivarlos a reemplazar el producto por la versión posterior pagada, que no incluye spyware.

Algunos ejemplos de productos de distribución gratuita conocidos que incluyen spyware son las aplicaciones de cliente de redes P2P (redes de pares). Spyfalcon o Spy Sheriff (entre muchas otras) pertenecen a una subcategoría específica de spyware: aparentan ser programas antispyware, pero en realidad ellos mismos son programas spyware.

Si se detecta un archivo como spyware en el equipo, se recomienda eliminarlo, ya que existe una gran probabilidad de que contenga códigos maliciosos.

6.1.7 Empaquetadores

Un programa empaquetador es un ejecutable de autoextracción y de tiempo de ejecución que acumula distintos tipos de malware en un solo paquete.

Los empaquetadores más comunes son UPX, PE_Compact, PKLite y ASPack. El mismo malware puede detectarse de manera diferente si se comprime con otro empaquetador. Los empaquetadores tienen la capacidad de hacer mutar sus “firmas” con el tiempo, lo cual dificulta mucho más la detección y eliminación del malware.

6.1.8 Aplicaciones potencialmente no seguras

Existen muchos programas legítimos cuya función es simplificar la gestión de los equipos en red. Sin embargo, en manos equivocadas, pueden ser utilizados con propósitos maliciosos. ESET NOD32 Antivirus brinda la opción de detectar dichas amenazas.

Aplicaciones potencialmente no seguras es la clasificación usada para programas comerciales y legítimos. Esta clasificación incluye programas como herramientas de acceso remoto, aplicaciones para adivinar contraseñas y registradores de pulsaciones (programas que registran las pulsaciones del teclado por parte del usuario).

Si descubre que hay una aplicación potencialmente no segura presente y activa en su equipo (y que usted no instaló), consulte a su administrador de red o elimine la aplicación.

6.1.9 Aplicaciones potencialmente no deseadas

Aplicaciones potencialmente no deseadas: estas aplicaciones no tienen necesariamente la intención de ser maliciosas, pero pueden afectar el rendimiento de su equipo en forma negativa. Dichas aplicaciones suelen requerir el consentimiento del usuario previo a la instalación. Si están presentes en el equipo, el sistema se comporta de manera diferente (al compararlo con el estado antes de su instalación). Los cambios más significativos son:

- Nuevas ventanas nunca antes vistas (ventanas emergentes, anuncios),
- Activación y ejecución de procesos ocultos,
- Incremento en el uso de los recursos del sistema,
- Cambios en los resultados de las búsquedas y
- La aplicación establece comunicaciones con servidores remotos.

6.2 Tecnología ESET

6.2.1 Bloqueador de exploits

Bloqueador de exploits está diseñado para fortalecer diferentes tipos de aplicaciones comúnmente explotadas como los navegadores web, los lectores de PDF, los clientes de correo electrónico y los componentes de MS Office. Funciona controlando el comportamiento de los procesos en busca de actividad sospechosa que puede indicar un exploit.

Cuando el bloqueador de exploits identifica un proceso sospechoso, puede detener el proceso inmediatamente y registrar datos acerca de la amenaza, que se envían al sistema de la nube ESET Live Grid cloud system. El laboratorio de amenazas de ESET procesa los datos y los utiliza para proteger mejor a los usuarios de amenazas desconocidas y ataques zero-day (malware recientemente lanzado para el que no hay una solución configurada previamente).

6.2.2 Exploración de memoria avanzada

Exploración de memoria avanzada trabaja en conjunto con el bloqueador de exploits para fortalecer la protección contra malware diseñado para evadir la detección por los productos antimalware con el uso de ofuscación o cifrado. En los casos en los que la emulación o la heurística ordinarias no detecten una amenaza, la exploración de memoria avanzada puede identificar un comportamiento sospechoso y buscar amenazas cuando se manifiestan en la memoria del sistema. Esta solución es efectiva contra malware severamente ofuscado.

