

ESET NOD32 Antivirus

Guía para el usuario

[Haga clic aquí para mostrar la versión de ayuda de este documento](#)

Copyright ©2024 de ESET, spol. s r.o.

ESET NOD32 Antivirus ha sido desarrollado por ESET, spol. s r.o.

Para obtener más información, visite <https://www.eset.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 autorización por escrito del autor.

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

Soporte técnico: <https://support.eset.com>

REV. 12/04/2024

1 ESET NOD32 Antivirus	1
1.1 Novedades	2
1.2 ¿Qué producto tengo?	2
1.3 Requisitos del sistema	3
1.3 Versión obsoleta de Microsoft Windows	4
1.4 Prevención	5
1.5 Páginas de ayuda	6
2 Instalación	7
2.1 Instalador activo	7
2.2 Instalación fuera de línea	9
2.3 Activación del producto	10
2.3 Ingreso de su clave de licencia durante la activación	11
2.3 Usar ESET HOME cuenta	12
2.3 Activación de la licencia de prueba	13
2.3 Clave de licencia de ESET gratuita	13
2.3 Falló la activación - situaciones comunes	14
2.3 Estado de licencia	14
2.3 Error de activación debido a una licencia sobreusada	15
2.3 Actualización de la licencia	16
2.3 Actualización del producto	17
2.3 Cambio de la licencia a una categoría inferior	18
2.3 Cambio del producto a una categoría inferior	18
2.4 Solucionador de problemas de instalación	19
2.5 Primera exploración después de la instalación	19
2.6 Reemplazo a una versión más reciente	20
2.6 Actualización automática de versión antigua del producto	21
2.7 Recomiende el producto de ESET a un amigo	21
2.7 Se instalará ESET NOD32 Antivirus	22
2.7 Cambiar a una línea diferente de productos	22
2.7 Registro	22
2.7 Progreso de la activación	22
2.7 La activación se completó correctamente.	22
3 Guía para principiantes	23
3.1 La ventana principal del programa	23
3.2 Actualizaciones	26
4 Trabajar con ESET NOD32 Antivirus	27
4.1 Protección del equipo	29
4.1 Motor de detección	30
4.1 Opciones avanzadas del motor de detección	34
4.1 Infiltración detectada	35
4.1 Protección del sistema de archivos en tiempo real	37
4.1 Niveles de desinfección	39
4.1 Cuándo modificar la configuración de la protección en tiempo real	40
4.1 Verificación de la protección en tiempo real	40
4.1 Qué hacer si la protección en tiempo real no funciona	40
4.1 Exclusiones de procesos	41
4.1 Agregado o edición de exclusiones de procesos	42
4.1 Protección basada en la nube	42
4.1 Filtro de exclusión para la protección basada en la nube	45
4.1 Exploración del equipo	45

4.1	Iniciador de la exploración personalizada	48
4.1	Progreso de la exploración	49
4.1	Registro de exploración del equipo	51
4.1	Exploración de malware	53
4.1	Exploración en estado inactivo	53
4.1	Perfiles de exploración	54
4.1	Objetos para explorar	55
4.1	Control del dispositivo	55
4.1	Editor de reglas del control del dispositivo	56
4.1	Dispositivos detectados	57
4.1	Agregado de reglas del control del dispositivo	57
4.1	Grupos de dispositivos	60
4.1	Sistema de prevención de intrusiones basado en el host (HIPS)	61
4.1	Ventana interactiva de HIPS	64
4.1	Se detectó un comportamiento ransomware potencial	65
4.1	Administración de reglas del HIPS	66
4.1	Configuración de reglas HIPS	67
4.1	Agregado de una aplicación/ruta de registro para HIPS	70
4.1	Configuración avanzada de HIPS	70
4.1	Controladores siempre permitidos para cargar	71
4.1	Modo de juego	71
4.1	Exploración en el inicio	72
4.1	Verificación de archivos de inicio automático	72
4.1	Protección de documentos	73
4.1	Exclusiones	73
4.1	Exclusiones de rendimiento	74
4.1	Agregar o editar exclusión de rendimiento	75
4.1	Formato de las exclusiones de ruta	76
4.1	Exclusiones de la detección	77
4.1	Agregar o editar exclusiones de la detección	79
4.1	Asistente para crear exclusiones de la detección	80
4.1	Exclusiones de HIPS	80
4.1	ThreatSense parámetros	81
4.1	Extensiones de archivos que no se analizarán	84
4.1	Parámetros adicionales de ThreatSense	85
4.2	Protección de Internet	86
4.2	Filtrado de protocolos	87
4.2	Aplicaciones excluidas	87
4.2	Direcciones IP excluidas	88
4.2	Agregar dirección IPv4	89
4.2	Agregar dirección IPv6	89
4.2	SSL/TLS	90
4.2	Certificados	91
4.2	Tráfico de red cifrada	92
4.2	Lista de certificados conocidos	92
4.2	Lista de aplicaciones SSL/TLS filtradas	93
4.2	Protección del cliente de correo electrónico	93
4.2	Integración con el cliente de correo electrónico	94
4.2	Barra de herramientas de Microsoft Outlook	95
4.2	Cuadro de diálogo de confirmación	95
4.2	Volver a explorar los mensajes	95

4.2 Protocolos de correo electrónico	95
4.2 Filtro para POP3, POP3S	97
4.2 Etiquetas de correo electrónico	97
4.2 Protección del acceso a la Web	98
4.2 Configuración avanzada de la protección de acceso a la web	100
4.2 Protocolos Web	101
4.2 Administración de direcciones URL	101
4.2 Lista de direcciones URL	102
4.2 Crear nueva lista de direcciones URL	103
4.2 Cómo agregar una máscara URL	104
4.2 Protección antiphishing	104
4.3 Actualización del programa	106
4.3 Configuración de la actualización	109
4.3 Actualizar reversión	111
4.3 Intervalo de tiempo de reversión	113
4.3 Actualizaciones del producto	113
4.3 Opciones de conexión	114
4.3 Cómo crear tareas de actualización	114
4.3 Cuadro de diálogo: es necesario reiniciar	115
4.4 Herramientas	115
4.4 Archivos de registro	116
4.4 Filtrado de registros	118
4.4 Configuración de registro	120
4.4 Procesos activos	121
4.4 Informe de seguridad	123
4.4 ESET SysInspector	124
4.4 Tareas programadas	125
4.4 Opciones de exploración programada	127
4.4 Resumen general de tareas programadas	128
4.4 Detalles de tarea	128
4.4 Programación de tarea	129
4.4 Sincronización de la tarea: una vez	129
4.4 Sincronización de la tarea: diariamente	129
4.4 Sincronización de la tarea: semanalmente	129
4.4 Sincronización de la tarea: desencadenada por un suceso	130
4.4 Omisión de una tarea	130
4.4 Detalles de la tarea: actualizar	131
4.4 Detalles de la tarea: ejecutar aplicación	131
4.4 Limpiador de sistema	131
4.4 Cuarentena	132
4.4 Servidor proxy	135
4.4 Seleccionar muestra para su análisis	136
4.4 Seleccionar muestra para su análisis: archivo sospechoso	137
4.4 Seleccionar muestra para su análisis: sitio sospechoso	137
4.4 Seleccionar muestra para su análisis: archivo con falso positivo	138
4.4 Seleccionar muestra para su análisis: sitio de falso positivo	138
4.4 Seleccionar muestra para su análisis: otros	139
4.4 Actualización de Microsoft Windows®	139
4.4 Cuadro de diálogo: actualizaciones del sistema	139
4.4 Información sobre la actualización	140
4.5 Ayuda y soporte	140

4.5 Acerca de ESET NOD32 Antivirus	141
4.5 ESET Noticias	141
4.5 Enviar datos de configuración del sistema	142
4.5 Soporte técnico	143
4.6 Cuenta ESET HOME	143
4.6 Conectarse a ESET HOME	145
4.6 Inicie sesión en ESET HOME	146
4.6 Error de inicio de sesión: errores comunes	147
4.6 Agregar dispositivo en ESET HOME	147
4.7 Interfaz del usuario	148
4.7 Elementos de la interfaz del usuario	148
4.7 Configuración del acceso	149
4.7 Contraseña para configuración avanzada	150
4.7 Ícono de la bandeja del sistema	150
4.7 Asistencia para lectores de pantalla	151
4.8 Notificaciones	151
4.8 Ventana de diálogo: estados de la aplicación	152
4.8 Notificaciones en el escritorio	153
4.8 Lista de notificaciones en el escritorio	154
4.8 Alertas interactivas	155
4.8 Mensajes de confirmación	157
4.8 Medios extraíbles	158
4.8 Reenvío	159
4.9 Configuración de privacidad	161
4.10 Perfiles	162
4.11 Accesos directos desde el teclado	163
4.12 Diagnósticos	164
4.12 Soporte técnico	165
4.12 Importación y exportación de una configuración	166
4.12 Restauración de todas las configuraciones en la sección actual	167
4.12 Revertir a la configuración predeterminada	167
4.12 Error al guardar la configuración	167
4.13 Exploración de la línea de comandos.	167
4.14 ESET CMD	170
4.15 Detección en estado inactivo	171
5 Preguntas habituales	172
5.1 Cómo actualizar ESET NOD32 Antivirus	173
5.2 Cómo quitar un virus del equipo	173
5.3 Cómo crear una nueva tarea en Tareas programadas	173
5.4 Cómo programar una exploración semanal del equipo	174
5.5 Cómo desbloquear la configuración avanzada	175
5.6 Cómo resolver la desactivación del producto desde ESET HOME	175
5.6 Producto desactivado, dispositivo desconectado	176
5.6 Producto no activado	176
6 Programa de mejora de la experiencia del cliente	176
7 Acuerdo de licencia de usuario final	177
8 Política de privacidad	189

ESSENTIAL SECURITY

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 ESET LiveGrid® utiliza velocidad y precisión para mantener el equipo seguro. El resultado es un sistema inteligente constantemente en alerta frente a los ataques y el software malicioso que podrían amenazar 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

Interfaz del usuario rediseñada	La interfaz del usuario en esta versión se ha rediseñado y simplificado considerablemente con base en los resultados de las pruebas de usabilidad. Todas las etiquetas y notificaciones de la interfaz gráfica del usuario se han revisado cuidadosamente. Ahora, la interfaz es compatible con idiomas de derecha a izquierda, como hebreo y árabe. La ayuda en línea se encuentra integrada en ESET NOD32 Antivirus y ofrece contenido de soporte actualizado en forma dinámica.
Modo oscuro	Una extensión que le ayuda a cambiar rápidamente la pantalla a un tema oscuro. Puede elegir su esquema de colores preferido en Elementos de la interfaz de usuario .
Antivirus y antispyware	Detecta en forma proactiva y desinfecta más cantidad de amenazas conocidas y desconocidas, tales como virus, gusanos, troyanos y rootkits. La 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 frecuente del motor de detección (anteriormente conocido como “base de datos de firmas de virus”) y de los módulos de programa es el mejor método para asegurar el máximo nivel de seguridad en su equipo.
ESET LiveGrid® (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 de dispositivos	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	Postpone 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.

Novedades

Novedades de la versión 16.1 de ESET NOD32 Antivirus

Intel® Threat Detection Technology

Tecnología basada en hardware que expone ransomware cuando intenta evitar la detección en la memoria. Su integración aumenta la protección contra ransomware a la vez que mantiene un alto rendimiento general del sistema. Consulte los [procesadores compatibles](#).

Modo oscuro

Esta característica le permite elegir un esquema de colores claros u oscuros para la interfaz gráfica de usuario de ESET NOD32 Antivirus. Ahora puede cambiar el esquema de colores en la esquina superior derecha de la [ventana principal del programa](#).

Se quitó la compatibilidad con Windows 7, 8 y 8.1.

ESET NOD32 Antivirus 16.1 solo es compatible con las versiones 10 y 11 de Windows. Para obtener más información, consulte [Versiones obsoletas de Microsoft Windows](#).



Para desactivar las **Notificaciones de novedades**, haga clic en **Configuración avanzada > Notificaciones > Notificaciones en el escritorio**. Haga clic en **Editar** junto a **Notificaciones de escritorio** y anule la selección de la casilla de verificación **Mostrar notificaciones de novedades** y haga clic en **Aceptar**. Para obtener más información sobre las notificaciones, consulte la sección [Notificaciones](#).

¿Qué producto tengo?

ESET ofrece capas múltiples de seguridad con productos nuevos, desde una solución de antivirus rápida y potente hasta una solución de seguridad todo en un uno con mínimo impacto en el sistema:


- ESET NOD32 Antivirus
- ESET Internet Security
- ESET Smart Security Premium

Para determinar qué producto tiene instalado abra la [ventana principal del programa](#) y verá el nombre del producto en la parte superior de la ventana (consulte el [Artículo de la base de conocimiento](#)).

La tabla a continuación detalla las funciones disponibles para cada producto específico.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Motor de detección	✓	✓	✓
Aprendizaje automático avanzado	✓	✓	✓

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Bloqueador de exploits	✓	✓	✓
Protección contra ataque basado en script	✓	✓	✓
Anti-Phishing	✓	✓	✓
Protección del acceso a la Web	✓	✓	✓
HIPS (incluida la Protección contra ransomware)	✓	✓	✓
Antispam		✓	✓
Firewall		✓	✓
Inspector de red		✓	✓
Protección de la cámara web		✓	✓
Protección contra ataques de red		✓	✓
Protección contra Botnet		✓	✓
Protección de banca y pagos en línea		✓	✓
Control parental		✓	✓
Anti-Theft		✓	✓
Password Manager			✓
ESET Secure Data			✓
ESET LiveGuard			✓

 Es posible que algunos de los productos anteriores no estén disponibles en su idioma / región.

Requisitos del sistema

Su sistema debe reunir los siguientes requisitos de hardware y software para que ESET NOD32 Antivirus funcione correctamente:


Procesadores compatibles

Intel o AMD procesador de 32 bits (x86) con conjunto de SSE2 o procesador de 64 bits (x64), 1 GHz o superior
procesador basado en ARM64, 1 GHz o superior

El sistema operativo es compatible

Microsoft® Windows® 11

Microsoft® Windows® 10

 Siempre intente mantener su sistema operativo actualizado.

Requisitos de características de ESET NOD32 Antivirus

Consulte los requisitos del sistema para características específicas de ESET NOD32 Antivirus en la tabla que aparece a continuación:

Característica	Requisitos
Intel® Threat Detection Technology	Consulte los procesadores compatibles .
Fondo transparente	Versión para Windows 10 RS4 y posterior.
Limpiador especializado	Procesador que no está basado en ARM64.
Limpiador de sistema	Procesador que no está basado en ARM64.
Bloqueador de exploits	Procesador que no está basado en ARM64.
Inspección profunda del comportamiento	Procesador que no está basado en ARM64.

Otros

Se requiere conexión a Internet para que la activación y las actualizaciones de ESET NOD32 Antivirus funcionen correctamente.

Si dos programas antivirus se ejecutan simultáneamente en un solo dispositivo, se producen conflictos inevitables entre los recursos del sistema, como la ralentización del sistema, la cual lo haría inoperable.

Versión obsoleta de Microsoft Windows

Problema

- Quiere instalar la versión más reciente de ESET NOD32 Antivirus en un equipo con Windows 7, Windows 8 (8.1) o Windows Home Server 2011
- ESET NOD32 Antivirus muestra un error de **Sistema operativo obsoleto** durante la instalación

Detalles

La versión más reciente de ESET NOD32 Antivirus (versión 16.1) requiere sistemas operativos Windows 10 o Windows 11.

Solución

Están disponibles las soluciones siguientes:

Actualizar a Windows 10 o Windows 11

El proceso de actualización es relativamente fácil y, en muchos casos, puede hacerlo sin perder archivos. Antes de actualizar a Windows 10:

1. Copia de seguridad de datos importantes.
2. Lea las [Preguntas frecuentes sobre la actualización a Windows 10](#) o las [Preguntas frecuentes sobre la actualización a Windows 11](#) de Microsoft y actualice su sistema operativo Windows.

Instale la versión 16.0 de ESET NOD32 Antivirus

Si no puede actualizar Windows, [instale la versión 16.0 de ESET NOD32 Antivirus](#). Para obtener más información, consulte la [Ayuda en línea sobre la versión 16.0 de ESET NOD32 Antivirus](#).

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 remotos](#). 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 LiveGrid®, 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 investigación 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 virus, gusanos, troyanos y rootkits más conocidos y desconocidos. Esto significa que, cada vez que accede a un archivo o lo abre, se lo explora para evitar actividades de malware. Se recomienda realizar una exploración completa del equipo al menos una vez por mes, ya que las firmas de malware varía y el motor de detección 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.

Páginas de ayuda

Bienvenido a la guía de usuario de ESET NOD32 Antivirus. La información que se proporciona aquí sirve para presentar el producto y ayudarlo a hacer que su equipo sea más seguro.

Introducción

Antes de utilizar ESET NOD32 Antivirus, puede leer información sobre diversos [tipos de detecciones](#) y [ataques remotos](#) que puede encontrarse al usar el equipo. También hemos recopilado una lista de [nuevas características](#) introducidas en ESET NOD32 Antivirus.

Comience por [instalar ESET NOD32 Antivirus](#). Si ya tiene ESET NOD32 Antivirus instalado, consulte [Trabajar con ESET NOD32 Antivirus](#).

Cómo usar las páginas de ayuda de ESET NOD32 Antivirus

La ayuda en línea se divide en diversos capítulos y subcapítulos. Pulse **F1** en ESET NOD32 Antivirus para ver información sobre la ventana abierta actualmente.

El programa le permite buscar en un tema de ayuda por palabra clave o buscar contenido una vez que introduce palabras o frases. La diferencia entre ambos métodos es que una palabra clave puede estar lógicamente relacionada con las páginas de ayuda que no contienen esa palabra clave específica en el texto. La búsqueda por palabras y frases buscará el contenido de todas las páginas y mostrará solo aquéllas que contengan la palabra o frase en el texto real.

A fin de garantizar la consistencia y ayudar a evitar la confusión, la terminología que se usa en esta guía se basa en la interfaz de usuario de ESET NOD32 Antivirus. También usamos un conjunto uniforme de símbolos para resaltar temas de interés o de una importancia particular.



Una nota es una observación breve. Aunque puede omitirlas, las notas pueden proporcionar información valiosa, tales como características específicas o un enlace a un tema relacionado.



Es algo que requiere su atención y no recomendamos dejarlo de lado. Normalmente, ofrece información que no es vital, pero sí importante.



Esta información requiere precaución y atención adicional. Las advertencias se incluyen específicamente para evitar que cometa errores potencialmente perjudiciales. Lea y comprenda el texto, ya que hace referencia a una configuración del sistema muy delicada o a algún elemento que puede ser de riesgo.



Este es un ejemplo de uso o ejemplo práctico que apunta a ayudarlo a entender cómo puede utilizarse una cierta función o característica.

Convención	Significado
En negrita	Nombres de elementos de interfaces como cuadros y botones de opciones.
<i>En cursiva</i>	Marcadores de posición de la información que proporciona. Por ejemplo, nombre de archivo o ruta significa que escriba la ruta real o el nombre del archivo.
Courier New	Comandos o ejemplos de códigos.
Hervínculo	Proporciona un acceso fácil y rápido a temas con referencias cruzadas o una ubicación web externa. Los hervínculos están resaltados en azul y pueden estar subrayados.
%ProgramFiles%	Directorio del sistema Windows que almacena los programas instalados.

Ayuda en línea es la fuente principal de contenido de ayuda. Siempre que tenga una conexión a Internet activa se mostrará automáticamente la versión más reciente de la Ayuda en línea.

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 Live](#): se ha descargado del sitio web o CD/DVD de ESET. El paquete de instalación es universal para todos los idiomas (elija el idioma correspondiente). El Instalador Live es un archivo pequeño; los archivos adicionales necesarios para la instalación de ESET NOD32 Antivirus se descargan automáticamente.
- [Instalación sin conexión](#): utiliza un archivo .exe más grande que el archivo del instalador Live y no necesita una conexión a Internet ni archivos adicionales para completar la instalación.

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.



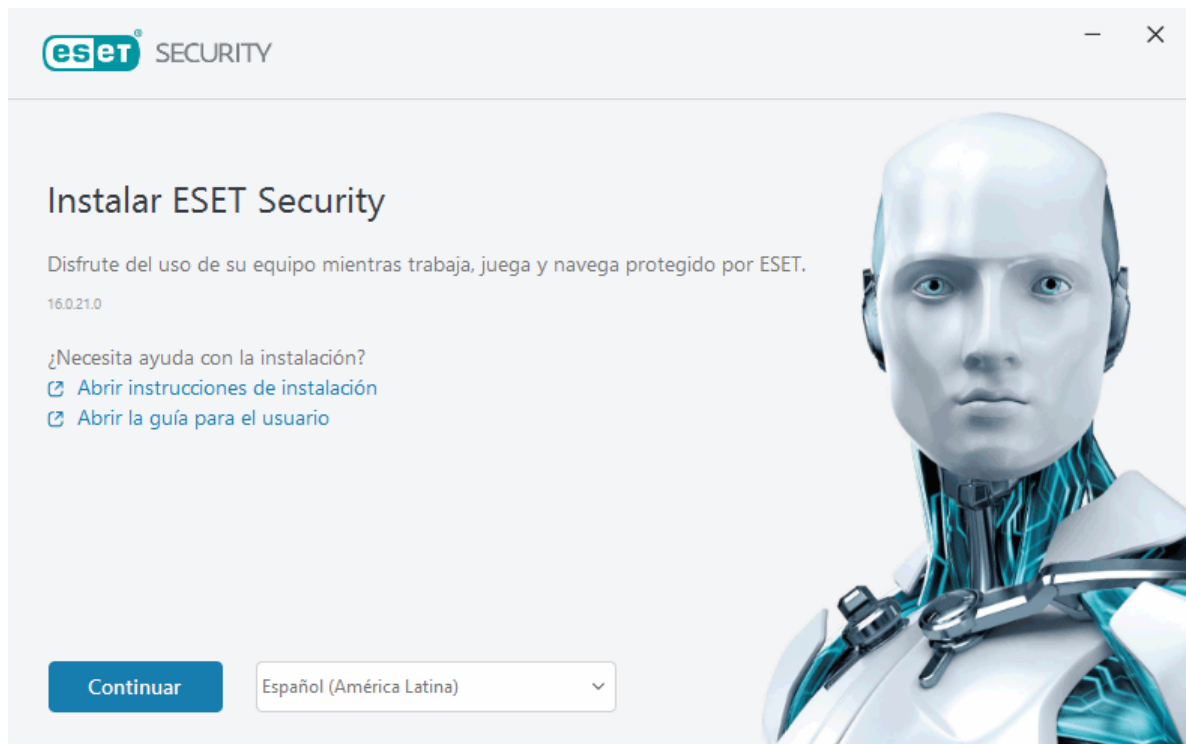
Es recomendable desinstalar cualquier otro programa antivirus que haya en el sistema. Consulte nuestro [artículo de la base de conocimiento de ESET](#) para obtener una lista de herramientas del desinstalador para el software antivirus común (disponible en inglés y otros idiomas más).

Instalador activo

Una vez que descargue el [Paquete de instalación del Instalador Live](#), haga doble clic en el archivo de instalación y siga las instrucciones detalladas en la ventana del instalador.



Para este tipo de instalación debe estar conectado a Internet.



1. Seleccione el idioma correspondiente en el menú desplegable y haga clic en **Continuar**.



Si está instalando una versión más reciente sobre la versión anterior con configuraciones protegidas con contraseña, escriba su contraseña. Puede configurar la contraseña de configuración en [Configuración del acceso](#).

2. Seleccione su preferencia para las siguientes características, lea el [Acuerdo de licencia para el usuario final](#) y la [Política de privacidad](#) y haga clic en **Continuar** o haga clic en **Permitir todo** y continúe para activar todas las características:

- [Sistema de comentarios de ESET LiveGrid®](#)
- [Aplicaciones potencialmente no deseadas](#)
- [Programa de mejora de la experiencia del cliente](#)



Al hacer clic en **Continuar** o **Permitir todo** y continuar, acepta el Acuerdo de licencia para el usuario final y la Política de privacidad.

3. Para activar, administrar y ver la seguridad del dispositivo desde ESET HOME, [conecte su dispositivo a la cuenta ESET HOME](#). Haga clic en **Omitir inicio de sesión** para continuar sin conectarse a ESET HOME. Puede [conectar su dispositivo a su cuenta de ESET HOME](#) más adelante.

4. Si sigue sin conectarse a ESET HOME, elija una opción de activación [***](#). Si está instalando una versión más reciente que la anterior, su clave de licencia se ingresará automáticamente.

5. El Asistente de instalación determina qué producto de ESET se instala según su licencia. La versión con más funciones de seguridad siempre está preseleccionada. Haga clic en **Cambiar producto** si desea [instalar una versión diferente del producto ESET](#). Haga clic en **Continuar** para iniciar el proceso de instalación. Podría demorar unos minutos.

i Si quedan restos (archivos o carpetas) de productos de ESET desinstalados en el pasado, se le pedirá que permita su eliminación. Haga clic en **Instalar** para continuar.

6. Haga clic en **Finalizar** para salir de la instalación.

! [Solucionador de problemas de instalación.](#)

i Después de instalar y activar el producto, los módulos comienzan a descargarse. La protección está iniciándose y es posible que algunas funciones no sean completamente funcionales a menos que la descarga esté completa.

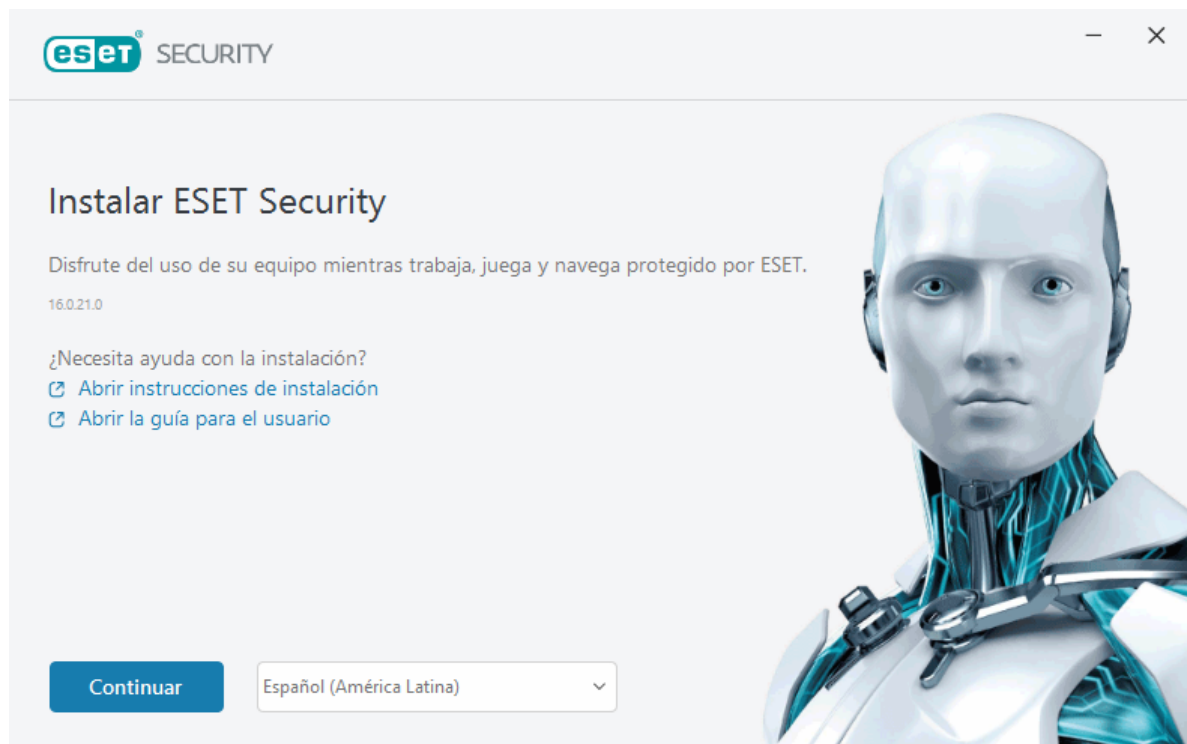
Instalación fuera de línea

Descargue e instale su producto de inicio para Windows de ESET utilizando el instalador sin conexión (.exe) que aparece a continuación. [Elija la versión del producto ESET Home que desea descargar](#) (32 bits, 64 bits o ARM).

ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Descargar versión para 64 bits	Descargar versión para 64 bits	Descargar versión para 64 bits
Descargar versión para 32 bits	Descargar versión para 32 bits	Descargar versión para 32 bits
Descargar ARM	Descargar ARM	Descargar ARM

! Si tiene una conexión activa a Internet, [instale el producto de ESET con el instalador Live.](#)

Una vez que haya iniciado el instalador sin conexión (.exe), el asistente de instalación lo guiará a través del proceso de configuración.



1. Seleccione el idioma correspondiente en el menú desplegable y haga clic en **Continuar**.

i Si está instalando una versión más reciente sobre la versión anterior con configuraciones protegidas con contraseña, escriba su contraseña. Puede configurar la contraseña de configuración en [Configuración del acceso](#).

2. Seleccione su preferencia para las siguientes características, lea el [Acuerdo de licencia para el usuario final](#) y la [Política de privacidad](#) y haga clic en **Continuar** o haga clic en **Permitir todo** y continúe para activar todas las características:

- [Sistema de comentarios de ESET LiveGrid®](#)
- [Aplicaciones potencialmente no deseadas](#)
- [Programa de mejora de la experiencia del cliente](#)

i Al hacer clic en **Continuar** o **Permitir todo** y continuar, acepta el Acuerdo de licencia para el usuario final y la Política de privacidad.

3. Haga clic en **Omitir inicio de sesión**. Cuando tenga conexión a Internet, puede [conectar su dispositivo a su cuenta ESET HOME](#).

4. Haga clic en **Omitir activación**. Para que la instalación funcione en su totalidad, ESET NOD32 Antivirus debe activarse después de la instalación. La [activación del producto](#) requiere una conexión activa a Internet.

5. El Asistente de instalación muestra qué producto ESET se instalará según el instalador sin conexión descargado. Haga clic en **Continuar** para iniciar el proceso de instalación. Podría demorar unos minutos.

i Si quedan restos (archivos o carpetas) de productos de ESET desinstalados en el pasado, se le pedirá que permita su eliminación. Haga clic en **Instalar** para continuar.

6. Haga clic en **Finalizar** para salir de la instalación.

 [Solucionador de problemas de instalación](#).

Activación del producto

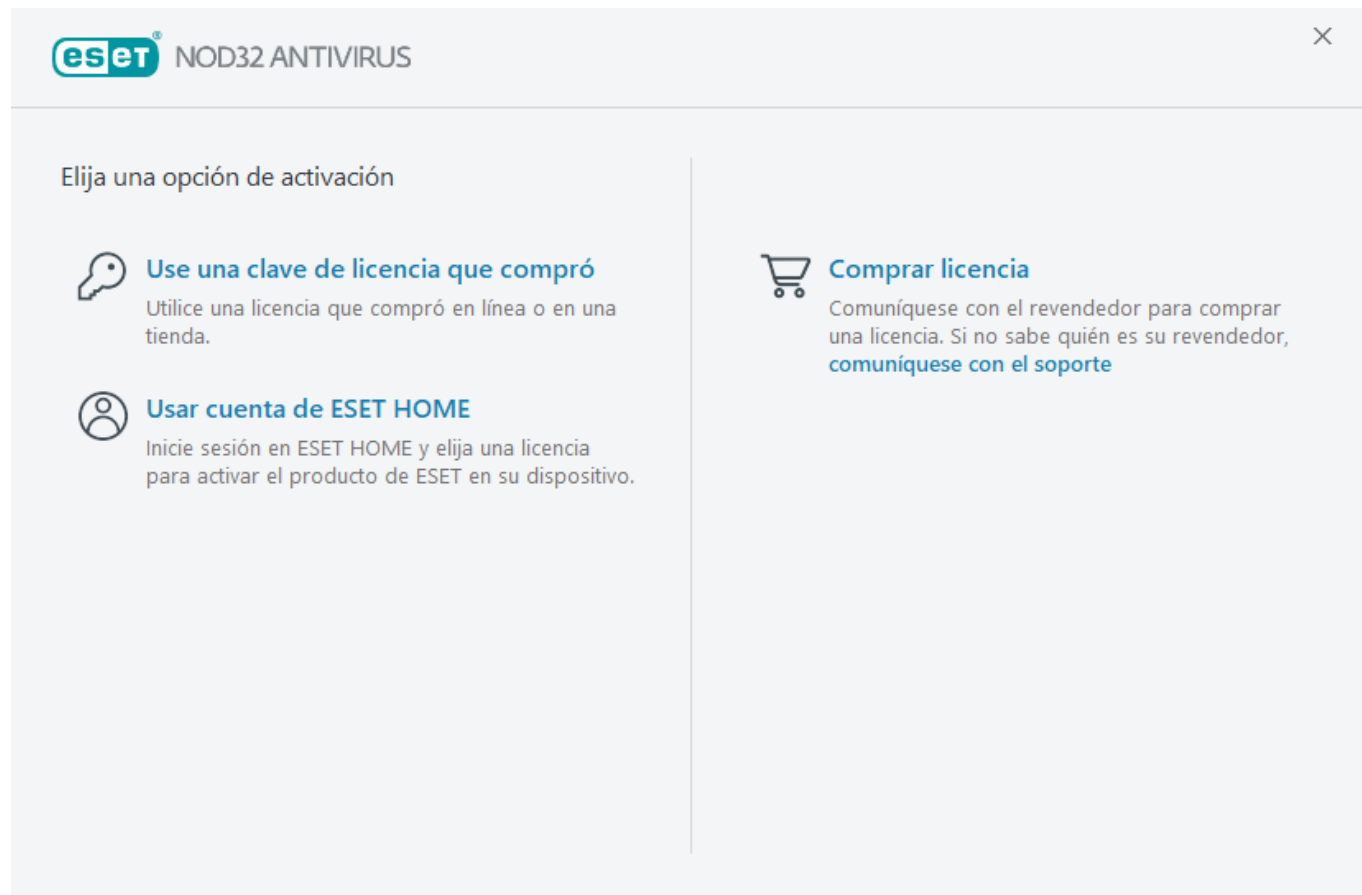
Hay varios métodos disponibles para activar su producto. La disponibilidad de un escenario de activación particular en la ventana de activación puede variar dependiendo del país y los medios de distribución (CD/DVD, página Web de ESET, etc.):

- Si compró una versión comercial del producto en caja o recibió un mensaje de correo electrónico con detalles de la licencia, active el producto haciendo clic en **Usar una clave de licencia comprada**. Por lo general, la clave de licencia aparece en el interior o al dorso del paquete del producto. Para que la activación se realice correctamente, deberá ingresar la clave de licencia tal como fue suministrada. Clave de licencia: una cadena única en el formato XXXX-XXXX-XXXX-XXXX-XXXX o XXXX-XXXXXXXXX que se utiliza para la identificación del propietario de la licencia y para la activación de la licencia.
- Tras seleccionar [Usar cuenta ESET HOME](#), se le pedirá que inicie sesión en su cuenta ESET HOME.
- Si desea evaluar ESET NOD32 Antivirus antes de realizar una compra, seleccione [Prueba gratuita](#). 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. Las [licencias completas](#) de productos hogareños de ESET Windows no son

gratuitas.

Podrá cambiar la licencia del producto en cualquier momento. Para realizar esto, haga clic en **Ayuda y soporte** > **Cambiar licencia** en la [ventana principal del programa](#). Verá la identificación de la licencia pública utilizada para identificar su licencia con el soporte de ESET.

 [¿Error en la activación del producto?](#)



Ingreso de su clave de licencia durante la activación

Las actualizaciones automáticas son importantes para su seguridad. ESET NOD32 Antivirus solo recibirá actualizaciones después de activarlas.

Al ingresar su **Clave de licencia**, es importante que la ingrese tal como está escrita:

- Clave de licencia: una cadena única en el formato XXXX-XXXX-XXXX-XXXX-XXXX que se usa para identificar al propietario de la licencia y para activarla.

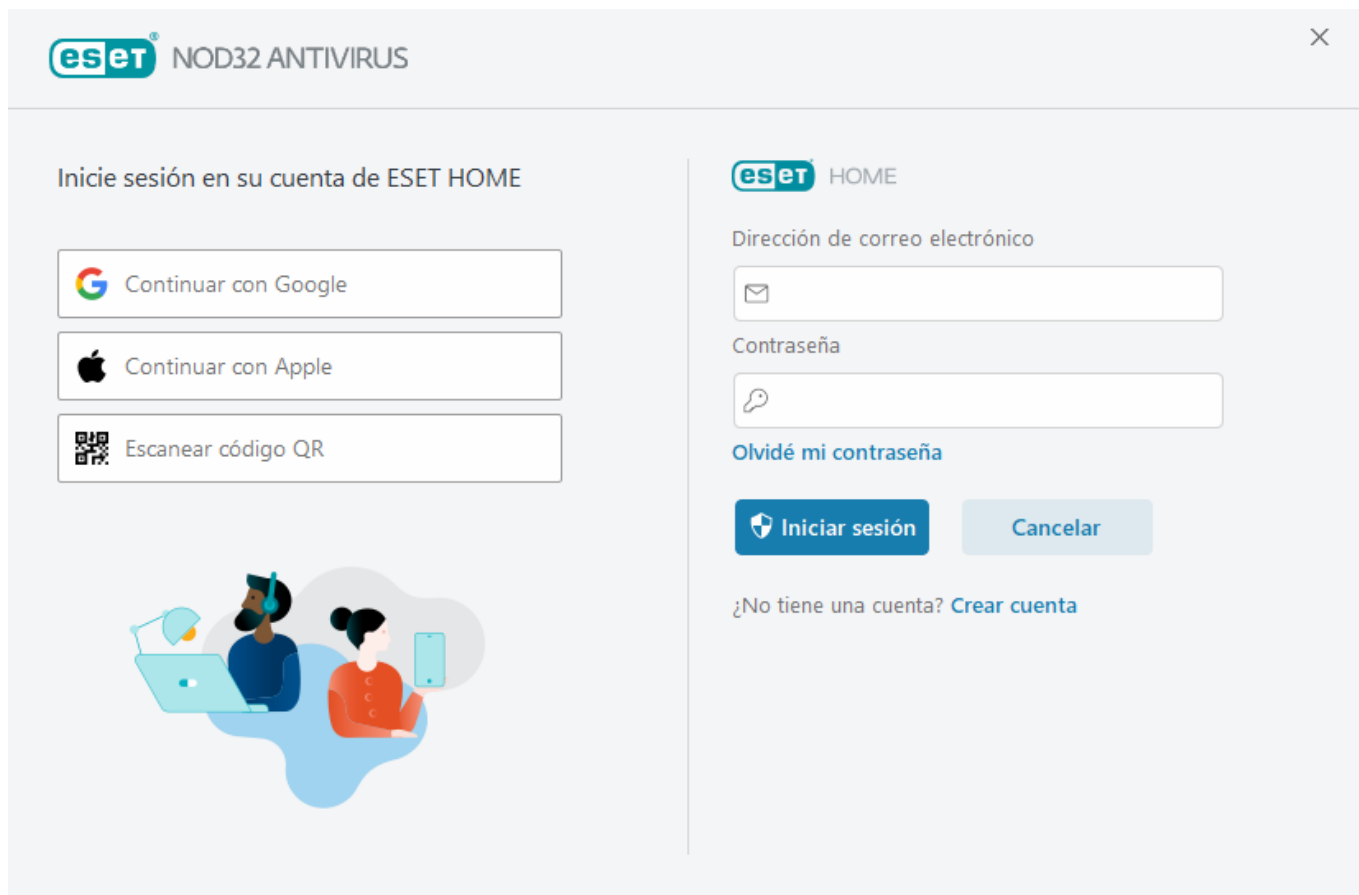
Le recomendamos copiar y pegar su Clave de licencia desde el correo electrónico de registro para asegurarse de no equivocarse.

Si no ingresó su Clave de licencia luego de la instalación, el producto no se activará. Puede activar ESET NOD32 Antivirus en la [ventana principal del programa](#) > **Ayuda y soporte** > **Activar licencia**.

Las [licencias completas](#) de productos hogareños de ESET Windows no son gratuitas.

Usar ESET HOME cuenta

Conecte su dispositivo a [ESET HOME](#) para ver y administrar todas las licencias y los dispositivos de ESET activados. Puede renovar, actualizar o ampliar la licencia y ver detalles importantes de ella. En el portal de administración o la aplicación para dispositivos móviles de ESET HOME, puede agregar diferentes licencias, descargar productos en sus dispositivos, comprobar el estado de seguridad del producto o compartir licencias por correo electrónico. Para obtener más información, visite [ayuda en línea de ESET HOME](#).



Tras seleccionar **Utilizar cuenta ESET HOME** como método de activación o al conectarse a la cuenta ESET HOME durante la instalación:

1. [Ingresa a su cuenta ESET HOME](#).

i Si no tiene una cuenta ESET HOME, haga clic en **Crear cuenta** para registrarse o consulte las instrucciones de la Ayuda en línea de [ESET HOME](#).
Si olvidó su contraseña, haga clic en **Olvidé mi contraseña** y siga los pasos de la pantalla o consulte las instrucciones de la [Ayuda en línea de ESET HOME](#).

2. Configure un **Nombre del dispositivo** para su dispositivo que se utilizará en todos los servicios ESET HOME y haga clic en **Continuar**.
3. Elija una licencia de activación o [agregue una nueva licencia](#). Haga clic en **Continuar** para activar ESET NOD32 Antivirus.

Activación de la licencia de prueba

Para activar su versión de prueba de ESET NOD32 Antivirus, ingrese una dirección de correo electrónico válida en los campos **Dirección de correo electrónico** y **Confirmar dirección de correo electrónico**. Tras la activación, se generará su licencia de ESET y se enviará a su correo electrónico. Esta dirección de correo electrónico también se usará para las notificaciones sobre el vencimiento del producto y otras comunicaciones con ESET. La versión de prueba solo puede activarse una vez.

Seleccione su país del menú desplegable **País** para registrar ESET NOD32 Antivirus con su distribuidor local, que le proporcionará soporte técnico.

Clave de licencia de ESET gratuita

La licencia completa para ESET NOD32 Antivirus no es gratuita.

La clave de licencia de ESET es una secuencia única de letras y números separados por guion que proporciona ESET para permitir el uso legal de ESET NOD32 Antivirus de conformidad con el [Acuerdo de licencia de usuario final](#). Todos los Usuarios finales tienen derecho a usar la clave de licencia solo en la medida en que tengan derecho a usar ESET NOD32 Antivirus según la cantidad de licencias otorgadas por ESET. La clave de licencia se considera confidencial y no se puede compartir. Sin embargo, puede [compartir los puestos de licencia mediante ESET HOME](#).

Existen fuentes en Internet que pueden proporcionar una clave de licencia de ESET "gratuita", pero recuerde:

- Hacer clic en un anuncio de "Licencia de ESET gratuita" puede comprometer su equipo o dispositivo e infectarlo con malware. El malware puede ocultarse en contenido web no oficial (p. ej., videos), sitios web que muestran anuncios para ganar dinero en base a sus visitas, etc. En general, estos son una trampa.
- ESET puede deshabilitar y deshabilita las licencias pirateadas.
- Tener una clave de licencia pirateada no cumple con el [Acuerdo de licencia de usuario final](#) que debe aceptar para instalar ESET NOD32 Antivirus.
- Compre licencias ESET solo a través de canales oficiales como www.eset.com, distribuidores de ESET (no compre licencias en sitios web de terceros no oficiales como eBay ni licencias compartidas de terceros).
- La [descarga](#) de un producto ESET NOD32 Antivirus es gratuita, pero la activación durante la instalación requiere una clave de licencia de ESET válida (puede descargarlo e instalarlo, pero sin activación, no funcionará).
- No comparta su licencia en Internet ni en las redes sociales (puede hacerse popular).

Para identificar e informar una licencia de ESET pirata, [visite nuestro artículo de la base de conocimiento](#) para obtener instrucciones.

Si no está seguro acerca de comprar un producto de seguridad de ESET, puede usar una versión de prueba mientras lo decide:

1. [Activar ESET NOD32 Antivirus con una licencia de prueba gratuita](#)

2. [Participar en el Programa ESET Beta](#)

3. [Instalar ESET Mobile Security](#) si está usado un dispositivo móvil Android, es freemium.

Para obtener un descuento/extender su licencia, [Renueve ESET](#).

Falló la activación - situaciones comunes

Si la activación de ESET NOD32 Antivirus no se realiza correctamente, las situaciones más habituales son:

- La clave de licencia ya está en uso.
- Ha introducido una clave de licencia no válida.
- Falta información en el formulario de activación o no es válida.
- Error al comunicarse con el servidor de activación.
- Sin conexión con los servidores de activación de ESET o con conexión deshabilitada.

Compruebe que ha introducido la clave de licencia correcta y que su conexión a Internet está activa. Intente activar ESET NOD32 Antivirus de nuevo. Si utiliza una cuenta ESET HOME para la activación, consulte la [Administración de licencias ESET HOME: ayuda en línea](#).

i Si recibe un error específico (por ejemplo, Licencia suspendida o Licencia sobreusada), siga las instrucciones del [estado de licencia](#).

Si sigue sin poder activarlo ESET NOD32 Antivirus, el [Solucionador de problemas de activación de ESET](#) lo guía por las preguntas habituales, errores y problemas de activación y licencia (disponible en inglés y en otros idiomas).

Estado de licencia

Su licencia puede tener estados distintos. Puede encontrar el estado de su licencia en [ESET HOME](#). Para agregar su licencia a su cuenta ESET HOME, consulte [Agregar una licencia](#).

i Si no tiene la cuenta ESET HOME, puede [crear una nueva cuenta ESET HOME](#).

Si el estado de la licencia no es **Activo**, recibirá un error durante la activación o una notificación en la [ventana principal del programa](#).

Para desactivar las notificaciones de estado de la licencia, abra **Configuración avanzada (F5) > Notificaciones > Estados de la aplicación**. Haga clic en **Editar** junto a **Estados de la aplicación**, expanda **Licencias** y anule la selección de la casilla de verificación situada junto a la notificación que desee deshabilitar. Deshabilitar la notificación no soluciona el problema.

Consulte en la siguiente tabla las descripciones y soluciones recomendadas para diferentes estados de licencia:

Estado de licencia	Descripción	Solución
Activo	La licencia es válida y no es necesario que intervenga. ESET NOD32 Antivirus puede activarse y puede encontrar los detalles de la licencia en la ventana principal del programa > Ayuda y soporte .	
Sobreusada	Más dispositivos de los permitidos están usando esta licencia. Recibirá un error de activación.	Consulte Error de activación debido a una licencia sobreusada para obtener más información.
Suspendida	Su licencia se suspendió debido a problemas de pago. Para usar la licencia, asegúrese de que sus datos de pago en ESET HOME estén actualizados o póngase en contacto con el distribuidor de la licencia. Puede recibir este error durante la activación o en la ventana principal del programa .	<p>Producto instalado—si tiene la cuenta ESET HOME, en la notificación que se muestra en la ventana principal del programa, haga clic en Administrar su licencia en ESET HOME y revise sus datos de pago. De lo contrario, póngase en contacto con el distribuidor de la licencia.</p> <p>Error de activación—si tiene la cuenta ESET HOME, en la ventana de error de activación, haga clic en Abrir ESET HOME y revise sus datos de pago. De lo contrario, póngase en contacto con el distribuidor de la licencia.</p>
Expiró	Su licencia ha vencido y no puede usar esta licencia para activar ESET NOD32 Antivirus. Puede recibir este error durante la activación o en la ventana principal del programa . Si ya tiene instalado ESET NOD32 Antivirus, el equipo no está protegido.	<p>Producto instalado—en la notificación que se muestra en la ventana principal del programa, haga clic en Renovar licencia y siga las instrucciones de ¿Cómo renuevo mi licencia?, o haga clic en Activar producto y elija su método de activación.</p> <p>Error de activación—en la ventana de error de activación, haga clic en Renovar licencia y siga las instrucciones de ¿Cómo renuevo mi licencia?, o escriba una clave de licencia nueva o renovada y haga clic en Renovar licencia.</p>

Error de activación debido a una licencia sobreusada

Problema

- Es posible que su licencia esté sobreusada o abusada.
- Error de activación debido a una licencia sobreusada

Solución

Hay más dispositivos de los permitidos por esta licencia. Puede ser víctima de una falsificación o piratería de software. No se puede utilizar la licencia para activar otros productos de ESET. Puede resolver este problema directamente si puede administrar la licencia de su cuenta de ESET HOME o si compró una licencia de una fuente legítima. Si aún no tiene una cuenta, cree una.

Si es el dueño de una licencia y no se le pidió que ingrese su dirección de correo electrónico:

1. Para administrar su licencia de ESET, abra un navegador web y vaya a <https://home.eset.com>. Acceda a ESET License Manager y quite o desactive puestos. Si desea obtener más información, consulte [Qué hacer en caso de licencia sobreusada](#).
2. Para identificar e informar una licencia de ESET pirata, [visite nuestro artículo Identificar e informar licencias ESET pirateadas](#) para obtener instrucciones.
3. Si no está seguro, haga clic en **Atrás** y envíe un mensaje de [correo electrónico al servicio de asistencia técnica de ESET](#).

Si usted no es propietario de una licencia, comuníquese con el propietario de esta licencia para brindarle información acerca de la imposibilidad de activar el producto ESET debido a una sobreutilización de la licencia. El propietario puede resolver el problema en el portal [ESET HOME](#).

Si se le pide que confirme su dirección de correo electrónico (solo en los casos graves), ingrese la dirección de correo electrónico que originalmente usó para comprar o activar su ESET NOD32 Antivirus.

Actualización de la licencia

Esta ventana de notificación aparece cuando ha cambiado la licencia usada para activar su producto ESET. Su licencia modificada le permite activar un producto con más características de seguridad. Si no se realizó ningún cambio, ESET NOD32 Antivirus le mostrará, una vez, una ventana de alerta llamada **Cambiar a un producto con más funciones**.

Sí (recomendado): instalará automáticamente el producto con más funciones de seguridad.

No, gracias: no se realizarán cambios y la notificación desaparecerá permanentemente.

Para cambiar el producto más tarde, consulte nuestro [artículo de la base de conocimiento de ESET](#). Para obtener más información sobre las licencias de ESET, consulte las [Preguntas frecuentes sobre licencias](#).

La tabla a continuación detalla las funciones disponibles para cada producto específico.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Motor de detección	✓	✓	✓
Aprendizaje automático avanzado	✓	✓	✓
Bloqueador de exploits	✓	✓	✓
Protección contra ataque basado en script	✓	✓	✓
Anti-Phishing	✓	✓	✓
Protección del acceso a la Web	✓	✓	✓
HIPS (incluida la Protección contra ransomware)	✓	✓	✓
Antispam		✓	✓
Firewall		✓	✓
Inspector de red		✓	✓
Protección de la cámara web		✓	✓

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Protección contra ataques de red		✓	✓
Protección contra Botnet		✓	✓
Protección de banca y pagos en línea		✓	✓
Control parental		✓	✓
Anti-Theft		✓	✓
Password Manager			✓
ESET Secure Data			✓
ESET LiveGuard			✓

Actualización del producto

Ha descargado un instalador predeterminado y decidió cambiar el producto que se activará o desea cambiar el producto instalado a uno con más funciones de seguridad.

[Cambie el producto durante la instalación.](#)

La tabla a continuación detalla las funciones disponibles para cada producto específico.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Motor de detección	✓	✓	✓
Aprendizaje automático avanzado	✓	✓	✓
Bloqueador de exploits	✓	✓	✓
Protección contra ataque basado en script	✓	✓	✓
Anti-Phishing	✓	✓	✓
Protección del acceso a la Web	✓	✓	✓
HIPS (incluida la Protección contra ransomware)	✓	✓	✓
Antispam		✓	✓
Firewall		✓	✓
Inspector de red		✓	✓
Protección de la cámara web		✓	✓
Protección contra ataques de red		✓	✓
Protección contra Botnet		✓	✓
Protección de banca y pagos en línea		✓	✓
Control parental		✓	✓
Anti-Theft		✓	✓
Password Manager			✓
ESET Secure Data			✓
ESET LiveGuard			✓

Cambio de la licencia a una categoría inferior

Esta ventana de diálogo aparece cuando ha cambiado la licencia utilizada para activar su producto ESET. Solo puede utilizarse su licencia modificada con un producto ESET diferente con menos características de seguridad. El producto se ha modificado automáticamente para evitar la pérdida de protección.

Para obtener más información sobre las licencias de ESET, consulte las [Preguntas frecuentes sobre licencias](#).

La tabla a continuación detalla las funciones disponibles para cada producto específico.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Motor de detección	✓	✓	✓
Aprendizaje automático avanzado	✓	✓	✓
Bloqueador de exploits	✓	✓	✓
Protección contra ataque basado en script	✓	✓	✓
Anti-Phishing	✓	✓	✓
Protección del acceso a la Web	✓	✓	✓
HIPS (incluida la Protección contra ransomware)	✓	✓	✓
Antispam		✓	✓
Firewall		✓	✓
Inspector de red		✓	✓
Protección de la cámara web		✓	✓
Protección contra ataques de red		✓	✓
Protección contra Botnet		✓	✓
Protección de banca y pagos en línea		✓	✓
Control parental		✓	✓
Anti-Theft		✓	✓
Password Manager			✓
ESET Secure Data			✓
ESET LiveGuard			✓

Cambio del producto a una categoría inferior

El producto que tiene instalado actualmente tiene más funciones de seguridad que el que está a punto de activar.

La tabla a continuación detalla las funciones disponibles para cada producto específico.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Motor de detección	✓	✓	✓
Aprendizaje automático avanzado	✓	✓	✓
Bloqueador de exploits	✓	✓	✓

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Protección contra ataque basado en script	✓	✓	✓
Anti-Phishing	✓	✓	✓
Protección del acceso a la Web	✓	✓	✓
HIPS (incluida la Protección contra ransomware)	✓	✓	✓
Antispam		✓	✓
Firewall		✓	✓
Inspector de red		✓	✓
Protección de la cámara web		✓	✓
Protección contra ataques de red		✓	✓
Protección contra Botnet		✓	✓
Protección de banca y pagos en línea		✓	✓
Control parental		✓	✓
Anti-Theft		✓	✓
Password Manager			✓
ESET Secure Data			✓
ESET LiveGuard			✓

Solucionador de problemas de instalación

Si se producen problemas durante la instalación, el Asistente de instalación proporciona un solucionador de problemas que resuelve el problema, si es posible.

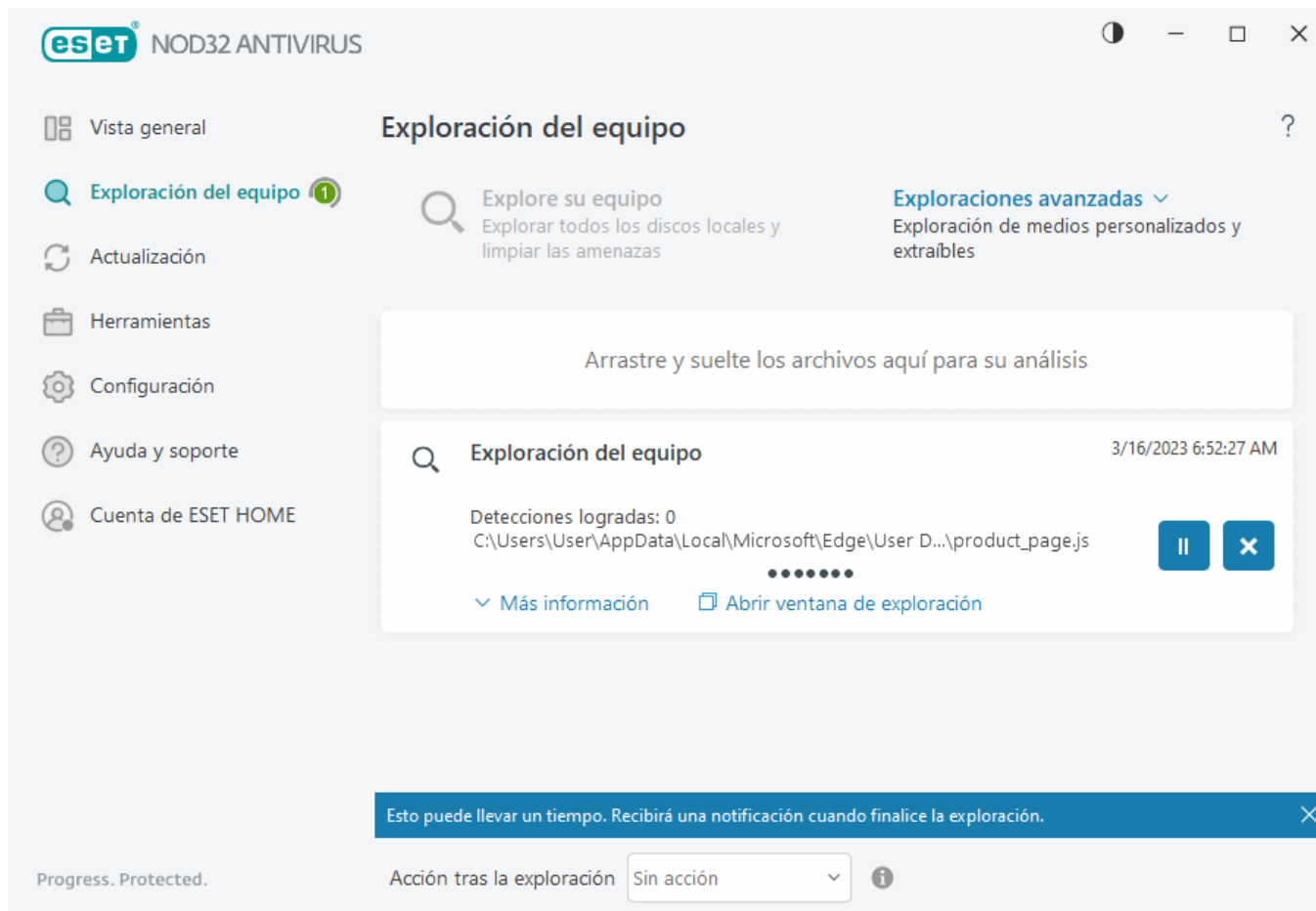
Haga clic en **Ejecutar solucionador de problemas** para iniciar el solucionador. Cuando termine, siga la solución recomendada.

Si el problema persiste, consulte la lista de [errores de instalación comunes y soluciones](#).

Primera exploración después de la instalación

Luego de instalar ESET NOD32 Antivirus, se iniciará una exploración del equipo automáticamente luego de la primera actualización exitosa para verificar códigos malintencionados.

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



Reemplazo a una versión más reciente

Las versiones nuevas de ESET NOD32 Antivirus se emiten para implementar mejoras o resolver problemas que no se pueden solucionar mediante la actualización automática de los módulos del programa. Actualizar 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 actualizar el programa por una versión posterior inmediatamente después de su lanzamiento, use uno de los siguientes métodos. Asegúrese de tener habilitada la opción **Actualizaciones de características de la aplicación** en **Configuración avanzada (F5) > Actualización > Perfiles > Actualizaciones**.
2. Manualmente, en la [ventana principal del programa](#) al hacer clic en **Buscar actualizaciones** en la sección **Actualizar**.
3. En forma manual, mediante la descarga e [instalación de la versión más reciente](#) sobre la instalación previa.

Para obtener información adicional e instrucciones ilustradas, consulte:

- [Actualizar productos ESET: verificar los módulos de productos más recientes](#)
- [¿Cuáles son los diferentes tipos de versiones y actualizaciones de productos ESET?](#)

Actualización automática de versión antigua del producto

Su versión del producto ESET ya no es compatible y se ha actualizado hacia la más reciente.

[Problemas comunes de instalación](#)

i Cada nueva versión de los productos ESET presenta una gran cantidad de reparación de errores y mejoras. Los clientes existentes con una licencia válida de un producto ESET pueden actualizar a la versión más reciente del mismo producto gratis.

Para completar la instalación:

1. Haga clic en **Aceptar y continuar** para aceptar el [Acuerdo de licencia de usuario final](#) y la [Política de privacidad](#). Si no acepta el Acuerdo de licencia de usuario final, haga clic en **Desinstalar**. No puede volver a la versión anterior.
2. Haga clic en **Permitir todo y continuar** para permitir [el Sistema de respuesta ESET LiveGrid®](#) y el [Programa de mejora de la experiencia del cliente](#), o bien, haga clic en **Continuar** si no quiere participar.
3. Tras activar el nuevo producto ESET con su clave de licencia, se mostrará la página Vista general. Si no se encuentra información de la licencia, continúe con una nueva licencia de prueba. Si la licencia que se usaba en el producto anterior no es válida, [active su producto ESET](#).
4. Es necesario reiniciar el dispositivo para completar la instalación.

Recomiende el producto de ESET a un amigo

Esta versión de ESET NOD32 Antivirus ahora ofrece bonos de recomendación, por lo tanto, puede compartir la experiencia de su producto de ESET con su familia y amigos. Incluso puede compartir las recomendaciones de un producto activado con una licencia de prueba. Cuando es usuario de prueba, por cada recomendación correcta que envíe y que resulte en una activación del producto, tanto usted como su amigo recibirán un mes adicional de protección completa.

Puede recomendar mediante el uso de su ESET NOD32 Antivirus instalado. El producto que puede recomendar depende del producto desde el que recomienda, consulte la tabla a continuación.

Su producto instalado	Producto que puede recomendar
ESET NOD32 Antivirus	ESET Internet Security
ESET Internet Security	ESET Internet Security
ESET Smart Security Premium	ESET Smart Security Premium

Recomiende un producto

Para enviar un enlace de recomendación, haga clic en **Recomendar a su amigo** en el menú principal de ESET NOD32 Antivirus. Haga clic en **Compartir enlace de recomendación**. Su producto generará un enlace de recomendación que se mostrará en una nueva ventana. Copie el enlace y envíelo a su familia y amigos. Existen

varias maneras de compartir su enlace de recomendación: directamente de su producto de ESET usando **compartir en Facebook**, **recomendar a contactos de Gmail** y **compartir en Twitter**.

Cuando sus amigos hagan clic en el enlace de recomendación que les envió, éste los dirigirá a una página web donde pueden descargar el producto y usarlo por otro mes de protección GRATUITA. Como usuario de prueba, usted recibirá una notificación por cada enlace de recomendación que se active correctamente y su licencia se extenderá automáticamente durante un mes más de protección GRATUITA. De esta manera, puede extender la protección GRATUITA hasta por 5 meses. Puede verificar el número de los enlaces de recomendación activados correctamente en la ventana **Recomendar a un amigo** de su producto de ESET.

i Es posible que la función de recomendación no esté disponible en su idioma/región.

Se instalará ESET NOD32 Antivirus

Este cuadro de diálogo puede mostrarse:

- Durante el proceso de instalación: haga clic en **Continuar** para instalar ESET NOD32 Antivirus.
- Al cambiar una licencia de ESET NOD32 Antivirus: haga clic en **Activar** para cambiar la licencia y activar ESET NOD32 Antivirus.

La opción **Cambiar producto** le permite cambiar entre los productos hogareños de ESET Windows según su licencia de ESET. Consulte [¿Qué producto tengo?](#) para obtener más información.

Cambiar a una línea diferente de productos

Según su licencia de ESET, puede cambiar entre varios productos hogareños de ESET Windows. Consulte [¿Qué producto tengo?](#) para obtener más información.

Registro

Registre su licencia al completar los campos que se incluyen en el formulario de registro y haga clic en Activar. Los campos marcados como requeridos son obligatorios. Esta información solo se usará en cuestiones relacionadas con su licencia de ESET.

Progreso de la activación

Espere unos segundos hasta que finalice el proceso de activación (el tiempo necesario puede variar en función de la velocidad de su conexión a Internet o su equipo).

La activación se completó correctamente.

Se completó el proceso de activación.

En unos segundos, se iniciará una actualización del módulo. Las actualizaciones periódicas de ESET NOD32 Antivirus se iniciarán inmediatamente.

La exploración inicial comenzará automáticamente en el plazo de 20 minutos después de la actualización del módulo.

Guía para principiantes

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

La ventana principal del programa

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

Instrucciones ilustradas

i Consulte [Abrir la ventana principal del programa de los productos de ESET para Windows](#) para obtener instrucciones ilustradas disponibles en inglés y en otros idiomas.

Puede seleccionar el esquema de colores de la interfaz gráfica de usuario de ESET NOD32 Antivirus en la esquina superior derecha de la ventana principal del programa. Haga clic en el ícono de **Esquema de colores** (el ícono cambia en función del esquema de colores seleccionado actualmente) junto al ícono **Minimizar** y seleccione el esquema de colores en el menú desplegable:

- **Igual que el color del sistema**— define el esquema de colores de ESET NOD32 Antivirus según la configuración del sistema operativo.
- **Oscuro**—ESET NOD32 Antivirus tendrá un esquema de colores oscuros (modo oscuro).
- **Claro**—ESET NOD32 Antivirus tendrá un esquema de colores estándar y claro.

Opciones del menú principal:

[Vista general](#): proporciona información sobre el estado de protección de ESET NOD32 Antivirus.

[Exploración del equipo](#): configura y ejecuta una exploración de tu ordenador o crea una exploración personalizada.


[Actualización](#) – muestra información sobre las actualizaciones del módulo y del motor de detección.

[Herramientas](#): proporciona acceso a características que ayudan a simplificar la administración del programa y ofrece opciones adicionales para usuarios avanzados.

[Configuración](#) – ofrece opciones de configuración para las características de protección de ESET NOD32 Antivirus (Protección del equipo y Protección de Internet) y acceso a Configuración avanzada.

[Ayuda y soporte técnico](#) – muestra información sobre su licencia, el producto de ESET instalado y vínculos a la [ayuda en línea](#), la [base de conocimiento de ESET](#) y el [soporte técnico](#).

[Cuenta ESET HOME](#) – [conecte su dispositivo a ESET HOME](#) o revise el estado de conexión de la cuenta ESET HOME. Use [ESET HOME](#) para ver y administrar su las licencias y los dispositivos de ESET activados.

 Para cambiar el esquema de colores de la interfaz gráfica de usuario de ESET NOD32 Antivirus, consulte [Elementos de la interfaz del usuario](#).

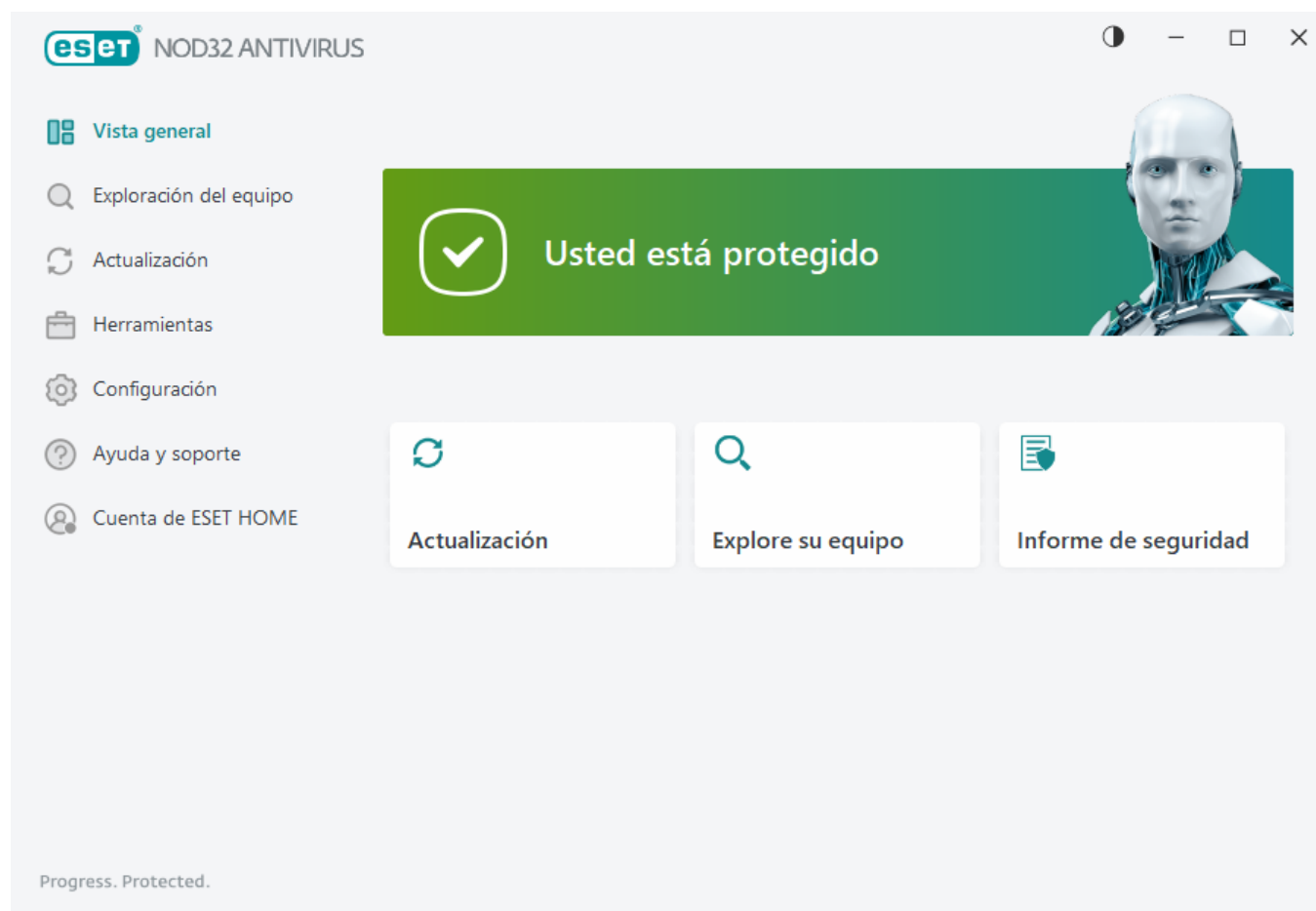
En la ventana **Vista general** se muestra información sobre la protección actual del equipo junto con vínculos rápidos a las características de seguridad de ESET NOD32 Antivirus.

En la ventana **Vista general** se muestran [notificaciones](#) con información detallada y soluciones recomendadas para mejorar la seguridad de ESET NOD32 Antivirus, activar funciones adicionales o garantizar la máxima protección. Si hay más notificaciones, haga clic en **X más notificaciones** para ampliar todas.

Actualización — Abre la página [Actualización](#) y comprueba si hay actualizaciones.

Exploración del equipo — Abre la página [Exploración del equipo](#) e inicia una [exploración estándar del equipo](#).

Informe de seguridad — Abre el [Informe de seguridad](#).

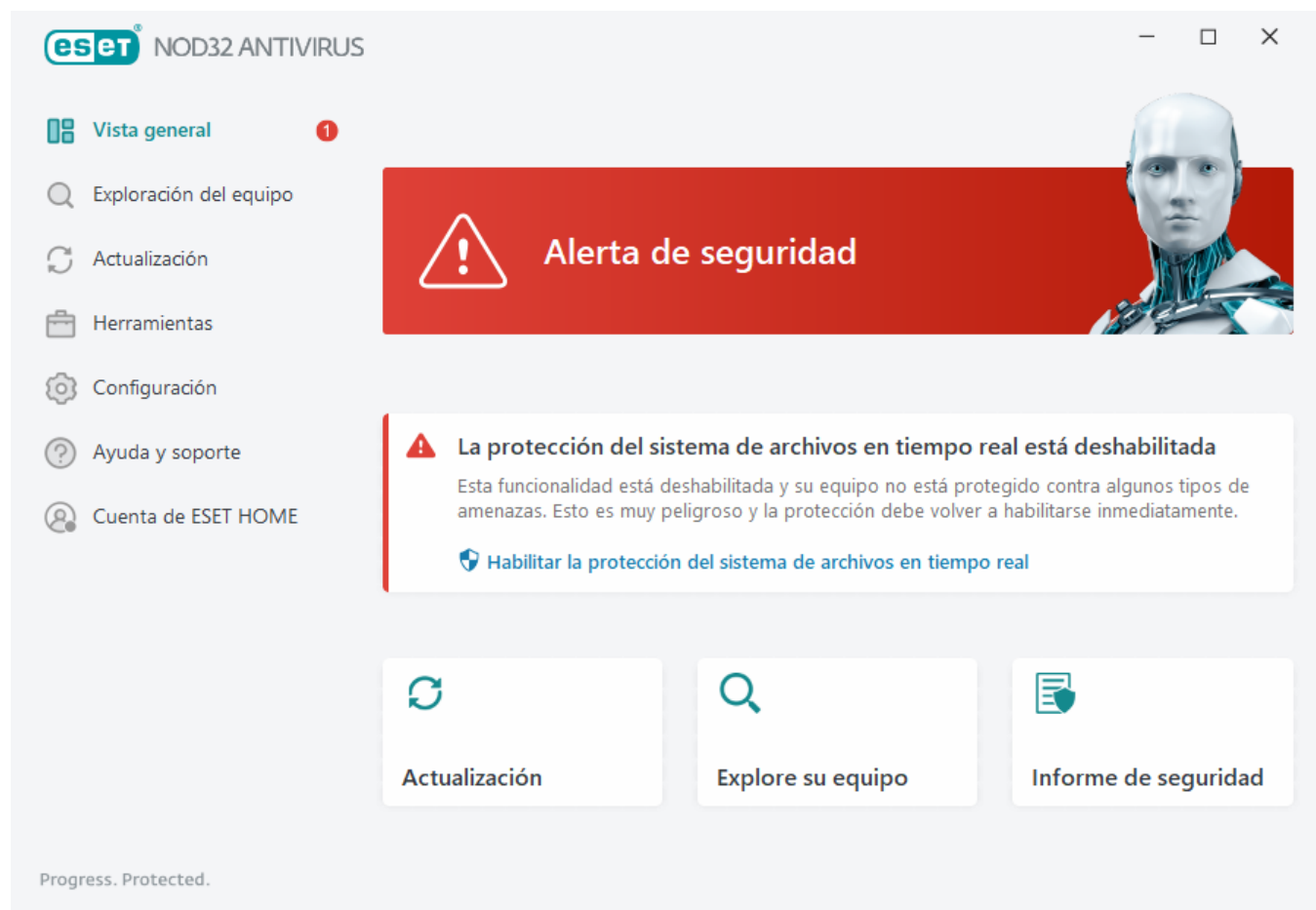


El ícono verde y el estado verde **Está protegido** indican que la máxima protección está asegurada.

¿Qué hacer si el programa no funciona correctamente?

Si un módulo de protección activo trabaja correctamente, el icono de estado de protección se volverá verde. Un signo de exclamación rojo o un icono de notificación naranja indican que no se asegura el máximo nivel de protección. Se muestra información adicional sobre el estado de protección de cada módulo y las soluciones

sugeridas para restaurar la protección total como una [notificación](#) en la ventana **Descripción general**. Para cambiar el estado de un módulo individual, haga clic en **Configuración** y seleccione el módulo deseado.



El ícono rojo y el estado rojo **Alerta de seguridad** indican que existen problemas críticos. Existen varios motivos por los cuales se puede mostrar este estado, por ejemplo:

- **El producto no está activado o La licencia está vencida** – Se indica mediante un icono rojo de estado de protección. Una vez que se vence la licencia, el programa no se podrá actualizar. Siga las instrucciones en la ventana de alerta para renovar la licencia.
- **El motor de detección está desactualizado** – este error aparecerá luego de varios intentos insatisfactorios de actualizar el motor de detección. 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](#).
- **Se deshabilitó la protección del sistema de archivos en tiempo real**: el usuario deshabilitó la protección en tiempo real. Su computadora no está protegida contra amenazas. Haga clic en **Habilitar protección del sistema de archivos en tiempo real** para volver a habilitar esta funcionalidad.
- **Protección antivirus y antispyware deshabilitada**: puede volver a activar la protección antivirus y antispyware con un clic en **Habilitar todos los módulos de protección antivirus y antispyware**.



El icono naranja indica una protección limitada. Por ejemplo, puede haber un problema con la actualización del programa o en poco tiempo se cumpliría la fecha de vencimiento de la licencia. Existen varios motivos por los cuales se puede mostrar este estado, por ejemplo:

- **Modo de juego activo**: habilitar el [Modo de juego](#) es un riesgo potencial de la seguridad. Si se activa

esta característica, se desactivan todas las ventanas de alerta y notificaciones, y se detienen las tareas programadas.

- **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.

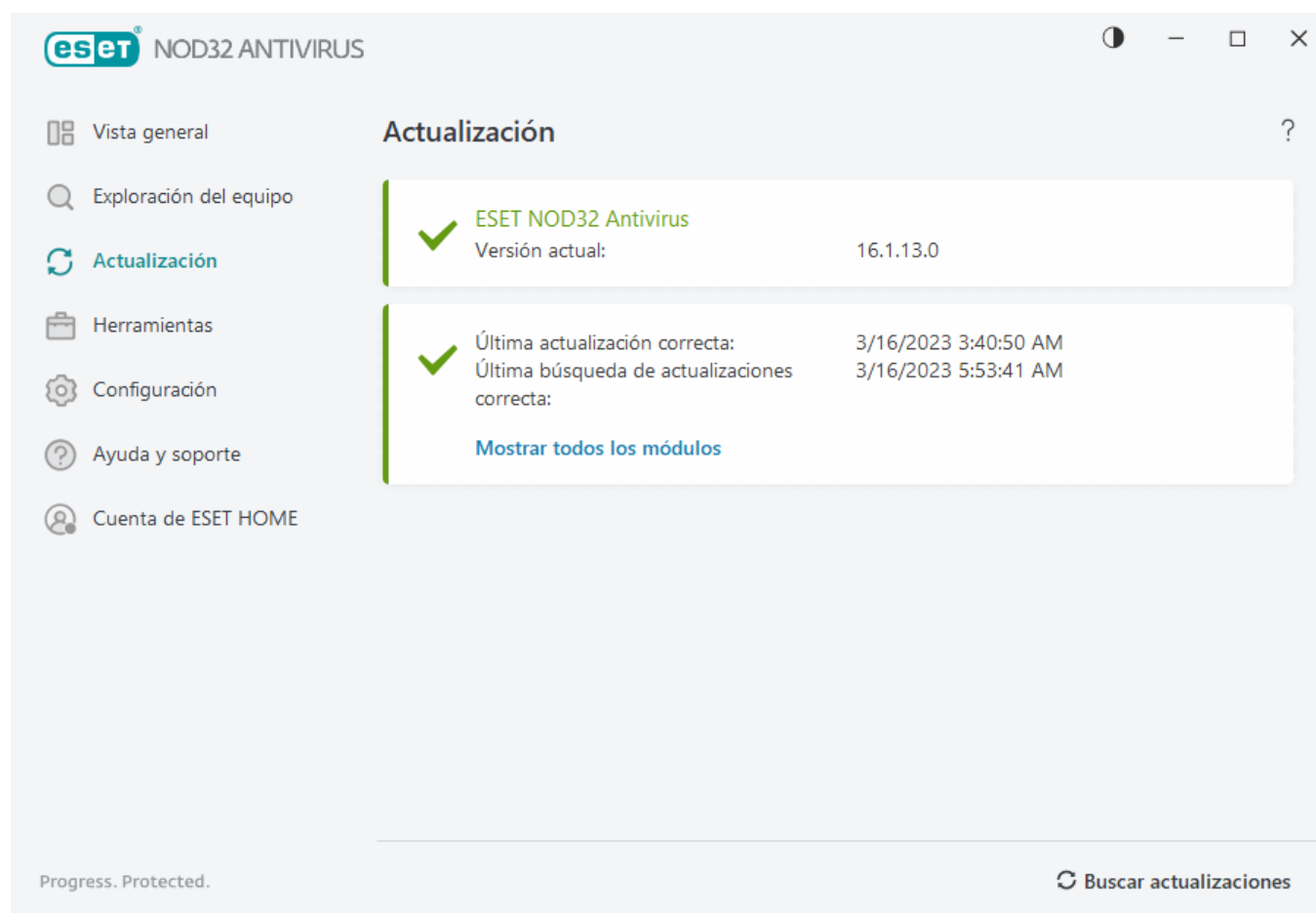
Si no puede solucionar el problema mediante las sugerencias, haga clic en **Ayuda y soporte** para acceder a los archivos de ayuda o buscar en la [base de conocimiento de ESET](#). Si aún necesita asistencia, puede enviar una petición de soporte. El Soporte técnico de ESET responderá rápidamente a sus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

Actualizaciones

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 se asegura de que los módulos del programa y los componentes del sistema estén siempre actualizados.

Al hacer clic en **Actualización** en la [ventana principal del programa](#), verá el estado actual de la actualización, incluyendo la fecha y la hora de la última actualización correcta y si es necesario actualizar.

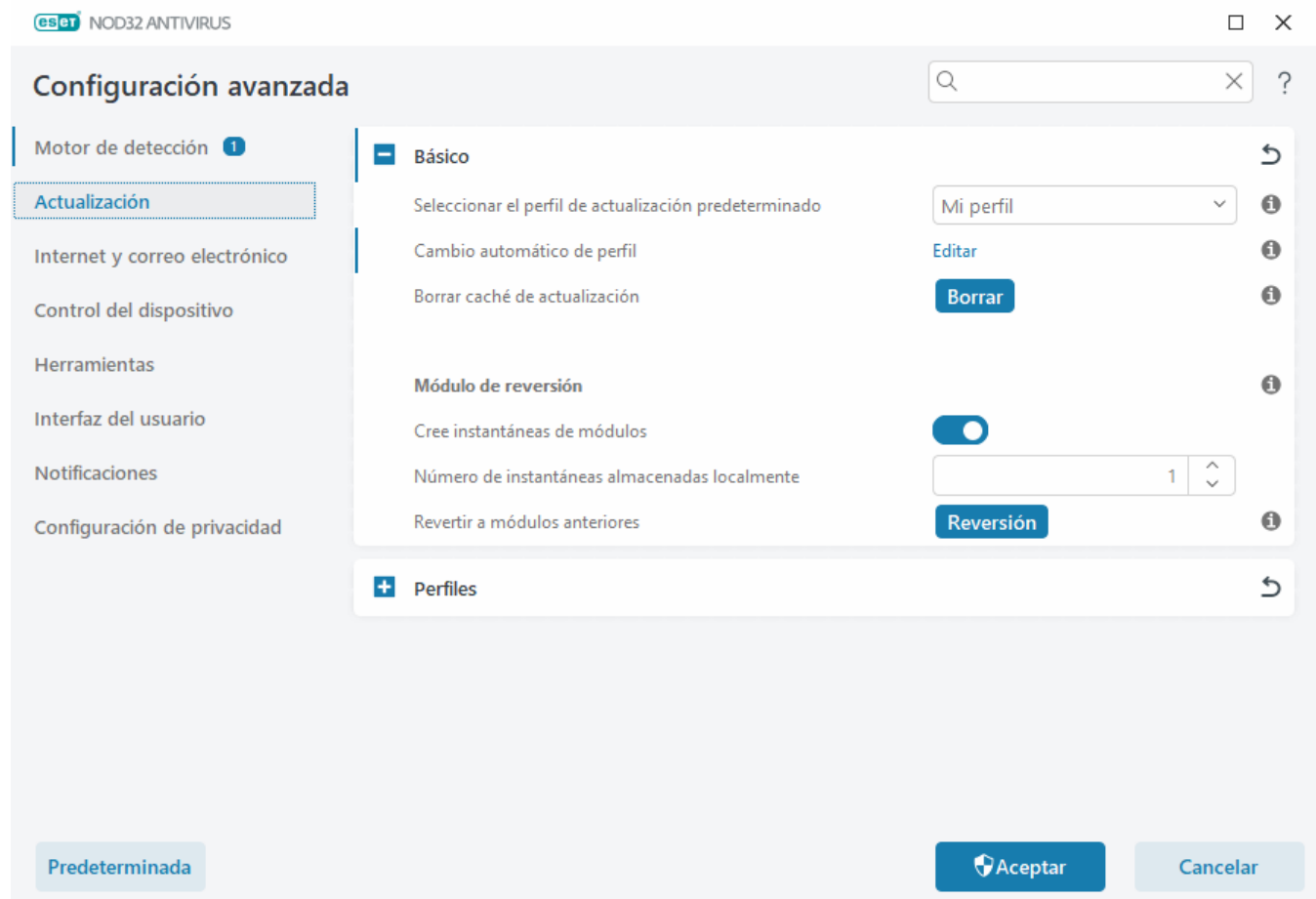
Además de las actualizaciones automáticas, puede hacer clic en **Buscar actualizaciones** para activar una actualización manual.



La ventana Configuración avanzada (haga clic en **Configuración** en el menú principal y luego en **Configuración avanzada** o presione la tecla **F5** del teclado) contiene opciones adicionales de actualización. Para configurar las

opciones avanzadas de actualización, como el modo de actualización, el acceso al servidor proxy y las conexiones LAN, haga clic en **Actualizar** en el árbol de configuración avanzada.

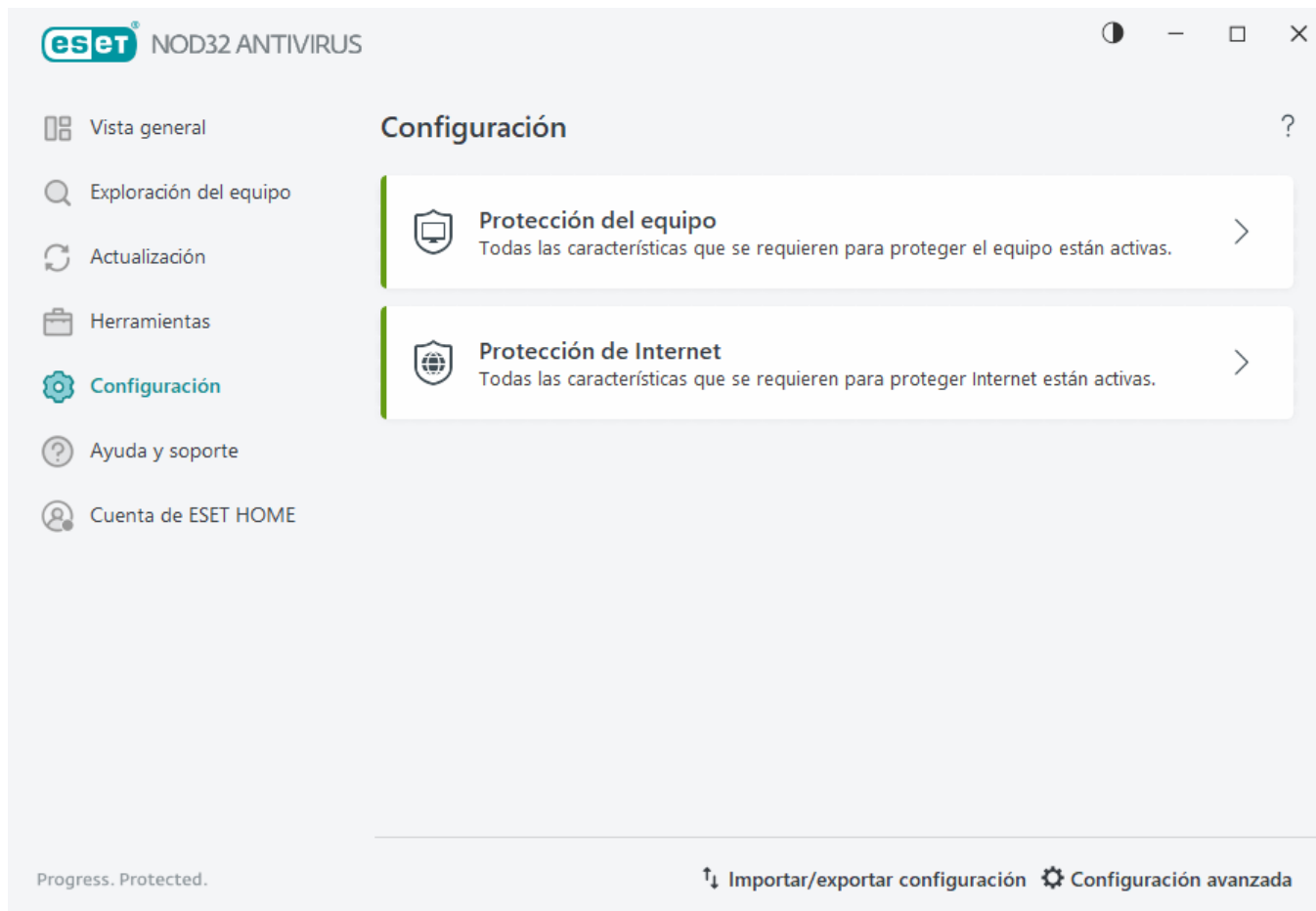
Si tiene problemas con una actualización, haga clic en **Borrar** para borrar la caché de actualización. Si aún así no puede actualizar los módulos del programa, consulte la sección [Resolución de problemas para el mensaje “Error de actualización de módulos”](#).



Trabajar con ESET NOD32 Antivirus

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

i Consulte la [ventana principal del programa](#) para ver la explicación de la página **Información general**.



El menú **Configuración** está dividido en las siguientes secciones:



Protección del equipo



Protección de Internet



Haga clic en un componente 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.
- **Control de dispositivos**: este módulo permite explorar, bloquear o ajustar los filtros o permisos extendidos y seleccionar la forma en que el usuario puede acceder y utilizar un dispositivo determinado (CD/DVD/USB...).
- **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.

La **configuración de Internet** 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(S) e IMAP(S).
- **Protección antiphishing**: filtra los sitios Web sospechosos de distribuir contenido que manipulan a los usuarios para que envíen información confidencial.


Para volver a habilitar un componente de seguridad, haga clic en el deslizador . El componente de seguridad habilitado tiene un ícono de conmutador verde .

Hay opciones adicionales disponibles en la parte inferior de la ventana de configuración. Utilice el enlace de **Configuración avanzada** para configurar parámetros más detallados para cada módulo. Para cargar los parámetros de configuración mediante un archivo de configuración .xml o para guardar los parámetros de configuración actuales en un archivo de configuración, use la opción [Importar/Exportar configuraciones](#).


Protección del equipo


Haga clic en **Protección del equipo** en la ventana **Configuración** para ver una descripción general de todos los módulos de protección:

- [Protección del sistema de archivos en tiempo real](#)
- [Control del dispositivo](#)
- [Sistema de prevención de intrusiones basado en el host \(HIPS\)](#)
- [Modo de juego](#)

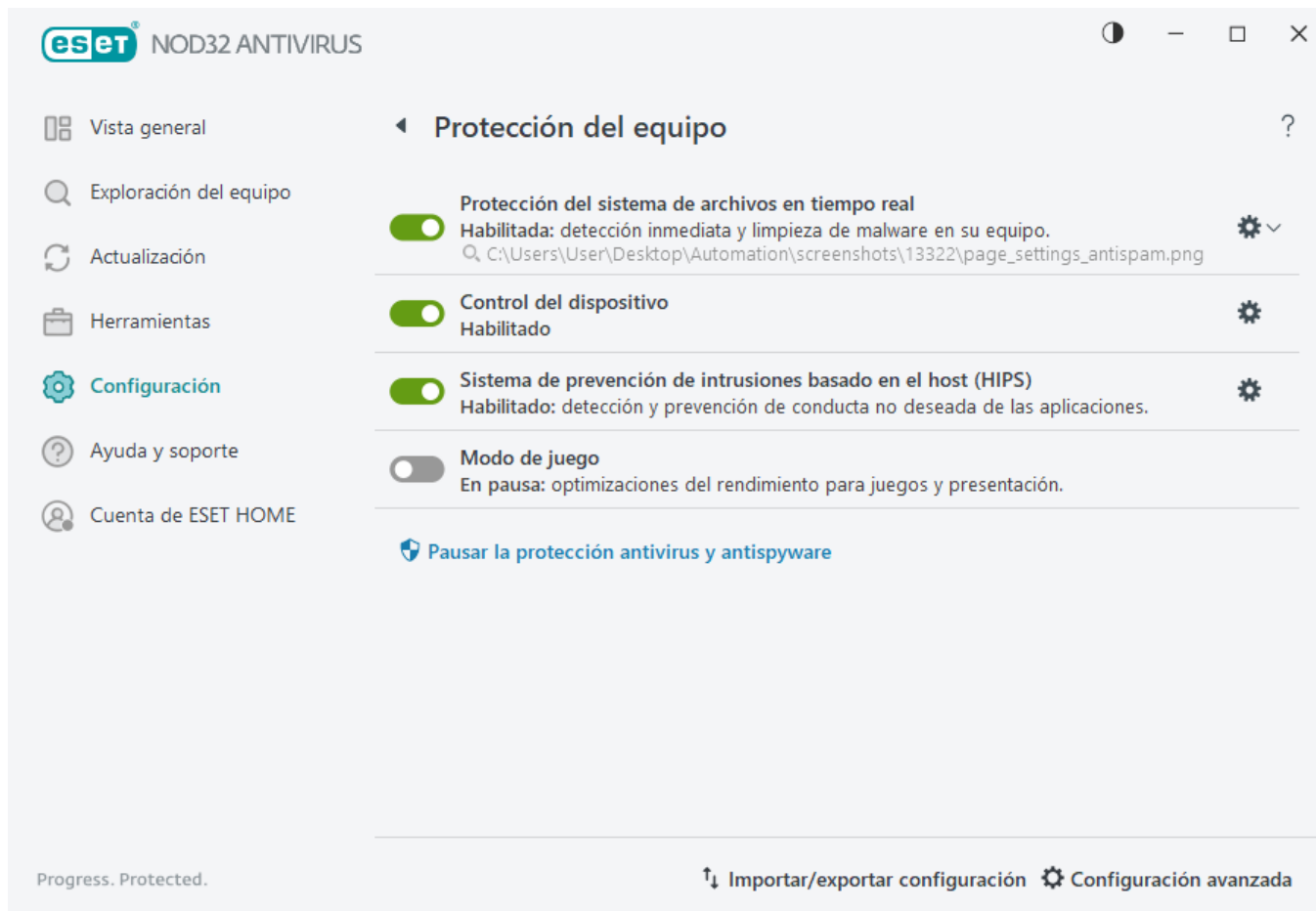
Para pausar o desactivar módulos de protección individuales, haga clic en el ícono de la barra deslizante .

 Desactivar los módulos de protección puede disminuir el nivel de protección del equipo.

Haga clic en el icono del engranaje  junto a un módulo de protección para acceder a las configuraciones avanzadas de dicho módulo.

Para la **protección del sistema de archivos en tiempo real**, haga clic en el icono del engranaje  y elija una de las siguientes opciones:

- **Configurar**: abre la Configuración avanzada de la protección del sistema de archivos en tiempo real.
- **Editar exclusiones**: abre la ventana [Configuración de exclusiones](#) para poder excluir archivos y carpetas de la exploración.



Pausar la protección antivirus y antispyware: deshabilita todos los módulos de protección antivirus y antispyware. Al deshabilitar la protección, se abrirá una ventana donde puede determinar durante cuánto tiempo se encontrará deshabilitada la protección mediante el menú desplegable **Intervalo temporal**. Solo use esta opción si es un usuario experimentado o si se lo indica el soporte técnico de ESET.