A diferencia del bloqueador de exploits, la exploración de memoria avanzada es un método posterior a la ejecución, lo que significa que existe un riesgo de que se haya realizado alguna actividad maliciosa antes de la detección de una amenaza; sin embargo en caso de que hayan fallado otras técnicas de detección, ofrece una capa adicional de seguridad.

6.2.3 ESET Live Grid

Creada en ThreatSense.Net® el sistema avanzado de alerta temprana, ESET Live Grid utiliza datos que los usuarios de ESET enviaron de todo el mundo y los envía al laboratorio de virus de ESET. Al proporcionar muestras sospechosas y metadatos from the wild, ESET Live Grid nos permite reaccionar inmediatamente ante las necesidades de nuestros clientes y mantener a ESET receptivo a las últimas amenazas. Los investigadores de malware de ESET utilizan la información para crear una instantánea precisa de la naturaleza y el alcance de amenazas globales, lo que nos ayuda a concentrarnos en los objetivos correctos. Los datos de ESET Live Grid tienen un rol importante al establecer las prioridades en nuestro procesamiento automático.

Además, implementa un sistema de reputación que ayuda a mejorar la eficiencia general de nuestras soluciones antimalware. Cuando se inspecciona un archivo ejecutable en el sistema de un usuario, su etiqueta hash primero se compara con una base de datos de elementos permitidos y bloqueados. Si se encuentra en la lista de permitidos, el archivo inspeccionado se considera limpio y también se lo marca para excluirlo en futuras exploraciones. Si se encuentra en la lista de bloqueados, se toman las acciones correspondientes en base a la naturaleza de la amenaza. Si no hay coincidencia, se explora el archivo completamente. En base a los resultados de la exploración, los archivos se clasifican en amenazas o no amenazas. Este enfoque tiene un impacto significativamente positivo en el rendimiento de la exploración.

Este sistema de reputación permite la detección efectiva de muestras de malware incluso antes de proporcionar sus firmas al equipo del usuario mediante una base de datos de virus actualizada (que sucede varias veces al día).

6.2.4 Bloqueador de exploits de Java

El Bloqueador de exploits de Java es una extensión de la protección existente del bloqueador de exploits. Controla Java y busca comportamiento similar al de exploits. Las muestras bloqueadas pueden informarse al analizador de malware, para que puedan crear firmas para bloquearlos en diferentes capas (bloqueo de URL, descarga de archivo, etc.).

6.3 Correo electrónico

El correo electrónico (o email) es una forma moderna de comunicación que tiene muchas ventajas. Es flexible, rápido y directo, y desempeñó un papel crucial en la proliferación de Internet a principios de la década de 1990.

Lamentablemente, debido a su alto grado de anonimato, el correo electrónico e Internet dejan un margen para las actividades ilegales como el envío de spam. El spam incluye avisos no solicitados, mensajes falsos y la proliferación de software malicioso (o malware). La desventaja y el peligro para el usuario se ven incrementados por el hecho de que el costo de enviar spam es mínimo y de que los creadores de spam cuentan con muchas herramientas para obtener nuevas direcciones de correo electrónico. Por otro lado, el volumen y la diversidad del spam lo hacen muy difícil de controlar. Cuanto más se use una dirección de correo electrónico, hay más probabilidades de que termine en la base de datos de un motor de spam. Algunos consejos para la prevención:

- Si es posible, no publique su dirección de correo electrónico en Internet
- Solo dé su dirección de correo electrónico a personas de confianza
- Si es posible, no use alias comunes; con alias más complejos, hay menos probabilidades de realizar un seguimiento
- No conteste los mensajes de spam que ya llegaron a su buzón de entrada
- Sea precavido al completar formularios de Internet; tenga un cuidado especial con opciones como “Sí, deseo recibir información”.
- Use direcciones de correo electrónico “especializadas”; por ejemplo, una para el trabajo, otra para comunicarse con las amistades, etc.
- De cuando en cuando, cambie su dirección de correo electrónico
- Use una solución antispam

6.3.1 Anuncios

Los anuncios por Internet constituyen una de las formas de publicidad de crecimiento más rápido. Sus principales ventajas de marketing son los costos mínimos y el alto nivel de direccionamiento; además, los mensajes se distribuyen casi de inmediato. Muchas empresas usan herramientas de marketing por correo electrónico para comunicarse en forma efectiva con clientes actuales y potenciales.