Motor de detección

El motor de detección brinda protección contra ataques maliciosos al sistema mediante el control de la comunicación de archivos, correo electrónico e Internet. Por ejemplo, si se detecta un objeto clasificado como malware, comenzará la corrección. El motor de detección puede eliminarlo primero bloqueándolo y luego realizar la limpieza, eliminación o la colocación en cuarentena.

Para configurar el motor de detección en detalle, haga clic en **Configuración avanzada** o presione la tecla **F5**.



Las modificaciones de la configuración del motor de detección deben realizarse únicamente por un usuario experimentado. La configuración incorrecta de los ajustes puede reducir el nivel de protección.

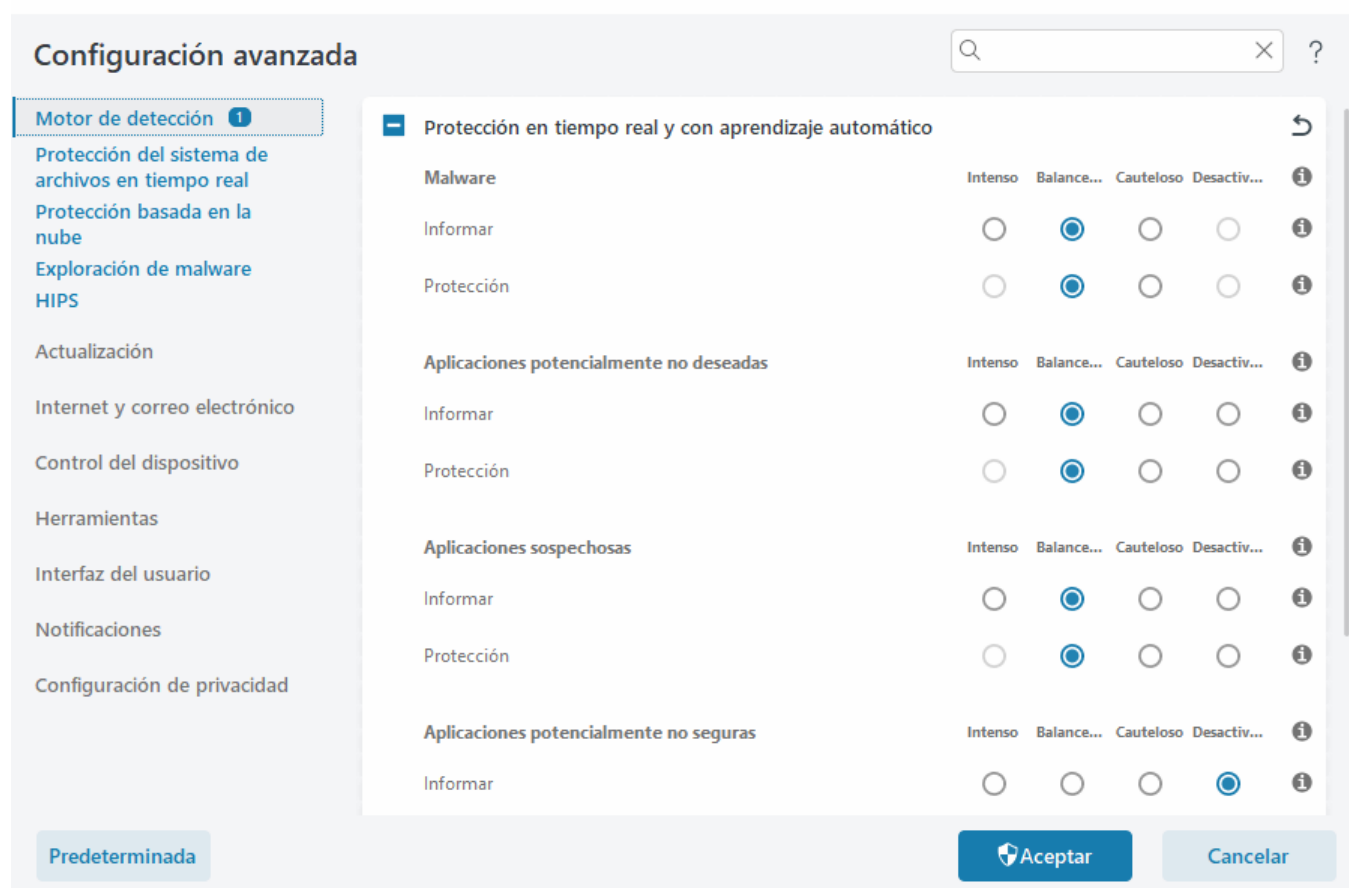
En esta sección:

- [Categorías de protección en tiempo real y con aprendizaje automático](#)
- [Exploración de malware](#)
- [Configuración de informes](#)
- [Configuración de protección](#)

Categorías de protección en tiempo real y con aprendizaje automático

La **protección en tiempo real y con aprendizaje automático** para todos los módulos de protección (p. ej., protección del sistema de archivos en tiempo real, protección de acceso a la Web, etc.) le permite configurar los niveles de protección y los informes de las siguientes categorías:

- **Malware:** un virus informático es un código malicioso que puede agregarse al principio o al final de archivos existentes en su ordenador. Sin embargo, el término “virus” suele utilizarse en forma errónea. “Malware” (software malicioso) es un término más preciso. La detección de malware se realiza mediante la combinación del módulo del motor de detección con el componente de aprendizaje automático. Obtenga más información sobre estos tipos de aplicaciones en el [Glosario](#).
- **Aplicaciones potencialmente no deseadas:** Grayware o aplicación potencialmente no deseada (PUA, ‘Potentially Unwanted Application’) es una amplia categoría de software, cuya intención no es tan inequívocamente maliciosa como con otros tipos de malware, como virus o troyanos. Sin embargo, puede instalar software adicional no deseado, cambiar el comportamiento del dispositivo digital o realizar actividades no aprobadas o esperadas por el usuario. Obtenga más información sobre estos tipos de aplicaciones en el [Glosario](#).
- Entre las **aplicaciones sospechosas**, se incluyen programas comprimidos con [empaquetadores](#) o protectores. Generalmente, los autores de malware explotan estos tipos de protectores para evadir la detección.
- **Aplicación potencialmente no segura :** hace referencia al software comercial y legítimo que puede utilizarse inadecuadamente para fines maliciosos. Algunos ejemplos de 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). Obtenga más información sobre estos tipos de aplicaciones en el [Glosario](#).



Protección mejorada



El aprendizaje automático avanzado ahora es parte del motor de detección y funciona como una capa avanzada de protección que mejora la detección según el aprendizaje automático. Obtenga más información sobre este tipo de protección en el [Glosario](#).

Exploración de malware

La configuración del explorador puede configurarse por separado para el explorador en tiempo real y la [exploración bajo demanda](#). De forma predeterminada, la **Configuración de la protección en tiempo real** está habilitada. Cuando está habilitada, la configuración de exploración bajo demanda pertinente se hereda de la sección de la **Protección en tiempo real y con aprendizaje automático**. Para obtener más información, consulte [Exploración de malware](#).

Configuración de informes

Cuando se produce una detección (p. ej., se encuentra una amenaza y se la clasifica como malware), la información se registra en el [Registro de detecciones](#), y se producen [Notificaciones en el escritorio](#) si están configuradas en ESET NOD32 Antivirus.

El umbral de informe está configurado para cada categoría (denominadas "CATEGORÍA"):

1. Malware

2.Aplicaciones potencialmente no deseadas

3.Potencialmente no seguro

4.Aplicaciones sospechosas

Los informes se realizan con el motor de detección, incluido el componente de aprendizaje automático. Puede establecer un umbral de informes más alto que el umbral de [protección](#) actual. Esta configuración de informes no influye en el bloqueo, [la desinfección](#) o la eliminación de [objetos](#).

Lea la información a continuación antes de modificar un umbral (o nivel) para los informes de CATEGORÍA:

Umbral	Explicación
Intenso	Configuración de máxima sensibilidad para informes de CATEGORÍA. Se informan más amenazas. La configuración como “ Intenso ” puede identificar erróneamente objetos como CATEGORÍA.
Balanceado	Configuración balanceada para informes de CATEGORÍA. Esta configuración se optimiza para equilibrar el rendimiento y la precisión de las tasas de detección y el número de objetos que se reportan falsamente.
Cauteloso	Configuración para informes de CATEGORÍA para minimizar la cantidad de objetos identificados en forma errónea al mismo tiempo que se mantiene un nivel suficiente de protección. Los objetos se reportan únicamente cuando la probabilidad es evidente y concuerda con el comportamiento de CATEGORÍA.
Desactivado	Los informes para CATEGORÍA no se encuentran activados, y las amenazas de este tipo no se detectan, reportan o desinfectan. Por lo tanto, esta configuración deshabilita la protección contra este tipo de amenazas. La opción “Desactivado” no está disponible para los informes de malware y es el valor predeterminado para las aplicaciones potencialmente no seguras.

✓ [Disponibilidad de módulos de protección de ESET NOD32 Antivirus](#)

La disponibilidad (habilitada o deshabilitada) de un módulo de protección para el umbral de una CATEGORÍA seleccionada es la siguiente:

	Intenso	Balanceado	Cauteloso	Desactivado**
Módulo de aprendizaje automático avanzado*	✓ (modo intenso)	✓ (modo conservador)	X	X
Módulo del motor de detección	✓	✓	✓	X
Otros módulos de protección	✓	✓	✓	X

* Disponibles en ESET NOD32 Antivirus versión 13.1 y posteriores.

** No recomendado

✓ [Determina la versión del producto, las versiones del módulo del programa y la fecha de la versión](#)

1. Haga clic en **Ayuda y soporte > Acerca de ESET NOD32 Antivirus**.
2. En la pantalla **Acerca de**, la primera línea muestra el número de la versión de su producto ESET.
3. Haga clic en **Componentes instalados** para acceder a información sobre módulos específicos.

Notas importantes

Hay varias notas importantes a tener en cuenta cuando se configura el umbral adecuado para su entorno:

- El umbral **Balanceado** se recomienda para la mayoría de las configuraciones.

- El umbral **Cauteloso** representa un nivel de protección comparable con el de versiones anteriores de ESET NOD32 Antivirus (versión 13.0 y anteriores). Se recomienda para entornos en los que la prioridad se enfoca en minimizar los objetos identificados en forma errónea por el software de seguridad.
- Mientras más alto sea el umbral de informes, más alta será la tasa de detección pero habrá más probabilidades de objetos identificados en forma errónea.
- Desde el punto de vista del mundo real, no existen garantías de una tasa de detección del 100 % ni tampoco 0 % de probabilidades de evitar la categorización incorrecta de objetos no infectados como malware.
- [Mantenga actualizados ESET NOD32 Antivirus y sus módulos](#) para maximizar el equilibrio entre desempeño, precisión de tasas de detección y cantidad de objetos informados en forma errónea.

Configuración de protección



Si se reporta un objeto clasificado como CATEGORÍA, el programa bloquea el objeto, luego se lo [desinfecta](#), elimina o coloca en [Cuarentena](#).

Lea la información a continuación antes de modificar un umbral (o nivel) para la protección de CATEGORÍA:

Umbral	Explicación
Intenso	Las amenazas reportadas de nivel intenso (o más bajo) se bloquean, y se inicia la corrección automática (por ejemplo, la desinfección). Esta configuración se recomienda cuando todos los equipos han sido explorados con configuración agresiva y cuando los objetos reportados en forma errónea han sido agregados a las exclusiones de detección.
Balanceado	Las amenazas reportadas de nivel balanceado (o más bajo) se bloquean, y se inicia la corrección automática (por ejemplo, la desinfección).
Cauteloso	Las detecciones reportadas de nivel cauteloso se bloquean, y se inicia la corrección automática (por ejemplo, la desinfección).
Desactivado	De utilidad para la identificación y exclusión de objetos reportados en forma errónea. La opción “Desactivado” no está disponible para la protección contra malware y es el valor predeterminado para las aplicaciones potencialmente no seguras.

✓ [Cuadro de conversión para ESET NOD32 Antivirus versión 13.0 y anteriores](#)

Al actualizar desde la versión 13.0 y anteriores a la versión 13.1 y posteriores, el nuevo estado del umbral será el siguiente:

Interruptor de categoría antes de la actualización		
Nuevo umbral de CATEGORÍA después de la actualización	Balanceado	Desactivado

Opciones avanzadas del motor de detección

Activar análisis avanzado mediante AMSI es la herramienta Microsoft Antimalware Scan Interface que permite analizar scripts PowerShell, scripts ejecutados por Windows Script Host y datos analizados con AMSI SDK.

Infiltración detectada

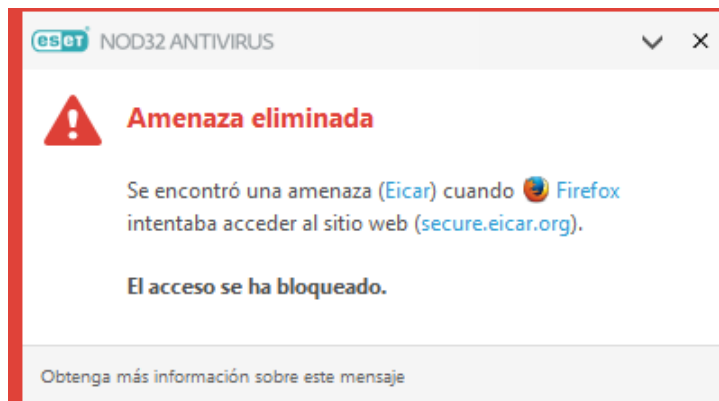
Las infiltraciones pueden llegar al sistema desde diversos puntos de entrada, como [páginas Web](#), carpetas compartidas, correo electrónico o [dispositivos extraíbles](#) (USB, discos externos, CD, DVD, etc.).

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 a petición](#)

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 información detallada sobre los objetos detectados/desinfectados, consulte [Archivos de registro](#). Para obtener más información sobre los niveles de desinfección y conducta, consulte [Nivel de desinfección](#).



Explorando el equipo para detectar archivos infectados

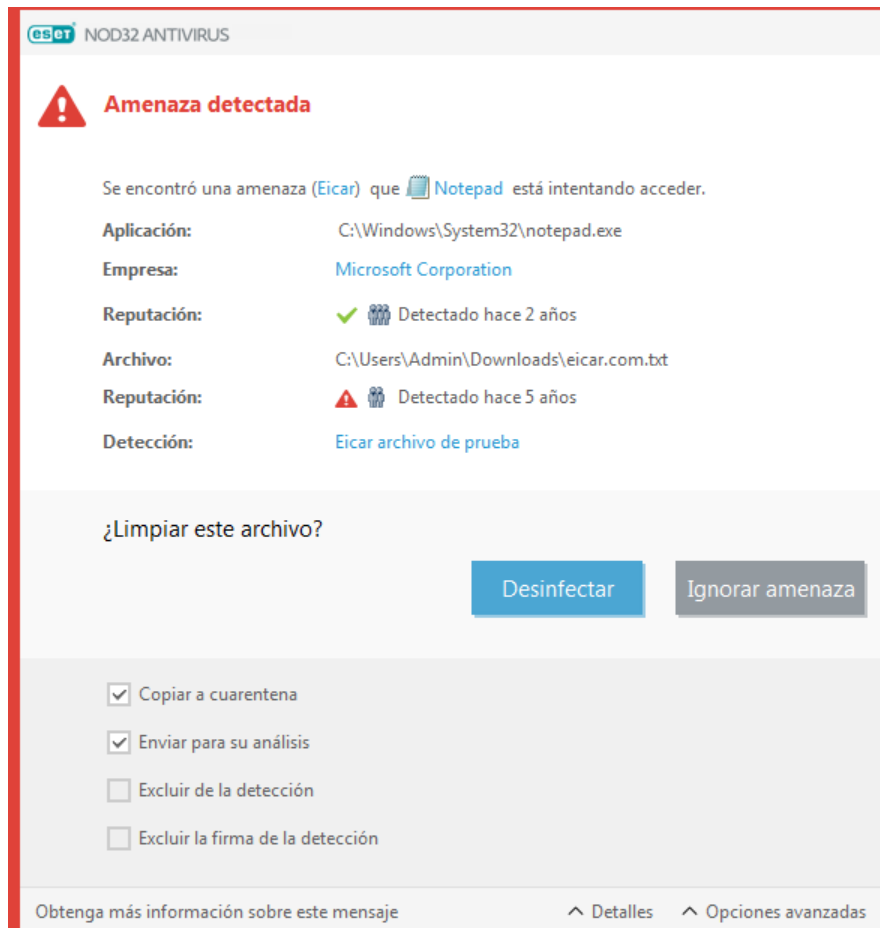
Si su equipo muestra signos de infección por malware, por ej., funciona más lento, con frecuencia no responde, etc., se recomienda hacer lo siguiente:

1. Abra ESET NOD32 Antivirus y haga clic en **Exploración del equipo**.
2. Haga clic en **Explorar el equipo** (para obtener más información, consulte en [Exploración del equipo](#)).
3. 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.

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 luego del reinicio del sistema).

Restauración desde Cuarentena

Para acceder a la cuarentena, diríjase a la [ventana principal del programa](#) ESET NOD32 Antivirus y haga clic en **Herramientas > Cuarentena**.

Los archivos en cuarentena también pueden restaurarse a su ubicación original:

- Para tal fin, use la función **Restaurar**, que se encuentra disponible en el menú contextual, al hacer clic con el botón secundario en un archivo específico en Cuarentena.
- Si un archivo está marcado como [aplicación potencialmente no deseada](#), se habilita la opción **Restaurar y**

excluir de la exploración. Consulte también [Exclusiones](#).

- El menú contextual también ofrece la opción **Restaurar a**, que le permite restaurar un archivo de una ubicación que no sea aquella en la que se lo eliminó.
- La funcionalidad de restauración no se encuentra disponible en algunos casos, por ejemplo, para archivos ubicados en una unidad de uso compartido de solo lectura.

Varias amenazas

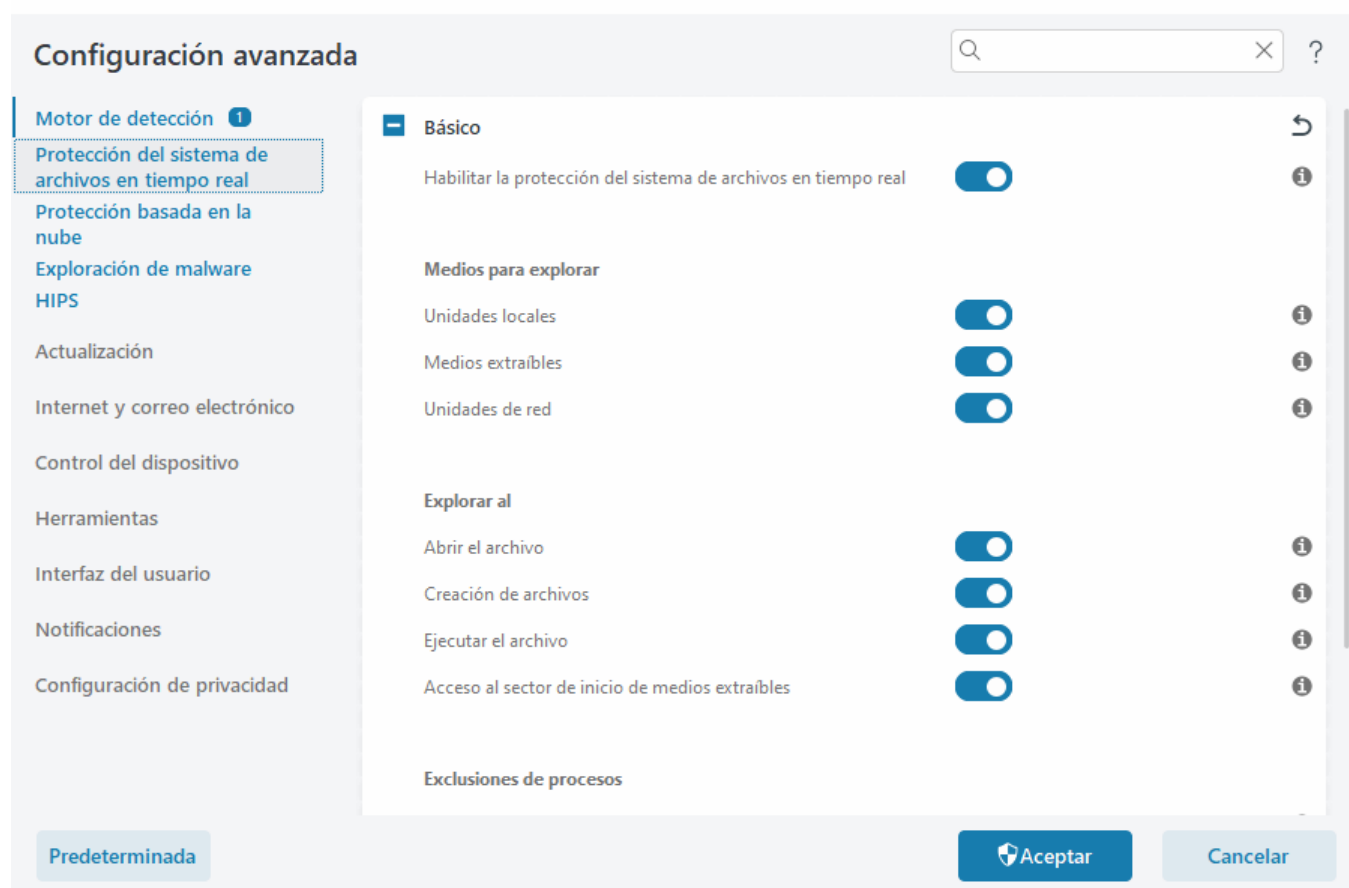
Si algún archivo infectado no se desinfectó durante la exploración del equipo (o el [Nivel de desinfección](#) estaba configurado en **Sin desinfección**), se muestra una ventana de alerta que le solicitará seleccionar las acciones para dichos archivos. Seleccione las acciones para los archivos (las 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.

Protección del sistema de archivos en tiempo real

La protección del sistema de archivos en tiempo real controla todos los archivos del sistema para detectar código malicioso al abrirllos, crearlos o ejecutarlos.



En forma predeterminada, la protección del sistema de archivos en tiempo real se ejecuta junto al inicio del sistema y proporciona una exploración ininterrumpida. No recomendamos deshabilitar la opción **Habilitar la protección del sistema de archivos en tiempo real** en la **Configuración avanzada** de **Motor de detección** > **Protección del sistema de archivos en tiempo real** > **Básica**.

Medios para explorar

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

- **Unidades locales** – Escanea todo el sistema y discos duros fijos (ejemplo: *C:*, *D:*).
- **Medios extraíbles** – Escanea CD/DVD, almacenamiento USB, tarjetas de memoria, etc.
- **Unidades de red** – Escanea todas las unidades de red asignadas (ejemplo: *H:* como *\\store04*) o unidades de red de acceso directo (ejemplo: *\\store08*).

Recomendamos que use la configuración predeterminada y solo modificarla en casos específicos, como por ej., si al explorar ciertos medios, se ralentizan significativamente las transferencias de archivos.

Explorar al

De forma predeterminada, todos los archivos se analizan 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** – Escanea al abrir un archivo.

- **Creación del archivo** – Escanea al crear o modificar un archivo.
- **Ejecución del archivo** – Escanea al ejecutar un archivo.
- **Acceso al sector de inicio de medios extraíbles** – Cuando se inserta un medio extraíble que contiene un sector de inicio en un dispositivo, se explora de inmediato el sector de inicio. Esta opción no habilita la exploración de archivos de medios extraíbles. La exploración de archivos de medios extraíbles se encuentra en **Medios para explorar > Medios extraíbles**. Para que **Acceso al sector de inicio de medios extraíbles** funcione correctamente, mantenga habilitado **Sectores de inicio/UEFI** en los parámetros de ThreatSense.

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). Se exploran los archivos nuevamente inmediatamente después de cada actualización del motor de detección. Este comportamiento se controla mediante el uso de la **Optimización inteligente**. Si se deshabilita esta **Optimización inteligente**, se exploran todos los archivos cada vez que se accede a los mismos. Para modificar esta configuración, presione **F5** para abrir **Configuración avanzada** y expandir **Motor de detección > Protección del sistema de archivos en tiempo real**. Haga clic en **Parámetro de ThreatSense > Otros** y seleccione o anule la selección de **Habilitar la optimización inteligente**.

Niveles de desinfección

Para acceder a la configuración de los niveles de desinfección para un módulo de protección deseado, expanda **Parámetros de ThreatSense** (por ejemplo, **Protección del sistema de archivos en tiempo real**) y, luego, haga clic en **Desinfección > Nivel de desinfección**.

Los parámetros de ThreatSense tienen los siguientes niveles de corrección (es decir, desinfección).


Corrección ESET NOD32 Antivirus

Nivel de desinfección	Descripción
Corregir siempre la detección	Intento de corregir la detección al limpiar objetos sin la intervención del usuario final. En algunos pocos casos (por ejemplo, en archivos de sistema), si la detección no se puede corregir, se deja al objeto informado en su ubicación original.
Corregir la detección si es seguro, de lo contrario conservar	Intento de corregir la detección al desinfectar objetos sin la intervención del usuario final. En algunos casos (por ejemplo, en archivos de sistema con archivos desinfectados o infectados), si una detección no se puede corregir, se deja al objeto informado en su ubicación original.
Corregir la detección si es seguro, de lo contrario preguntar	Intento de corregir la detección al desinfectar objetos. En algunos casos, si no se puede realizar ninguna acción, el usuario final recibe una alerta interactiva y debe seleccionar una acción de corrección (por ejemplo, eliminar o ignorar). Esta configuración se recomienda en la mayoría de los casos.

Nivel de desinfección	Descripción
Preguntar siempre al usuario final	El usuario final visualiza una ventana interactiva al desinfectar objetos y debe seleccionar una acción de corrección (por ejemplo, eliminar o ignorar). Este nivel está diseñado para los usuarios más avanzados que conocen los pasos a seguir en caso de hallar una detección.

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.

Después de la instalación de ESET NOD32 Antivirus, todos los ajustes de configuración se optimizan para proporcionar el máximo nivel de seguridad del sistema para los usuarios. Para restaurar la configuración predeterminada, haga clic  al lado de cada pestaña en la ventana (**Configuración avanzada > Motor de detección > Protección del sistema de archivos en tiempo real**).

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 www.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 (European Institute for Computer Antivirus Research, 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>. Después de introducir esta URL en su navegador, debería visualizar un mensaje que indica que se eliminó la amenaza.

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 desactiva la protección en tiempo real sin darse cuenta, debe reactivar la función. Para reactivar la protección en tiempo real, vaya a **Configuración** en la [ventana principal del programa](#) y haga clic en **Protección del equipo > 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 **Habilitar la protección del sistema de archivos en tiempo real** está deshabilitada. Para asegurarse de que esta opción esté habilitada, vaya a **Configuración avanzada (F5)** y haga clic en **Motor de detección > Protección del sistema de archivos en tiempo real**.

Si la protección en tiempo real no detecta ni desinfecta infiltraciones

Asegúrese de que no haya otros programas antivirus instalados en el equipo. Si hay dos programas antivirus instalados a la vez, es posible que tengan conflictos entre ellos. 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 al iniciar el sistema (y está activada la opción **Activar protección del sistema de archivos en tiempo real**), es posible que se deba a conflictos con otros programas. Para resolver este problema, [cree un registro de ESET SysInspector y envíelo a Soporte técnico de ESET para su análisis](#).

Exclusiones de procesos

La funcionalidad de Exclusiones de procesos le permite excluir procesos de la aplicación de la protección del sistema de archivos en tiempo real. Para mejorar la velocidad de la copia de seguridad, la integridad del proceso y la disponibilidad del servicio, se utilizan ciertas técnicas que se conoce que entran en conflicto con la protección contra el malware a nivel del archivo durante la copia de seguridad. La única manera de evitar con efectividad ambas situaciones consiste en desactivar el software contra el malware. Al excluir procesos específicos (por ejemplo, los que corresponden a la solución de la copia de seguridad), todas las operaciones de que se atribuyen a dichos procesos excluidos se ignoran y consideran seguras, por lo tanto, se minimiza la interferencia con el proceso de copia de seguridad. Le sugerimos que sea precavido al crear exclusiones: una herramienta de copia de seguridad que se ha excluido puede acceder a archivos infectados sin ejecutar una alerta, motivo por el cual solo se autorizan los permisos extendidos en el módulo de protección en tiempo real.

 No debe confundirse con [Extensiones de archivo excluidas](#), [Exclusiones de HIPS](#), [Exclusiones de detección](#) o [Exclusiones de rendimiento](#).

Las exclusiones de los procesos contribuyen a atenuar el riesgo de que se produzcan conflictos y mejorar el rendimiento de las aplicaciones excluidas, lo que, a su vez, tiene un efecto positivo en el rendimiento general y la estabilidad del sistema operativo. La exclusión de un proceso o aplicación es una exclusión de su archivo ejecutable (.exe).

Puede añadir archivos ejecutables en la lista de procesos excluidos desde **Configuración avanzada (F5) > Motor de detección > Protección del sistema de archivos en tiempo real > Exclusiones de procesos**.

Esta característica ha sido diseñada para excluir herramientas de copia de seguridad. El hecho de excluir procesos de la herramienta de copia de seguridad de la exploración no solo garantiza la estabilidad del sistema, sino que también afecta el rendimiento de la copia de seguridad, ya que la copia de seguridad no se ve ralentizada cuando se está ejecutando.

Haga clic en **Editar** para abrir la ventana de administración de **Exclusiones de procesos**, donde puede [agregar exclusiones](#) y buscar un archivo ejecutable (por ejemplo, *Backup-tool.exe*), que se excluirá de la exploración.



Tan pronto se agrega el archivo .exe a las exclusiones, la actividad de este proceso no se somete a la monitorización de ESET NOD32 Antivirus y no se ejecutan exploraciones en ninguna operación de archivos que lleva a cabo este proceso.

Si no utiliza la función de buscar al seleccionar el proceso ejecutable, deberá ingresar manualmente la ruta completa al ejecutable. De lo contrario, la exclusión no funcionará correctamente y es posible que [HIPS](#) muestre errores.

También puede **Editar** los procesos existentes o **Eliminarlos** de las exclusiones.

En la [protección de acceso a la web](#), no se tiene en cuenta esta exclusión. Por lo tanto, si excluye el archivo ejecutable del navegador web, seguirán explorándose los archivos descargados. De esta manera, pueden seguir detectándose las infiltraciones. Esta situación es solo un ejemplo. No recomendamos crear exclusiones para navegadores web.

Agregado o edición de exclusiones de procesos

Esta ventana de diálogo le permite **agregar** procesos excluidos del motor de detección. Las exclusiones de los procesos contribuyen a atenuar el riesgo de que se produzcan conflictos y mejorar el rendimiento de las aplicaciones excluidas, lo que, a su vez, tiene un efecto positivo en el rendimiento general y la estabilidad del sistema operativo. La exclusión de un proceso o aplicación es una exclusión de su archivo ejecutable (.exe).

Seleccione la ruta del archivo de una aplicación exceptuada al hacer clic en ... (por ejemplo, *C:\Program Files\Firefox\Firefox.exe*). NO ingrese el nombre de la aplicación.

✓ Tan pronto se agrega el archivo .exe a las exclusiones, la actividad de este proceso no se somete a la monitorización de ESET NOD32 Antivirus y no se ejecutan exploraciones en ninguna operación de archivos que lleva a cabo este proceso.

Si no utiliza la función de buscar al seleccionar el proceso ejecutable, deberá ingresar manualmente la ruta completa al ejecutable. De lo contrario, la exclusión no funcionará correctamente y es posible que [HIPS](#) muestre errores.

También puede **Editar** los procesos existentes o **Eliminarlos** de las exclusiones.

Protección basada en la nube

ESET LiveGrid® (creada en el sistema avanzado de alerta temprana ESET ThreatSense.Net) utiliza los datos que los usuarios de ESET enviaron de todo el mundo y los envía al laboratorio de investigación de ESET. Al proporcionar muestras sospechosas y metadatos, ESET LiveGrid® nos permite reaccionar inmediatamente ante las necesidades de nuestros clientes y mantener a ESET receptivo a las últimas amenazas.

Se encuentran disponibles las siguientes opciones:

Habilitar el sistema de reputación de ESET LiveGrid®

El sistema de reputación de ESET LiveGrid® ofrece listas blancas y negras basadas en la nube.

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 en ESET LiveGrid®.


Habilitar el sistema de comentarios de ESET LiveGrid®

Además del sistema de reputación de ESET LiveGrid®, el sistema de comentarios de ESET LiveGrid® recopilará

información sobre su equipo relacionada con las amenazas recientemente detectadas. Esta información puede incluir:



- Muestra o copia del archivo en el que apareció la amenaza
- Ruta al archivo
- Nombre del archivo
- Fecha y hora
- El proceso por el que apareció la amenaza en el ordenador
- 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 extensiones específicas, como *.doc* o *.xls*, siempre se excluyen. También puede agregar otras extensiones si hay archivos específicos que usted o su organización prefieren no enviar.

 Obtenga más información sobre el envío de datos relevantes en la [Política de privacidad](#).

Puede elegir no habilitar ESET LiveGrid®

No perderá funcionalidad alguna en el software, pero, en algunos casos, ESET NOD32 Antivirus puede responder más rápido a las nuevas amenazas cuando se habilita ESET LiveGrid®. Si ya usó ESET LiveGrid® y lo deshabilitó, es posible que hayan quedado paquetes de datos para enviar. Aun después de su desactivación, dichos paquetes se enviarán a ESET. Una vez que se envíe toda la información actual, no se crearán más paquetes.

 Lea más sobre ESET LiveGrid® en el [glosario](#).
 Consulte nuestras [instrucciones ilustradas](#) disponibles en inglés y en otros idiomas para activar o desactivar ESET LiveGrid® en ESET NOD32 Antivirus.

Configuración de la protección basada en la nube, en la Configuración avanzada

Para acceder a la configuración de ESET LiveGrid®, abra **Configuración avanzada (F5) > Motor de detección > Protección en la nube**.

- **Habilitar el sistema de reputación ESET LiveGrid® (recomendado)** – el sistema de reputación ESET LiveGrid® mejora la eficacia de las soluciones anti-malware de ESET al comparar los archivos analizados con una base de datos de elementos de listas blancas y listas negras en la nube.
- **Habilitar el sistema de comentarios de ESET LiveGrid®** – Envía los datos de envío relevantes (descritos en la **sección de envío de muestra** a continuación) junto con informes de falla y estadísticas al laboratorio de investigación de ESET para un mayor análisis.
- **Enviar informes de error y datos de diagnóstico**: envíe datos de diagnóstico relacionados con ESET LiveGrid®, como informes de falla y módulos de volcado de memoria. Recomendamos mantener esta

función habilitada para ayudar a ESET a diagnosticar problemas, mejorar los productos y garantizar una mejor protección del usuario final.

- **Enviar estadísticas anónimas** – permita a ESET recopilar información acerca de amenazas detectadas recientemente como el nombre de la amenaza, la fecha y la hora de detección, el método de detección y los metadatos asociados, la versión del producto, y la configuración, incluida la información sobre su sistema.
- **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. No recibirá respuesta alguna de ESET a menos que se necesite información adicional.

Envío de muestras

Envío manual de muestras: le permite enviar muestras a ESET manualmente desde el menú contextual, [Cuarentena](#) o [Herramientas](#).

Envío automático de muestras detectadas

Seleccione qué tipo de muestras se enviarán a ESET para su análisis y para mejorar la detección futura (el tamaño máximo predeterminado de la muestra es de 64 MB). Se encuentran disponibles las siguientes opciones:

- **Todas las muestras detectadas:** todos los [objetos](#) detectados por el [motor de detección](#) (incluso las aplicaciones potencialmente no deseadas cuando se habilitan en la configuración del explorador).
- **Todas las muestras, excepto los documentos:** todos los objetos detectados, excepto los **documentos** (consulte a continuación).
- **No enviar:** los objetos detectados no se enviarán a ESET.

Envío automático de muestras sospechosas

Estas muestras también se enviarán a ESET si el motor de detección no las detecta. Por ejemplo, muestras que casi no se detectan o alguno de los [módulos de protección de](#) ESET NOD32 Antivirus consideran estas muestras sospechosas o con un comportamiento poco claro (el tamaño máximo predeterminado de la muestra es de 64 MB).

- **Ejecutables:** incluye archivos ejecutables, como .exe, .dll, .sys.
- **Archivos:** incluye tipos de archivos, como .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.
- **Scripts:** incluye tipos de archivos de script, como .bat, .cmd, .hta, .js, .vbs, .ps1.
- **Otros** – Incluye tipos de archivos como .jar, .reg, .msi, .sfw, .lnk.
- **Posibles correos electrónicos spam** – permite enviar partes de correos electrónicos con spam o correos electrónicos con spam completos adjuntos a ESET para que realice un análisis más profundo. Activar esta opción mejora la detección global de spam, que incluye mejoras en la detección futura de spam para usted.
- **Documentos:** incluye documentos Microsoft Office o PDF con contenido activo o sin este.

✓ [Expandir para ver una lista de todos los tipos de archivos de documento incluidos](#)

ACCDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWFX, EPS, IWORK_NUMBERS, IWORK_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2_ENCRYPTED, OLE2_MACRO, OLE2_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD_XML, WPC, WPS, XLS, XLS_XML, XLSB, XLSM, XLSX, XPS

Exclusiones

El [filtro de exclusión](#) le permite excluir archivos o ciertas carpetas del envío (por ejemplo, puede ser útil para excluir archivos que puedan contener información confidencial, como documentos u hojas de cálculo). Los archivos incluidos en la lista nunca se enviarán a los laboratorios de ESET para su análisis, aunque contengan un código sospechoso. 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.



Para excluir archivos descargados de `download.domain.com`, vaya a **Configuración avanzada > Motor de detección > Protección basada en la nube > Envío de muestras** y haga clic en **Editar** junto a **Exclusiones**. Agregue la exclusión `.download.domain.com`.

Tamaño máximo de muestras (MB): define el tamaño máximo de las muestras (1-64 MB).

Filtro de exclusión para la protección basada en la nube

El filtro de exclusión permite excluir ciertos archivos o carpetas del envío de muestras. Los archivos incluidos en la lista nunca se enviarán a los laboratorios de ESET para su análisis, aunque contengan un código sospechoso. Los tipos de archivo comunes (tales como .doc, etc.) se excluyen de forma predeterminada.



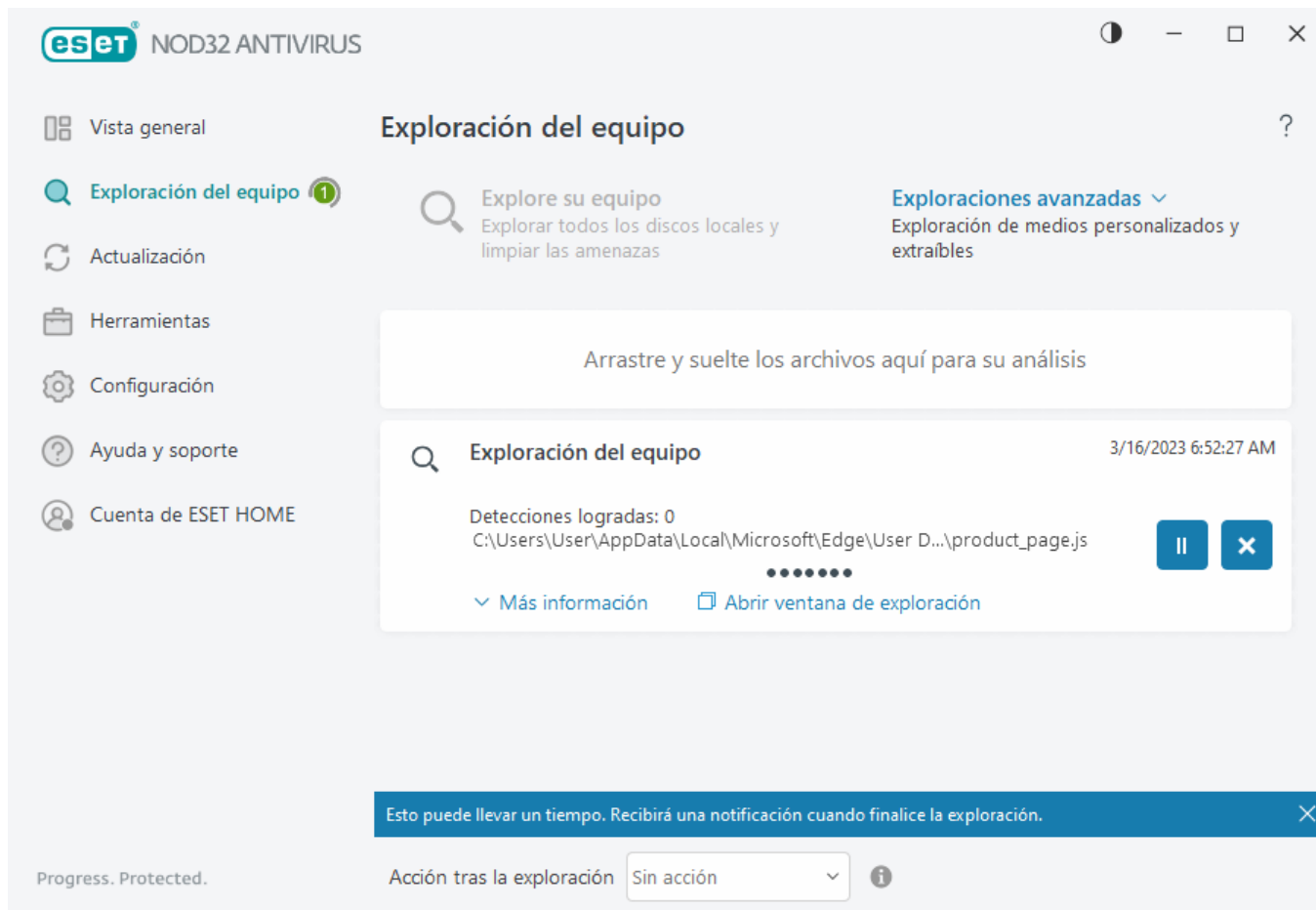
Esta función resulta útil para excluir archivos que puedan contener información confidencial, como documentos u hojas de cálculo.



Para excluir archivos descargados de `download.domain.com`, haga clic en **Configuración avanzada > Motor de detección > Protección en la nube > Envío de muestras > Exclusiones** y agregue la exclusión `*download.domain.com*`.

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 se ejecuten en forma habitual como parte de las medidas de seguridad de rutina, no solo cuando existen sospechas de una infección. 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 el motor de detección es obsoleto 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**. **Explorar el equipo** explora de manera rápida el sistema sin especificar parámetros de exploración. **La exploración personalizada** (en Exploración avanzada) le permite seleccionar perfiles de exploración predefinidos diseñados para ciertas ubicaciones de destino y elegir objetos de exploración específicos.

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

De forma predeterminada, ESET NOD32 Antivirus intentará limpiar o quitar de forma automática las detecciones encontradas durante la exploración del equipo. En algunos casos, si no se puede realizar ninguna acción, recibe una alerta interactiva y debe seleccionar una acción de limpieza (por ejemplo, quitar o ignorar). Para cambiar el nivel de limpieza y para obtener información más detallada, consulte [Limpieza](#). Para revisar exploraciones anteriores, consulte [Archivos de registro](#).

Explore su equipo

Explore el equipo le permite iniciar rápidamente una exploración del equipo y desinfectar los archivos infectados sin necesidad de la intervención del usuario. La ventaja de la **Explore el equipo** es su facilidad de uso y que no requiere una configuración detallada de la exploración. Esta exploración verifica todos los archivos de las unidades locales y limpia 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](#).

También puede utilizar la función **Arrastrar y soltar para explorar** un archivo o una carpeta manualmente haciendo clic en el archivo o la carpeta, moviendo el puntero del mouse hacia el área marcada al mismo tiempo que mantiene el botón pulsado, y luego lo suelta. Después de eso, la aplicación se mueve al primer plano.

Las siguientes opciones de exploración están disponibles en **Exploraciones avanzadas**:



Exploración personalizada

La **Exploración personalizada** permite especificar parámetros de exploración, como los objetos o métodos. La ventaja de la **Exploración personalizada** consiste en que puede 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 **Explore el equipo**: 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 malware y otras amenazas potenciales.

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



Repetir la última exploración

Le permite lanzar rápidamente la exploración realizada anteriormente, con los mismos ajustes.

El menú desplegable **Acción después de la exploración** permite establecer una acción que se realice automáticamente tras finalizar una exploración:

- **Sin acción** – después de la finalización de la exploración, no se llevará a cabo ninguna acción.
- **Apagar** – el equipo se apaga después de la finalización de la exploración.
- **Reiniciar si es necesario**: el equipo se reinicia solo si es necesario para completar la limpieza de las amenazas detectadas.
- **Reiniciar** – cierra todos los programas abiertos, y reinicia el equipo luego de la finalización de la exploración.
- **Reiniciar si es necesario**: el equipo fuerza el reinicio solo si es necesario para completar la limpieza de las amenazas detectadas.
- **Forzar reinicio**: fuerza el cierre de todos los programas abiertos sin esperar la intervención del usuario y reinicia el equipo cuando finaliza la exploración.
- **Suspender**– guarda su sesión y pone el equipo en un estado de energía baja para que pueda volver a trabajar rápidamente.
- **Hibernar**– toma todo lo que se está ejecutando en la memoria RAM y lo envía a un archivo especial de su disco duro. Su equipo se apaga, pero reanudará su estado anterior la próxima vez que lo inicie.

i Las acciones **Suspender** o **Hibernar** están disponibles en función de la configuración de Activar o Hibernar del sistema operativo o de las capacidades de su equipo/computadora portátil. Tenga en cuenta que un equipo en suspensión aún es un equipo en funcionamiento. Sigue ejecutando funciones básicas y utilizando electricidad cuando el equipo funciona con la alimentación de la batería. Para preservar la vida útil de la batería, como cuando viaja fuera de su oficina, recomendamos utilizar la opción Hibernar.

La acción seleccionada comenzará tras la finalización de las exploraciones en ejecución. Cuando seleccione **Apagar** o **Reiniciar**, aparecerá un cuadro de diálogo de confirmación con una cuenta regresiva de 30 segundos (haga clic en **Cancelar** para desactivar la acción solicitada).

i 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 programo una exploración semanal del equipo?](#)

Iniciador de la exploración personalizada

Puede usar la exploración personalizada para explorar la memoria operativa, la red o las partes específicas de un disco, en lugar del disco completo. Para hacerlo, haga clic en **Exploraciones avanzadas > Exploración personalizada** y seleccione los objetivos específicos de la estructura de la carpeta (árbol).

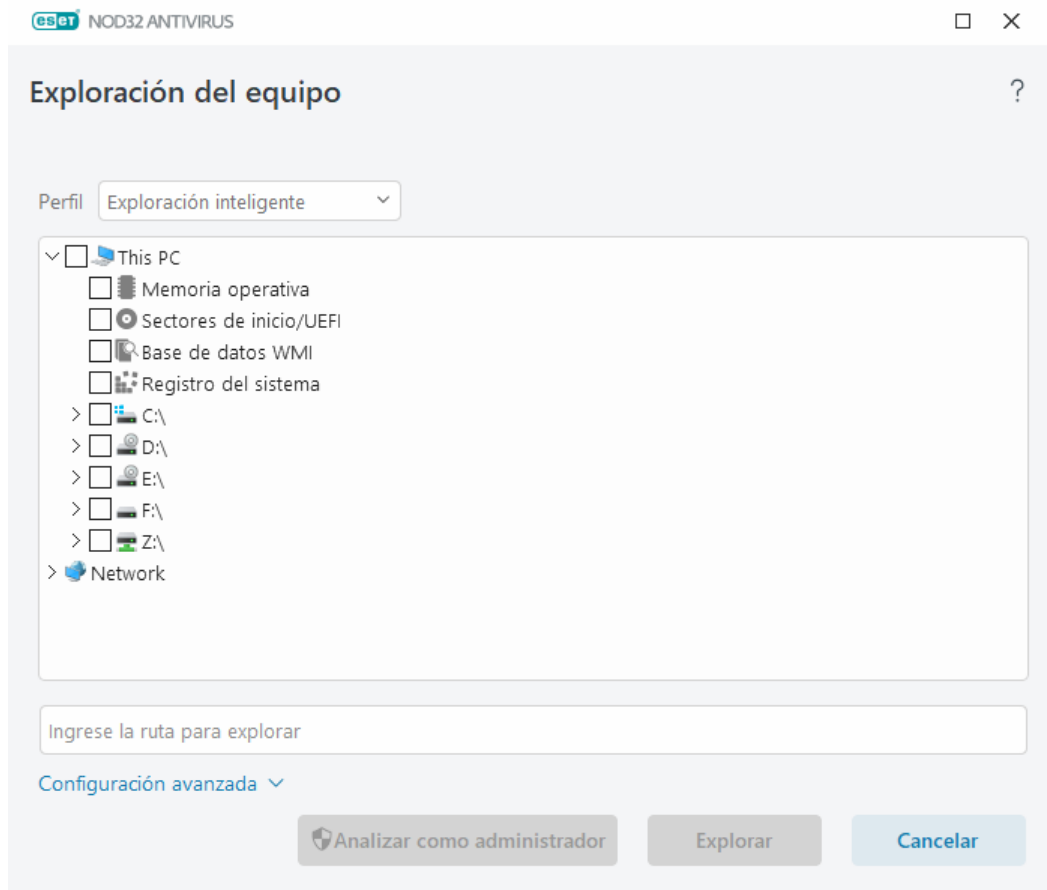
En el menú desplegable **Perfil**, puede elegir un perfil que podrá usar al explorar objetos específicos. El perfil predeterminado es **Análisis inteligente**. Hay otros tres perfiles de exploración predefinidos denominados **Exploración exhaustiva**, **Exploración del menú contextual** y **Exploración del equipo**. Estos perfiles de exploración usan diferentes [parámetros deThreatSense](#). Las opciones disponibles se describen en **Configuración avanzada (F5) > Motor de detección > Exploraciones de malware > Exploración bajo demanda > [Parámetros de ThreatSense](#)**.

La estructura de la carpeta (árbol) también contiene objetos específicos para explorar.

- **Memoria operativa** – explora todos los procesos y datos que la memoria operativa utiliza actualmente.
- **Sectores de inicio/UEFI** – explora los sectores de inicio y UEFI para detectar la presencia de virus. Lea más sobre el análisis UEFI en el [glosario](#).
- **Base de datos WMI**: explora la base de datos Windows Management Instrumentation (WMI) en su totalidad, todos los espacios de nombre, las instancias y propiedades. Busca referencias para archivos infectados o malware insertados como datos.
- **Registro del sistema**: explora el registro del sistema en su totalidad, como claves y subclaves. Busca referencias para archivos infectados o malware insertados como datos. Al desinfectar las detecciones, la referencia permanece en el registro para garantizar que no se pierdan datos importantes.

Para ir rápidamente a un objeto de exploración (archivo o carpeta), escriba su ruta en el campo de texto que aparece debajo de la estructura de árbol. La ruta distingue entre mayúsculas y minúsculas. Para incluir el objeto en la exploración, marque la casilla de verificación en la estructura de árbol.

i **Cómo programar una exploración semanal del equipo**
Para programar una tarea regular, lea el capítulo [Cómo programar una exploración semanal del equipo](#).



Puede configurar los parámetros de limpieza de la exploración en **Configuración avanzada** (F5) > **Motor de detección** > **Exploración bajo demanda** > **Parámetros de ThreatSense** > **Limpieza**. Para ejecutar una exploración sin acciones de limpieza, haga clic en **Configuración avanzada** y seleccione **Explorar sin limpieza**. El historial de la exploración se guarda en el registro de la exploración.

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

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. Use en esta opción si el usuario actual no tiene los privilegios necesarios para acceder a los archivos que desea explorar. Este botón no está disponible si el usuario actual no puede realizar operaciones UAC como administrador.

i Para ver el registro de exploración del equipo cuando finaliza una exploración, haga clic en [Mostrar registro](#).

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.

i 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. Se pueden encontrar más detalles en nuestro [artículo de la base de conocimiento](#).



Cómo programar una exploración semanal del equipo

Para programar una tarea regular, lea el capítulo [Cómo programar una exploración semanal del equipo](#).

Progreso de la exploración – la barra de progreso muestra el porcentaje de objetos ya explorados en comparación con los objetos que aún faltan explorar. El estado de progreso de la exploración proviene de la cantidad total de objetos incluidos en la exploración.

Destino – el nombre del objeto actualmente explorado y su ubicación.

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

Pausar – pone una exploración en pausa.

Reanudar – esta opción es visible cuando el progreso de la exploración está en pausa. Haga clic en **Reanudar** para proseguir con la exploración.

Detener – finaliza la exploración.

Desplazarse por el registro de exploración – si la opción está habilitada, el registro de exploración se desplazará hacia abajo automáticamente a medida que las nuevas entradas se van agregando para que sean visibles las más recientes.



Haga clic en la lupa o flecha para mostrar los detalles sobre la exploración actualmente en ejecución. Si desea ejecutar otra exploración en paralelo, haga clic en **Explorar el equipo** o **Exploraciones avanzadas > Exploración personalizada**.

The screenshot shows the ESET NOD32 ANTIVIRUS application window. The main title is 'Exploración del equipo'. On the left is a sidebar with icons for 'Vista general', 'Exploración del equipo' (highlighted with a green circle and a '1' badge), 'Actualización', 'Herramientas', 'Configuración', 'Ayuda y soporte', and 'Cuenta de ESET HOME'. The main area contains a search icon and the text 'Explore su equipo' and 'Explorar todos los discos locales y limpiar las amenazas'. To the right, there's a link for 'Exploraciones avanzadas' with a dropdown arrow. Below this is a large white box with the text 'Arrastre y suelte los archivos aquí para su análisis'. The main scan window shows 'Exploración del equipo' with a timestamp of '3/16/2023 6:52:27 AM'. It reports 'Detecciones logradas: 0' and lists a file path: 'C:\Users\User\AppData\Local\Microsoft\Edge\User D...\product_page.js'. There are pause and close buttons for the scan. Below the file path are links for 'Más información' and 'Abrir ventana de exploración'. At the bottom, a blue notification bar says 'Esto puede llevar un tiempo. Recibirá una notificación cuando finalice la exploración.' with a close button. Below the notification bar, there's a status bar with 'Progress. Protected.' and a dropdown menu for 'Acción tras la exploración' currently set to 'Sin acción'.

El menú desplegable **Acción después de la exploración** permite establecer una acción que se realice automáticamente tras finalizar una exploración:

- **Sin acción** – después de la finalización de la exploración, no se llevará a cabo ninguna acción.
- **Apagar** – el equipo se apaga después de la finalización de la exploración.
- **Reiniciar si es necesario**: el equipo se reinicia solo si es necesario para completar la limpieza de las amenazas detectadas.
- **Reiniciar** – cierra todos los programas abiertos, y reinicia el equipo luego de la finalización de la exploración.
- **Reiniciar si es necesario**: el equipo fuerza el reinicio solo si es necesario para completar la limpieza de las amenazas detectadas.
- **Forzar reinicio**: fuerza el cierre de todos los programas abiertos sin esperar la intervención del usuario y reinicia el equipo cuando finaliza la exploración.
- **Suspender**– guarda su sesión y pone el equipo en un estado de energía baja para que pueda volver a trabajar rápidamente.
- **Hibernar**– toma todo lo que se está ejecutando en la memoria RAM y lo envía a un archivo especial de su disco duro. Su equipo se apaga, pero reanudará su estado anterior la próxima vez que lo inicie.

i Las acciones **Suspender** o **Hibernar** están disponibles en función de la configuración de Activar o Hibernar del sistema operativo o de las capacidades de su equipo/computadora portátil. Tenga en cuenta que un equipo en suspensión aún es un equipo en funcionamiento. Sigue ejecutando funciones básicas y utilizando electricidad cuando el equipo funciona con la alimentación de la batería. Para preservar la vida útil de la batería, como cuando viaja fuera de su oficina, recomendamos utilizar la opción Hibernar.

La acción seleccionada comenzará tras la finalización de las exploraciones en ejecución. Cuando seleccione **Apagar** o **Reiniciar**, aparecerá un cuadro de diálogo de confirmación con una cuenta regresiva de 30 segundos (haga clic en **Cancelar** para desactivar la acción solicitada).

Registro de la exploración del equipo

Cuando termine la exploración, se abrirá el [registro de la exploración del equipo](#) con toda la información relevante relativa a la exploración en particular. El registro de la exploración proporciona información como la siguiente:

- Versión del motor de detección:
- Fecha y hora de inicio
- Lista de discos, carpetas y archivos explorados
- Nombre de la exploración programada (solo [exploración programada](#))
- Estado de la exploración
- Cantidad de objetos explorados

- Cantidad de detecciones encontradas
- Hora de finalización
- Tiempo total de exploración




Se omite el nuevo inicio de una [tarea de exploración programada del equipo](#) si se sigue ejecutando la misma tarea programada que se ejecutó anteriormente. La tarea de exploración programada omitida creará un registro de exploración del equipo con 0 objetos analizados y el estado **No se inició la exploración porque la exploración anterior todavía estaba en ejecución.**

Para buscar registros de exploración anteriores, en la [ventana principal del programa](#), seleccione **Herramientas > Archivos de registro**. En el menú desplegable, seleccione **Exploración del equipo** y haga doble clic en el registro deseado.



Para obtener más información sobre los registros "no se puede abrir", "error al abrir" o "archivo dañado", consulte el [artículo de nuestra base de conocimiento de ESET](#).

Haga clic en el ícono de la barra deslizante  **Filtrado** para abrir la ventana [Filtrado de registros](#) para reducir la búsqueda según criterios personalizados. Para ver el menú contextual, haga clic derecho en una entrada de registro específica:

Acción	Uso
Filtrar los mismos registros	Activa el filtrado de registros. El registro solo mostrará los registros del mismo tipo que el seleccionado.
Filtrar	Esta opción abre la ventana de filtrado de registros y le permite definir los criterios de entradas de registro específicas. Acceso directo: Ctrl+Shift+F
Deshabilitar el filtro	Activa la configuración del filtro. Si activa el filtro por primera vez, debe definir la configuración y se abrirá la ventana de filtrado de registros.
Deshabilitar el filtro	Desactiva el filtro (es lo mismo que hacer clic en el botón de la parte inferior).
Copiar	Copia los registros seleccionados en el portapapeles. Acceso directo: Ctrl+C
Copiar todo	Copia todos los registros en la ventana.
Exportar	Exporta los registros seleccionados del portapapeles en un archivo XML.
Exportar todo	Esta opción exporta todos los registros de la ventana en un archivo XML.
Descripción de la detección	Abre la enciclopedia de amenazas de ESET, que contiene información detallada sobre los peligros y los síntomas de la infiltración resaltada.

Exploración de malware

Es posible acceder a la sección **Exploración de malware** desde **Configuración avanzada (F5) > Motor de detección > Exploración de malware** y allí obtendrá opciones para seleccionar los parámetros de exploración. Esta sección contiene los siguientes elementos:

Perfil seleccionado – Un conjunto específico de parámetros que usa en la exploración bajo demanda. Para crear uno nuevo, haga clic en **Editar** junto a la **Lista de perfiles**. Consulte [Perfiles de exploración](#) para obtener información detallada.

Destinos de exploración: si solo desea explorar un destino específico, puede hacer clic en **Editar** junto a **Destinos de exploración** y elegir una opción del menú desplegable o puede seleccionar los objetos específicos desde la estructura (de árbol) de la carpeta. Consulte [Destinos de exploración](#) para obtener información detallada.

Parámetros de ThreatSense: en esta sección se encuentran las opciones de configuración avanzada, tales como las extensiones de los archivos que desea controlar, los métodos de detección utilizados, etc. Haga clic para abrir una pestaña con las opciones avanzadas del explorador.

Exploración en estado inactivo

Puede habilitar la exploración en estado inactivo en **Configuración avanzada** en **Motor de detección > Exploración de malware > Exploración en estado inactivo**.

Exploración en estado inactivo

Configure la barra deslizante junto a **Habilitar la exploración en estado inactivo** para habilitar esta función. Cuando el equipo está en estado inactivo, se realiza una exploración silenciosa en todas las unidades locales.

De forma predeterminada, la exploración en estado inactivo no se ejecutará cuando el equipo (portátil) está funcionando con la energía de la batería. Puede anular esta configuración al activar la barra deslizante junto a **Ejecutar incluso si el equipo recibe alimentación de la batería** en la Configuración avanzada.

Encienda el interruptor **Habilitar registro** 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**).

DetECCIÓN en estado inactivo

Consulte [Desencadenadores de detección en estado inactivo](#) para obtener una lista completa de condiciones que deben cumplirse para activar la exploración del estado inactivo.

Haga clic en [Configuración de los parámetros del motor ThreatSense](#) para modificar los parámetros de exploración (por ejemplo, los métodos de detección) para el explorador en estado inactivo.

Perfiles de exploración

Hay cuatro perfiles de exploración predefinidos en ESET NOD32 Antivirus:

- **Análisis inteligente** – Es el perfil de exploración avanzada predeterminado. El perfil de análisis inteligente utiliza la tecnología de optimización inteligente, que excluye los archivos que se encontraron limpios en una exploración anterior y que no se han modificado desde esa exploración. Esto permite tener tiempos de exploración más bajos con un impacto mínimo en la seguridad del sistema.
- **Exploración del menú contextual** – Puede iniciar la exploración del menú contextual de cualquier archivo desde el menú contextual. El perfil de exploración del menú contextual le permite definir una configuración de exploración que se utilizará cuando se ejecuta la exploración de esta manera.
- **Exploración exhaustiva** – El perfil de exploración exhaustiva no utiliza la optimización inteligente de forma predeterminada, por lo que no se excluye ningún archivo de la exploración mediante este perfil.
- **Exploración del equipo** – Es el perfil predeterminado utilizado en la exploración estándar 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 **Motor de detección > Escaneos de malware > exploración bajo demanda > Lista de perfiles**. La ventana **Administrador de perfiles** 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.

i Suponga que desea crear su propio perfil de exploración y la configuración de **Explore su equipo** es parcialmente adecuada, pero no desea explorar [empaquetadores en tiempo real](#) o [aplicaciones potencialmente no seguras](#) y, además, quiere aplicar una **Reparar siempre la detección**. Ingrese el nombre de su nuevo perfil en la ventana **Administrador de perfiles** y haga clic en **Agregar**. Seleccione su nuevo perfil desde el menú desplegable **Perfil seleccionado** y ajuste los parámetros restantes para cumplir con sus requisitos, y haga clic en **Aceptar** para guardar su nuevo perfil.

Objetos para explorar

En el menú desplegable **Objetivos de exploración**, puede seleccionar objetivos de exploración predefinidos.

- **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.
- **Selección personalizada** – cancela todas las selecciones anteriores.

La estructura de la carpeta (árbol) también contiene objetos específicos para explorar.

- **Memoria operativa** – explora todos los procesos y datos que la memoria operativa utiliza actualmente.
- **Sectores de inicio/UEFI** – explora los sectores de inicio y UEFI para detectar la presencia de virus. Lea más sobre el análisis UEFI en el [glosario](#).
- **Base de datos WMI:** explora la base de datos Windows Management Instrumentation (WMI) en su totalidad, todos los espacios de nombre, las instancias y propiedades. Busca referencias para archivos infectados o malware insertados como datos.
- **Registro del sistema:** explora el registro del sistema en su totalidad, como claves y subclaves. Busca referencias para archivos infectados o malware insertados como datos. Al desinfectar las detecciones, la referencia permanece en el registro para garantizar que no se pierdan datos importantes.

Para ir rápidamente a un objeto de exploración (archivo o carpeta), escriba su ruta en el campo de texto que aparece debajo de la estructura de árbol. La ruta distingue entre mayúsculas y minúsculas. Para incluir el objeto en la exploración, marque la casilla de verificación en la estructura de árbol.

Control de dispositivos

ESET NOD32 Antivirus proporciona el control del dispositivo automático (CD/DVD/USB/...). Este módulo permite 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 el uso de dispositivos con contenido no solicitado.

Dispositivos externos admitidos:

- Almacenamiento en disco (HDD, disco USB extraíble)
- CD/DVD
- Impresora USB
- FireWire Almacenamiento
- Bluetooth Dispositivo

- Lector de tarjeta inteligente
- Dispositivo de imagen
- Módem
- LPT/COM puerto
- Dispositivo portátil
- Todos los tipos de dispositivos

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

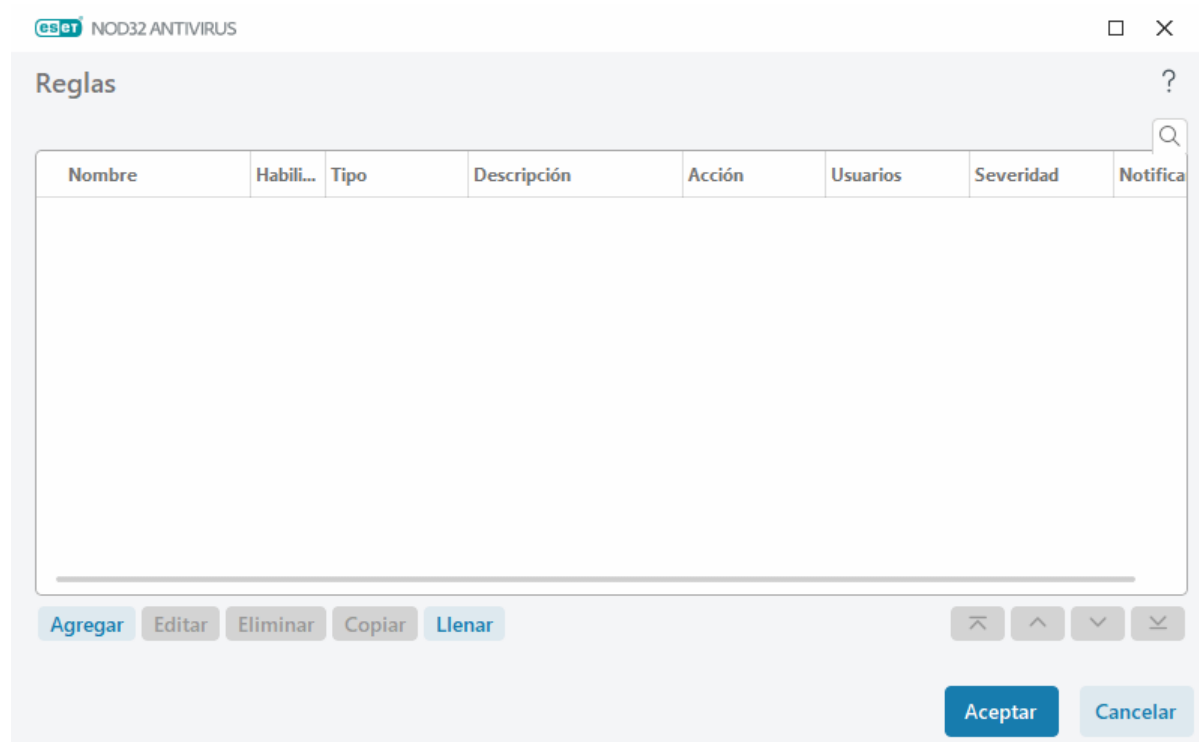
Habilitar la barra deslizante junto a **Habilitar control del dispositivo** para activar la función de Control del dispositivo en ESET NOD32 Antivirus; necesitará reiniciar su equipo para que se aplique este cambio. Una vez que el Control de dispositivos esté habilitado, podrá definir las **Reglas** en la ventana [Editor de reglas](#).

i Puede crear distintos grupos de dispositivos para los que se aplicarán reglas diferentes. También puede crear solo un grupo de dispositivos para el que se aplicará la regla con la acción **Permitir o Bloquear escritura**. Esto garantiza que el Control de dispositivos bloquee los dispositivos no reconocidos cuando se conectan a su equipo.

Si se inserta un dispositivo bloqueado por una regla existente, se visualizará una ventana de notificación y no se otorgará el acceso al dispositivo.

Editor de reglas del control del dispositivo

La ventana **Editor de reglas del 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. También consulte [Agregar reglas de control del dispositivo](#).

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.

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 desea conservar la regla.

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.


Las entradas del registro se pueden ver en la [ventana principal del programa](#) > **Herramientas** > [Archivos de registro](#).

El [Registro del control de dispositivos](#) registra todas las instancias en las que se activa el Control de dispositivos.

Dispositivos detectados

El botón **Llenar** proporciona una visión general de todos los dispositivos actualmente conectados con información acerca de: el tipo de dispositivo, el proveedor del dispositivo, el modelo y el número de serie (si está disponible).


Seleccione un dispositivo de la lista de Dispositivos detectados y haga clic en **Aceptar** para [agregar una regla de control de dispositivos](#) con información predefinida (se puede ajustar toda la configuración).

Los dispositivos en modo de baja alimentación (suspensión) están marcados con un ícono de advertencia . Para activar el botón **Aceptar** y agregar una regla para este dispositivo:

- Vuelva a conectar el dispositivo.
- Utilice el dispositivo (por ejemplo, inicie la aplicación Cámara en Windows para activar una cámara web).

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.

 NOD32 ANTIVIRUS
 ✕

Agregar regla ?

Nombre

Regla habilitada

☒

Tipo de dispositivo

Almacenamiento en disco

Acción

Permitir

Tipo de criterios

Dispositivo

Proveedor

Modelo

Número de serie

Severidad de registro

Siempre

Lista de usuarios

[Editar](#)

Notificar al usuario

☒

Aceptar

Ingresa una descripción de la regla en el campo **Nombre** para tener una mejor identificación. Haga clic en la barra deslizante junto a **Regla habilitada** para deshabilitar o habilitar 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 (Almacenamiento en disco/Dispositivo portátil/Bluetooth/FireWire/...). La información sobre los tipos de dispositivos se recopila del sistema operativo y se puede ver en el administrador de dispositivos del sistema siempre y cuando un dispositivo esté conectado al equipo. Los dispositivos de almacenamiento incluyen los discos externos o los lectores de tarjetas de memoria convencionales conectados por medio de USB o FireWire. Los lectores de tarjetas inteligentes incluyen todos los lectores de tarjetas inteligentes con un circuito integrado, tal como las tarjetas SIM o las tarjetas de autenticación. Los ejemplos de dispositivos de imágenes son los módulos de exploración o cámaras. Debido a que estos dispositivos solo proporcionan información acerca de sus acciones y no proporcionan información acerca de los usuarios, solo se pueden bloquear en forma global.

Acción

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

- **Permitir** – se permitirá el acceso total al dispositivo.
- **Bloquear** – se bloqueará el acceso al dispositivo.
- **Bloquear escritura** – solo se permitirá el acceso de lectura al dispositivo.
- **Advertir** – siempre que se conecte un dispositivo, se le notificará al usuario si está permitido/bloqueado, y

se generará una entrada de registro. Los dispositivos no se recuerdan, pero sin embargo se mostrará una notificación durante las conexiones posteriores del mismo dispositivo.

Tenga en cuenta que no todas las Acciones (permisos) están disponibles para todos los tipos de dispositivos. Si es un tipo de dispositivo de almacenamiento, las cuatro Acciones estarán disponibles. Para los dispositivos de no almacenamiento, solo hay tres Acciones disponibles (por ejemplo, **Bloquear escritura** no está disponible para Bluetooth, por lo que los dispositivos Bluetooth solo se pueden permitir, bloquear o advertir).

Tipo de criterios

Seleccione **Grupo de dispositivos** o **Dispositivo**.

A continuación, se muestran parámetros adicionales que se pueden usar para ajustar las reglas de diferentes dispositivos. Todos los parámetros distinguen entre mayúsculas y minúsculas y admiten comodines (*, ?):

- **Proveedor** – filtre por nombre o ID 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.



Si no se definen estos parámetros, la regla ignorará estos campos mientras realiza la coincidencia. Los parámetros de filtrado de los campos de texto distinguen entre mayúsculas y minúsculas y admiten comodines (un signo de interrogación (?) representa un carácter único, mientras que un asterisco (*) representa una cadena de cero o más caracteres).



Para ver información sobre un dispositivo, cree una regla para ese tipo de dispositivo, conecte el dispositivo a su equipo, y luego verifique los detalles del dispositivo en el [Registro del control de dispositivos](#).

Severidad de registro

ESET NOD32 Antivirus guarda todos los sucesos importantes en un archivo de registro, que se puede ver directamente desde el menú principal. Haga clic en **Herramientas > Archivos de registro** y luego seleccione **Control del dispositivo** en el menú desplegable **Registro**.

- **Siempre** – registra todos los eventos.
- **Diagnóstico** – registra la información necesaria para ajustar el programa.
- **Información** – registra los mensajes de información, incluidos los mensajes de actualizaciones correctas, y todos los historiales antes mencionados.
- **Advertencia** – registra los errores críticos y mensajes de advertencia.
- **Ninguno** – no se realizará registro alguno.

Lista de usuarios

Las reglas se pueden limitar a ciertos usuarios o grupos de usuarios al agregarlos a la Lista de usuarios haciendo clic en **Editar** junto a **Lista de usuarios**.

- **Agregar** – abre los **Tipos de objetos: Usuarios o grupos** que permite seleccionar los usuarios deseados.
- **Quitar** – quita el usuario seleccionado del filtro.

Limitaciones de la lista de usuarios

La lista de usuarios no puede definirse para reglas con [tipos de dispositivos](#) específicos:



- Impresora USB
- Dispositivo Bluetooth
- Lector de tarjeta inteligente
- Dispositivo de imagen
- Módem
- Puerto LPT/COM

Notificar al usuario: Si se inserta un dispositivo bloqueado por una regla existente, se visualizará una ventana de notificación.

Grupos de dispositivos



El dispositivo conectado a su equipo puede presentar un riesgo de seguridad.

La ventana Grupos de dispositivos se divide en dos partes. La parte derecha de la ventana contiene una lista de los dispositivos que pertenecen al grupo respectivo, y la parte izquierda de la ventana contiene los grupos creados. Seleccione un grupo para mostrar los dispositivos en el panel derecho.

Cuando abre la ventana Grupos de dispositivos y selecciona un grupo, puede agregar o eliminar dispositivos de la lista. Otra forma de agregar dispositivos al grupo es importarlos desde un archivo. Como alternativa, puede hacer clic en el botón **Llenar**, y todos los dispositivos conectados a su equipo se incluirán en una lista en la ventana **Dispositivos detectados**. Seleccione un dispositivo de la lista que se completó para agregarlo al grupo con clic en **ACEPTAR**.

Elementos de control

Agregar – puede agregar un grupo si escribe su nombre o un dispositivo a un grupo existente, en función de la parte de la ventana en la que haga clic en el botón.

Editar – le permite modificar el nombre del grupo seleccionado o los parámetros del dispositivo (proveedor, modelo, número de serie).

Eliminar – elimina el grupo o el dispositivo seleccionado, dependiendo de la parte de la ventana en la que haya hecho clic en el botón.

Importar – importa una lista de dispositivos desde un archivo de texto. Para importar dispositivos desde un archivo de texto, se requiere el formato correcto:

- Cada dispositivo se inicia en una línea nueva.
- **Proveedor, Modelo y Serie** deben estar presentes para cada dispositivo y separados con una coma.

✓ Este es un ejemplo de contenido del archivo de texto:
Kingston,DT 101 G2,001CCE0DGRFC0371
04081-0009432,USB2.0 HD WebCam,20090101

Exportar – exporta una lista de dispositivos hacia un archivo.

El botón **Llenar** proporciona una visión general de todos los dispositivos actualmente conectados con información acerca de: el tipo de dispositivo, el proveedor del dispositivo, el modelo y el número de serie (si está disponible).

Agregar dispositivo

Haga clic en **Agregar** en la ventana derecha para agregar un dispositivo a un grupo existente. A continuación, se muestran parámetros adicionales que se pueden usar para ajustar las reglas de diferentes dispositivos. Todos los parámetros distinguen entre mayúsculas y minúsculas y admiten comodines (*, ?):

- **Proveedor** – filtre por nombre o ID 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.
- **Descripción**— descripción del dispositivo para una mejor organización.

i Si no se definen estos parámetros, la regla ignorará estos campos mientras realiza la coincidencia. Los parámetros de filtrado de los campos de texto distinguen entre mayúsculas y minúsculas y admiten comodines (un signo de interrogación [?] representa un carácter único, mientras que un asterisco [*] representa una cadena de cero o más caracteres).

Haga clic en **Aceptar** para guardar los cambios. Haga clic en **Cancelar** para salir de la ventana **Grupos de dispositivos** sin guardar los cambios.

i Tras crear un grupo de dispositivos, tendrá que [agregar una nueva regla de control del dispositivo](#) para el grupo de dispositivos creado y elegir la acción que se debe tomar.

Tenga en cuenta que no todas las Acciones (permisos) están disponibles para todos los tipos de dispositivos. Las cuatro acciones están disponibles si se trata de un dispositivo de tipo almacenamiento. Para los dispositivos de no almacenamiento, solo hay tres acciones disponibles (por ejemplo, **Bloquear escritura** no está disponible para Bluetooth; por lo tanto, los dispositivos Bluetooth solo se pueden permitir, bloquear o advertir).

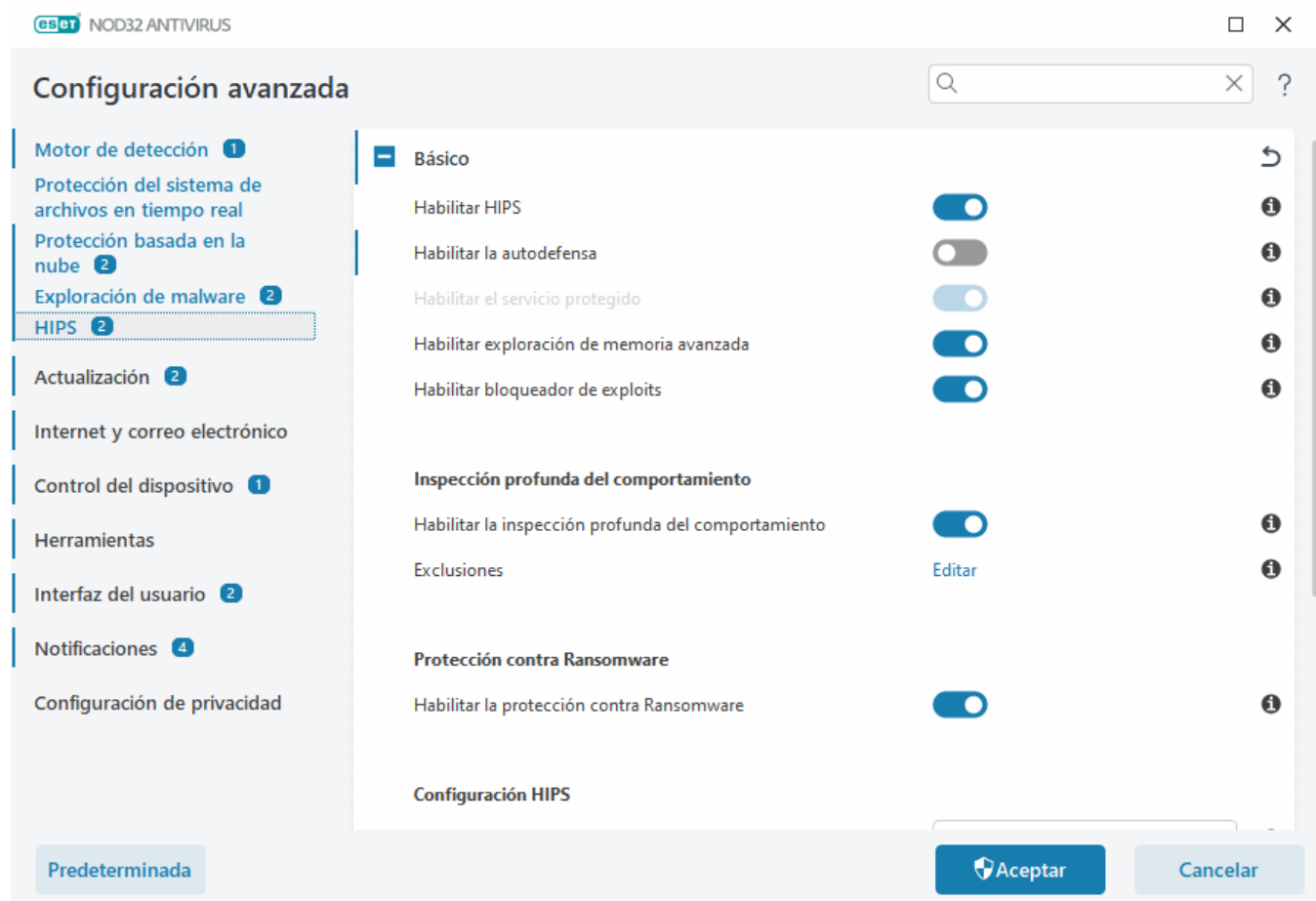
Sistema de prevención de intrusiones basado en el host (HIPS)

! Las modificaciones de la configuración del HIPS deben realizarse únicamente por un usuario experimentado. La configuración incorrecta de HIPS puede llevar a la inestabilidad del sistema.

El **Sistema de prevención de intrusiones basado en el host (HIPS)** protege su sistema contra 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. El HIPS es independiente 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 puede encontrar en **Configuración avanzada (F5) > Motor de detección > HIPS > Básico**. El estado de HIPS (habilitado/deshabilitado) se muestra en [la ventana principal del programa](#) de ESET NOD32 Antivirus, en **Configuración > Protección del equipo**.



Básico

Habilitar HIPS: HIPS se habilita de manera predeterminada en ESET NOD32 Antivirus. Al desactivar HIPS, se desactivan el resto de las características de HIPS, como Bloqueador de exploits.

Habilitar la autodefensa: ESET NOD32 Antivirus utiliza la tecnología incorporada de **autodefensa** como parte de HIPS para evitar que el software malicioso corrompa o deshabilite su protección antivirus y antispyware. La autodefensa protege al sistema crucial y los procesos de ESET, las claves de registro y los archivos de ser manipulados.

Habilitar el servicio protegido: habilita la protección para ESET Service (ekrn.exe). Cuando está habilitado, el servicio se inicia como un proceso de Windows protegido para defender contra ataques de malware.

Habilitar explorador de memoria avanzado: trabaja en conjunto con el Bloqueador de exploits para fortalecer la protección contra el malware diseñado para evadir la detección por los productos antimalware con el uso de ofuscación o cifrado. La exploración de memoria avanzada está habilitada en forma predeterminada. Lea más información sobre este tipo de protección en el [glosario](#).

Habilitar 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. El bloqueador de exploits está habilitado en forma predeterminada. Lea más información sobre este tipo de protección en el [glosario](#).

Inspección profunda del comportamiento

Habilitar inspección profunda del comportamiento: otra capa de protección que es parte de la función de HIPS. Esta extensión de HIPS analiza el comportamiento de todos los programas que se ejecutan en su equipo y le advierte si el comportamiento de los procesos es malicioso.

[Las exclusiones de HIPS para la inspección profunda del comportamiento](#) permiten excluir procesos de la exploración. Para asegurarse de que todos los objetos se exploren en busca de amenazas, recomendamos únicamente crear exclusiones cuando sea absolutamente necesario.

Escudo contra ransomware

Habilitar protección contra ransomware: es otra capa de protección que funciona como parte de la función HIPS. Debe tener habilitado el sistema de reputación de ESET LiveGrid® para que funcione la protección de ransomware. [Lea más información sobre este tipo de protección](#).

Habilitar Intel® Threat Detection Technology – ayuda a detectar ataques de ransomware mediante el uso de la única telemetría de CPU Intel para aumentar la eficacia de detección, reducir las alertas de falso positivo y ampliar la visibilidad para capturar técnicas de evasión avanzadas. Consulte los [procesadores compatibles](#).

Configuración HIPS

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

Modo de filtrado	Descripción
Modo automático	Las operaciones están habilitadas, excepto las que se encuentran bloqueadas por las 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	Bloquea todas las operaciones que no están definidas por una regla específica que las permite.
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 HIPS , pero su prioridad es inferior a la de las reglas creadas manualmente o en el modo automático. Cuando selecciona el Modo de aprendizaje en el menú desplegable Modo de filtrado , la configuración del modo de aprendizaje finalizará cuando esté disponible. Seleccione el intervalo de tiempo durante el que desea activar el modo de aprendizaje; el tiempo máximo es de 14 días. Cuando el tiempo especificado haya pasado, se le solicitará que edite las reglas creadas por HIPS mientras estuvo en el modo de aprendizaje. También puede elegir un modo de filtrado diferente, o posponer la decisión y continuar utilizando el modo de aprendizaje.

Modo configurado después del vencimiento del modo de aprendizaje: seleccione el modo de filtrado que se usará después del vencimiento del modo de aprendizaje. Después del vencimiento, la opción **Preguntar al usuario** requerirá privilegios administrativos para realizar un cambio en el modo de filtrado de HIPS.

El sistema HIPS monitorea los sucesos dentro del sistema operativo y reacciona consecuentemente en función de

reglas similares a las que usa el firewall. Haga clic en **Editar** junto a **Reglas** para abrir el editor de **reglas HIPS**. En la ventana de reglas HIPS, puede seleccionar, agregar, editar o quitar reglas. Para más información sobre la creación de reglas y las operaciones de HIPS, consulte [Cómo editar una regla de HIPS](#).

Ventana interactiva de HIPS

La ventana de notificación de HIPS le permite crear una regla en función de cualquier acción nueva que el HIPS detecte para, posteriormente, definir las condiciones mediante las cuales se permitirá o denegará dicha acción.

Las reglas creadas a partir de la ventana de notificación se consideran equivalentes a las creadas manualmente. En consecuencia, la regla creada desde una ventana de diálogo puede ser menos específica que la que activa la ventana de diálogo. Esto significa que, después de crear una regla en el cuadro de diálogo, la misma operación puede activar la misma ventana. Para más información, consulte [Prioridad para reglas de HIPS](#).

Si la acción predeterminada para una regla está configurada en **Preguntar siempre**, una ventana de diálogo aparecerá cada vez que se active la regla. Puede elegir **Denegar** o **Permitir** la operación. Si no elige una acción en el tiempo dado, se seleccionará una nueva acción en función de las reglas.

Recordar hasta salir de la aplicación hace que la acción (**Permitir/Denegar**) se utilice hasta que haya un cambio de reglas o del modo de filtrado, una actualización de módulo del HIPS o un reinicio del sistema. Las reglas temporales se eliminarán después de cualquiera de estas tres acciones.

La opción **Crear regla y recordar permanentemente** creará una nueva regla HIPS que puede modificarse más adelante en la sección [Administración de reglas del HIPS](#) (requiere de privilegios de administración).

Haga clic en **Detalles** al pie para ver qué aplicación activa la operación, cuál es la reputación del archivo o qué tipo de operación se le pide autorizar o rechazar.

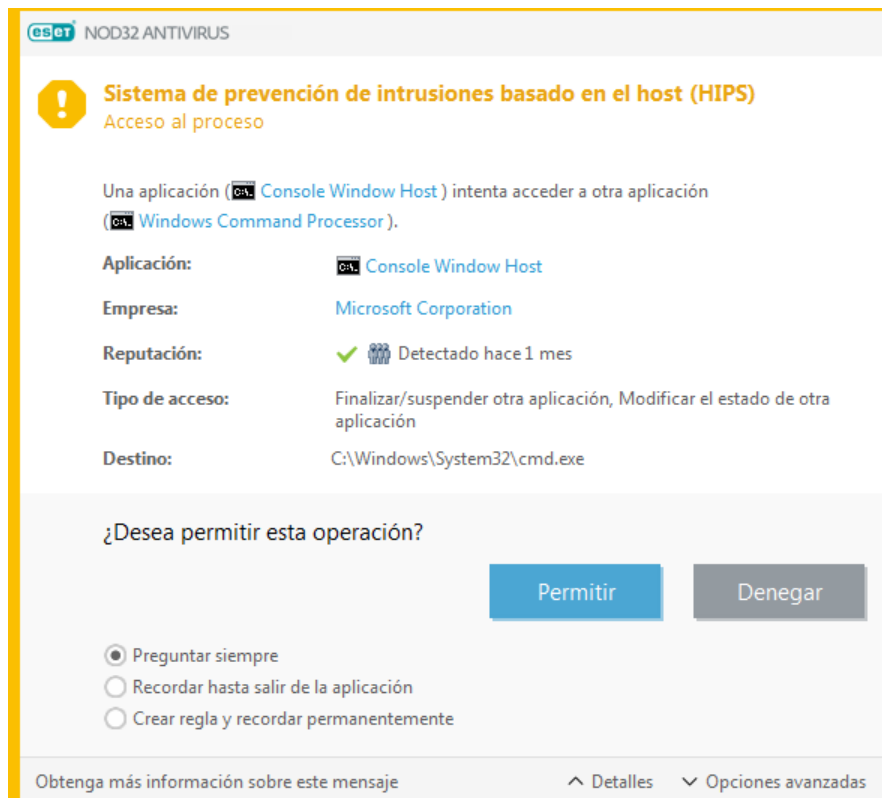
Para acceder a las configuraciones de parámetros de reglas más detallados, haga clic en **Opciones avanzadas**. Las opciones de abajo se encuentran disponibles si elige **Crear regla y recordar permanentemente**:

- **Crear una regla válida solo para esta aplicación:** si quita la marca de verificación de esta casilla, se creará la regla para todas las aplicaciones de origen.
- **Solo para la operación:** elija el archivo de la regla/la aplicación/la operación de registro. [Consulte las descripciones de todas las operaciones del HIPS](#).
- **Solo para el destino:** elija el archivo de la regla/la aplicación/el destino del registro.

¿Notificaciones del HIPS interminables?

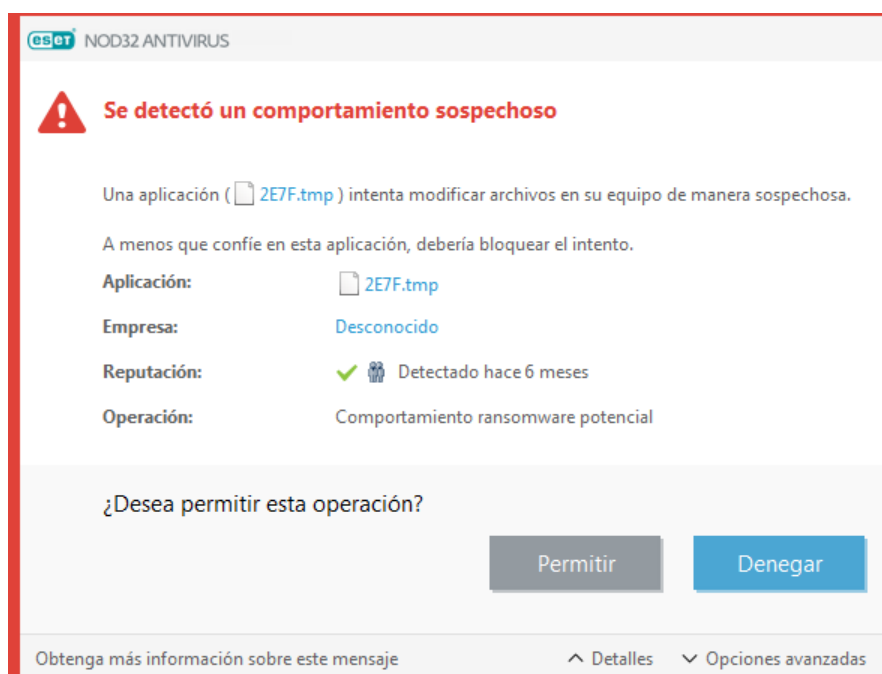


Para evitar que aparezcan las notificaciones, cambie el modo de filtrado a **Modo automático** en **Configuración avanzada (F5) > Motor de detección > HIPS > Básico**.



Se detectó un comportamiento ransomware potencial

Esta ventana interactiva aparecerá cuando se detecta un comportamiento ransomware potencial. Puede elegir **Denegar** o **Permitir** la operación.



Haga clic en **Detalles** para ver los parámetros específicos de detección. La ventana de diálogo le permite **Enviar el archivo para su análisis** o **Excluirlo de la detección**.

! Para que la [protección contra Ransomware](#) funcione correctamente, ESET LiveGrid® debe estar habilitado.

Administración de reglas del HIPS

Una lista de reglas definidas por el usuario y agregadas automáticamente desde el sistema HIPS. Encontrará más detalles sobre la creación de reglas y las operaciones del sistema HIPS en el capítulo [Configuración de reglas HIPS](#). También consulte [Principio general de HIPS](#).

Columnas

Regla – nombre de la regla definido por el usuario o elegido automáticamente.

Habilitada: desactive la barra deslizante si desea conservar la regla en la lista, pero no quiere usarla.

Acción – la regla especifica una acción; **Permitir**, **Bloquear** o **Preguntar**; que se deberá llevar a cabo bajo las condiciones adecuadas.

Orígenes – la regla solo se utilizará si una aplicación o las aplicaciones accionan el evento.

Destinos – la regla solo se utilizará si la operación se relaciona con un archivo, una aplicación o una entrada de registro específicos.

Severidad de registro – si activa esta opción, la información sobre esta regla se incluirá en el [registro de HIPS](#).

Notificar – si se acciona un evento, aparece una ventana de notificación emergente pequeña en la esquina inferior derecha.

Elementos de control

Agregar – crea una regla nueva.

Editar – le permite editar las entradas seleccionadas.

Quitar – quita las entradas seleccionadas.

Prioridad para reglas del HIPS

No hay opciones para ajustar el nivel de prioridad de las reglas del HIPS utilizando los botones arriba/abajo.

- Todas las reglas que usted cree tienen la misma prioridad
- Cuanto más específica la regla, mayor la prioridad (por ejemplo, la regla para una aplicación específica tiene mayor prioridad que la regla para todas las aplicaciones).
- A nivel interno, HIPS contiene reglas de prioridad elevada a las que usted no puede acceder (por ejemplo, no puede sobrescribir las reglas definidas de autodefensa)
- No se aplicará una regla que usted cree y que podría inmovilizar el sistema operativo (tendrá la prioridad más baja)

Editar una regla HIPS

Consulte primero la [administración de reglas HIPS](#).

Nombre de la regla – nombre de la regla definido por el usuario o elegido automáticamente.

Acción – especifica una acción; **Permitir**, **Bloquear** o **Preguntar**; que se deberá llevar a cabo si se cumple con las condiciones.

Operaciones que afectan – debe seleccionar el tipo de operación a la que se aplicará la regla. La regla solo se utilizará para este tipo de operación y para el destino seleccionado.

Habilitada – deshabilite la barra deslizante si desea conservar la regla en la lista pero no quiere aplicarla.

Severidad de registro – si activa esta opción, la información sobre esta regla se incluirá en el [registro de HIPS](#).

Notificar al usuario – si se acciona un evento, aparece una ventana de notificación emergente pequeña en la esquina inferior derecha.

La regla está compuesta por partes que describen las condiciones que la accionan:

Aplicaciones de origen—la regla solo se utilizará si esta aplicación o estas aplicaciones accionan el evento. Seleccione **Aplicaciones específicas** en el menú desplegable y haga clic en **Agregar** para agregar archivos nuevos, o puede seleccionar **Todas las aplicaciones** en el menú desplegable para agregar todas las aplicaciones.

Archivos de destino: la regla solo se usará si la operación está relacionada con este destino. Seleccione **Archivos específicos** en el menú desplegable y haga clic en **Agregar** para agregar carpetas o archivos nuevos, o puede seleccionar **Todos los archivos** en el menú desplegable para agregar todos los archivos.