Este tipo de publicidad es legítima, ya que el destinatario puede estar interesado en recibir información comercial sobre ciertos productos. No obstante, muchas empresas envían mensajes comerciales masivos no solicitados. En esos casos, la publicidad por correo electrónico cruza la línea y se convierte en spam.

La cantidad de correo electrónico no solicitado comenzó a ser un problema y no muestra signos de desacelerar. Los creadores de los correos electrónicos no solicitados suelen tratar de disfrazar el spam, haciéndolos pasar por mensajes legítimos.

6.3.2 Mensajes falsos

Un mensaje falso (o hoax) es información falsa que se propaga por Internet. Los mensajes falsos generalmente se envían a través del correo electrónico o de herramientas de comunicación como ICQ y Skype. El mensaje en sí suele ser una broma o una leyenda urbana.

Los mensajes falsos propagados por virus informáticos tienen el propósito de provocar miedo, incertidumbre y duda en los destinatarios, haciéndoles creer que un “virus no detectable” presente en su equipo está borrando archivos y recuperando contraseñas, o realizando otras actividades perjudiciales para el sistema.

Para perpetuarse, algunos mensajes falsos le piden al destinatario que los reenvíen a sus contactos. Hay una gran variedad de mensajes falsos: los transmitidos por telefonía móvil, pedidos de ayuda, personas que ofrecen enviarle

al destinatario dinero desde el exterior, etc. Es prácticamente imposible determinar el propósito de su creador.

Cuando un mensaje instiga al destinatario a reenviarlo a todos sus conocidos, es muy probable que se trate de un mensaje falso. Existen muchos sitios Web en Internet para verificar si un correo electrónico es legítimo. Antes de reenviar dichos mensajes, el usuario debe realizar una búsqueda en Internet sobre todos los que sospeche que puedan ser falsos.

6.3.3 Phishing

El término phishing define una actividad criminal que utiliza técnicas de ingeniería social (manipula a los usuarios para obtener información confidencial). Su propósito es obtener el acceso a datos confidenciales, como números de cuentas bancarias, códigos de identificación personal, etc.

Muchas veces logran el acceso mediante el envío de correos electrónicos encubiertos como correos legítimos de personas o empresas confiables (por ej., una institución financiera, una compañía de seguros, etc.). El correo puede parecer realmente genuino y suele incluir gráficos y contenidos tomados originalmente de la fuente real por la que se hace pasar. Le solicita al usuario que ingrese, por diversas excusas (verificación de datos, operaciones financieras), ciertos datos personales, como números de cuentas bancarias, nombres de usuario y contraseñas, etc. Si ingresa estos datos, pueden ser robados y malversados con facilidad.

Hay que tener en cuenta que los bancos, compañías de seguros y otras empresas legítimas nunca solicitarán nombres de usuario o contraseñas en un correo electrónico no solicitado.

6.3.4 Reconocimiento de fraudes de spam

En general, existen varios indicadores que ayudan a identificar mensajes de spam (correo no solicitado) en su buzón de entrada. Si el mensaje cumple con al menos alguno de los siguientes criterios, probablemente se trate de un mensaje de spam.

- La dirección del remitente no pertenece a una persona de su lista de contactos.
- Se le ofrece una gran cantidad de dinero, pero antes usted tiene que enviar una pequeña cantidad.
- Le solicitan que ingrese, por diversas excusas (verificación de datos, operaciones financieras), ciertos datos personales, como números de cuentas bancarias, nombres de usuario y contraseñas, etc.
- Está escrito en un idioma extranjero.
- Le ofrecen que adquiera un producto en el que usted no está interesado. Si igual decide comprarlo, antes verifique que el remitente del mensaje sea un proveedor confiable (consulte al fabricante original del producto).
- Algunas palabras tienen errores de ortografía para engañar el filtro del programa antispam. Por ejemplo, “vaigra” en lugar de “viagra”, etc.