Aplicaciones— la regla solo se utilizará si la operación está relacionada con este destino. Seleccione **Aplicaciones específicas** en el menú desplegable y haga clic en **Agregar** para agregar carpetas o archivos nuevos, o puede seleccionar **Todas las aplicaciones** en el menú desplegable para agregar todas las aplicaciones.

Entradas de registro— la regla solo se utilizará si la operación está relacionada con este destino. Seleccione **Entradas específicas** en el menú desplegable y haga clic en **Agregar** para ingresarlas en forma manual o haga clic en **Abrir el editor de registros** para seleccionar una clave del Registro. Además, puede seleccionar **Todas las entradas** en el menú desplegable para agregar todas las aplicaciones.



Algunas operaciones de reglas específicas predefinidas por el sistema HIPS no se pueden bloquear y están permitidas en forma predeterminada. Además, el sistema HIPS no monitorea todas las operaciones del sistema. HIPS monitorea las operaciones que se pueden considerar no seguras.

Descripciones de las operaciones más importantes:

Operaciones de archivos

- **Eliminar el archivo** – la aplicación pide permiso para eliminar el archivo de destino.
- **Escribir en el archivo** – la aplicación pide permiso para escribir en el archivo de destino.
- **Acceso directo al disco** – la aplicación está intentando leer el disco o escribir en él de una forma que no es

la estándar, lo que evade los procedimientos comunes de Windows. Esto puede provocar que se modifiquen los archivos sin haber aplicado las reglas correspondientes. Esta operación puede haberse generado por malware que intenta evadir la detección, un software de creación de copias de seguridad que intenta hacer una copia exacta del disco, o un administrador de particiones que intenta reorganizar los volúmenes de disco.

- **Instalar enlace global** – se refiere al llamado de la función SetWindowsHookEx de la biblioteca MSDN.
- **Cargar controlador** – instalación y carga de controladores en el sistema.

Operaciones de la aplicación

- **Depurar otra aplicación** – adjuntar un depurador al proceso. Cuando se depura una aplicación, es posible ver y modificar muchos detalles de su conducta, así como acceder a sus datos.
- **Interceptar eventos desde otra aplicación** – la aplicación de origen está intentando capturar eventos dirigidos a una aplicación específica (por ejemplo, un keylogger que intenta capturar eventos del navegador).
- **Finalizar/suspender otra aplicación** – suspende, reanuda o termina un proceso (se puede acceder directamente desde el Explorador de procesos o el Panel de procesos).
- **Iniciar una aplicación nueva** – inicio de aplicaciones o procesos nuevos.
- **Modificar el estado de otra aplicación** – la aplicación de origen está intentando escribir en la memoria de las aplicaciones de destino o ejecutar un código en su nombre. Esta funcionalidad puede resultar útil para proteger una aplicación esencial mediante su configuración como aplicación de destino en una regla que bloquee el uso de dicha operación.

Operaciones de registros

- **Modificar la configuración del inicio** – cualquier cambio en la configuración que defina qué aplicaciones se ejecutarán durante el inicio de Windows. Pueden encontrarse, por ejemplo, al buscar la clave Run en el registro de Windows.
- **Eliminar del registro** – eliminar una clave de registro o su valor.
- **Volver a nombrar la clave de registro** – volver a nombrar claves de registros.
- **Modificar el registro** – crear nuevos valores de claves de registro, modificar los valores existentes, cambiar datos de lugar en el árbol de la base de datos o configurar derechos de usuarios o de grupos para las claves de registro.



Puede usar caracteres globales con ciertas restricciones al ingresar un destino. En lugar de usar una clave específica, se puede usar el símbolo * (asterisco) en las rutas del registro. Por ejemplo, *HKEY_USERS*\software* puede significar *HKEY_USER.default\software* pero no *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895.default\software*. *HKEY_LOCAL_MACHINE\system\ControlSet** no es una ruta válida a una clave de registro. Una ruta a una clave de registro que contenga * define “esta ruta o cualquier ruta de cualquier nivel que se encuentre después de ese símbolo”. Esta es la única manera de usar caracteres globales para archivos de destino. Primero se evaluará la parte específica de la ruta y luego la ruta que sigue al carácter global (*).

 Si crea una regla muy genérica, se mostrará la advertencia sobre este tipo de regla.

En el siguiente ejemplo, mostraremos cómo restringir las conductas no deseadas de una aplicación específica:

1. Póngale un nombre a la regla y seleccione **Bloquear** (o **Preguntar** si prefiere elegir más adelante) desde el menú desplegable **Acción**.
2. Habilite la barra deslizante junto a **Notificar al usuario** para mostrar una notificación cada vez que se aplique una regla.
3. Seleccione [al menos una operación](#) en la sección **Operaciones que afectan** para la cual se aplicará la regla.
4. Haga clic en **Siguiente**.
5. En la ventana **Aplicaciones de origen**, seleccione **Aplicaciones específicas** en el menú desplegable para aplicar la nueva regla a todas las aplicaciones que intenten llevar a cabo alguna de las operaciones de aplicaciones seleccionadas en las aplicaciones que especificó.
6. Haga clic en **Agregar** y, luego, en ... para elegir una ruta para una aplicación específica y, luego, presione **Aceptar**. Añada más aplicaciones si lo prefiere.
Por ejemplo: *C:\Program Files (x86)\Untrusted application\application.exe*
7. Seleccione la operación **Escribir en el archivo**.
8. Seleccione **Todos los archivos** del menú desplegable. De esta manera, se bloquearán los intentos por escribir archivos por parte de la(s) aplicación(es) seleccionada(s) en el paso anterior.
9. Haga clic en **Finalizar** para guardar la regla nueva.

eset NOD32 ANTIVIRUS ✕

Configuraciones de reglas HIPS ?

Nombre de regla

Acción

Operaciones que afectan

Archivos de destino ☐

Aplicaciones ☐

Entradas de registro ☐

Habilitado ☒

Severidad de registro

Notificar al usuario ☐

Atrás Siguiente Cancelar

Agregado de una aplicación/ruta de registro para HIPS

Para seleccionar la ruta al archivo de una aplicación, haga clic en la opción Cuando seleccione una carpeta, se incluirán todas las aplicaciones que se encuentren en esta ubicación.

La opción **Abrir el editor de registros** iniciará el editor del registro de Windows (regedit). Al agregar una ruta de registro, ingrese la ubicación correcta en el campo **Valor**.

Ejemplos de la ruta al archivo o registro:

- *C:\Archivos de programa\Internet Explorer\iexplore.exe*
- *HKEY_LOCAL_MACHINE\system\ControlSet*

Configuración avanzada de HIPS

Las opciones que se muestran a continuación resultan útiles para la depuración y el análisis de la conducta de una aplicación.

[Controladores siempre permitidos para cargar](#) – los controladores seleccionados siempre tienen permitido cargar independientemente del modo de filtrado configurado, a menos que se bloquee explícitamente por una regla de usuario.

Registrar todas las operaciones bloqueadas: todas las operaciones bloqueadas se escribirán en el registro de HIPS. Utilice esta característica solo cuando se resuelvan problemas o lo solicite el soporte técnico de ESET, ya que puede generar un archivo de registro muy grande y ralentizar su equipo.

Notificar cuando ocurran cambios en las aplicaciones de inicio – muestra una notificación del escritorio cada vez que se agrega o quita una aplicación del inicio del sistema.

Controladores siempre permitidos para cargar

Los controladores que se muestran en esta lista siempre tendrán permitido cargar independientemente del modo de filtrado de HIPS, a menos que se bloquee explícitamente por una regla de usuario.

Agregar – agrega un controlador nuevo.

Editar – edita un controlador seleccionado.

Quitar – elimina un controlador de la lista.

Restablecer – vuelve a cargar un conjunto de controladores del sistema.


i Haga clic en **Restablecer** si no desea que se incluyan los controladores que ha agregado en forma manual. Esto puede ser útil si ha agregado varios controladores y no puede eliminarlos de la lista en forma manual.

i Tras la instalación, la lista de controladores está vacía. ESET NOD32 Antivirus rellena la lista automáticamente con el correr del tiempo.

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 de alerta y notificaciones 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.

Puede habilitar o deshabilitar el Modo de juego en la [ventana principal del programa](#) en **Configuración >**

Protección del equipo con un clic en  junto a **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 aparecerá en naranja el **Modo de juego activo**.

Active **Habilitar el modo de juego al ejecutar aplicaciones en modo de pantalla completa automáticamente** en **Configuración avanzada (F5) > Herramientas > Modo de juego** para que este modo inicie cada vez que inicie una aplicación en pantalla completa y se detenga después de salir de la aplicación.

Active **Deshabilitar el modo de juego automáticamente después** para definir el tiempo que debe transcurrir para que el modo de juego se deshabilite automáticamente.

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 del motor de detección. 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 cambiar la configuración, vaya 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](#).

Verificación de archivos de inicio automático

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

El menú desplegable **Escanear objetivo** especifica la profundidad de la exploración para los archivos que se ejecutan al inicio del sistema en base a un algoritmo sofisticado. Los archivos se organizan en orden descendente de acuerdo con los siguientes criterios:

- **Todos los archivos registrado** (la mayoría de los archivos escaneados)
- **Archivos poco usados**
- **Archivos usados habitualmente**
- **Archivos de uso frecuente**
- **Solo los archivos más frecuentemente utilizados** (los archivos menos explorados)

También se incluyen dos grupos específicos:

- **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, dll 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 los archivos que se exploran son fijas para cada grupo anterior. Si elige una profundidad inferior de exploración de los archivos ejecutados al iniciar el sistema, los archivos no explorados se explorarán cuando se abren o ejecutan.


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

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

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 Microsoft ActiveX. 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 manejan un alto volumen de documentos de Microsoft Office.

Para activar la protección de documentos, abra la **Configuración avanzada (F5) > Motor de detección > Exploración de malware > Protección de documentos** y haga clic en la barra deslizante junto a **Habilitar la protección de documentos**.

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

Exclusiones

Las **Exclusiones** permiten excluir [objetos](#) del motor de detección. Para asegurarse de que todos los objetos se exploren, recomendamos crear únicamente exclusiones cuando sea absolutamente necesario. Las situaciones donde es posible que necesite excluir un objeto pueden incluir la exploración de las entradas de una base de datos grande que podría reducir la velocidad de su equipo durante una exploración o software que entra en conflicto con la exploración.

[Exclusiones de rendimiento](#) – permiten excluir archivos y carpetas de la exploración. También son útiles para excluir la exploración a nivel de archivos de aplicaciones de juegos o cuando provoca un comportamiento anormal del sistema o para obtener un mejor rendimiento.

Las [Exclusiones de la detección](#) permiten excluir objetos de la detección por el nombre, ruta o hash de la detección. Las exclusiones de la detección no excluyen archivos y carpetas de la exploración como las exclusiones de rendimiento. Las exclusiones de la detección excluyen objetos solo cuando el motor de detección los detecta y existe una regla pertinente en la lista de exclusiones.

No debe confundirse con otros tipos de exclusiones:

- [Exclusiones de procesos](#) – Todas las operaciones de archivos atribuidas a procesos de aplicaciones excluidas se excluyen de la exploración (podría ser necesario para mejorar la velocidad de la copia de seguridad y la disponibilidad del servicio).
- [Extensiones de archivo excluidas](#)
- [Exclusiones de HIPS](#)

- [Filtro de exclusión para la protección basada en la nube](#)

Exclusiones de rendimiento

Las exclusiones de rendimiento permiten excluir archivos y carpetas de la exploración.

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

Puede añadir archivos y carpetas en la lista de exclusiones para que se excluyan de la exploración desde **Configuración avanzada (F5) > Motor de detección > Exclusiones > Exclusiones de rendimiento > Editar**.

i No debe confundirse con [Exclusiones de detección](#), [Extensiones de archivo excluidas](#), [Exclusiones de HIPS](#) o [Exclusiones de procesos](#).

Para [excluir un objeto](#) (ruta: archivo o carpeta) de la exploración, haga clic en **Agregar** e ingrese la ruta aplicable o selecciónelo en la estructura de árbol.

i 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.

Elementos de control

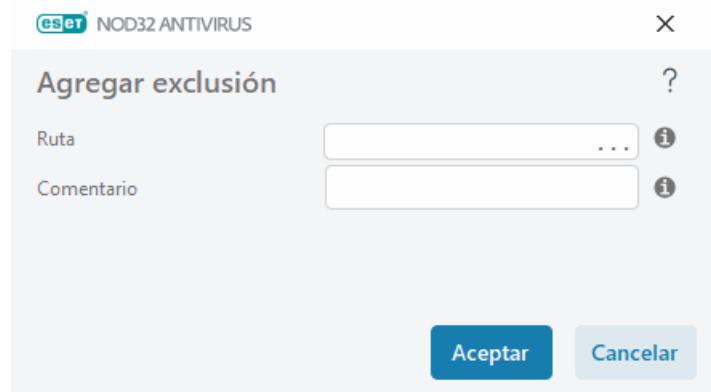
- **Agregar** – excluye objetos de la detección.
- **Editar** – le permite editar las entradas seleccionadas.
- **Eliminar**: quita las entradas seleccionadas (CTRL + clic para seleccionar múltiples entradas).

Agregar o editar exclusión de rendimiento

Esta ventana de diálogo excluye una ruta específica (archivo o directorio) para este equipo.

Seleccione la ruta o introdúzcala manualmente

- i** Para elegir una ruta que corresponda, haga clic en ... en el campo **Ruta**.
Al escribir manualmente, vea más [ejemplos de formatos de exclusiones](#) a continuación.



Puede usar comodines para excluir un grupo de archivos. Un signo de interrogación (?) representa un carácter único, mientras que un asterisco (*) representa una cadena de cero o más caracteres.

Formato de las exclusiones

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



Ejemplos:

- C:\Tools*: la ruta debe terminar con la barra diagonal inversa (\) y el asterisco (*) para indicar que es una carpeta y que se excluirá todo el contenido de la carpeta (archivos y subcarpetas).
- C:\Tools*.*: el mismo comportamiento que C:\Tools*
- C:\Tools– La carpeta Tools no se excluirá.. Desde el punto de vista del módulo de exploración, Tools también puede ser un nombre de archivo.
- C:\Tools*.dat – Excluirá archivos .dat en la carpeta Tools.
- C:\Tools\sg.dat – Excluirá este archivo en particular ubicado en la ruta exacta.

Variables del sistema en las exclusiones

Puede usar variables del sistema como %PROGRAMFILES% para definir las exclusiones de exploración.

- Para excluir la carpeta Archivos de programa con esta variable del sistema, use la ruta %PROGRAMFILES%* (recuerde que debe agregar barra diagonal inversa al final de la ruta) cuando agregue exclusiones.
- Si desea excluir todos los archivos y carpetas en un subdirectorio de %PROGRAMFILES%, use la ruta %PROGRAMFILES%\Directorio_excluido*



[Expandir la lista de variables del sistema compatibles](#)

Las siguientes variables pueden usarse en el formato de exclusión de ruta:

- %ALLUSERSPROFILE%
- %COMMONPROGRAMFILES%
- %COMMONPROGRAMFILES(X86)%
- %COMSPEC%
- %PROGRAMFILES%
- %PROGRAMFILES(X86)%
- %SystemDrive%
- %SystemRoot%
- %WINDIR%
- %PUBLIC%

No se admiten las variables del sistema específicas del usuario (p. ej., %TEMP% o %USERPROFILE%) ni las variables de entorno (p. ej., %PATH%).

No se admiten comodines en el medio de una ruta

Es posible que el uso de comodines en el medio de la ruta (p. ej., C:\Tools*\Data\file.dat) funcione, pero no se admite oficialmente para las exclusiones de rendimiento.

Cuando usa [Exclusiones de la detección](#), no hay restricciones para el uso de comodines en el medio de la ruta.

Orden de exclusiones

- No hay opciones para ajustar el nivel de prioridad de las exclusiones utilizando los botones de arriba/abajo.



- Cuando la primera regla aplicable es encontrada por el explorador, la segunda regla aplicable no será evaluada.
- Mientras menos reglas haya, mejor es el desempeño del explorador.
- Evite la creación de reglas concurrentes.

Formato de las exclusiones de ruta

Puede usar comodines para excluir un grupo de archivos. Un signo de interrogación (?) representa un carácter único, mientras que un asterisco (*) representa una cadena de cero o más caracteres.

Formato de las exclusiones

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

✓ Ejemplos:

- C:\Tools*: la ruta debe terminar con la barra diagonal inversa (\) y el asterisco (*) para indicar que es una carpeta y que se excluirá todo el contenido de la carpeta (archivos y subcarpetas).
- C:\Tools*.*: el mismo comportamiento que C:\Tools*
- C:\Tools – La carpeta Tools no se excluirá.. Desde el punto de vista del módulo de exploración, Tools también puede ser un nombre de archivo.
- C:\Tools*.dat – Excluirá archivos .dat en la carpeta Tools.
- C:\Tools\sg.dat – Excluirá este archivo en particular ubicado en la ruta exacta.

Variables del sistema en las exclusiones

Puede usar variables del sistema como %PROGRAMFILES% para definir las exclusiones de exploración.

- Para excluir la carpeta Archivos de programa con esta variable del sistema, use la ruta %PROGRAMFILES%* (recuerde que debe agregar barra diagonal inversa al final de la ruta) cuando agregue exclusiones.
- Si desea excluir todos los archivos y carpetas en un subdirectorio de %PROGRAMFILES%, use la ruta %PROGRAMFILES%\Directorio_excluido*

✓ [Expandir la lista de variables del sistema compatibles](#)

Las siguientes variables pueden usarse en el formato de exclusión de ruta:

- %ALLUSERSPROFILE%
- %COMMONPROGRAMFILES%
- %COMMONPROGRAMFILES(X86)%
- %COMSPEC%
- %PROGRAMFILES%
- %PROGRAMFILES(X86)%
- %SystemDrive%
- %SystemRoot%
- %WINDIR%
- %PUBLIC%

No se admiten las variables del sistema específicas del usuario (p. ej., %TEMP% o %USERPROFILE%) ni las variables de entorno (p. ej., %PATH%).

Exclusiones de la detección

Las exclusiones de la detección permiten excluir objetos de la detección mediante el filtro del nombre de la detección, la ruta del objeto o su hash.

Cómo funcionan las exclusiones de la detección

Las exclusiones de la detección no excluyen archivos y carpetas de la exploración como las [Exclusiones de rendimiento](#). Las exclusiones de la detección excluyen objetos solo cuando el motor de detección los detecta y existe una regla pertinente en la lista de exclusiones.

- ✓ Por ejemplo (consulte la primera fila de la imagen a continuación), cuando se detecta un objeto como Win32/Adware.Optmedia y el archivo detectado es C:\Recovery\file.exe. En la segunda fila, cada archivo que tenga el hash SHA-1 pertinente siempre será excluido independientemente del nombre de la detección.

Exclusiones de la detección



Criterios del objeto	Excluir detección	Comentario
C:\Recovery*.*	Win32/Advare.Optmedia	
678C1422DE867141B947EA700E8A2D6114AFAE97	Cualquier detección	SuperApi.exe

Agregar

Editar

Eliminar

Importar

Exportar

Aceptar

Cancelar

Para garantizar que se detecten todas las amenazas, recomendamos crear exclusiones solo cuando sea absolutamente necesario.

Puede añadir archivos y carpetas a la lista de exclusiones, vaya a **Configuración avanzada (F5) > Motor de detección > Exclusiones > Exclusiones de la detección > Editar**.

i No debe confundirse con [Exclusiones de rendimiento](#), [Extensiones de archivo excluidas](#), [Exclusiones de HIPS](#) o [Exclusiones de procesos](#).

Para [excluir un objeto \(por su nombre de detección o hash\)](#) del motor de detección, haga clic en **Agregar**.

Para [Aplicaciones potencialmente no deseadas](#) y [Aplicaciones potencialmente no seguras](#), también se puede crear la exclusión por su nombre de detección:

- En la ventana de alerta que informa sobre la detección (haga clic en **Mostrar opciones avanzadas** y luego seleccione **Excluir de la detección**).
- En el menú contextual Archivos de registro, con el [asistente para Crear exclusiones de la detección](#).
- Al hacer clic en **Herramientas > Cuarentena** y luego clic derecho en el archivo en cuarentena y seleccionar **Restaurar y excluir de la exploración** del menú contextual.

Criterios de objeto de exclusiones de la detección

- **Ruta** – Limite una exclusión de la detección para una ruta específica (o cualquiera).
- **Nombre de detección**: si se muestra el nombre de una [detección](#) junto a un archivo excluido, significa que el archivo solo se excluirá en lo que respecta a la dicha detección, pero no se excluirá completamente. Si dicho archivo más tarde se infecta con otro malware, el módulo antivirus lo detectará.
- **Hash**: excluye un archivo en base a hash específico SHA-1, independientemente del tipo de archivo, su

ubicación, nombre o extensión.

Agregar o editar exclusiones de la detección

Excluir detección

Se debe proporcionar un nombre válido de detección de ESET. Para un nombre de detección válido, vaya a [Archivos de registro](#) y seleccione **Detecciones** en el menú desplegable de archivos de registro. Esto resulta útil cuando se detecta una [muestra con falso positivo](#) en ESET NOD32 Antivirus. Las exclusiones de infiltraciones reales son muy peligrosas, considere excluir solo archivos/directorios afectados haciendo clic en ... en el campo **Ruta** o solo temporalmente. Las exclusiones también se aplican para [aplicaciones potencialmente no deseadas](#), aplicaciones potencialmente peligrosas o aplicaciones sospechosas.

Consulte también [Formato de las exclusiones de ruta](#).



eset NOD32 ANTIVIRUS

Editar exclusión

Ruta: C:\Recovery*.*

Hash:

Nombre de detección: Win32/Advare.Optmedia

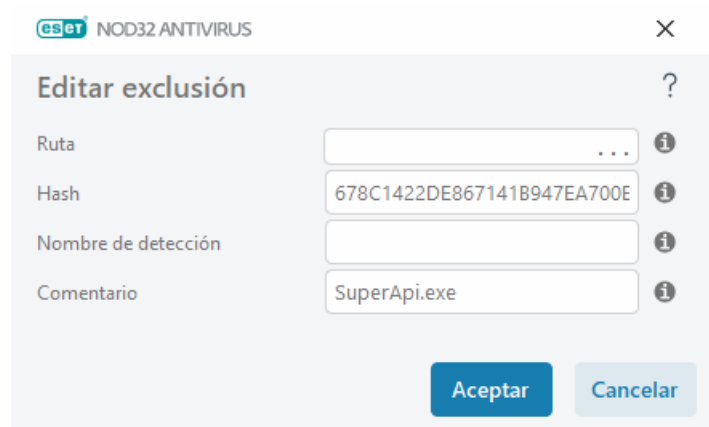
Comentario:

Aceptar Cancelar

Consulte el ejemplo de [Ejemplo de exclusiones de la detección](#) a continuación.

Excluir hash

Excluye un archivo en base a hash específico SHA-1, independientemente del tipo de archivo, su ubicación, nombre o extensión.



eset NOD32 ANTIVIRUS

Editar exclusión

Ruta:

Hash: 678C1422DE867141B947EA700E

Nombre de detección:

Comentario: SuperApi.exe

Aceptar Cancelar

Exclusiones por nombre de detección

Para excluir una detección específica por su nombre, ingrese el nombre de detección válido:

Win32/Adware.Optmedia

- ✓ También puede usar el siguiente formato cuando excluya una detección en la ventana de alerta de ESET NOD32 Antivirus:

@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt

@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan

@NAME=Win32/Bagle.D@TYPE=worm

Elementos de control

- **Agregar** – excluye objetos de la detección.
- **Editar** – le permite editar las entradas seleccionadas.
- **Eliminar**: quita las entradas seleccionadas (CTRL + clic para seleccionar múltiples entradas).

Asistente para crear exclusiones de la detección

También puede crear una exclusión de la detección desde el menú contextual de [Archivos de registro](#) (no disponible para las detecciones de malware):

1. En la [ventana principal del programa](#), haga clic en **Herramientas > Archivos de registro**.
2. Haga clic derecho en una detección del **Registro de detecciones**.
3. Haga clic en **Crear exclusión**.

Para excluir una o más detecciones en función de los **Criterios de exclusión**, haga clic en **Modificar criterios**:

- **Archivos exactos** – Excluir cada archivo por hash SHA-1.
- **Detección** – Excluir cada archivo por nombre de detección.
- **Ruta + Detección** – Excluir cada archivo por ruta y nombre de detección, incluido el nombre del archivo (p. ej., *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*).

La opción recomendada se selecciona de forma predeterminada en función del tipo de detección.

De manera opcional, puede agregar un **Comentario** antes de hacer clic en **Crear exclusión**.

Exclusiones de HIPS

Las exclusiones le permiten excluir procesos de la inspección profunda del comportamiento de HIPS.

Para editar las exclusiones de HIPS, vaya a **Configuración avanzada (F5) > Motor de detección > HIPS > Básico > Exclusiones > Modificar**.



No debe confundirse con [Extensiones de archivo excluidas](#), [Exclusiones de detección](#), [Exclusiones de rendimiento](#) o [Exclusiones de procesos](#).

Para excluir un objeto, haga clic en **Agregar** e ingrese la ruta a un objeto o selecciónelo en la estructura de árbol. También puede Editar o Eliminar las entradas seleccionadas.

ThreatSense parámetros

ThreatSense está 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 de la exploración del código, la emulación del código, las firmas genéricas y 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 simultáneamente varios flujos de datos para maximizar la eficiencia y la tasa de detección. La tecnología de ThreatSense también elimina los rootkits de forma correcta.

Las opciones de configuración del motor ThreatSense le 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 **ThreatSense parámetros** ubicado en la ventana de Configuración avanzada de cualquier módulo que use la tecnología ThreatSense (ver abajo). Diferentes situaciones de seguridad pueden requerir diferentes configuraciones. Por este motivo, ThreatSense puede configurarse en forma individual para los siguientes módulos de protección:

- Protección del sistema de archivos en tiempo real
- Exploración en estado inactivo
- Exploración en el inicio
- 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.

Objetos para explorar

Esta sección le 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/UEFI: explora los sectores de inicio para detectar la presencia de virus en el Master Boot Record. [Lea más sobre UEFI en el glosario.](#)

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

Archivos – 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 de autoextracción: los archivos de autoextracción (SFX) son los archivos que se pueden extraer a sí mismos.

Empaquetadores de tiempo de ejecución: después de su ejecución, los empaquetadores de tiempo de ejecución (a diferencia de los tipos de archivos estándar) se descomprimen en la memoria. Además de los empaquetadores estáticos estándar (UPX, yoda, ASPack, FSG, etc.), el explorador puede reconocer varios tipos de empaquetadores adicionales mediante el uso de la emulación del código.

Opciones de exploración

Seleccione 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 de esta tecnología radica en su capacidad de identificar software malicioso que antes no existía o que no era reconocido por la versión anterior del motor de detección. La desventaja es la probabilidad (muy reducida) de identificar falsos positivos.

Heurística avanzada/Firmas de ADN: la heurística avanzada está compuesta por un algoritmo heurístico exclusivo, desarrollado por ESET, optimizado para detectar gusanos informáticos y troyanos que se crearon con lenguajes de programación de última generación. El uso de la heurística avanzada incrementa significativamente la capacidad de detección de amenazas de los productos de ESET. Las firmas tienen la capacidad de detectar e identificar los virus en forma confiable. Mediante el uso del sistema de actualizaciones automáticas, las nuevas firmas están disponibles en el transcurso de unas pocas horas tras el descubrimiento de una amenaza. La desventaja de las firmas es que solo detectan los virus que ya conocen (o las versiones ligeramente modificadas de estos virus).

Desinfección

La configuración de la desinfección determina el comportamiento de ESET NOD32 Antivirus durante la desinfección de objetos. Existen cuatro niveles de desinfección:

Los parámetros de ThreatSense tienen los siguientes niveles de corrección (es decir, desinfección).

Corrección ESET NOD32 Antivirus

Nivel de desinfección	Descripción
Corregir siempre la detección	Intento de corregir la detección al limpiar objetos sin la intervención del usuario final. En algunos pocos casos (por ejemplo, en archivos de sistema), si la detección no se puede corregir, se deja al objeto informado en su ubicación original.
Corregir la detección si es seguro, de lo contrario conservar	Intento de corregir la detección al desinfectar objetos sin la intervención del usuario final. En algunos casos (por ejemplo, en archivos de sistema con archivos desinfectados o infectados), si una detección no se puede corregir, se deja al objeto informado en su ubicación original.
Corregir la detección si es seguro, de lo contrario preguntar	Intento de corregir la detección al desinfectar objetos. En algunos casos, si no se puede realizar ninguna acción, el usuario final recibe una alerta interactiva y debe seleccionar una acción de corrección (por ejemplo, eliminar o ignorar). Esta configuración se recomienda en la mayoría de los casos.
Preguntar siempre al usuario final	El usuario final visualiza una ventana interactiva al desinfectar objetos y debe seleccionar una acción de corrección (por ejemplo, eliminar o ignorar). Este nivel está diseñado para los usuarios más avanzados que conocen los pasos a seguir en caso de hallar una detección.

Exclusiones

Una extensión es la 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.

Otros

Cuando se configuran los valores de los parámetros del motor ThreatSense para una exploración del equipo bajo demanda, las siguientes opciones en la sección **Otros** 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 los recursos del sistema, es posible activar la exploración en segundo plano con baja prioridad y reservar los recursos para las aplicaciones.

Registrar todos los objetos – El [Registro de la exploración](#) mostrará todos los archivos explorados en los archivos comprimidos de autoextracción, incluidos los que no estén infectados (podría generar muchos datos de registro de exploración e incrementar el tamaño del archivo del registro de exploración).

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.

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).

Límites

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

Configuración de los objetos

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 para el objeto (seg.): define el valor máximo de tiempo para explorar un objeto en un contenedor (como un archivo RAR/ZIP o un correo electrónico con varios adjuntos). Esta configuración no rige para archivos independientes. Si en esta opción se ingresó un valor definido por el usuario y el tiempo ha transcurrido, la exploración se detendrá lo antes posible, sin importar si finalizó la exploración de cada uno de los archivos en un objeto de contenedor.

En el caso de un archivo con varios archivos grandes, la exploración se detendrá en cuanto se extraiga un archivo (por ejemplo, cuando la variable definida por el usuario es de 3 segundos, pero la extracción de un archivo demora 5 segundos). El resto de los archivos del archivo general no se explorarán una vez que haya transcurrido esa cantidad de tiempo.

Para limitar el tiempo de exploración, incluidos los archivos más grandes, use las opciones **Tamaño máximo del objeto** y **Tamaño máximo del archivo incluido en el archivo comprimido** (no se recomienda debido a posibles riesgos para la seguridad).

Valor predeterminado: ilimitado.

Configuración de la exploración de archivos comprimidos

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. El valor máximo es **3 GB**.



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

Extensiones de archivos que no se analizarán

Las extensiones de archivo que no se analizarán forman parte de los [parámetros de ThreatSense](#). Para configurar las extensiones de archivo que no se analizarán, haga clic en **parámetros de ThreatSense** de la ventana Configuración avanzada de cualquier [módulo que utilice tecnología ThreatSense](#).


Una extensión es la 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.

 No debe confundirse con [Exclusiones de procesos](#), [Exclusiones HIPS](#) o [Exclusiones de archivo/carpeta](#).

En forma predeterminada, se exploran todos los archivos. Se puede agregar cualquier extensión a la lista de archivos excluidos de la exploración.

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.

 Para agregar una nueva extensión a la lista, haga clic en **Agregar**. Ingrese la extensión en el campo vacío (por ejemplo, `tmp`) y haga clic en **Aceptar**. Cuando selecciona **Ingresar múltiples valores**, puede agregar varias extensiones de archivo delimitadas por líneas, comas, o punto y coma (por ejemplo, seleccione **Punto y coma** del menú desplegable como separador y escriba `edb;eml;tmp`). Puede utilizar un símbolo especial (?) (signo de interrogación). El signo de interrogación representa cualquier símbolo (por ejemplo `?db`).

 Para ver la extensión exacta (si la hubiera) de un archivo en un sistema operativo Windows, debe marcar la casilla De verificación **Extensiones de nombre de archivo** en **Windows Explorer > Ver** (pestaña).

Parámetros ThreatSense adicionales

Para modificar esta configuración, vaya a **Configuración avanzada (F5) > Motor de detección > Protección del sistema de archivos en tiempo real > Parámetros ThreatSense adicionales**.

Parámetros de ThreatSense adicionales para archivos creados o modificados recientemente.

La probabilidad de infección en los archivos recién creados o modificados es comparativamente superior a la de los archivos existentes. Por este motivo, el programa comprueba estos archivos con parámetros de exploración adicionales. ESET NOD32 Antivirus usa heurística avanzada, que puede detectar nuevas amenazas antes de que se actualice el motor de detección junto con métodos de exploración basados en firmas.

Además de los archivos recién creados, la exploración también se realiza en **Archivos comprimidos de autoextracción (.sfx)** y **Empaquetadores de tiempo de ejecución** (archivos ejecutables comprimidos internamente). De forma predeterminada, los archivos se exploran hasta el nivel 10 de anidamiento y se comprueban independientemente de su tamaño real. Para modificar la configuración de la exploración de archivos, anule la selección de la opción **Configuración predeterminada de exploración de archivos**.


Parámetros adicionales de ThreatSense para los archivos ejecutados


Heurística avanzada para la ejecución de archivos: de forma predeterminada, se utiliza la [Heurística avanzada](#) cuando se ejecutan los archivos. Cuando está habilitada, recomendamos mantener la [Optimización inteligente](#) y [ESET LiveGrid®](#) habilitados para mitigar el impacto en el rendimiento del sistema.

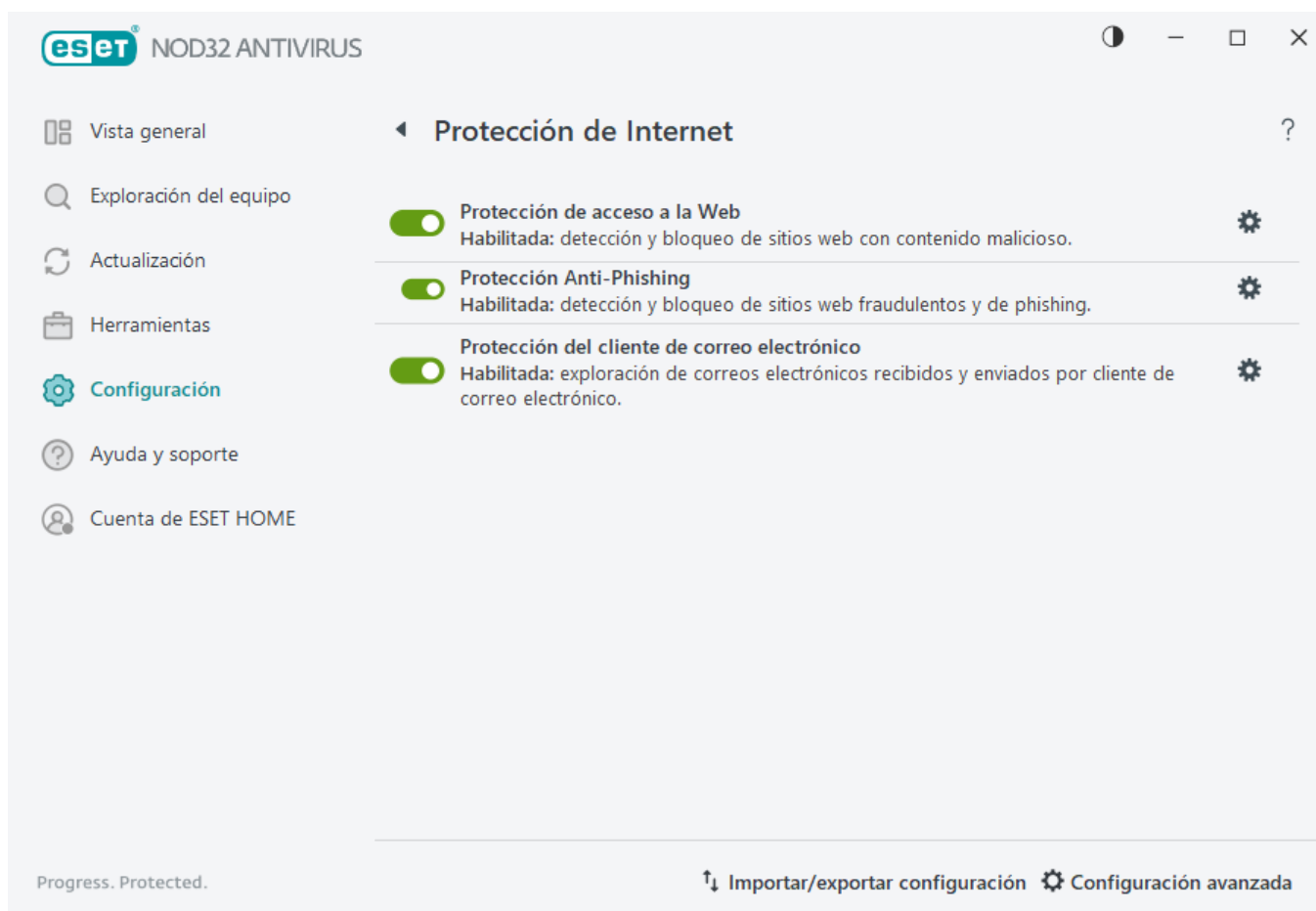
Heurística avanzada al ejecutar archivos de medios extraíbles: la heurística avanzada emula un código en un entorno virtual y evalúa su comportamiento antes de permitir la ejecución del código desde los medios extraíbles.


Protección de Internet

Para configurar la protección de Internet y correo electrónico, haga clic en **Protección de Internet** en la ventana **Configuración**. Desde aquí es posible acceder a configuraciones más detalladas del programa.

Para pausar o desactivar módulos de protección individuales, haga clic en el ícono de la barra deslizante .

 Desactivar los módulos de protección puede disminuir el nivel de protección del equipo.



Haga clic en el icono del engranaje  junto a un módulo de protección para acceder a las configuraciones avanzadas de dicho módulo.

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](#).

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

[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). Mediante el complemento del programa para su cliente de correo electrónico, ESET NOD32 Antivirus proporciona el control de todas las comunicaciones desde el cliente de correo electrónico.

Filtrado de protocolos

El motor de exploración de ThreatSense, que integra perfectamente todas las técnicas avanzadas para la exploración de malware, proporciona la protección antivirus para los protocolos de aplicación. El filtrado de protocolos funciona en forma automática, independientemente del navegador de Internet o del cliente de correo electrónico utilizado. Para editar las configuraciones cifradas (SSL/TLS), vaya a **Configuración avanzada** (F5) > **Internet y correo electrónico** > [SSL/TLS](#).

Habilitar el filtrado del contenido de los protocolos de aplicación – se puede utilizar para deshabilitar el filtrado de protocolos. Tenga en cuenta que muchos de los componentes de ESET NOD32 Antivirus (Protección del acceso a la web, Protección de los protocolos de correo electrónico, Antiphishing, Control parental) dependen de esto y no funcionarán sin el mismo.

Aplicaciones excluidas – le permite excluir del aplicaciones específicas del filtrado de protocolos. Es útil cuando el filtrado de protocolos causa problemas de compatibilidad.

Direcciones IP excluidas – le permite excluir del filtrado de protocolos direcciones remotas específicas. Es útil cuando el filtrado de protocolos causa problemas de compatibilidad.

Agrega (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*).

Ejemplo de direcciones IP excluidas

Direcciones IPv4 y máscara:

- *192.168.0.10*: agrega la dirección IP de un equipo individual al que debe aplicarse la regla.
- *192.168.0.1 a 192.168.0.99*: escriba la primera y la última dirección IP para especificar el rango de IP (de varios equipos) al que se debe aplicar la regla.
- ✓ Subred (un grupo de computadoras) 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*.

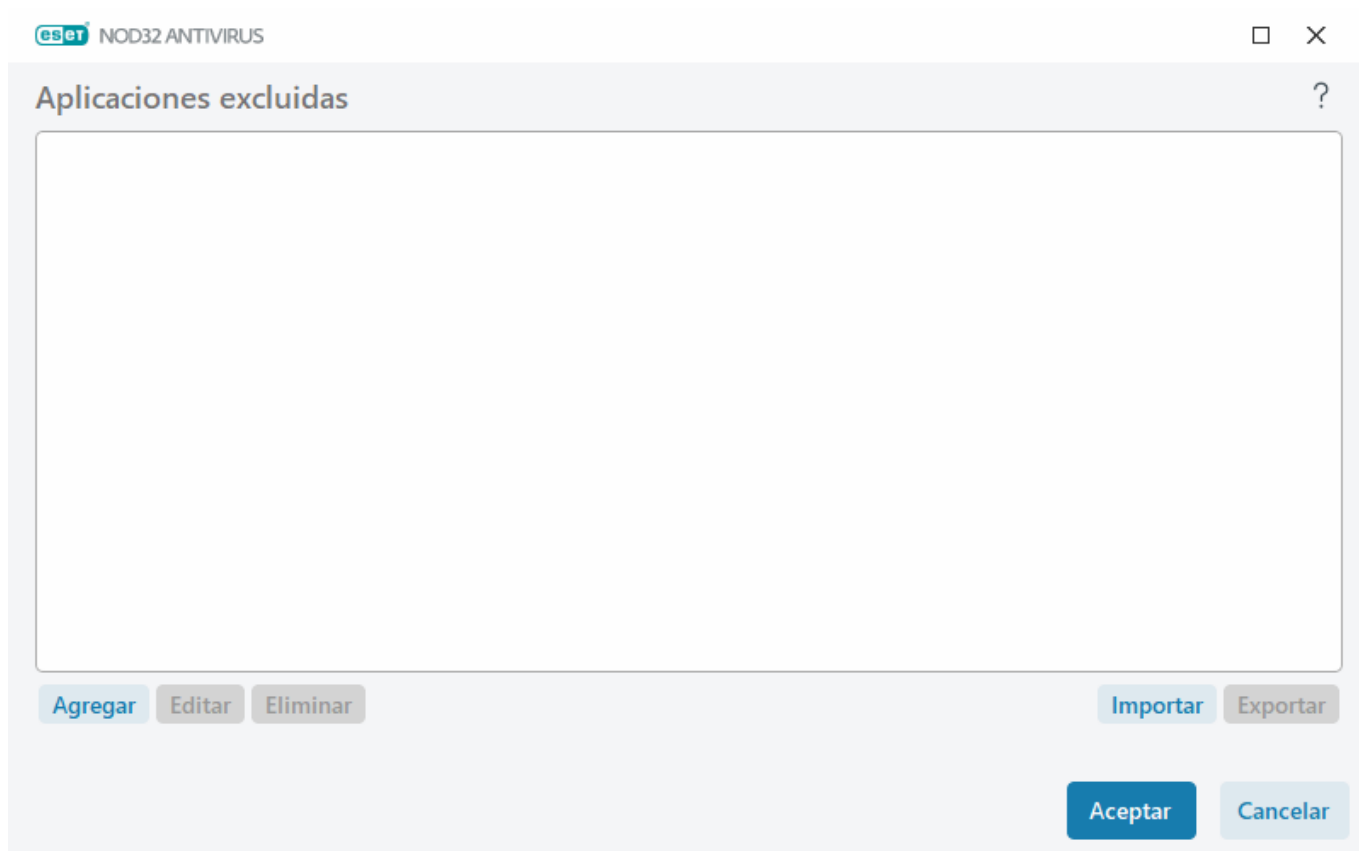
Dirección IPv6 y máscara:

- *2001:718:1c01:16:214:22ff:fec9:ca5*: la dirección IPv6 de un equipo individual al que debe aplicarse la regla.
- *2002:c0a8:6301:1::1/64*: la dirección IPv6 con un prefijo de 64 bits; eso significa *2002:c0a8:6301:0001:0000:0000:0000:0000 a 2002:c0a8:6301:0001:ffff:ffff:ffff:ffff*

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 solamente para las 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.

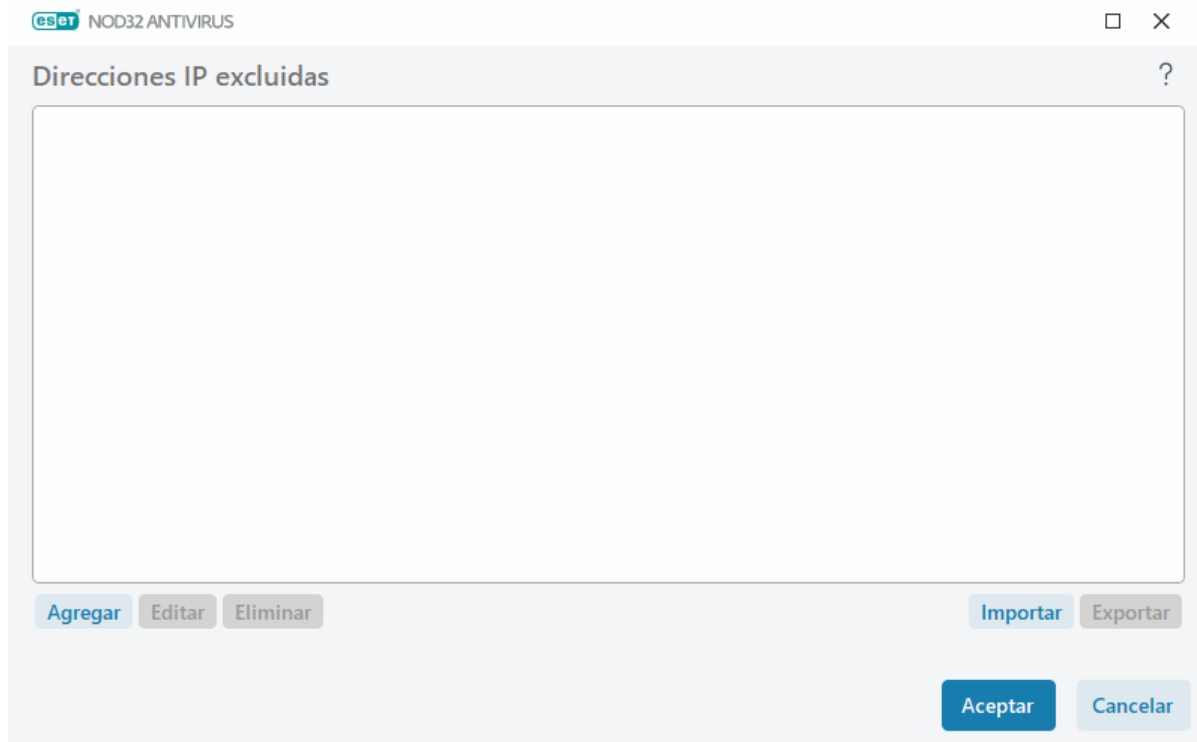


Direcciones IP excluidas

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.

Haga clic en **Agregar** para agregar una dirección IP, un rango de direcciones o una subred de un punto remoto, al que se debe aplicar la lista de filtrado de protocolos.

Haga clic en **Quitar** para eliminar las entradas seleccionadas de la lista.



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*.

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*).

SSL/TLS

ESET NOD32 Antivirus tiene la capacidad de verificar las amenazas en las comunicaciones que usan el protocolo SSL. Puede usar varios modos de filtrado para examinar las comunicaciones protegidas por SSL mediante certificados de confianza, certificados desconocidos o certificados excluidos de la verificación de las comunicaciones protegidas por SSL.

Habilitar el filtrado del protocolo SSL/TLS: si se deshabilita el filtrado de protocolos, el programa no explorará las comunicaciones con el protocolo SSL.

el modo de filtrado de protocolos SSL/TLS está disponible en las siguientes opciones:

Modo de filtrado	Descripción
Modo automático	El modo predeterminado solo explorará las aplicaciones correspondientes, como los navegadores web y los clientes de correo electrónico. Puede anularlo si selecciona las aplicaciones para las cuales se explorarán sus comunicaciones.
Modo interactivo	Si ingresa un nuevo sitio protegido por SSL (con un certificado desconocido), se mostrará un cuadro de diálogo para la selección de acción . Este modo le permite crear una lista de certificados/aplicaciones SSL que se excluirán de la exploración.
Modo de política	Modo automático: 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 está marcado como de confianza (se encuentra en la lista de certificados de confianza), se permite la comunicación con el servidor y se filtra el contenido del canal de comunicación.

La **Lista de aplicaciones SSL/TLS filtradas** puede usarse para personalizar la conducta de ESET NOD32 Antivirus para aplicaciones específicas

Lista de certificados conocidos: le permite personalizar la conducta de ESET NOD32 Antivirus para certificados SSL específicos.

Excluir la comunicación con dominios de confianza – cuando está habilitada, la comunicación con dominios de confianza se excluirá de la verificación. La fiabilidad del dominio es determinada por la lista blanca incorporada.

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

Certificado raíz

Agregar el certificado raíz a los navegadores conocidos: 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). Cuando está habilitado, ESET NOD32 Antivirus agrega automáticamente el certificado ESET SSL Filter CA a los navegadores conocidos (por ejemplo, Opera). Para los navegadores que usan el almacén de certificaciones del sistema, el certificado se agrega en forma automática. Por ejemplo, Firefox se configura de manera automática para confiar en las autoridades raíz en la tienda de certificados del sistema.

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.

Validez del certificado

Si no se puede demostrar la confianza del certificado: en algunos casos, el certificado de un sitio web no se puede verificar mediante el almacén de Autoridades de Certificación de Raíz de Confianza (TRCA). Por lo tanto, alguien (por ejemplo, el administrador de un servidor Web o una pequeña empresa) ha firmado el certificado y considerar este certificado como confiable no siempre es un riesgo. La mayoría de las grandes empresas (por ejemplo, los bancos) usan un certificado firmado por las TRCA. Si se selecciona **Preguntar sobre la validez del certificado** (predeterminado), se solicita al usuario que seleccione la acción a realizar cuando se establezca una comunicación cifrada. Puede seleccionar **Bloquear las comunicaciones que usan el certificado** para finalizar siempre las conexiones cifradas a los sitios con certificados no verificados.

Si el certificado está dañado: significa que la firma del certificado no es correcta o que está dañado. En este caso, se recomienda dejar seleccionada la opción **Bloquear comunicaciones que usan el certificado**. Si se selecciona **Preguntar sobre la validez del certificado**, se solicita al usuario que seleccione la acción a realizar cuando se establezca la comunicación cifrada.

Ejemplos ilustrados



Los siguientes artículos de la base de conocimiento de ESET pueden estar disponibles solo en inglés:

- [Notificaciones de certificados en productos hogareños de ESET Windows](#)
- Se muestra el mensaje "[Tráfico de red cifrado: Certificado no confiable](#)" al visitar las páginas web

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). En el caso de los navegadores que usan el almacén de certificaciones del sistema, el certificado se agrega en forma automática (p. 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.

Tráfico de red cifrada

Si su sistema está configurado para usar una exploración del protocolo SSL, se mostrará una ventana de diálogo para elegir una acción en dos situaciones distintas:

Primero, si un sitio web usa un certificado no válido o que no se puede verificar, y ESET NOD32 Antivirus está configurado para preguntarle al usuario en dichos casos (de forma predeterminada, "sí" para los certificados que no se pueden verificar; "no" para los que no son válidos), un cuadro de diálogo le preguntará si desea **Permitir** o **Bloquear** la conexión. Si el certificado no está ubicado en Trusted Root Certification Authorities store (TRCA), se considera no confiable.

Segundo, si el **modo de filtrado de protocolos SSL** está configurado en **Modo interactivo**, un cuadro de diálogo para cada sitio web le preguntará si desea **Explorar** o **Ignorar** el tráfico. Algunas aplicaciones verifican que su tráfico SSL no esté modificado ni inspeccionado por nadie; en dichos casos, ESET NOD32 Antivirus debe **Ignorar** dicho tráfico para que la aplicación siga funcionando.

Ejemplos ilustrados



Los siguientes artículos de la base de conocimiento de ESET pueden estar disponibles solo en inglés:

- [Notificaciones de certificados en productos hogareños de ESET Windows](#)
- Se muestra el mensaje "[Tráfico de red cifrado: Certificado no confiable](#)" al visitar las páginas web

En los dos casos, el usuario puede elegir recordar la acción seleccionada. Las acciones guardadas se almacenan en la [Lista de certificados conocidos](#).

Lista de certificados conocidos

La **Lista de certificados conocidos** se puede utilizar para personalizar la conducta de ESET NOD32 Antivirus para certificados SSL específicos, y para recordar las acciones elegidas si se selecciona el **Modo interactivo** en el **modo de filtrado de protocolos SSL/TSL**. La lista se puede ver y editar en **Configuración avanzada (F5) > Internet y correo electrónico > SSL/TSL > Lista de certificados conocidos**.

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

Columnas

Nombre— nombre del certificado.

Emisor del certificado— nombre del creador del certificado.

Sujeto del certificado— el campo del sujeto identifica la entidad asociada con la clave pública almacenada en el campo de la clave pública del sujeto.

Acceso— seleccione **Permitir** o **Bloquear** como la **Acción de acceso** para permitir o bloquear la comunicación asegurada por este certificado, independientemente de su confianza. Seleccione **Auto** para permitir certificados de confianza y solicitar los que no son de confianza. Seleccione **Preguntar** para preguntarle siempre al usuario qué hacer.

Explorar— seleccione **Explorar** o **Ignorar** como la **Acción de exploración** para explorar o ignorar la comunicación asegurada por este certificado. Seleccione **Auto** para explorar en el modo automático y preguntar en el modo

interactivo. Seleccione **Preguntar** para preguntarle siempre al usuario qué hacer.

Elementos de control

Agregar – agregar un nuevo certificado y ajustar su configuración con respecto al acceso y a las opciones de exploración.

Editar – Seleccione el certificado que desea configurar y haga clic en **Editar**.

Eliminar – Seleccione el certificado que desea eliminar y haga clic en **Quitar**.

Aceptar/cancelar – haga clic en **Aceptar** si desea guardar los cambios o en **Cancelar** si desea salir sin guardar.

Lista de aplicaciones SSL/TLS filtradas

La **Lista de aplicaciones SSL/TLS filtradas** se puede usar para personalizar la conducta de ESET NOD32 Antivirus para aplicaciones específicas y para recordar las acciones elegidas cuando el **modo de filtrado de protocolos SSL/TLS** está en el **Modo interactivo**. La lista se puede ver y editar en **Configuración avanzada (F5) > Internet y correo electrónico > SSL/TLS > Lista de aplicaciones SSL/TLS filtradas**.

La ventana **Lista de aplicaciones SSL/TLS filtradas** consiste en:

Columnas

Aplicación – elija un archivo ejecutable desde el árbol del directorio, haga clic en la opción ... e ingrese la ruta en forma manual.

Acción de exploración – seleccione **Explorar** o **Ignorar** para explorar o ignorar la comunicación. Seleccione **Auto** para explorar en el modo automático y preguntar en el modo interactivo. Seleccione **Preguntar** para preguntarle siempre al usuario qué hacer.

Elementos de control

Agregar– agregar la aplicación filtrada.

Editar: seleccione la aplicación que desea configurar y haga clic en **Editar**.

Quitar: seleccione la aplicación que desea quitar y haga clic en **Quitar**.

Importar/Exportar: importe aplicaciones desde un archivo o guarde la lista actual de aplicaciones en un archivo.

Aceptar/Cancelar – haga clic en **Aceptar** si desea guardar los cambios o en **Cancelar** si desea salir sin guardar.

Protección del cliente de correo electrónico

Consulte [Integración de ESET NOD32 Antivirus en su cliente de correo electrónico](#) para configurar la integración.

Las configuraciones de cliente de correo electrónico se ubican en **Configuración avanzada (F5) > Internet y correo electrónico > Protección del cliente de correo electrónico > Clientes de correo electrónico**.

Cientes de correo electrónico

Habilitar protección de correo electrónico mediante complementos de clientes: cuando esté deshabilitada, la protección mediante complementos de cliente de correo electrónico estará apagada.

Correo electrónico para explorar

Seleccione los correos electrónicos que desea analizar:

- Correo electrónico recibido
- Correo electrónico enviado
- Correo electrónico leído
- Correo electrónico modificado



Recomendamos mantener **Habilitar protección de correo electrónico mediante complementos de clientes** habilitado. Incluso si la integración no está habilitada o no es funcional, la comunicación por correo electrónico todavía está protegida por el [filtrado de protocolos](#) (IMAP/IMAPS y POP3/POP3S).

Acción a 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 acción alguna.

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 de elementos eliminados.

Mover el correo electrónico a la carpeta (acción predeterminada): los correos electrónicos infectados se enviarán automáticamente a la carpeta especificada.

Carpeta – especificar la carpeta personalizada donde desea mover los correos electrónicos infectados al detectarlos.

Integración con el cliente de correo electrónico

La integración de ESET NOD32 Antivirus con su cliente de correo electrónico aumenta el nivel de protección activa frente a código malicioso en los mensajes de correo electrónico. Si su cliente de correo electrónico es compatible, puede habilitar la integración en ESET NOD32 Antivirus. Cuando se integra a su cliente de correo electrónico, la barra de herramientas de ESET NOD32 Antivirus se inserta directamente en el cliente de correo electrónico, lo que permite una protección de correo electrónico más eficaz. Las configuraciones de integración se ubican en **Configuración avanzada (F5) > Internet y correo electrónico > Protección del cliente de correo electrónico > Integración con el cliente de correo electrónico**.

[Microsoft Outlook](#) es actualmente el único cliente de correo electrónico compatible. La protección de correo electrónico funciona como un complemento. 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. Consulte este [artículo de la base de conocimiento de ESET](#) para ver una

lista completa de las versiones compatibles de Microsoft Outlook.

Optimización de la gestión de adjuntos: si la optimización está deshabilitada, todos los archivos adjuntos se exploran inmediatamente. Es posible que experimente una ralentización del rendimiento del cliente de correo electrónico.

Procesamiento avanzado de cliente de correo electrónico: si experimenta lentitud en el sistema al trabajar con su cliente de correo electrónico, deshabilite esta opción.

Barra de herramientas de Microsoft Outlook

La protección de Microsoft Outlook funciona como un módulo de complemento. Después de instalar ESET NOD32 Antivirus, se agrega a Microsoft Outlook la siguiente barra de herramientas con las opciones de protección antivirus/ :

ESET NOD32 Antivirus: haga doble clic en el ícono para abrir la ventana principal de ESET NOD32 Antivirus.

Volver a explorar los mensajes – permite iniciar la verificación del correo electrónico en forma manual. Puede especificar los mensajes que se van a verificar así como activar la exploración repetida de los correos electrónicos recibidos. Para obtener más información, consulte la sección [Protección del cliente de correo electrónico](#).

Configuración del módulo de exploración – muestra las opciones de configuración de la [Protección del cliente de correo electrónico](#).

Cuadro de diálogo de confirmación

Esta notificación sirve para corroborar que el usuario realmente desee realizar la acción seleccionada, para eliminar posibles errores.

Por otro lado, el cuadro de diálogo también ofrece la opción de deshabilitar las confirmaciones.

Volver a explorar los mensajes

La barra de herramientas de ESET NOD32 Antivirus, integrada en los clientes de correo electrónico, les permite a los usuarios especificar varias opciones de verificación del correo electrónico. La opción **Volver a explorar los mensajes** ofrece dos modos de exploración:

Todos los mensajes de la carpeta actual – explora los mensajes en la carpeta actualmente abierta.

Solo los mensajes seleccionados – explora únicamente los mensajes marcados por el usuario.

La casilla de verificación **Volver a explorar los mensajes ya explorados** le proporciona al usuario la opción de realizar otra exploración en los mensajes que ya se habían explorado antes.

Protocolos de correo electrónico

IMAP y POP3 son los protocolos de uso más generales para recibir comunicaciones de correo electrónico en una aplicación de cliente de correo electrónico. El protocolo de acceso a mensajes de Internet (IMAP, 'Internet

Message Access Protocol') 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. El módulo de protección que proporciona este control se ejecuta automáticamente cuando se inicia el sistema y queda activo en la memoria.

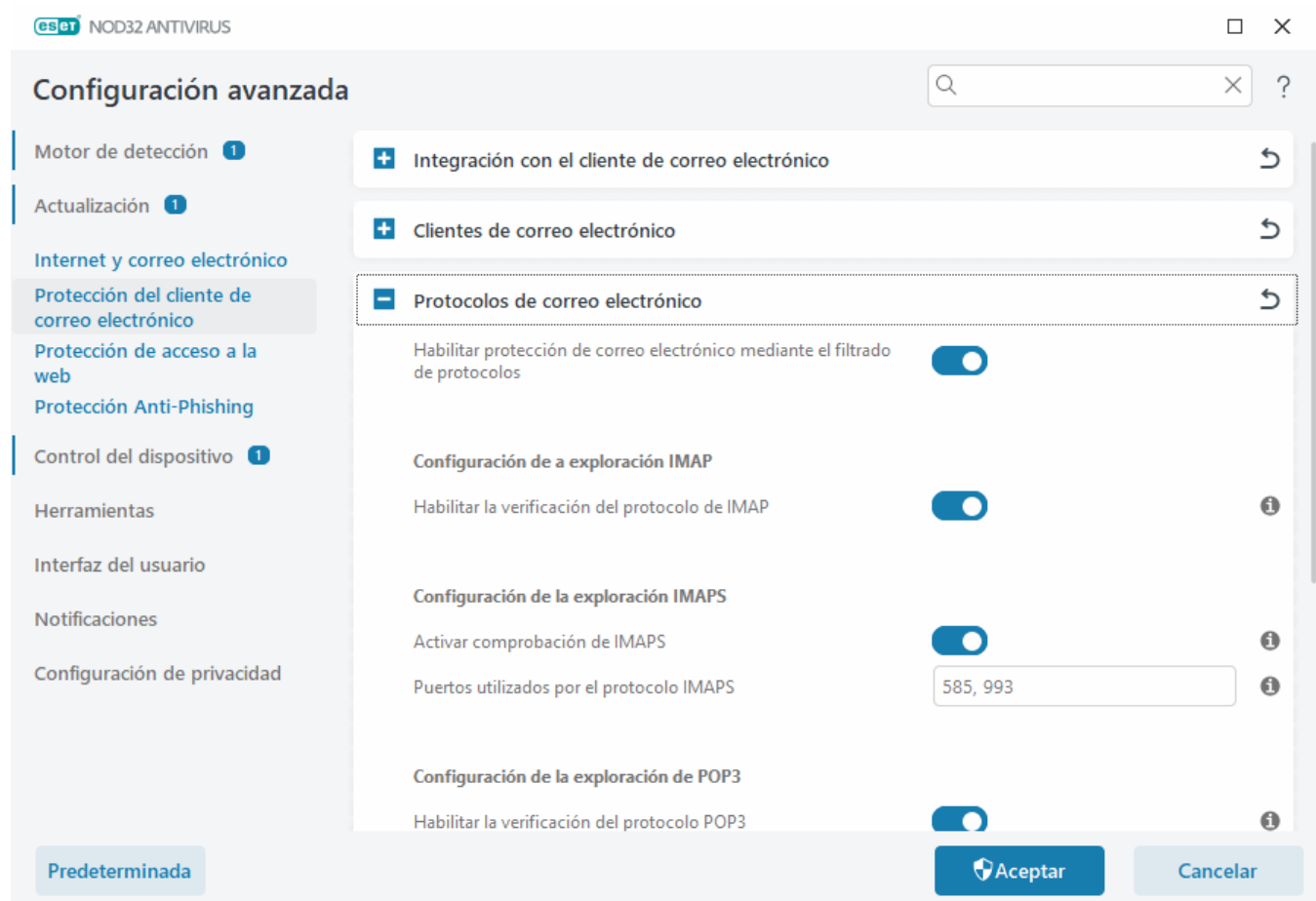
ESET NOD32 Antivirus proporciona protección para estos protocolos, independientemente del cliente de correo electrónico usado, y sin requerir una nueva configuración del cliente de correo electrónico. De manera predeterminada, toda la comunicación mediante los protocolos POP3 y IMAP se explora, sin tener en cuenta los números de puerto POP3/IMAP predeterminados.

El protocolo IMAP no se explora. Sin embargo, la comunicación con el servidor Microsoft Exchange puede explorarse mediante el [módulo de integración](#) en clientes de correo electrónico, como Microsoft Outlook.

Recomendamos habilitar **Habilitar protección de correo electrónico por complemento de cliente**. Para configurar la verificación del protocolo IMAP/IMAPS y POP3/POP3S, navegue hacia **Configuración avanzada > Internet y correo electrónico > Habilitar la protección del cliente de correo electrónico > Protocolos de correo electrónico**.

ESET NOD32 Antivirus también admite la exploración de los protocolos IMAPS (585, 993) y POP3S (995), que usan un canal cifrado para transferir información entre el servidor y el cliente. ESET NOD32 Antivirus verifica la comunicación mediante el SSL (protocolo de capa de conexión segura) y la TLS (seguridad de la capa de transporte). El programa solo explorará el tráfico en los puertos definidos en **Puertos utilizados por los protocolos IMAPS/POP3S**, independientemente de la versión del sistema operativo. Si es necesario, puede agregar otros puertos de comunicación. Cuando hay varios números de puerto, deben delimitarse con una coma.

La comunicación cifrada se explorará de forma predeterminada. Para ver la configuración del módulo de exploración, abra la Configuración avanzada > **Internet y correo electrónico > [SSL/TLS](#)**.



Filtro para POP3, POP3S

El protocolo POP3 es el protocolo más popular usado para recibir comunicaciones por correo electrónico en una aplicación cliente de correo electrónico. ESET NOD32 Antivirus proporciona protección para este protocolo independientemente del cliente de correo electrónico utilizado.

El módulo de protección que proporciona este control se ejecuta automáticamente cuando se inicia el sistema y 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. De forma predeterminada, se exploran todas las comunicaciones en el puerto 110, pero de ser necesario, se pueden agregar otros puertos de comunicación. Los números de puerto múltiples deben delimitarse con una coma.

La comunicación cifrada se explorará de forma predeterminada. Para ver la configuración del módulo de exploración, abra la Configuración avanzada > **Internet y correo electrónico** > [SSL/TLS](#).

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).

Etiquetas de correo electrónico

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

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 que, en ocasiones raras, los mensajes de etiqueta pueden omitirse en mensajes HTML problemáticos o si los mensajes están adulterados por malware. Los mensajes de etiqueta se pueden añadir a los correos electrónicos recibidos y leídos, enviados o a ambas categorías. Se encuentran disponibles las siguientes opciones:

- **Nunca:** no se agregan mensajes de etiqueta.
- **Cuando ocurre una detección:** 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.

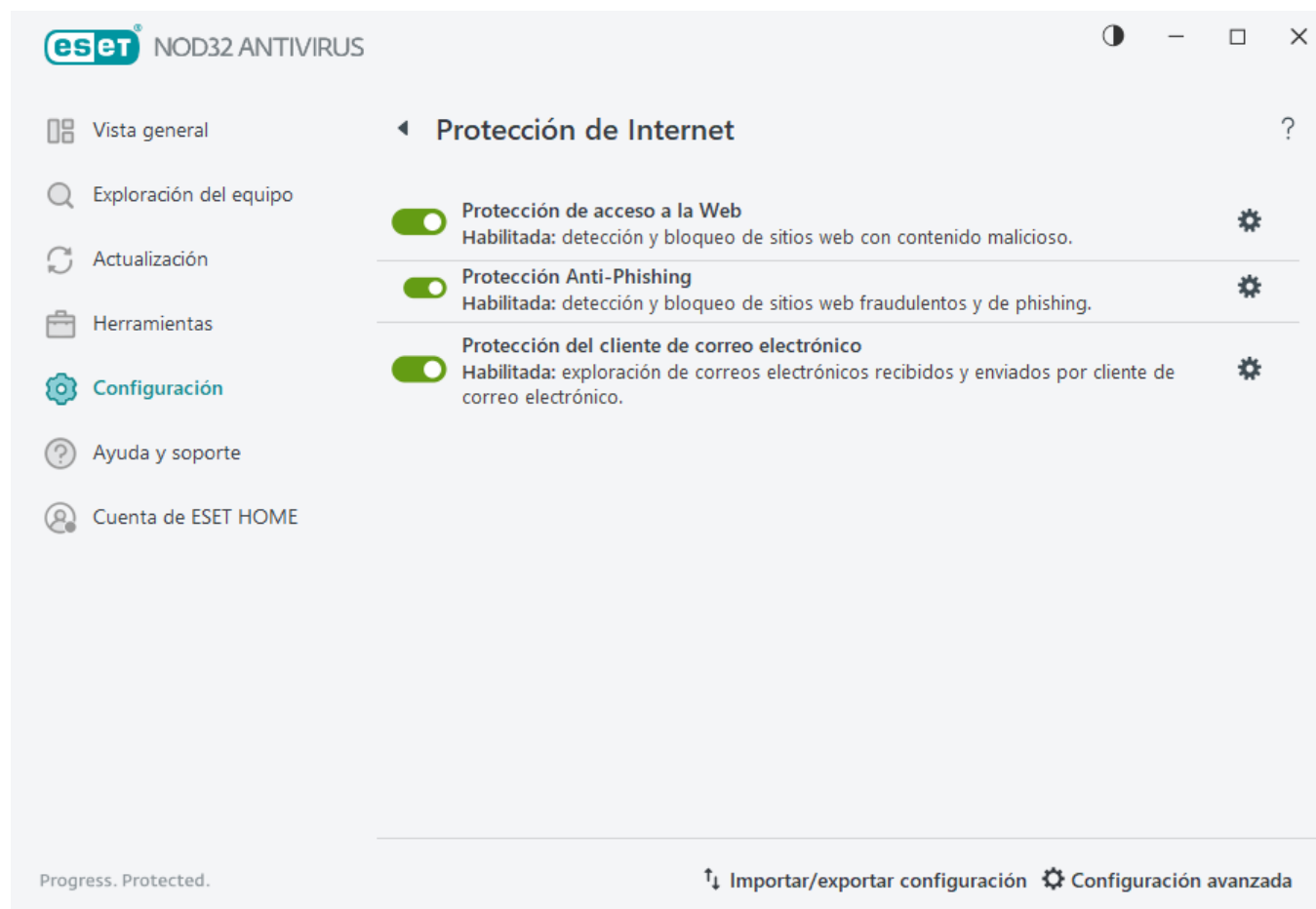
Texto para agregar en el asunto del correo electrónico detectado: si desea modificar el formato del prefijo en el asunto de un correo electrónico infectado, edite esta plantilla. Esta función reemplazará el asunto del mensaje «Hola» por el siguiente formato: «[detección %NOMBRE DE DETECCIÓN%] Hola». La variable %DETECTIONNAME% representa la amenaza detectada.

Protección del acceso a la Web

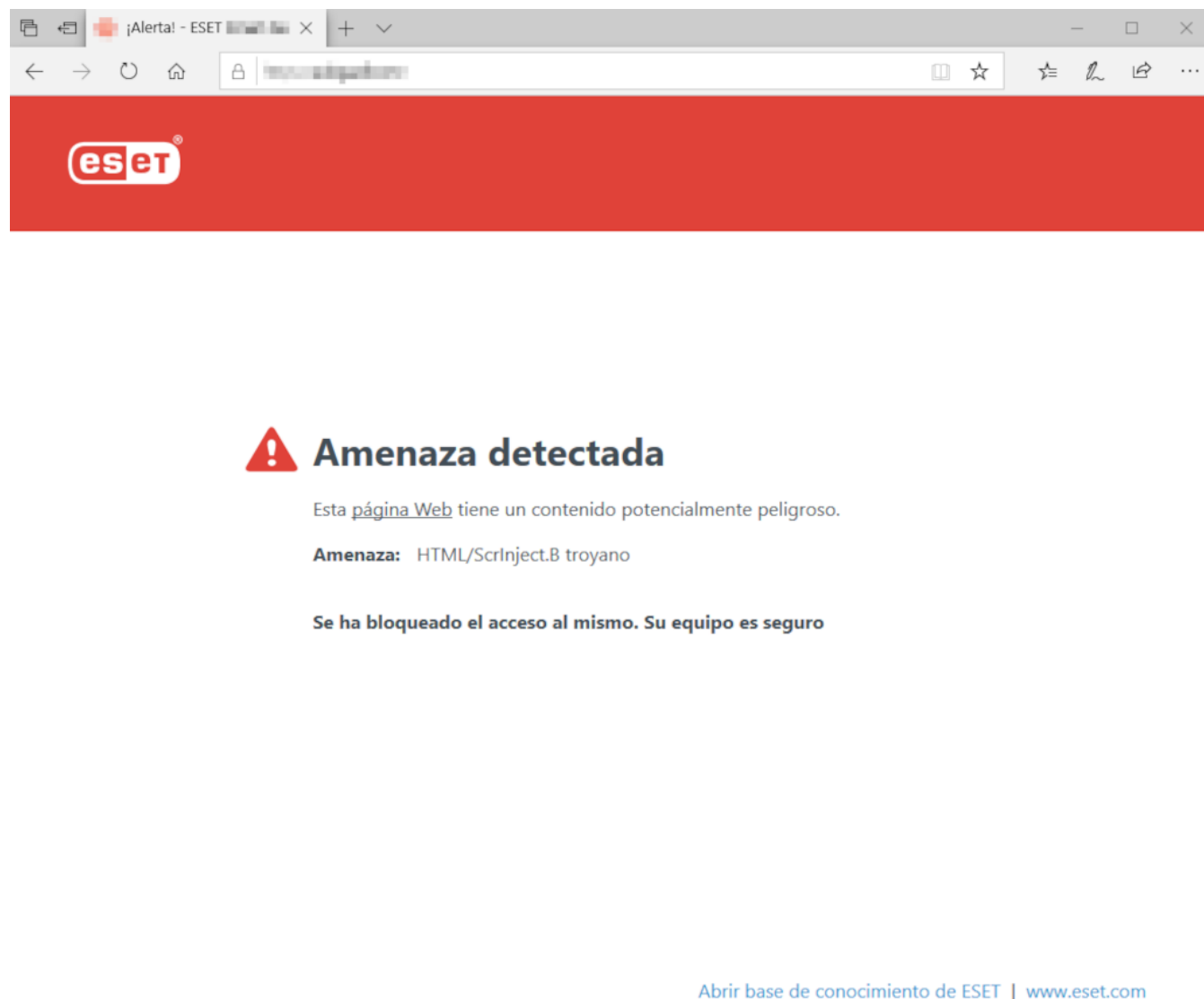
La conectividad a Internet es una función estándar del equipo personal. Lamentablemente, también se convirtió en el medio principal para transferir códigos maliciosos. La protección de acceso a la web explora la comunicación HTTP (protocolo de transferencia de hipertexto) y HTTPS (comunicación cifrada)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

El acceso a las páginas web que se sabe que tienen contenido malicioso se bloquea antes de que se descargue el contenido. Las demás páginas web se exploran con el motor de exploración ThreatSense durante la carga, y se bloquean si se detecta contenido malicioso. La protección de acceso a la web le permite [bloquear o permitir el acceso a direcciones URL y excluir las direcciones de la exploración](#).

Se recomienda firmemente que la protección del acceso a la Web esté habilitada. Puede acceder a esta opción desde la [ventana principal del programa](#) > **Configuración** > **Protección de Internet** > **Protección del acceso a la Web**.



Protección de acceso a la web mostrará al siguiente mensaje en su navegador cuando el sitio web esté bloqueado:



Instrucciones ilustradas



Los siguientes artículos de la base de conocimiento de ESET pueden estar disponibles solo en inglés:

- [Impedir que Protección de acceso a la web bloquee un sitio web seguro](#)
- [Bloquear un sitio web con ESET NOD32 Antivirus](#)

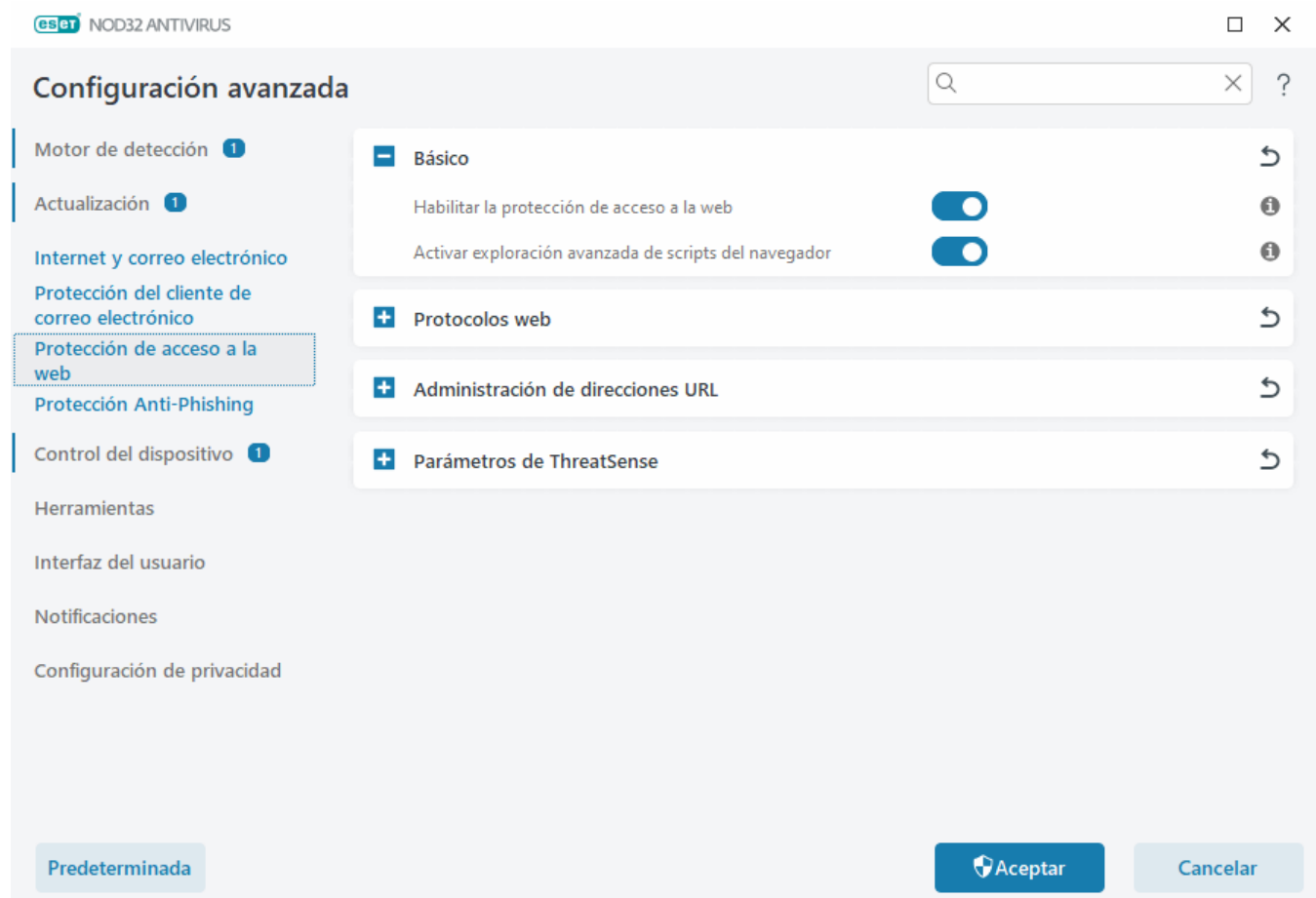
Las siguientes opciones están disponibles en **Configuración avanzada (F5) > Internet y correo electrónico > Protección del acceso a la Web**:

[Básico](#) – Para habilitar o deshabilitar esta función desde Configuración avanzada.

[Protocolos de Internet](#) – Le permite configurar la supervisión de estos protocolos estándar, que son utilizados por la mayoría de los navegadores de Internet.

[Administración de direcciones URL](#) – Le permite especificar las direcciones URL que se desea bloquear, permitir o excluir de la verificación.

[ThreatSense parámetros](#): la configuración avanzada del módulo de exploración de virus le permite configurar propiedades como, por ejemplo, los tipos de objetos que se explorarán (correos electrónicos, archivos comprimidos, etc.), los métodos de detección para la protección del acceso a la Web, etc.



Configuración avanzada de la protección de acceso a la web

Las siguientes opciones están disponibles en **Configuración avanzada** (F5) > **Internet y correo electrónico** > **Protección de acceso a la Web** > **Básico**:

Habilitar la protección de acceso a la web – Cuando está deshabilitada, no se ejecuta la [Protección del acceso a la web](#) ni la [Protección anti-phishing](#). Esta opción solo está disponible cuando el filtrado de protocolos SSL/TLS está habilitado.

Activar exploración avanzada de scripts del navegador – Si está habilitado, el motor de detección verificará todos los programas de JavaScript ejecutados por navegadores de Internet.

i Se recomienda firmemente dejar habilitada la protección del acceso a la web.

Protocolos Web

En forma predeterminada, ESET NOD32 Antivirus está configurado para supervisar el protocolo HTTP utilizado por la mayoría de los navegadores de Internet.

Configuración de la exploración de HTTP

El tráfico de HTTP se supervisa siempre en todos los puertos para todas las aplicaciones.

Configuración de a exploración de HTTPS

ESET NOD32 Antivirus también 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 la comunicación mediante los protocolos SSL (protocolo de capa de socket seguro) y TLS (seguridad de la capa de transporte). El programa solo explorará el tráfico en los puertos (443, 0-65535) definidos en **Puertos utilizados por el protocolo HTTPS**, independientemente de la versión del sistema operativo.

La comunicación cifrada se explorará de forma predeterminada. Para ver la configuración del módulo de exploración, abra la Configuración avanzada > **Internet y correo electrónico** > [SSL/TLS](#).

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 exploración del contenido.

[Habilitar el filtrado de protocolos SSL/TLS](#) debe estar seleccionado si desea filtrar las direcciones HTTPS además de las páginas Web HTTP. De lo contrario, solo se agregarán los dominios de los sitios HTTPS que haya visitado, y no se agregará la URL completa.

No será posible acceder a los sitios web incluidos en la **Lista de direcciones bloqueadas**, a menos que también estén incluidos en la **Lista de direcciones permitidas**. Los sitios web en la **Lista de direcciones excluidas de la exploración del contenido** no se exploran en busca de códigos maliciosos cuando se accede a los mismos.

Si desea bloquear todas las direcciones HTTP excepto las direcciones presentes en la **Lista de direcciones permitidas** activa, agregue un * a la **Lista de direcciones bloqueadas** activa.

Pueden utilizarse los símbolos especiales * (asterisco) y ? (signo de interrogación) en las listas. El asterisco sustituye cualquier cadena de caracteres y el signo de interrogación sustituye cualquier símbolo. Cuando especifique direcciones excluidas, debe tener especial cuidado, 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 **Lista activa**. Si desea recibir una notificación cuando se introduzca una dirección de la lista actual, seleccione **Notificar al aplicar**.

Dominio de confianza



Las direcciones no se filtrarán si la configuración de **Internet y correo electrónico** > **SSL/TLS** > **Excluir la comunicación con dominios de confianza** está activada y el dominio se considera de confianza.

Lista de direcciones



Nombre de la lista	Tipos de direcciones	Descripción de la lista
Lista de direcciones permitidas	Permitido	
Lista de direcciones bloqueadas	Bloqueado	
Lista de direcciones excluidas de la exploración del contenido	El malware encontrado se...	

Agregar

Editar

Eliminar

Importar

Exportar

Agregar un comodín (*) a la lista de direcciones bloqueadas para bloquear todas las URL excepto aquellas incluidas en una lista de direcciones permitidas.

Aceptar

Cancelar

Elementos de control

Agregar – crea una nueva lista además de las predefinidas. Esto puede ser útil si desea separar de manera lógica los diferentes grupos de direcciones. Por ejemplo, una lista de direcciones bloqueadas puede contener direcciones de una lista negra pública externa, mientras que una segunda lista puede contener su propia lista negra, lo que facilita la actualización de la lista externa mientras que mantiene intacta la suya.

Editar – modifica las listas existentes. Use esto para agregar o eliminar las direcciones.

Eliminar – elimina las listas existentes. Solo es posible para las listas creadas con la opción **Agregar**, no con las opciones predeterminadas.

Lista de direcciones URL

En esta sección, puede especificar las listas de direcciones HTTP que se bloquearán, permitirán o excluirán de la verificación.

De forma predeterminada, se pueden utilizar estas tres listas:

- **Lista de direcciones excluidas de la exploración de contenidos:** no se comprobará la existencia de códigos maliciosos en ninguna de las direcciones agregadas a esta lista.
- **Lista de direcciones permitidas** – si se habilita Permitir el acceso solo a las direcciones HTTP de la lista de direcciones permitidas, y la lista de direcciones bloqueadas contiene un * (coincidir con todo), el usuario podrá acceder únicamente a las direcciones que se encuentran en esta lista. Las direcciones de esta lista se permiten incluso si están incluidas en la lista de direcciones bloqueadas.
- **Lista de direcciones bloqueadas:** el usuario no tendrá acceso a las direcciones especificadas en esta lista, a menos que también aparezcan en la lista de direcciones permitidas.

Haga clic en **Agregar** para crear una lista nueva. Para eliminar las listas seleccionadas, haga clic en **Quitar**.

Lista de direcciones



Nombre de la lista	Tipos de direcciones	Descripción de la lista
Lista de direcciones permitidas	Permitido	
Lista de direcciones bloqueadas	Bloqueado	
Lista de direcciones excluidas de la exploración del contenido	El malware encontrado se...	

Agregar

Editar

Eliminar

Importar

Exportar

Agregar un comodín (*) a la lista de direcciones bloqueadas para bloquear todas las URL excepto aquellas incluidas en una lista de direcciones permitidas.

Aceptar

Cancelar

Instrucciones ilustradas



Los siguientes artículos de la base de conocimiento de ESET pueden estar disponibles solo en inglés:

- [Impedir que Protección de acceso a la web bloquee un sitio web seguro](#)
- [Bloquear un sitio web con los productos hogareños de ESET Windows](#)

Para obtener más información, consulte la [Administración de direcciones URL](#).

Crear nueva lista de direcciones URL

Este cuadro de diálogo le permite configurar una nueva [lista de direcciones URL o máscaras](#) que se bloquearán, se permitirán o se excluirán en la comprobación.

Puede configurar las siguientes opciones:

Tipo de lista de direcciones – hay tres tipos de listas disponibles:

- **El malware encontrado se ha ignorado** – no se comprobará la existencia de códigos maliciosos en ninguna de las direcciones agregadas a esta lista.
- **Bloqueado** – se bloqueará el acceso a las direcciones especificadas en esta lista.
- **Permitido** – se permitirá el acceso a las direcciones especificadas en esta lista. Las direcciones de esta lista se permiten incluso si coinciden con las de la lista de direcciones bloqueadas.

Nombre de la lista – especifique el nombre de la lista. Este campo no estará disponible al editar una de las listas predefinidas.

Descripción de la lista – escriba una breve descripción de la lista (opcional). No está disponible al editar una de las listas predefinidas.

Para activar una lista, seleccione **Lista activa** junto a esa lista. Si desea recibir una notificación cuando se utilice

una lista específica al acceder a sitios web, seleccione **Notificar cuando se aplique**. Por ejemplo, recibirá una notificación si un sitio web está bloqueado o permitido por estar incluido en una lista de direcciones bloqueadas o permitidas. Esta notificación incluirá el nombre de la lista que contiene el sitio web especificado.

Severidad de registro – información sobre la lista específica que se usa al acceder a sitios web y que se puede escribir en los [archivos de registro](#).

Elementos de control

Agregar – agregue una dirección URL nueva a la lista (ingrese múltiples valores con separadores).

Editar – modifica la dirección existente en la lista. Solo está disponible para direcciones creadas con **Agregar**.

Quitar – elimina las direcciones existentes en la lista. Solo está disponible para direcciones creadas con **Agregar**.

Importar – importe un archivo con direcciones URL (valores separados por un salto de línea; por ejemplo, *.txt al usar codificación UTF-8).

Cómo agregar una máscara URL

Consulte las indicaciones de este cuadro de diálogo antes de ingresar la máscara de dominio/dirección deseada.

ESET NOD32 Antivirus les permite a los usuarios bloquear el acceso a determinados sitios Web para evitar que el navegador de Internet muestre su contenido. Además, permite especificar las direcciones que se van a excluir de la verificación. Si se desconoce el nombre completo del servidor remoto o si el usuario desea especificar un grupo completo de servidores remotos, se pueden usar las máscaras para identificar dicho grupo. Las máscaras incluyen los símbolos “?” y “*”:

- use ? para sustituir un símbolo
- use * para sustituir una cadena de texto.

Por ejemplo, *.c?m se aplica a todas las direcciones cuya última parte comience con la letra c, termine con la letra m y contenga un símbolo desconocido entre las dos (.com, .cam, etc.).

Una primera secuencia “*.” se trata de modo especial si se utiliza al comienzo del nombre del dominio. Primero, el comodín * no coincide con carácter de barra (“/”) en este caso. Esto es para evitar evadir la máscara, por ejemplo la máscara *.domain.com no coincidirá con *http://anydomain.com/anypath#.domain.com* (dicho sufijo puede anexarse a cualquier URL sin afectar la descarga). Y segundo, el “*.” también coincide con una cadena vacía en este caso especial. Esto es para permitir que coincida todo el dominio incluidos los subdominios usando una sola máscara. Por ejemplo la máscara *.domain.com también coincide con *http://domain.com*. Utilizar *.domain.com sería incorrecto, ya que también coincidiría con *http://anotherdomain.com*.

Protección antiphishing

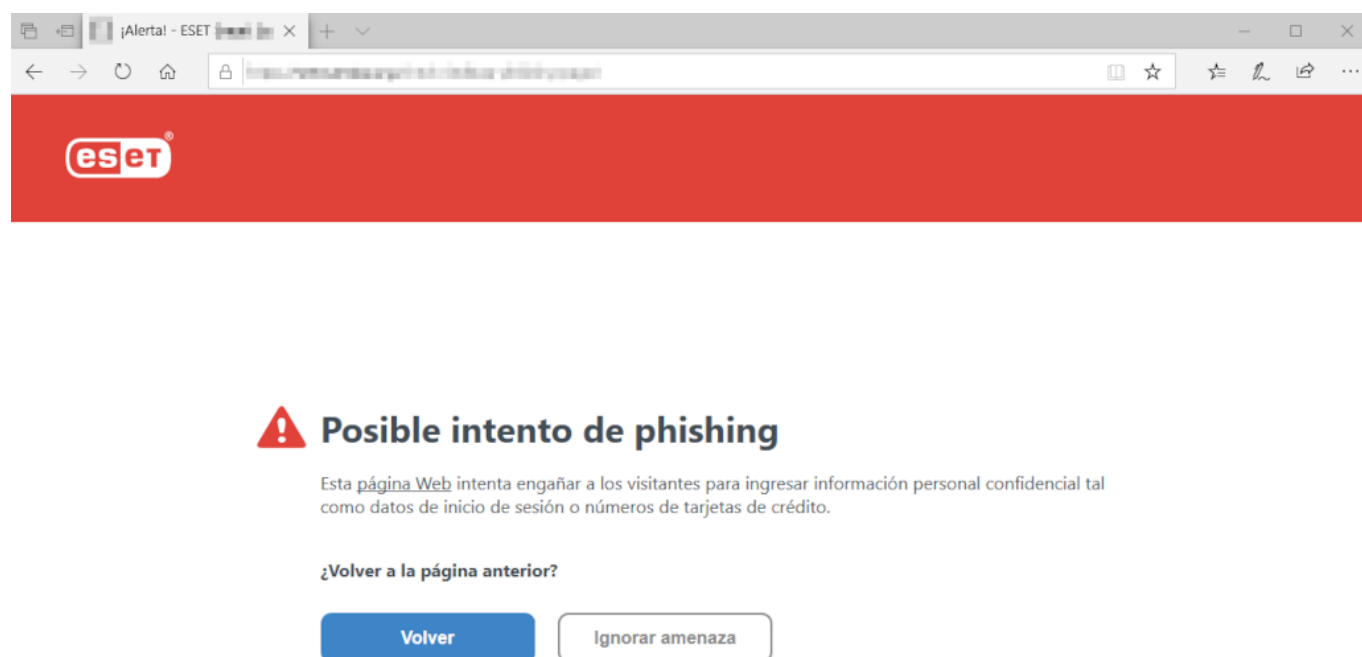
El phishing es una actividad delictiva que usa la ingeniería social (manipulación de usuarios para obtener información confidencial). El phishing se utiliza para acceder a datos confidenciales, como números de cuentas bancarias, códigos PIN, etc. Obtenga más información sobre esta actividad en el [glosario](#). ESET NOD32 Antivirus incluye protección antiphishing, que bloquea las páginas web conocidas por distribuir este tipo de contenido.

La protección antiphishing está activada de forma predeterminada. Puede acceder a esta configuración desde la [ventana principal del programa](#) > **Configuración avanzada** (F5) > **Internet y correo electrónico** > **Protección antiphishing**.

Visite nuestro [Artículo de la base de conocimiento](#) para obtener más información acerca de la protección antiphishing en ESET NOD32 Antivirus.

Acceso a un sitio Web de phishing

Cuando ingrese a un sitio web de phishing reconocido, su navegador web mostrará el siguiente cuadro de diálogo. Si aún desea acceder al sitio web, haga clic en **Ignorar amenaza** (no recomendado).



[Informar las páginas bloqueadas incorrectamente](#)

[Obtener más información acerca de la suplantación de identidad \(phishing\)](#) | www.eset.com

i 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, use la herramienta [Administración de direcciones URL](#). En **Configuración avanzada** (F5) > **Internet y correo electrónico** > **Protección del acceso a la web** > **Administración de direcciones URL** > **Lista de direcciones** > **Editar** agregue a la lista el sitio web que desea editar.

Informar una página de phishing

El vínculo **Informar** le permite informar a ESET los sitios web maliciosos o de phishing que deben analizarse.



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 ese caso, puede [Informar una página bloqueada incorrectamente](#).

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

Actualización del programa

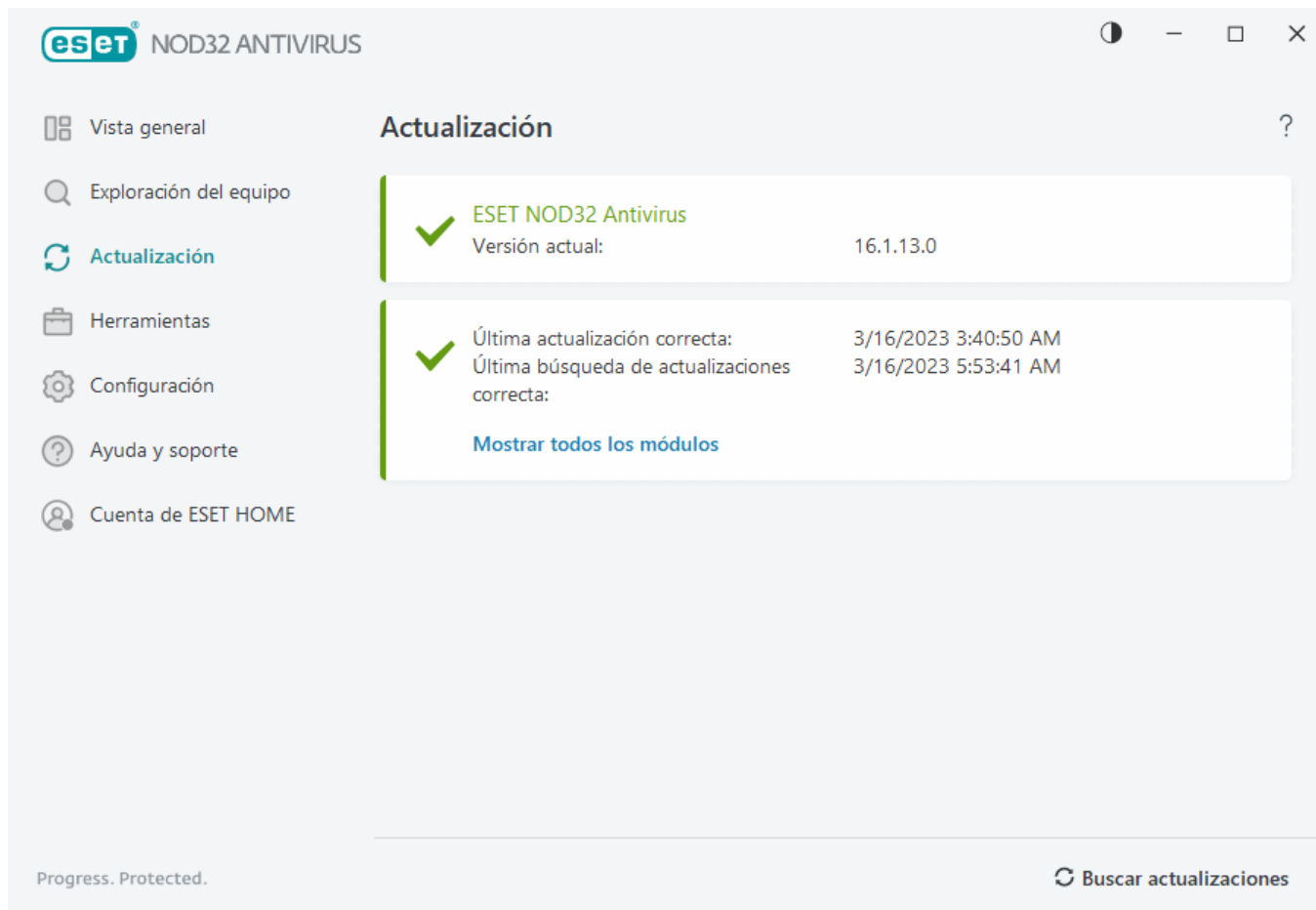
La actualización habitual de ESET NOD32 Antivirus es la mejor forma de asegurar el máximo nivel de seguridad en el equipo. El módulo de actualización se asegura de que los módulos del programa y los componentes del sistema estén siempre actualizados.

Al hacer clic en **Actualización** en la [ventana principal del programa](#), verá el estado actual de la actualización, incluyendo la fecha y la hora de la última actualización correcta y si es necesario actualizar.

Además de las actualizaciones automáticas, puede hacer clic en **Buscar actualizaciones** para activar una actualización manual. La actualización frecuente de los módulos y componentes del programa es un aspecto importante para mantener una protección completa contra los códigos maliciosos. Preste atención a su configuración y funcionamiento. Debe activar su producto mediante su clave de licencia para recibir las actualizaciones. Si no lo hizo durante la instalación, puede ingresar su clave de licencia mediante cuando realiza una actualización para acceder a los servidores de actualización de ESET.



ESET le provee su clave de licencia por correo electrónico después de la compra de ESET NOD32 Antivirus.



Versión actual: muestra el número de la versión actual instalada.

Última actualización exitosa: muestra la fecha de la última actualización exitosa. Si no visualiza una fecha reciente, es posible que los módulos de producto no estén actualizados.

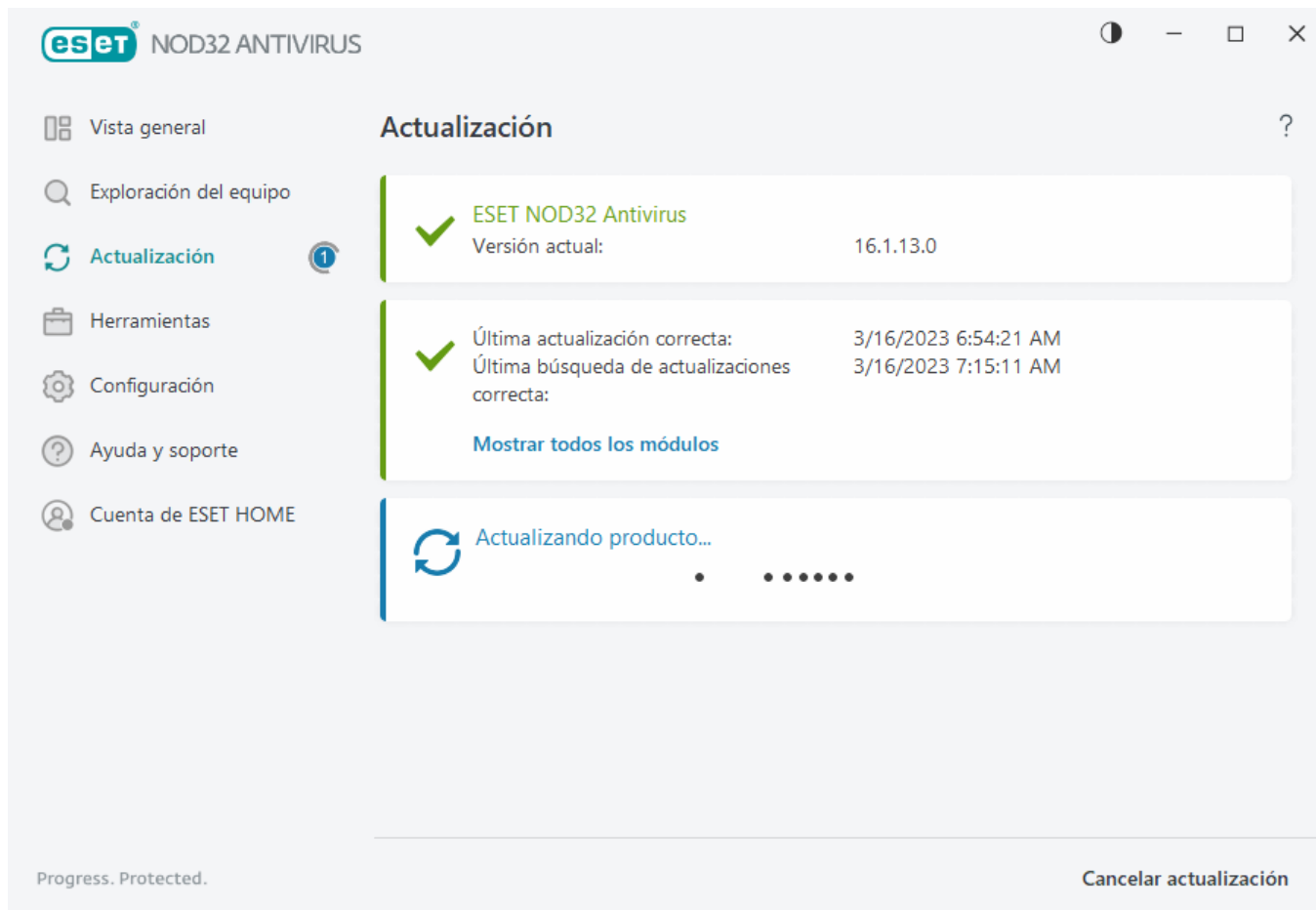
Último verificación exitosa de actualizaciones: muestra la fecha de la última verificación exitosa de actualizaciones.

Mostrar todos los módulos: muestra la lista de módulos de programa instalados.

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

Proceso de actualización

Luego de hacer clic en **Buscar actualizaciones**, 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**.

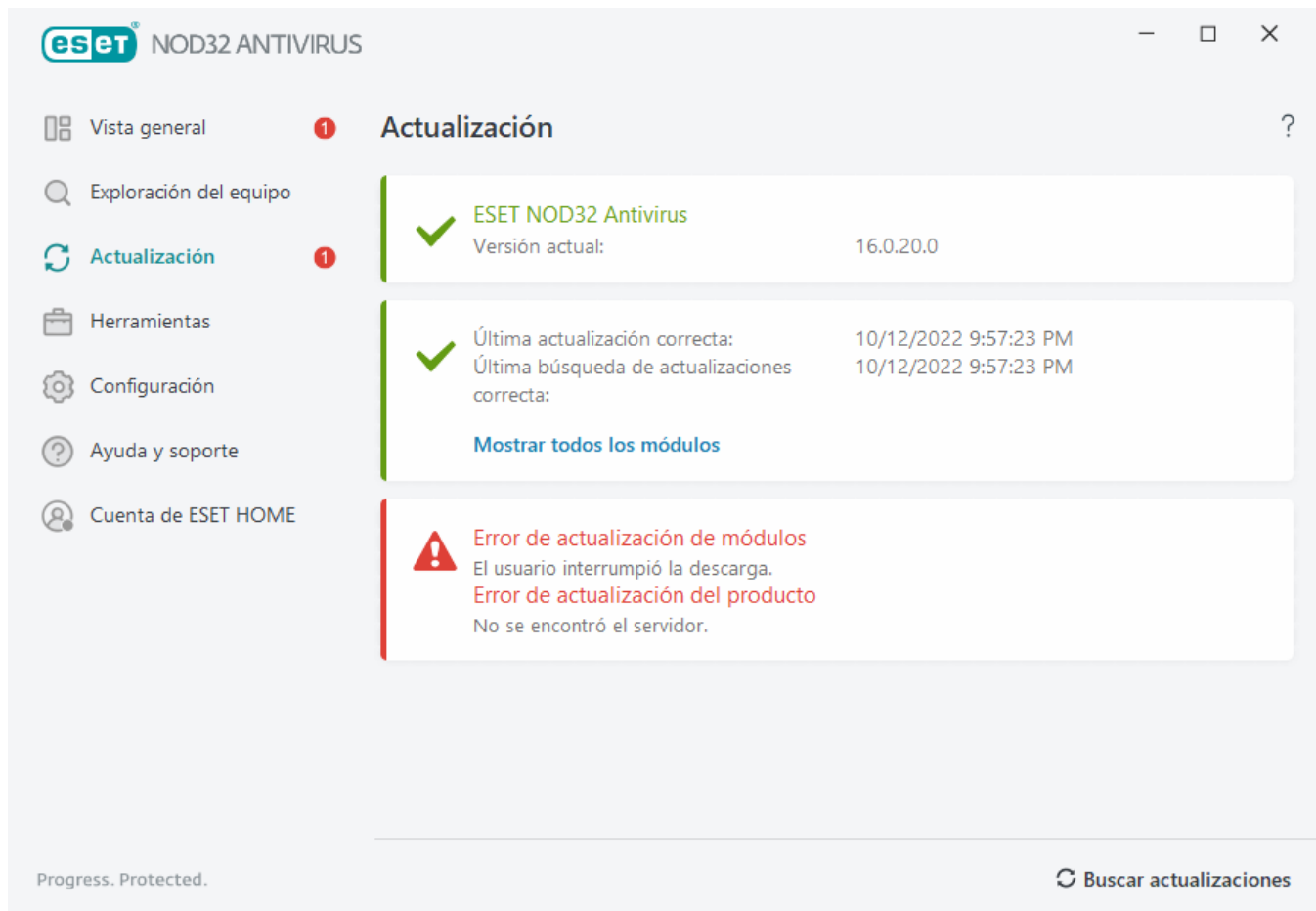


En circunstancias normales, puede ver la marca de verificación verde en la ventana **Actualización** que indica que el programa está actualizado. Si este no es el caso, el programa está desactualizado y más vulnerable a una infección. Actualice los módulos lo antes posible.

Última actualización exitosa

Si recibe un mensaje de actualización insatisfactoria de los módulos, puede deberse a los siguientes problemas:

1. **Licencia no válida:** la licencia que se usa para la activación no es válida o está vencida. En la [ventana principal del programa](#), haga clic en **Ayuda y soporte** > **Cambiar licencia** y active su producto.
2. **Se produjo un error al descargar los archivos de actualización:** una causa posible de este error es la [configuración de la conexión a Internet](#) incorrecta. 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.



Recomendamos reiniciar su equipo después de una actualización exitosa de ESET NOD32 Antivirus a una versión de producto más reciente para asegurarse de que todos los módulos del programa se actualizaron correctamente. No es necesario que reinicie su computadora luego de las actualizaciones regulares de los módulos.



Para obtener más información, visite este [artículo sobre el mensaje «Falló la actualización de los módulos» de la sección de resolución de problemas](#).

Configuración de la actualización

Las opciones de configuración de la actualización están disponibles en el árbol de **Configuración avanzada** (F5) en **Actualización > Básico**. Esta sección especifica la información del origen de la actualización, como los servidores de actualización que se utilizan y los datos de autenticación para estos servidores.

— Básico

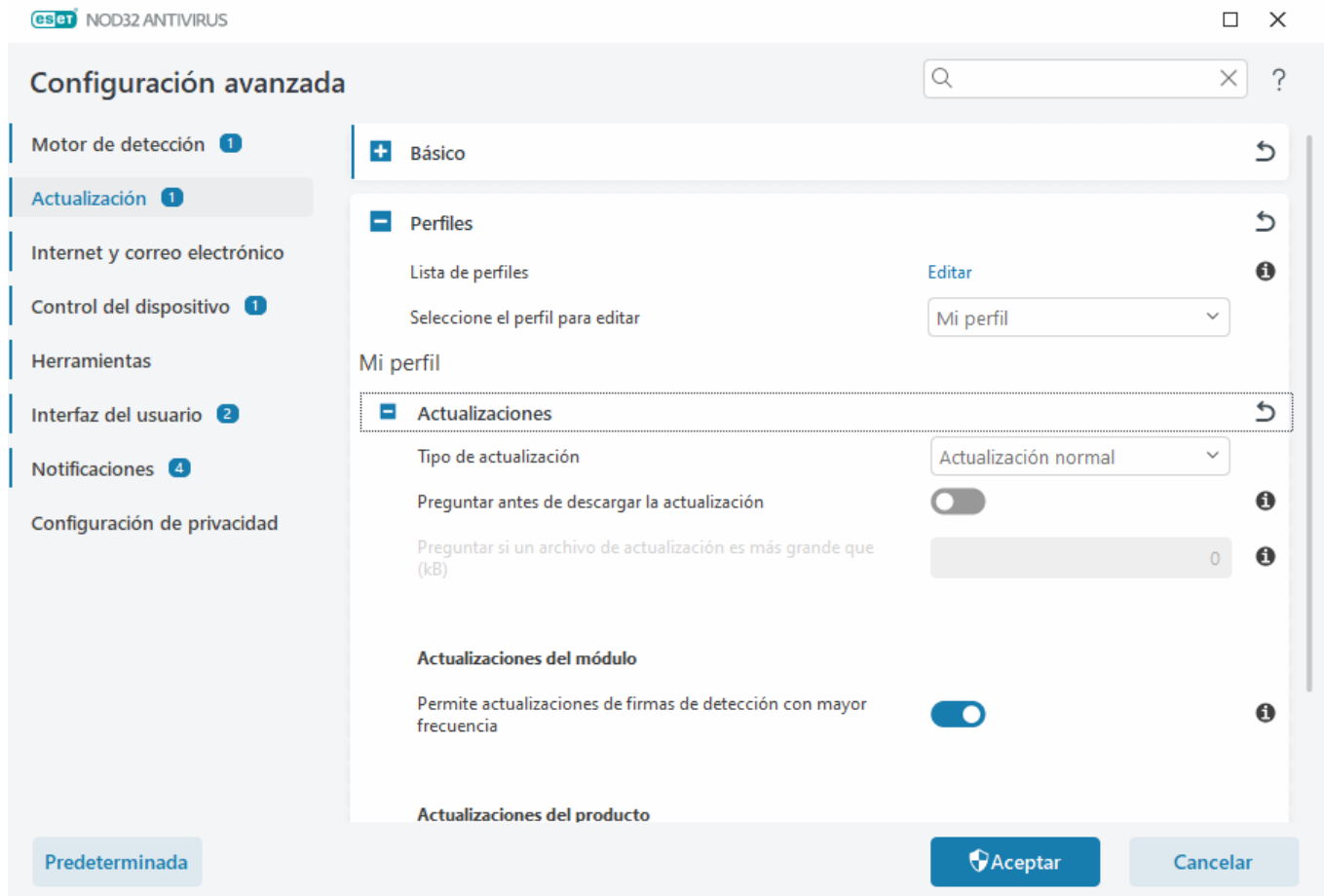
El perfil de actualización que está actualmente en uso (a menos que se configure uno específico en **Configuración avanzada > Firewall > Redes conocidas**) se muestra en el menú desplegable **Seleccionar perfil de actualización predeterminado**.

Para crear un nuevo perfil, consulte la sección [Actualizar perfiles](#).

Si experimenta alguna dificultad cuando intenta descargar las actualizaciones del motor de detección o de los módulos, haga clic en **Borrar** para borrar la caché o los archivos de actualización temporales.

Reversión de módulo

Si sospecha que la nueva actualización del motor de detección 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.



Para que las actualizaciones se descarguen correctamente, es esencial que complete correctamente todos los parámetros de actualización. Si usa un firewall, asegúrese de que el programa de ESET tenga permiso para comunicarse con Internet (por ejemplo, una comunicación HTTP).

Perfiles

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 **Seleccionar perfil para editar** muestra el perfil seleccionado actualmente, que en forma predeterminada está configurado en **Mi perfil**. Para crear un perfil nuevo, haga clic en **Editar** junto a la **Lista de perfiles**, ingrese su propio **Nombre de perfil** y luego haga clic en **Agregar**.

Actualizaciones

De forma predeterminada, el **Tipo de actualización** está configurado en **Actualización normal** para garantizar que los archivos de actualización se descarguen automáticamente del servidor de ESET con la menor carga de tráfico de red. 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 al lanzamiento mediante el 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 establecidas en todo momento y NO DEBEN utilizarse en estaciones de trabajo y servidores de producción donde se necesita de estabilidad y disponibilidad máximas.

Preguntar antes de descargar la actualización: el programa mostrará una notificación en la que puede elegir confirmar o rechazar la descarga de archivos de actualización.

Preguntar si el tamaño de un archivo de actualización es mayor que (kB): el programa mostrará un diálogo de confirmación si el tamaño del archivo de actualización es mayor que el valor especificado. Si el tamaño del archivo de actualización se encuentra configurado en 0 kB, el programa siempre mostrará un diálogo de confirmación.

Actualizaciones del módulo

Habilitar actualizaciones más frecuentes de firmas de detección – las firmas de detección se actualizarán en intervalos más cortos. Deshabilitar esta configuración puede afectar negativamente la tasa de detección.

Actualizaciones del producto

Actualizaciones de características de la aplicación: instala automáticamente nuevas versiones de ESET NOD32 Antivirus.

Opciones de conexión

Para utilizar un servidor proxy para descargar actualizaciones, consulte la sección [Opciones de conexión](#).

Actualizar reversión

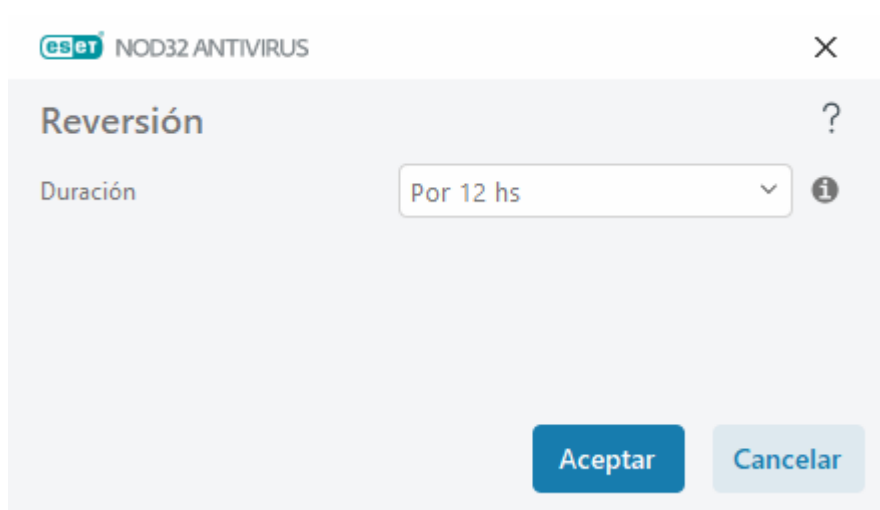
Si sospecha que la nueva actualización del motor de detección o los módulos de programas pueden ser inestables o estar corruptos, puede hacer una reversión a la versión anterior y deshabilitar cualquier actualización de manera temporal. O bien puede habilitar las actualizaciones que se deshabilitaron anteriormente si las pospuso de manera indefinida.

ESET NOD32 Antivirus registra instantáneas del motor de detección y de los módulos de programas para usar con la característica de revisión. Para crear instantáneas de la base de datos de virus, deje **Crear instantáneas de los módulos** habilitado. Cuando **Crear instantáneas de los módulos** está habilitado, la primera instantánea se crea durante la primera actualización. La siguiente se crea después de 48 horas. El campo **Cantidad de instantáneas almacenadas localmente** define la cantidad de instantáneas anteriores del motor de detección que se almacenaron.



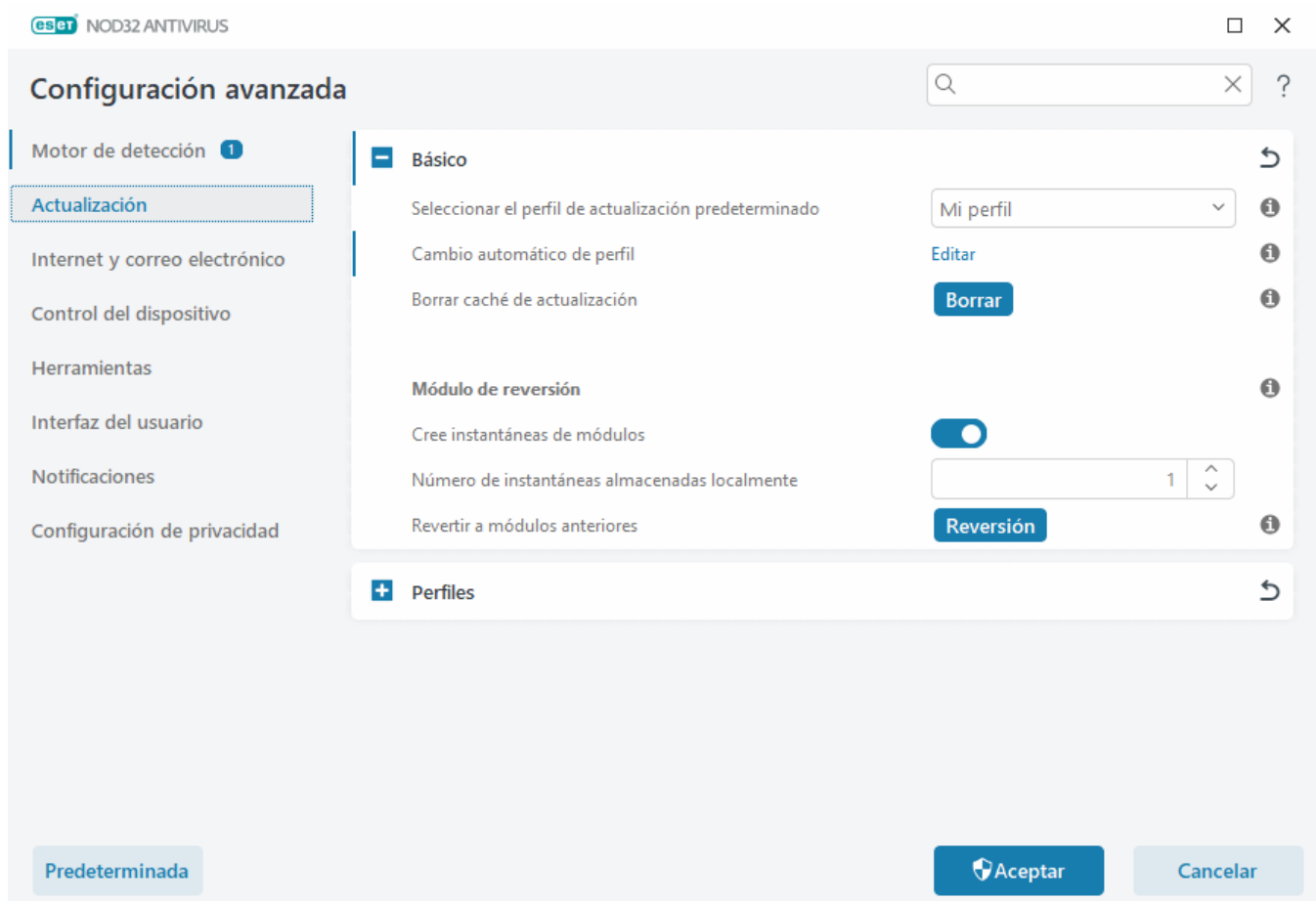
Cuando se alcanza la cantidad máxima de instantáneas (por ejemplo, tres), la instantánea más antigua se reemplaza con una nueva cada 48 horas. ESET NOD32 Antivirus revierte las versiones de actualización del motor de detección y del módulo del programa a la instantánea más antigua.

Si hace clic en **Revertir (Configuración avanzada (F5) > Actualizar > Básico)**, debe seleccionar un intervalo de tiempo en el menú desplegable **Duración** que represente el período de tiempo en el que el motor de detección y las actualizaciones del módulo de programa estarán en pausa.



Seleccione **Hasta que se revoque** si desea posponer las actualizaciones periódicas de forma indefinida hasta restaurar la funcionalidad manualmente. ESET no recomienda seleccionar esta opción porque representa un riesgo de seguridad potencial.

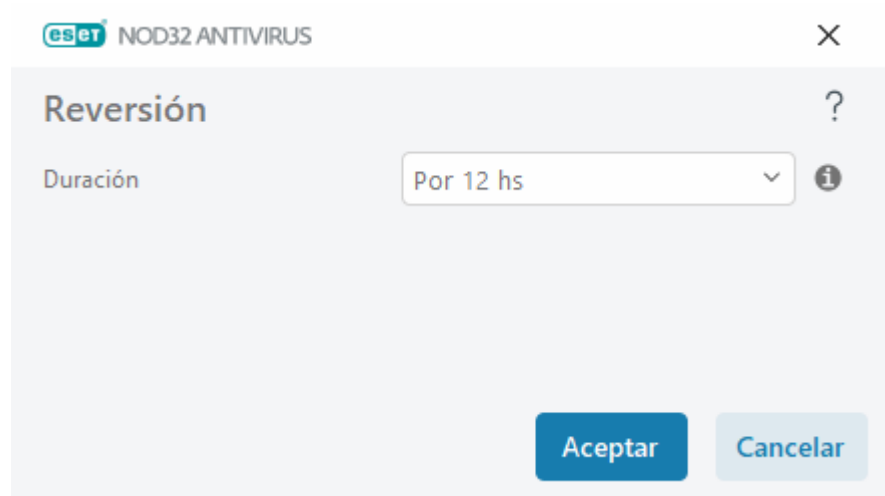
Si se realiza una reversión, el botón **Revertir** cambia a **Permitir actualizaciones**. No se permiten las actualizaciones durante el intervalo de tiempo seleccionado desde el menú desplegable **Suspender actualizaciones**. La versión del motor de detección regresa a la versión más antigua disponible y se guarda como una instantánea en el sistema local de archivos del equipo.



Suponga que 22700 es el número de versión más reciente del motor de detección y que 22698 y 22696 se guardan como instantáneas del motor de detección. Tenga en cuenta que 22697 no está disponible porque. En este ejemplo, el equipo se apagó durante la actualización de 22697 y se ofreció una actualización más reciente antes de descargar 22697. Si ha ingresado 2 (dos) en el campo **Cantidad de instantáneas almacenadas localmente** y hace clic en **Revertir**, el motor de detección (incluidos los módulos de programa) se restaurará a la versión número 22696. Este proceso puede tardar unos minutos. Revise si la versión del motor de detección se ha revertido en la pantalla [Actualizar](#).

Intervalo de tiempo de reversión

Si hace clic en **Revertir** (**Configuración avanzada** (F5) > **Actualizar** > **Básico**), debe seleccionar un intervalo de tiempo en el menú desplegable **Duración** que represente el período de tiempo en el que el motor de detección y las actualizaciones del módulo de programa estarán en pausa.



Seleccione **Hasta que se revoque** si desea posponer las actualizaciones periódicas de forma indefinida hasta restaurar la funcionalidad manualmente. ESET no recomienda seleccionar esta opción porque representa un riesgo de seguridad potencial.

Actualizaciones del producto

La sección **Actualizaciones del producto** le permite instalar actualizaciones de características nuevas cuando están disponibles automáticamente.

Las actualizaciones de características de la aplicación presentan nuevas características o cambian las que ya existen de versiones anteriores. Puede realizarse automáticamente sin la intervención del usuario, pero también puede elegir recibir una notificación. Después de instalar una actualización de características de la aplicación, es posible que sea necesario reiniciar el equipo.

Actualizaciones de características de la aplicación: cuando esta opción está activada, las actualizaciones de las características de la aplicación se realizarán automáticamente.

Opciones de conexión

Para acceder a las opciones de configuración del servidor proxy para un perfil de actualización determinado, haga clic en **Actualizar** en el árbol de **Configuración avanzada** (F5) y luego haga clic en **Perfiles > Actualizaciones > Opciones de conexión**. Haga clic en el menú desplegable **Modo de proxy** y seleccione una de las siguientes tres opciones:

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

Cuando seleccione la opción **Usar la configuración global del servidor proxy**, se usarán las opciones de configuración del servidor proxy ya especificadas en la sección **Configuración avanzada > Herramientas > Servidor proxy**.

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 en los siguientes casos:

- Uso de un servidor proxy diferente al definido en **Configuración avanzada > Herramientas > Servidor proxy** para actualizar ESET NOD32 Antivirus. En esta configuración, la información del proxy nuevo se debe especificar en dirección de **Servidor de proxy**, **Puerto** de comunicación (3128, predeterminado) y **Nombre de usuario** y **Contraseña** para el servidor proxy, si fuera 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 se cambia (p. ej., cambia el ISP), verifique desde esta ventana que la configuración del proxy sea la correcta. De lo contrario, el programa no podrá conectarse con los servidores de actualización.

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

Use conexión directa si el proxy no está disponible – si no puede llegar al proxy durante la actualización, se evadirá.



Los campos **Nombre de usuario** y **Contraseña** de esta sección son específicos del servidor proxy. Complete estos campos solo si necesita el nombre de usuario y la contraseña para acceder al servidor proxy. Estos campos solo deberían completarse si tiene la certeza de que se requiere una contraseña para acceder a Internet a través de un servidor proxy.

Cómo crear tareas de actualización

Las actualizaciones pueden accionarse manualmente con un clic en **Buscar actualizaciones** en la ventana primaria que se muestra al hacer clic en **Actualizar** 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 después tras conexión de acceso telefónico**
- **Actualización automática luego del 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](#).

Cuadro de diálogo: es necesario reiniciar

Después de actualizar ESET NOD32 Antivirus con una nueva versión, es necesario reiniciar el equipo. Las versiones nuevas de ESET NOD32 Antivirus se emiten para implementar mejoras o corregir problemas que las actualizaciones automáticas de los módulos del programa no pueden resolver.

La nueva versión de ESET NOD32 Antivirus puede instalarse automáticamente, en función de la [configuración de actualización del programa](#), o manualmente mediante la [descarga e instalación de una versión más reciente](#) con respecto a la anterior.

Haga clic en **Reiniciar ahora** para reiniciar el equipo. Si tiene pensado reiniciar el equipo más tarde, haga clic en **Recordarme más tarde**. Posteriormente, puede reiniciar el equipo manualmente desde la sección **Vista general** de la [ventana principal del programa](#).

Herramientas

El menú **Herramientas** incluye características que ofrecen seguridad adicional y ayudan a simplificar la administración de ESET NOD32 Antivirus. Están disponibles las siguientes herramientas:



[Archivos de registro](#)



[Procesos en ejecución](#) (si ESET LiveGrid® se encuentra habilitado en ESET NOD32 Antivirus)



[Informe de seguridad](#)



[ESET SysInspector](#)



[Tareas programadas](#)



[Limpiador de sistema](#)

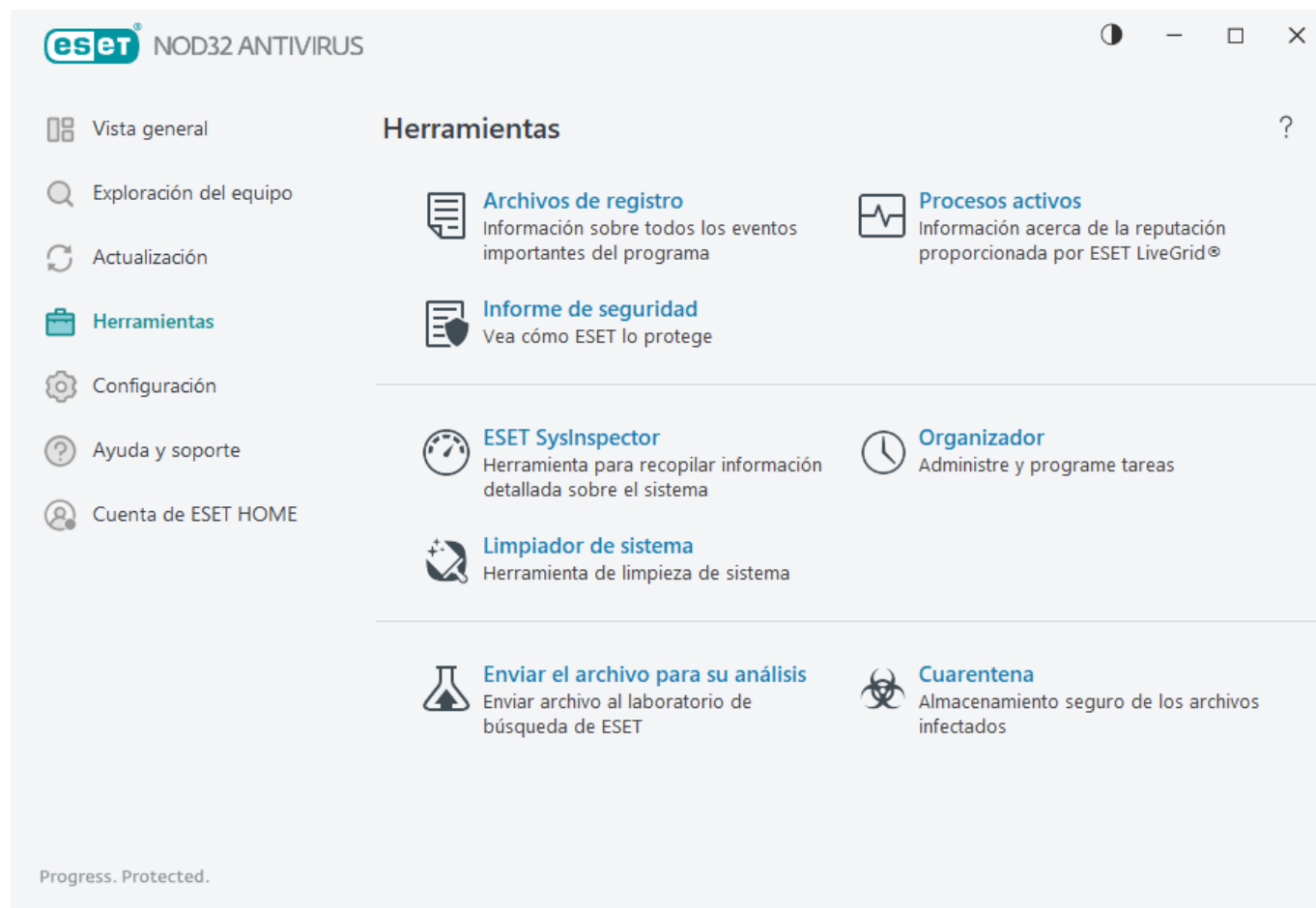


[Enviar muestra para su análisis](#) (puede que no esté disponible en función de la configuración de [ESET](#))

[LiveGrid®](#)).

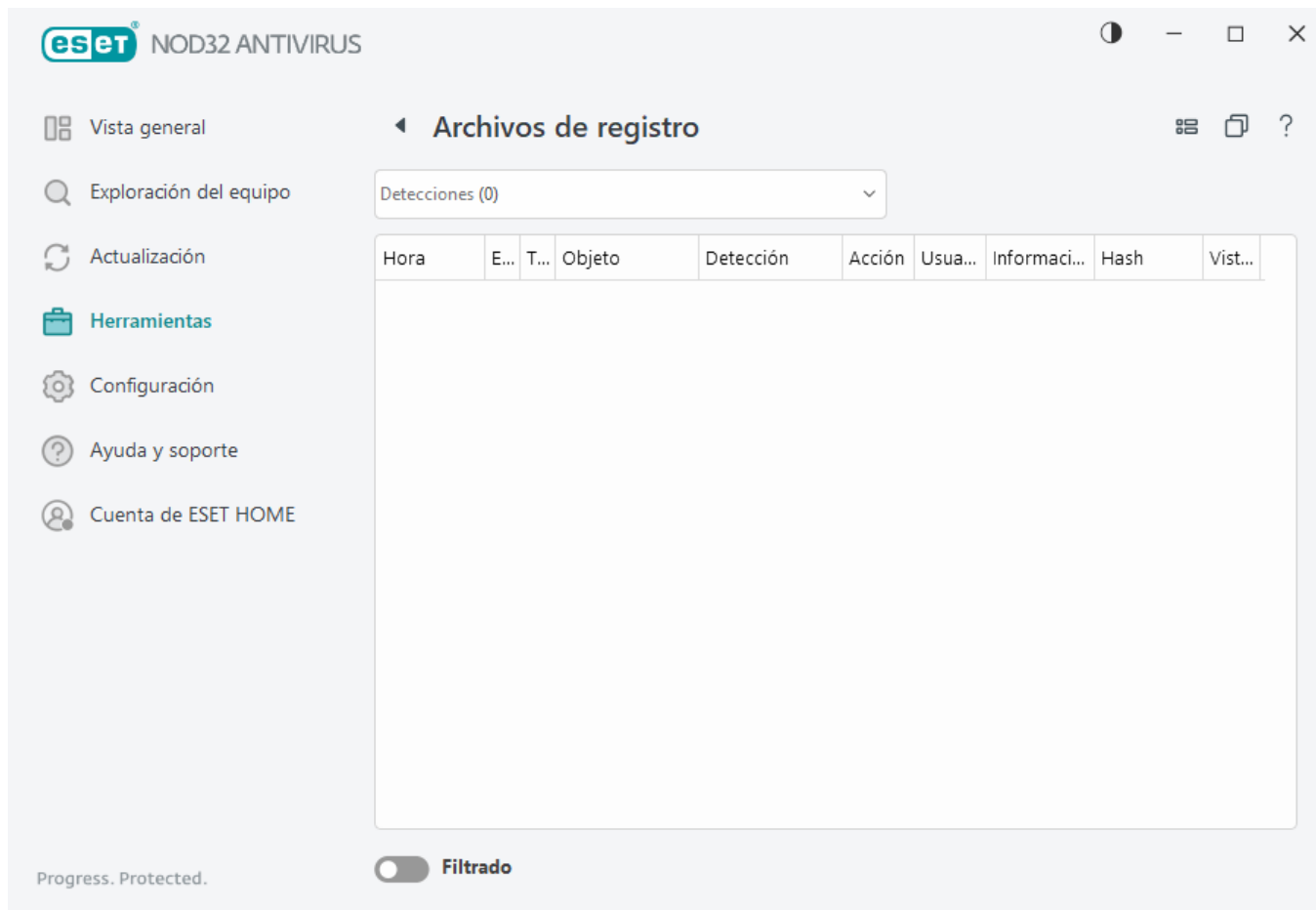


[Cuarentena](#)



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. 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 archivar 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.

- **Amenazas detectadas:** el registro de amenazas ofrece información detallada sobre las infiltraciones y amenazas detectadas por ESET NOD32 Antivirus. La información de registro incluye la hora de la detección, el tipo de exploración, el tipo de objeto, el nombre de la detección, la acción realizada y el nombre del usuario registrado cuando se detectó la infiltración, el hash y la primera ocurrencia. Las infiltraciones no limpiadas se marcan siempre con texto rojo sobre un fondo rojo claro. Mientras que las infiltraciones limpiadas se marcan con texto amarillo sobre un fondo blanco. Las aplicaciones no deseadas o potencialmente inseguras no limpiadas se marcan con texto amarillo sobre fondo blanco.
- **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 anteriores. Cada línea corresponde a un único exploración del equipo. Haga doble clic en cualquier entrada para visualizar los [detalles de la exploración seleccionado](#).
- **HIPS:** contiene historiales de las reglas [HIPS](#) específicas que están marcadas 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.
- **Sitios Web filtrados** Esta lista es útil si quiere consultar los sitios Web bloqueados por la [Protección del acceso a la Web](#). Cada registro incluye la hora, la dirección URL, el usuario y la aplicación de creación de

conexión con un 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. También puede ver detalles tales como el tipo de dispositivo, número de serie, nombre del proveedor y tamaño del medio (si está disponible).

Seleccione los contenidos de cualquier registro y presione **CTRL + C** para copiarlo al portapapeles. Mantenga presionado **CTRL** o **SHIFT** para seleccionar varias entradas.

Haga clic en  **Filtrado** para abrir la ventana [Filtrado de registros](#) donde puede definir los criterios de filtrado.

Haga clic con el botón secundario en un registro específico para abrir el menú contextual. Las siguientes opciones se encuentran disponibles en el menú contextual:

- **Mostrar**— muestra información más detallada acerca del registro seleccionado en una ventana nueva.
- **Filtrar los mismos historiales** — luego de activar este filtro, solo verá los historiales del mismo tipo (diagnósticos, advertencias, ...).
- **Filtrar** — Después de hacer clic en esta opción, la ventana [Filtrado de registros](#) le permitirá definir los criterios de filtrado para entradas de registros específicas.
- **Habilitar filtro** — activa las configuraciones de los filtros.
- **Deshabilitar el filtro** — borra todas las configuraciones del filtro (descritas arriba).
- **Copiar/Copiar todo:** copia información sobre los registros seleccionados.
- **Copiar celda**—copia el contenido de la celda en la que se hace clic con el botón derecho.
- **Quitar/Quitar todo:** quita los registros seleccionados o todos los registros mostrados. Esta acción requiere privilegios de administrador.
- **Exportar/Exportar todo:** exporta información acerca de los registros seleccionados o de todos los registros en formato XML.
- **Buscar/Buscar siguiente/Buscar anterior:** después de hacer clic en esta opción, puede definir los criterios de filtrado para resaltar la entrada específica desde la ventana Filtrado de registros.
- **Descripción de la detección:** abre la enciclopedia de amenazas de ESET, que contiene información detallada sobre los peligros y los síntomas de la infiltración registrada.
- **Crear exclusión** — Cree una nueva [Exclusión de la detección con un asistente](#) (no disponible para la detección de malware).

Filtrado de registros

Haga clic en  **Filtre** en **Herramientas > Archivos de registro** para definir los criterios de filtrado.

La característica de filtrado de registros lo ayudará a encontrar la información que busca, en particular, cuando hay muchos registros. Le permite acotar los registros, por ejemplo, si busca un tipo de evento, un estado o un periodo de tiempo específicos. Puede filtrar los registros al especificar ciertas opciones de búsqueda y solo se mostrarán los registros que sean pertinentes (en función de dichas opciones de búsqueda) en la ventana Archivos de registro.

Escriba la palabra clave que está buscando en el campo **Buscar texto**. Utilice el menú desplegable **Buscar en columnas** para acotar la búsqueda. Elija uno o más registros del menú desplegable **Tipos de registro**. Defina el **periodo de tiempo** para el que quiere que se muestren los resultados. También puede usar otras opciones de búsqueda, como **Solo coincidir palabras completas** o **Coincidir mayúsculas y minúsculas**.

Buscar el texto

Escriba una cadena (palabra o una parte de una palabra). Solo se mostrarán los registros que contengan dicha cadena. Se omitirán otros registros.

Buscar en columnas

Seleccione qué columnas se tomarán en cuenta en la búsqueda. Puede marcar una o más columnas para utilizar en la búsqueda.

Tipos de historiales

Elija uno o más tipos de registro del menú desplegable:

- **Diagnóstico** – registra la información necesaria para ajustar el programa y todos los historiales antes mencionados.
- **Informativo** – registra los mensajes de información, que incluyen los mensajes de actualizaciones correctas, y todos los historiales antes mencionados.
- **Advertencias** – registra los errores críticos y los mensajes de advertencia.
- **Errores** – se registrarán errores tales como “Error al descargar el archivo” y los errores críticos.
- **Crítico** – registra solo los errores críticos (error al iniciar la protección antivirus,

Período de tiempo

Defina el momento a partir del cual desea que se muestren los resultados.

- **Sin especificar** (predeterminado): no busca en un periodo de tiempo, sino en todo el registro.
- **Ayer**
- **Última semana**
- **El mes pasado**
- **Período de tiempo**: puede especificar el periodo de tiempo exacto (Desde: y Hasta:) para filtrar únicamente los registros del periodo de tiempo especificado.

Solo coincidir palabras completas

Utilice la casilla de verificación si quiere buscar palabras completas para resultados más precisos.

Coincidir mayúsculas y minúsculas

Habilite esta opción si es importante para usted usar letras mayúsculas o minúsculas al filtrar. Una vez que haya configurado las opciones de filtrado/búsqueda, haga clic en **Aceptar** para mostrar los registros filtrados o en **Buscar** para comenzar a buscar. Los archivos de registro se buscan de arriba hacia abajo, comenzado por su posición actual (el registro que está resaltado). La búsqueda se detiene cuando encuentra el primer registro coincidente. Presione **F3** para buscar el siguiente registro o haga clic con el botón secundario y seleccione **Buscar** para refinar las opciones de búsqueda.

Configuración de registro

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 > 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 antes mencionados.
- **Informativo** – registra los mensajes de información, que incluyen los mensajes de actualizaciones correctas, y todos los historiales antes mencionados.
- **Advertencias** – registra los errores críticos y los mensajes de advertencia.
- **Errores** – se registrarán errores tales como “Error al descargar el archivo” y los errores críticos.
- **Crítico** – registra solo los errores críticos (error al iniciar la protección antivirus etc.)

i Todas las conexiones bloqueadas se grabarán cuando seleccione el nivel de detalle Diagnóstico.

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

Habilitar protocolo del texto habilita el almacenamiento de los registros en otro formato de archivo distinto del de los [Archivos de registro](#):

- **Directorio de destino:** el directorio donde se almacenarán los archivos de registro (solo se aplica a texto/CSV). Cada sección de registro tiene su propio archivo con un nombre de archivo predefinido (por ejemplo, virlog.txt para la sección de archivos de registro **Detecciones**, si usa un formato de archivo de texto sin formato para almacenar los registros).
- **Tipo** – si selecciona el formato de archivo **Texto**, los registros se almacenarán en un archivo de texto, y los datos se separarán mediante tabulaciones. Lo mismo se aplica para el formato del archivo **CSV** separado por comas. Si elige **Evento**, los registros se almacenarán en el registro Windows Event (se puede ver mediante el Visor de eventos en el Panel de control) en lugar del archivo.
- **Eliminar todos los archivos de registro** – borra todos los registros almacenados seleccionados actualmente en el menú desplegable **Tipo**. Se mostrará una notificación acerca de la eliminación correcta de los registros.



Para ayudar a resolver los problemas más rápidamente, ESET le puede solicitar que proporcione los registros de su equipo. El ESET Log Collector le facilita la recopilación de la información necesaria. Para obtener más información acerca del ESET Log Collector, visite nuestro [artículo de la Base de conocimiento de ESET](#).

Procesos en ejecución

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 LiveGrid®](#).

Procesos activos

Esta ventana muestra una lista de los archivos seleccionados con información adicional de ESET LiveGrid®. Se indica la reputación de cada uno, junto con la cantidad de usuarios y el momento de detección inicial.

Reputación	Proceso	PID	Cantidad de ...	Tiempo d...	Nombre de la aplicación
Good	smss.exe	364	Good	hace 1 año	Microsoft® Windows® ...
Good	csrss.exe	472	Good	hace 2 años	Microsoft® Windows® ...
Good	wininit.exe	552	Good	hace 3 me...	Microsoft® Windows® ...
Good	winlogon.exe	624	Good	hace 2 se...	Microsoft® Windows® ...
Good	services.exe	696	Good	hace 1 año	Microsoft® Windows® ...
Good	lsass.exe	704	Good	hace 3 me...	Microsoft® Windows® ...
Good	svchost.exe	832	Good	hace 6 me...	Microsoft® Windows® ...
Good	fontdrvhost.exe	864	Good	hace 1 mes	Microsoft® Windows® ...
Good	dwm.exe	436	Good	hace 2 años	Microsoft® Windows® ...
Good	wudfhost.exe	1532	Good	hace 6 me...	Microsoft® Windows® ...
Good	vboxservice.exe	1600	Yellow	hace 2 años	Oracle VM VirtualBox G...
Good	efwd.exe	1764	Yellow	hace 3 días	ESET Security
Good	spoolsv.exe	2916	Good	hace 2 se...	Microsoft® Windows® ...
Good	akvcamassistant.exe	3108	Yellow	hace 2 años	AKVCamAssistant
Good	sihost.exe	4652	Good	hace 2 años	Microsoft® Windows® ...
Good	taskhostw.exe	3336	Good	hace 6 me...	Microsoft® Windows® ...
Good	ctfmon.exe	4228	Good	hace 2 años	Microsoft® Windows® ...

Progress. Protected. [Mostrar detalles](#)

Reputación – en la mayoría de los casos, la tecnología ESET NOD32 Antivirus y ESET LiveGrid® 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 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).

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 clic con el botón secundario en un área de la barra de tareas y luego haga clic en **Administrador de tareas**, o presione **Ctrl+Shift+Esc** en el teclado.

i Las aplicaciones conocidas marcadas como Seguras (verde) están definitivamente limpias (están en la lista blanca) y se excluirán de la exploración para mejorar el rendimiento.

PID : el número del identificador de procesos se puede usar como parámetro en diversas llamadas de funciones como ajustar la prioridad del proceso.

Cantidad de usuarios – la cantidad de usuarios que usan una aplicación específica. Estos datos se recopilan con la tecnología ESET LiveGrid®.

Tiempo de descubrimiento – periodo transcurrido desde que la tecnología ESET LiveGrid® descubrió la aplicación.

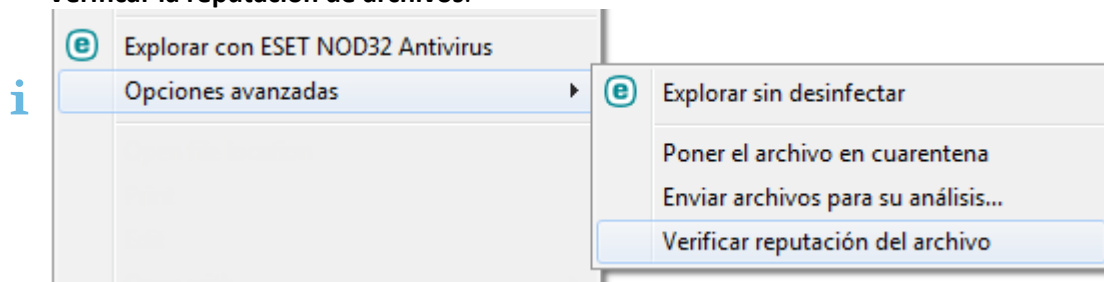
i La aplicación marcada como Desconocida (naranja) no es necesariamente software malicioso. Por lo general, solo se trata de una aplicación nueva. Si no está seguro con respecto al archivo, puede [enviar el archivo para su análisis](#) al laboratorio de investigación de ESET. Si el archivo resulta ser una aplicación maliciosa, se agregará su detección a una de las próximas actualizaciones.

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

Haga clic sobre una aplicación para mostrar los siguientes detalles de dicha aplicación:

- **Ruta** – ubicación de una aplicación en su equipo.
- **Tamaño** – tamaño del archivo ya sea en kB (kilobytes) o MB (megabytes).
- **Descripción** – características del archivo según la descripción proporcionada por el sistema operativo.
- **Empresa** – nombre del proveedor o del proceso de la aplicación.
- **Versión** – información proporcionada por el desarrollador de la aplicación.
- **Producto** – nombre de la aplicación y/o nombre comercial.
- **Creado el/Modificado el:** fecha y hora de la creación (modificación).

También puede verificar la reputación de los archivos que no sean programas o procesos activos. Para ello, haga clic con el botón secundario en un explorador de archivos y seleccione **Opciones avanzadas** > **Verificar la reputación de archivos**.




Informe de seguridad

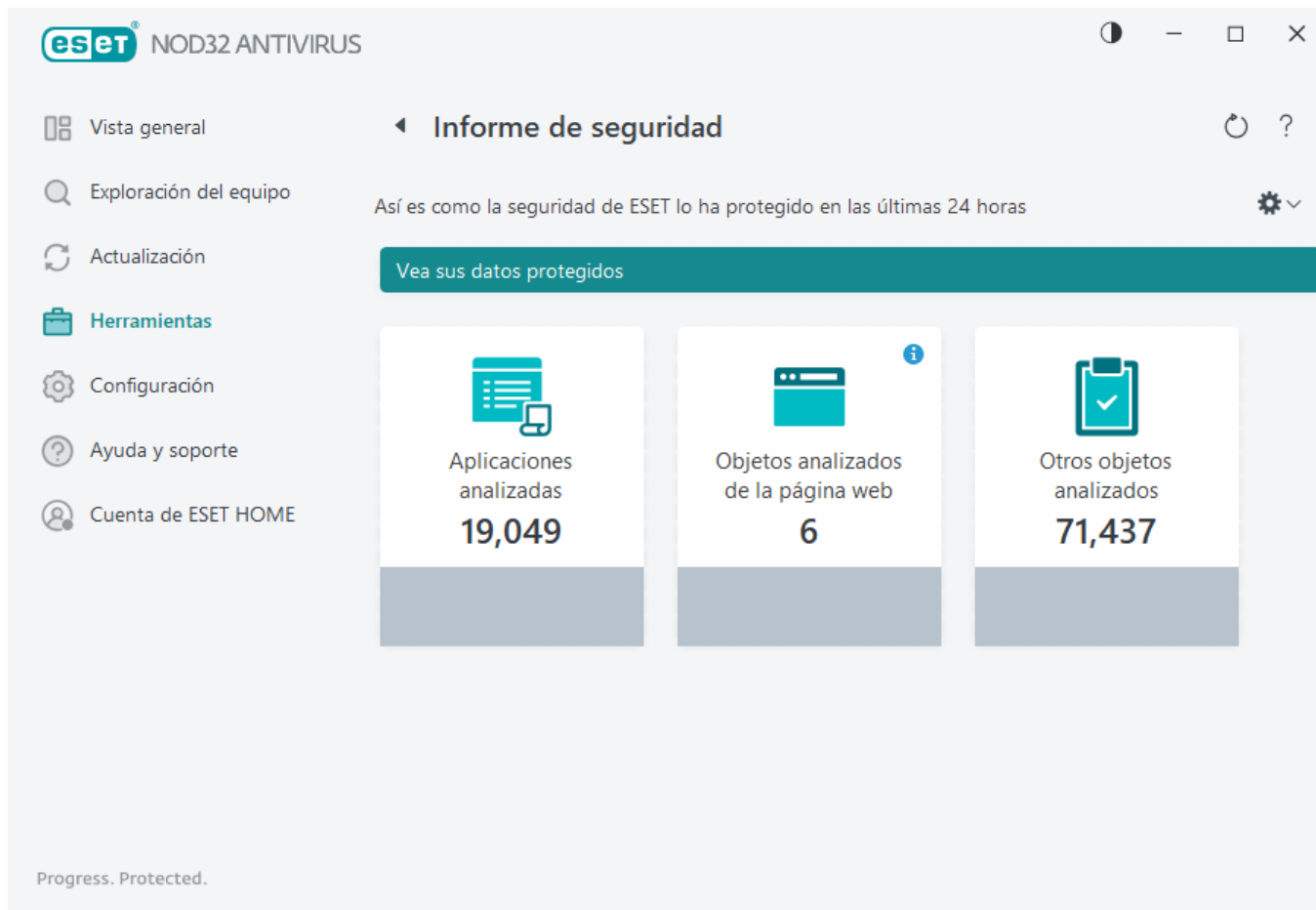
Esta función proporciona una descripción general de las estadísticas para las siguientes categorías:

- **Páginas web bloqueadas** – Muestra el número de páginas web bloqueadas (URL en la lista negra para PUA, phishing, router hackeado, IP o certificado).
- **Objetos de correo electrónico infectados detectados** – Muestra el número de [objetos](#) de correo electrónico infectados que se han detectado.
- **PUA detectadas** – Muestra el número de [aplicaciones potencialmente no deseadas](#) (PUA).
- **Documentos revisados** – Muestra el número de objetos de documento explorados.
- **Aplicaciones exploradas**: muestra el número de objetos ejecutables explorados.
- **Otros objetos revisados** – Muestra el número de otros objetos explorados.
- **Objetos de páginas web explorados**: muestra el número de objetos explorados de la página web.
- **Objetos del correo electrónico analizados**: muestra el número de objetos del correo electrónico analizados.

El orden de estas categorías depende del valor numérico, desde el más alto hasta el más bajo. No se visualizan las categorías con valores cero. Haga clic en **Mostrar más** para expandir y mostrar categorías ocultas.

Una vez que la función está activada, ya no aparecerá como no funcional en el informe de seguridad.

Haga clic en la rueda de engranaje  en la esquina superior derecha, donde puede **Habilitar/deshabilitar las notificaciones del informe de seguridad** o puede seleccionar si los datos que se mostrarán serán de los últimos 30 días o desde que se activó el producto. Si ESET NOD32 Antivirus tiene menos de 30 días de instalación, sólo se puede seleccionar el número de días desde la instalación. El período de 30 días se establece de forma predeterminada.



Restablecer los datos eliminará todas las estadísticas así como los datos existentes para el informe de seguridad. Esta acción debe confirmarse, a menos que se desactive la opción **Preguntar antes de restablecer las estadísticas** en **Configuración avanzada > Notificaciones > Alertas interactivas > Mensajes de confirmación > Editar**.

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, 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. Para aprender a usar ESET SysInspector, consulte la [Ayuda en línea de ESET SysInspector](#).

La ventana ESET SysInspector muestra la siguiente información de los registros:

- **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:

- **Mostrar**: abre el registro seleccionado de ESET SysInspector. También puede hacer clic derecho en un

archivo de registro determinado y seleccionar **Mostrar** en el menú contextual.

- **Crear** – crea un nuevo registro. Espere a que se genere ESET SysInspector (estado **Creado**) antes de intentar acceder al registro.
- **Eliminar** – elimina los registros seleccionados de la lista.

Los siguientes elementos están disponibles en el menú contextual cuando se seleccionan uno o más archivos de registro:

- **Mostrar** – abre el registro seleccionado en ESET SysInspector (equivale a hacer doble clic en el registro).
- **Crear** – crea un nuevo registro. Espere a que se genere ESET SysInspector (estado **Creado**) antes de intentar acceder al registro.
- **Eliminar** – elimina los registros seleccionados de la lista.
- **Eliminar todo** – elimina todos los registros.
- **Exportar** – exporta el registro a un archivo .xml o .xml comprimido. El registro se exporta a C:\ProgramData\ESET\ESET Security\SysInspector.

Tareas programadas

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

Para acceder a las tareas programadas, diríjase a la [ventana principal del programa](#) ESET NOD32 Antivirus y haga 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.

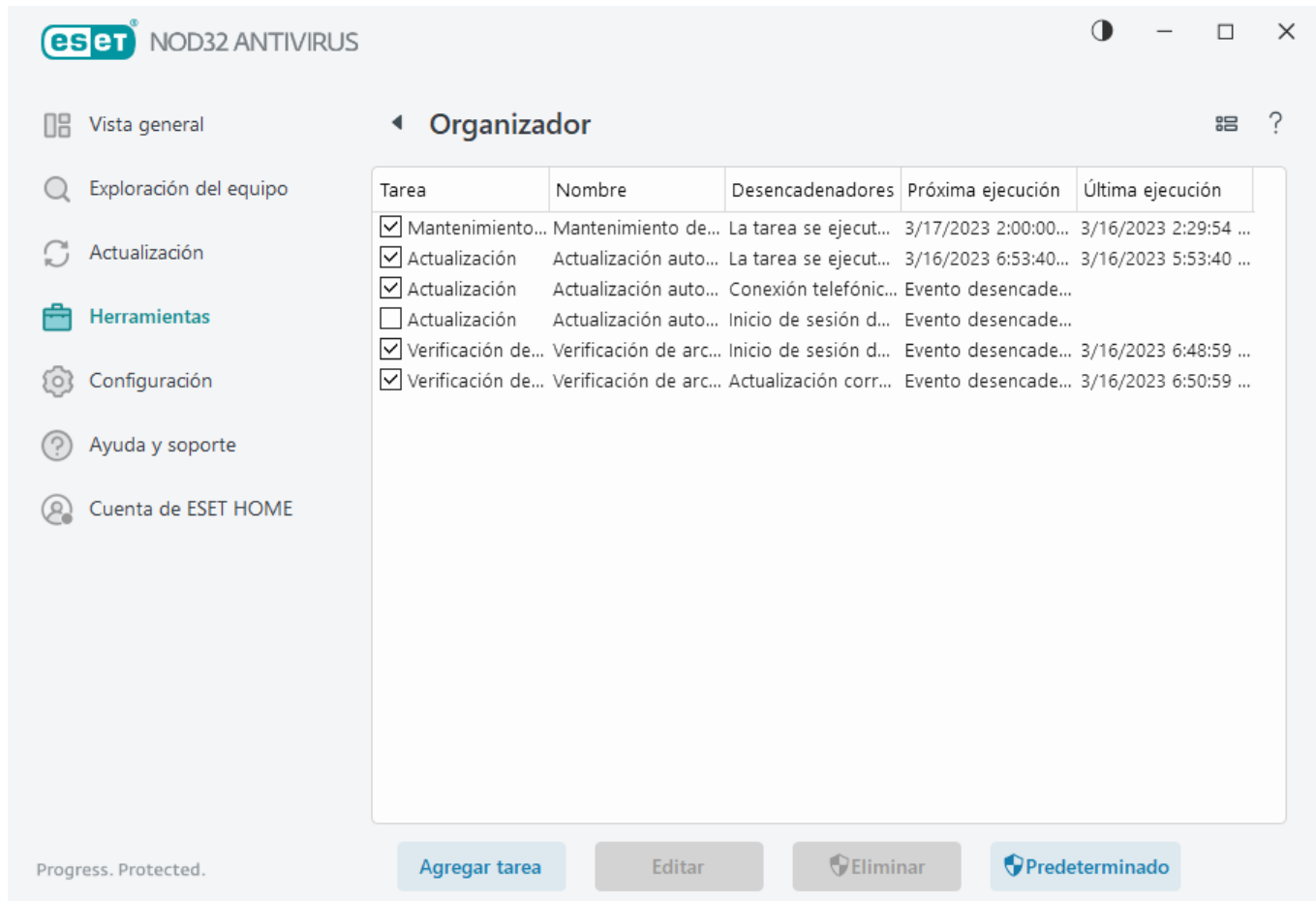
Esta sección sirve para programar las siguientes tareas: la actualización de módulos, la tarea de exploración, la verificación de archivos de inicio del sistema y el mantenimiento de registros. Puede agregar o eliminar tareas directamente desde la ventana principal de Tareas programadas (haga clic en **Agregar tarea** o **Eliminar** en el sector inferior). Puede restaurar la lista de tareas programadas a los valores predeterminados y eliminar todos los cambios haciendo clic en **Predeterminado**. Haga un clic con el botón secundario 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. Use 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 después tras conexión de acceso telefónico**
- **Actualización automática luego del registro del usuario**
- **Verificación de archivos de inicio automática** (después del registro del usuario)

- **Exploración automática de archivos durante el inicio del sistema** (tras la actualización correcta del motor de detección)

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



Agregar una nueva tarea

1. Haga clic en **Agregar tarea** en el sector inferior de la ventana.

2. Ingrese el nombre de la tarea.

3. Seleccione la tarea deseada desde el menú desplegable:

- **Ejecutar aplicación externa** – programa la ejecución de una aplicación externa.
- **Mantenimiento de registros**: los archivos de registro también contienen remanentes de historiales eliminados. Esta tarea optimiza los historiales de los archivos de registro en forma habitual para que funcionen eficazmente.
- **Verificación de archivos de inicio del sistema**: verifica los archivos que tienen permiso para ejecutarse al iniciar el sistema o tras el registro del usuario.
- **Crear una instantánea de estado del equipo**: crea una instantánea del equipo de [ESET SysInspector](#), que recopila información detallada sobre los componentes del sistema (por ejemplo, controladores, aplicaciones) y evalúa el nivel de riesgo de cada componente.

- **Exploración del equipo a pedido:** realiza una exploración del equipo de los archivos y las carpetas de su equipo.
- **Actualización:** programa una tarea de actualización mediante la actualización de módulos.

4. Haga clic en la barra deslizante junto a **Habilitado** para activar la tarea (puede hacerlo luego al seleccionar/anular la selección de la casilla de verificación en la lista de tareas programadas), haga clic en **Siguiente** y seleccione una de las opciones de programación:

- **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 en el día y a la hora especificados.
- **Cuando se cumpla la condición** – la tarea se ejecutará tras un suceso especificado.

5. Seleccione **Omitir tarea al ejecutar con alimentación de la batería** para reducir los recursos del sistema mientras un equipo portátil se ejecuta con alimentación de la batería. La tarea se ejecutará en la fecha y hora especificadas en los campos de **Ejecución de la tarea**. Si la tarea no se pudo ejecutar en el momento predefinido, puede especificar cuándo se realizará nuevamente:

- **A la próxima hora programada**
- **Lo antes posible**
- **Inmediatamente, si la hora desde la última ejecución supera (horas):** representa el tiempo transcurrido desde la primera ejecución omitida de la tarea. Si se supera este tiempo, la tarea se ejecutará inmediatamente. Establezca la hora con el siguiente control de giro.

Para revisar la tarea programada, haga clic con el botón derecho en la tarea y, a continuación, haga clic en **Mostrar detalles de la tarea**.

Opciones de exploración programada

En esta ventana, puede especificar opciones avanzadas para una tarea de exploración programada del equipo.

Para ejecutar una exploración sin acciones de limpieza, haga clic en **Configuración avanzada** y seleccione **Explorar sin limpieza**. El historial de la exploración se guarda en el registro de la exploración.

Cuando se encuentra seleccionado **Ignorar exclusiones**, los archivos con extensiones que solían ser excluidas de la exploración serán analizadas sin excepción.

El menú desplegable **Acción después de la exploración** permite establecer una acción que se realice automáticamente tras finalizar una exploración:

- **Sin acción** – después de la finalización de la exploración, no se llevará a cabo ninguna acción.
- **Apagar** – el equipo se apaga después de la finalización de la exploración.

- **Reiniciar si es necesario:** el equipo se reinicia solo si es necesario para completar la limpieza de las amenazas detectadas.
- **Reiniciar** – cierra todos los programas abiertos, y reinicia el equipo luego de la finalización de la exploración.
- **Reiniciar si es necesario:** el equipo fuerza el reinicio solo si es necesario para completar la limpieza de las amenazas detectadas.
- **Forzar reinicio:** fuerza el cierre de todos los programas abiertos sin esperar la intervención del usuario y reinicia el equipo cuando finaliza la exploración.
- **Suspender**– guarda su sesión y pone el equipo en un estado de energía baja para que pueda volver a trabajar rápidamente.
- **Hibernar**– toma todo lo que se está ejecutando en la memoria RAM y lo envía a un archivo especial de su disco duro. Su equipo se apaga, pero reanudará su estado anterior la próxima vez que lo inicie.

i Las acciones **Suspender** o **Hibernar** están disponibles en función de la configuración de Activar o Hibernar del sistema operativo o de las capacidades de su equipo/computadora portátil. Tenga en cuenta que un equipo en suspensión aún es un equipo en funcionamiento. Sigue ejecutando funciones básicas y utilizando electricidad cuando el equipo funciona con la alimentación de la batería. Para preservar la vida útil de la batería, como cuando viaja fuera de su oficina, recomendamos utilizar la opción Hibernar.

La acción seleccionada comenzará tras la finalización de las exploraciones en ejecución. Cuando seleccione **Apagar** o **Reiniciar**, aparecerá un cuadro de diálogo de confirmación con una cuenta regresiva de 30 segundos (haga clic en **Cancelar** para desactivar la acción solicitada).

Seleccione **No se puede cancelar la exploración** para denegarles a los usuarios sin privilegios la capacidad de detener las medidas tomadas luego de la exploración.

Seleccione la opción **El usuario puede pausar la exploración durante (min.)** si desea permitir que el usuario limitado pause la exploración del equipo durante un periodo especificado.

Consulte también [Progreso de la exploración](#).

Resumen general de tareas programadas

Esta ventana de diálogo muestra información detallada acerca de la tarea programada seleccionada cuando hace doble clic en una tarea personalizada o clic derecho en una tarea programada personalizada y, luego, clic en **Mostrar detalles de la tarea**.

Detalles de tarea

Escriba el **Nombre de la tarea**, seleccione una de las opciones del **Tipo de tarea** y, a continuación, haga clic en **Siguiente**:

- **Ejecutar aplicación externa** – programa la ejecución de una aplicación externa.
- **Mantenimiento de registros:** los archivos de registro también contienen remanentes de historiales

eliminados. Esta tarea optimiza los historiales de los archivos de registro en forma habitual para que funcionen eficazmente.

- **Verificación de archivos de inicio del sistema:** verifica los archivos que tienen permiso para ejecutarse al iniciar el sistema o tras el registro del usuario.
- **Crear una instantánea de estado del equipo:** crea una instantánea del equipo de [ESET SysInspector](#), que recopila información detallada sobre los componentes del sistema (por ejemplo, controladores, aplicaciones) y evalúa el nivel de riesgo de cada componente.
- **Exploración del equipo a pedido:** realiza una exploración del equipo de los archivos y las carpetas de su equipo.
- **Actualización:** programa una tarea de actualización mediante la actualización de módulos.

Programación de tarea

La tarea se realizará reiteradamente en el intervalo de tiempo especificado. 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 luego de un suceso especificado.

Omitir tarea al ejecutar con alimentación de la batería: la tarea no se ejecutará si su equipo recibe alimentación de la batería en el momento en que la tarea debería iniciarse. Esto también es así en los equipos que reciben alimentación de un SAI.

Sincronización de la tarea: una vez

Ejecución de la tarea: la tarea especificada se ejecutará una sola vez en la fecha y a la hora especificadas.

Sincronización de la tarea: diariamente

La tarea se ejecutará todos los días a la hora especificada.

Sincronización de la tarea: Semanalmente

La tarea se ejecutará todas las semanas en los días y horarios seleccionados.

Sincronización de la tarea: desencadenada por un suceso

La tarea se accionará por uno de los siguientes sucesos:

- Cada vez que se inicie el equipo
- La primera vez que se inicie el equipo en el día
- Conexión a Internet/VPN por módem
- Actualización correcta del módulo
- Actualización correcta del producto
- Inicio de sesión del usuario
- Detección de amenazas

Cuando se programa una tarea accionada por un suceso, puede especificar el intervalo mínimo entre dos ejecuciones completas de la tarea. Por ejemplo, si inicia la sesión en su equipo varias veces al día, seleccione 24 horas para realizar la tarea solo en el primer inicio de sesión del día y, posteriormente, al día siguiente.

Omisión de una tarea

Una tarea se puede [omitir cuando el equipo está funcionando con baterías o si está desconectado](#). Seleccione cuándo debería ejecutarse la tarea entre una de estas opciones y haga clic en **Siguiente**:

- **En la siguiente hora programada:** la tarea se ejecutará si el equipo está activado en la siguiente hora programada.
- **Lo antes posible:** la tarea se ejecutará cuando el equipo esté activado.
- **Inmediatamente, si la hora desde la última ejecución programada supera (horas):** representa el tiempo transcurrido desde la primera ejecución omitida de la tarea. Si se supera este tiempo, la tarea se ejecutará inmediatamente.

De inmediato, en caso de que se supere el tiempo establecido desde la última ejecución programada (en horas) – ejemplos

Se configura una tarea de ejemplo para que se ejecute reiteradamente cada hora. La opción **Inmediatamente, si la hora desde la última ejecución programada excede (horas)** se selecciona y el tiempo superado se establece en dos horas. La tarea se ejecuta a las 13:00 y, cuando finaliza, el equipo queda en suspensión:

- El equipo se reactiva a las 15:30. La primera ejecución omitida de la tarea fue a las 14:00. Solo han transcurrido 1,5 horas desde las 14:00, por lo que la tarea se ejecutará a las 16:00.
- El equipo se reactiva a las 16:30. La primera ejecución omitida de la tarea fue a las 14:00. Han transcurrido dos horas y media desde las 14:00, por lo que la tarea se ejecutará inmediatamente.

Detalles de la tarea: actualizar

Si desea actualizar el programa desde dos servidores de actualización, será necesario crear dos perfiles de actualización diferentes. Si el primero no logra descargar los archivos de actualización, el programa cambia automáticamente al perfil alternativo. Esto es conveniente, por ejemplo, para equipos portátiles, que suelen actualizarse desde un servidor de actualización de la red de área local, pero cuyos dueños normalmente se conectan a Internet por medio de otras redes. Por lo tanto, si falla el primer perfil, el segundo descargará automáticamente los archivos de actualización desde los servidores de actualización de ESET.

Detalles de la tarea: ejecutar aplicación

En esta tarea se programa la ejecución de una aplicación externa.

Archivo ejecutable – elija un archivo ejecutable desde el árbol del directorio, haga clic en la opción ... e ingrese la ruta en forma manual.

Carpeta de trabajo – defina el directorio de trabajo de la aplicación externa. Todos los archivos temporales del **Archivo ejecutable** seleccionado se crearán dentro de este directorio.

Parámetros – parámetros de la línea de comandos de la aplicación (opcional).

Haga clic en **Finalizar** para aplicar la tarea.

Limpiador de sistema

El limpiador del sistema es una herramienta que lo ayuda a restaurar el equipo a un estado utilizable luego de eliminar la amenaza. El malware puede desactivar utilidades como el Editor de registro, el Administrador de tareas o las Actualizaciones de Windows. El limpiador de sistema restaura los valores predeterminados y las configuraciones para un sistema determinado con un solo clic.

El limpiador de sistema informa problemas de cinco categorías de configuración:

- **Configuración de seguridad:** cambios en la configuración que pueden causar una mayor vulnerabilidad de su equipo, como actualizaciones de Windows.
- **Configuración del sistema:** cambios en la configuración del sistema que pueden cambiar el comportamiento de su equipo, como asociaciones de archivos.
- **Aspecto del sistema:** configuración que afecta el aspecto de su sistema, como su fondo de escritorio.
- **Funciones desactivadas:** funciones importantes y aplicaciones que pueden estar deshabilitadas.
- **Restauración del sistema de Windows:** configuraciones para la función Restaurar sistema de Windows, que le permite restaurar su sistema a un estado anterior.

Se puede solicitar la limpieza del sistema:

- cuando se encuentra una amenaza

- cuando un usuario hace clic en **Restablecer**

Puede revisar los cambios y restablecer las configuraciones si fuese necesario.



i Solo un usuario con derechos de administrador puede realizar acciones en el Limpiador del sistema.

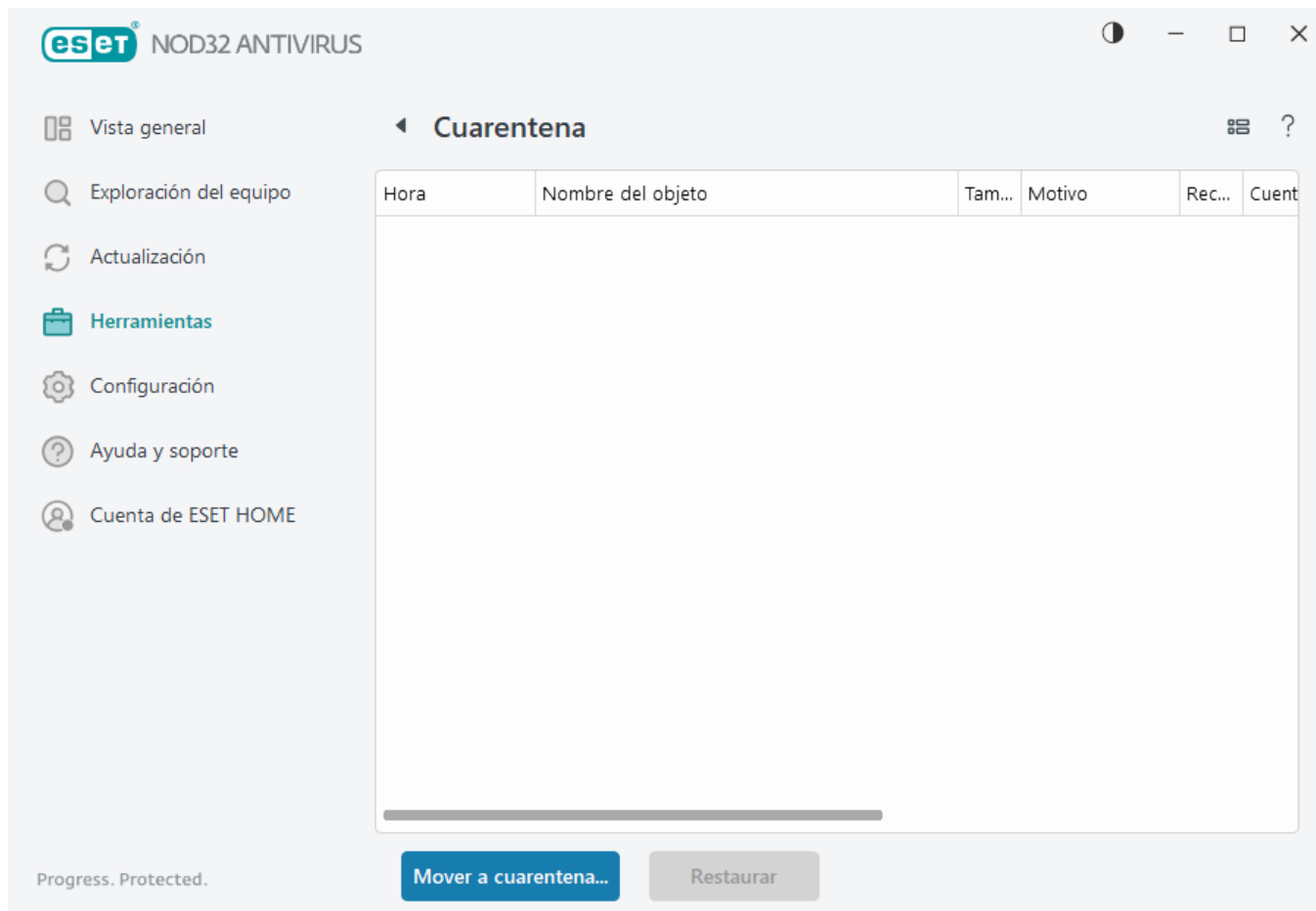
Cuarentena

La principal función de la cuarentena es almacenar de forma segura los objetos informados (como malware, archivos infectados o aplicaciones potencialmente no deseadas).

Para acceder a la cuarentena, diríjase a la [ventana principal del programa](#) ESET NOD32 Antivirus y haga clic en **Herramientas > Cuarentena**.

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 del archivo,
- su tamaño en bytes,
- el motivo (por ejemplo, objeto agregado por el usuario),
- y la cantidad de amenazas (por ejemplo, detecciones duplicadas del mismo archivo o si un archivo contiene varias infiltraciones).



Envío de archivos a cuarentena

ESET NOD32 Antivirus dispone los archivos eliminados en cuarentena de manera automática (si usted no canceló esta opción en la [ventana de alerta](#)).

Los archivos adicionales deberían ponerse en cuarentena si:

- a.no pueden limpiarse,
- b.no es seguro o recomendable eliminarlos,
- c.ESET NOD32 Antivirus los detecta de manera falsa,
- d.un archivo presenta un comportamiento sospechoso pero el [escáner](#) no lo detecta.

Para poner un archivo en cuarentena, cuenta con varias opciones:

- a.Use la función Arrastrar y soltar para poner un archivo en cuarentena manualmente al hacer clic en el archivo, mover el puntero del mouse hacia el área marcada al mismo tiempo que mantiene el botón pulsado, y luego lo suelta. Después de eso, la aplicación se mueve al primer plano.
- b.Haga clic derecho en el archivo > haga clic en **Opciones avanzadas > Archivo en cuarentena**.
- c.Haga clic en **Mover a cuarentena** desde la ventana **Cuarentena**.
- d.También puede usarse el menú contextual para este fin. Haga clic con el botón secundario en la ventana **Cuarentena** y seleccione **Cuarentena**.

Restauración desde Cuarentena

Los archivos en cuarentena también pueden restaurarse a su ubicación original:

- Para tal fin, use la función **Restaurar**, que se encuentra disponible en el menú contextual, al hacer clic con el botón secundario en un archivo específico en Cuarentena.
- Si un archivo está marcado como [aplicación potencialmente no deseada](#), se habilita la opción **Restaurar y excluir de la exploración**. Consulte también [Exclusiones](#).
- El menú contextual también ofrece la opción **Restaurar a**, que le permite restaurar un archivo de una ubicación que no sea aquella en la que se lo eliminó.
- La funcionalidad de restauración no se encuentra disponible en algunos casos, por ejemplo, para archivos ubicados en una unidad de uso compartido de solo lectura.

Eliminar de la cuarentena

Haga clic con el botón secundario en un elemento determinado y seleccione **Eliminar de la Cuarentena**, o seleccione el elemento que desea eliminar y presione **Eliminar** en su teclado. También puede seleccionar varios elementos y eliminarlos todos juntos. Los elementos eliminados se eliminarán en forma permanente de su dispositivo y cuarentena.

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, haga un clic derecho en el archivo y seleccione **Enviar para su análisis** desde el menú contextual.

Descripción de la detección

Haga clic derecho en un elemento y en **Descripción de la detección** para abrir la enciclopedia de amenazas de ESET que contiene información detallada sobre los peligros y los síntomas de la infiltración registrada.

Instrucciones ilustradas

Los siguientes artículos de la base de conocimiento de ESET pueden estar disponibles solo en inglés:



- [Restaurar un archivo en cuarentena en ESET NOD32 Antivirus](#)
- [Eliminar un archivo en cuarentena en ESET NOD32 Antivirus](#)
- [Mi producto ESET me envió una notificación sobre una detección. ¿Qué debo hacer?](#)

Error en la cuarentena

Los motivos por los que archivos concretos no pueden moverse a la cuarentena son los siguientes:

- **No tiene los permisos de lectura:** significa que no puede ver el contenido de un archivo.
- **No tiene los permisos de escritura:** significa que no puede modificar el contenido del archivo, es decir, agregar nuevo contenido o eliminar el contenido existente.

- **El archivo que está intentando poner en cuarentena es demasiado grande:** debe reducir el tamaño del archivo.

Cuando reciba el mensaje de error "Ha fallado la cuarentena", haga clic en **Más información**. Aparece la ventana de lista de errores de cuarentena y se mostrarán el nombre del archivo y el motivo por el que el archivo no puede ponerse en cuarentena.

Servidor proxy

En redes de LAN muy extensas, la comunicación entre su equipo e Internet puede tener como intermediario un servidor proxy. Al utilizar esta configuración, 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.

La configuración del servidor proxy se puede modificar en la [ventana principal del programa](#) > **Configuración** > **Configuración avanzada** > **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 utilizarán los parámetros aquí ingresados.

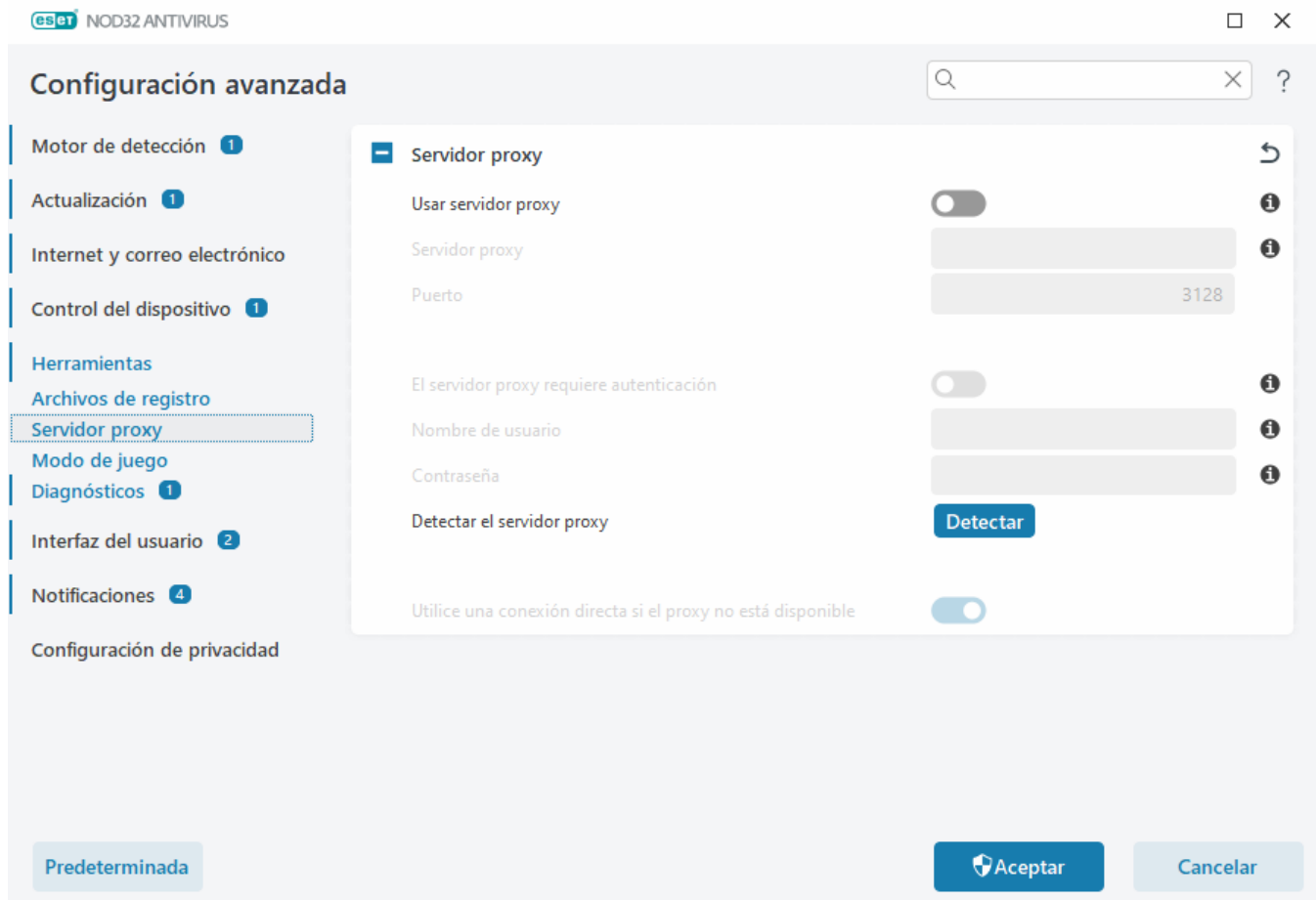
Para especificar la configuración del servidor proxy en esta etapa, seleccione **Usar servidor proxy** e ingrese la dirección del servidor proxy en el campo **Servidor proxy** junto con el número de **Puerto** correspondiente.

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

i En la configuración del **Servidor proxy**, debe ingresar su Nombre de usuario y Contraseña en forma manual.

Use conexión directa si el proxy no está disponible – Si ESET NOD32 Antivirus está configurado para usar proxy y no puede llegar al proxy, ESET NOD32 Antivirus evadirá el proxy y se comunicará directamente con los servidores ESET.

La configuración del servidor proxy también puede establecerse desde Configuración avanzada de la actualización (**Configuración avanzada** > **Actualizar** > **Perfiles** > **Actualizaciones** > **Opciones de conexión** seleccionando **Conexión a través de un servidor proxy** del menú desplegable **Modo de proxy**). Esta configuración se aplica al perfil de actualización determinado y se recomienda para equipos portátiles, ya que suelen recibir las actualizaciones de firmas de virus desde ubicaciones remotas. Para obtener más información sobre esta configuración, consulte [Configuración de actualización avanzada](#).



Seleccionar 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 investigación de ESET para su análisis (es posible que no esté disponible según la configuración de ESET LiveGrid® que usted tenga).

Antes de enviar muestras a ESET

No envíe una muestra excepto que cumpla con, al menos, uno de los siguientes criterios:

- Su producto ESET no detecta la muestra en absoluto
- El programa detecta erróneamente la muestra como una amenaza
- No aceptamos sus archivos personales (aquellos que le gustaría que ESET explore para detectar malware) como muestras (el Laboratorio de investigación de ESET no realiza exploraciones a pedido de los usuarios)
- Recuerde utilizar un tema descriptivo e incluir la mayor cantidad de información posible sobre el archivo (por ejemplo, una captura de pantalla o el sitio Web desde donde realizó la descarga).

Puede realizar el envío de una muestra (un archivo o un sitio web) para que ESET lo analice por medio de uno de estos métodos:

1. Utilice el formulario de ejemplo de envío para su producto. Está ubicado en **Herramientas > Enviar muestra para su análisis**. El tamaño máximo de una muestra enviada es de 256 MB.
2. Como alternativa, puede enviar el archivo por correo electrónico. Si prefiere esta opción, comprima el archivo utilizando WinRAR/WinZIP, proteja el archivo con la contraseña "infected" y envíelo a samples@eset.com.
3. Para denunciar spam o falsos positivos de spam, consulte nuestro [artículo incluido en la base de](#)

[conocimientos de ESET.](#)

En el formulario **Seleccionar muestra para su análisis**, seleccione la descripción del menú desplegable **Motivo por el cual se envía la muestra** que mejor se adapte a su mensaje:

- [Archivo sospechoso](#)
- [Sitio sospechoso](#) (un sitio web que se encuentra infectado por algún malware),
- [Sitio falso positivo](#)
- [Archivo falso positivo](#) (un archivo que se detecta como una infección pero no está infectado),
- [Otro](#)

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. Seleccione **Enviar de manera anónima** para dejarlo vacío.

Es posible que no obtenga respuesta de ESET.

i 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. Si la muestra resulta ser una aplicación maliciosa o sitio malicioso, se agregará su detección a una de las próximas actualizaciones de ESET.

Seleccionar muestra para su análisis: archivo sospechoso

Signos y síntomas observados de infección de malware – ingrese una descripción sobre la conducta de los archivos sospechosos observada en el equipo.

Origen del archivo (dirección URL o proveedor): ingrese el origen del archivo (la procedencia) e indique cómo lo encontró.

Notas e información adicional – aquí puede agregar información adicional o descripciones útiles para el procesamiento del archivo sospechoso.

i Aunque solo el primer parámetro, **Signos y síntomas observados de infección de malware**, es obligatorio, el suministro de información adicional ayudará en forma significativa a nuestros laboratorios en la etapa de identificación y en el procesamiento de muestras.

Seleccionar muestra para su análisis: sitio sospechoso

Seleccione uno de los siguientes del menú desplegable **Problemas del sitio**:

- **Infectado** – un sitio web que contiene virus u otro malware distribuidos por varios métodos.

- El **phishing** utilizarse para obtener el acceso a datos confidenciales, como números de cuentas bancarias, PIN, etc. Lea más información sobre este tipo de ataque en el [glosario](#).
- **Fraudulento** – un sitio web fraudulento o engañoso, especialmente para obtener una ganancia rápida.
- Seleccione **Otro** si las opciones mencionadas previamente no se aplican al sitio que va a enviar.

Notas e información adicional – aquí puede agregar información adicional o una descripción que ayudarán a analizar el sitio web sospechoso.

Seleccionar muestra para su análisis: archivo con falso positivo

Le solicitamos que envíe los archivos detectados como una infección pero que no se encuentran infectados para mejorar nuestro motor antivirus y antispyware y ayudar a otros a estar protegidos. Los falsos positivos (FP) pueden generarse cuando el patrón de un archivo coincide con el mismo patrón incluido en un motor de detección.

Nombre y versión de la aplicación – el título del programa y su versión (por ejemplo, número, alias o nombre del código).

Origen del archivo (dirección URL o proveedor) – ingrese el origen del archivo (la procedencia) e indique cómo lo encontró.

Propósito de la aplicación – la descripción general de la aplicación, el tipo de aplicación (por ej., navegador, reproductor multimedia, etc.) y su funcionalidad.

Notas e información adicional – aquí puede agregar información adicional o descripciones útiles para el procesamiento del archivo sospechoso.

i Los primeros tres parámetros son obligatorios para identificar aplicaciones legítimas y distinguirlas del código malicioso. Al proporcionar información adicional, ayudará significativamente a nuestros laboratorios en el proceso de identificación y en el procesamiento de las muestras.

Seleccionar muestra para su análisis: sitio de falso positivo

Le solicitamos que envíe los sitios que se detectan como infectados, fraudulentos o phishing pero no lo son. Los falsos positivos (FP) pueden generarse cuando el patrón de un archivo coincide con el mismo patrón incluido en un motor de detección. Envíenos esta página web para mejorar nuestro motor antivirus y antiphishing y ayudar a proteger a los demás.

Notas e información adicional: aquí puede agregar información adicional o descripciones útiles que ayudarán durante el procesamiento del sitio web sospechoso.

Seleccionar muestra para su análisis: otros

Use este formulario si el archivo no se puede categorizar como **Archivo sospechoso** o **Falso positivo**.

Motivo por el cual se envía el archivo – ingrese una descripción detallada y el motivo por el cual envía el archivo.

Actualización de Microsoft Windows®

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 después de 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.

Cuadro de diálogo: actualizaciones del sistema

Si hay actualizaciones para su sistema operativo, ESET NOD32 Antivirus muestra una notificación en la [ventana principal del programa](#) > **Vista general**. Haga clic en **Más información** para abrir la ventana de actualizaciones del sistema.

La ventana de actualizaciones del sistema muestra la lista de actualizaciones disponibles que ya están preparadas para su descarga e instalación. El tipo de actualización aparece junto a su nombre.

Haga doble clic en cualquier fila de actualización para mostrar la ventana [Actualizar información](#) con información adicional.

Haga clic en **Ejecutar actualización del sistema** para descargar e instalar todas las actualizaciones del sistema operativo incluidas en la lista.

Información sobre la actualización

La ventana de actualizaciones del sistema muestra la lista de actualizaciones disponibles que ya están preparadas para su descarga e instalación. El nivel de prioridad de la actualización aparece junto al nombre de la actualización.

Haga clic en **Ejecutar la actualización de sistema** para comenzar la descarga e instalación de las actualizaciones de sistema operativo.

Haga un clic derecho en cualquier línea de actualización y, a continuación, haga clic en **Mostrar información** para abrir una nueva ventana con información adicional.

Ayuda y soporte

ESET NOD32 Antivirus contiene herramientas de solución de problemas e información de soporte que lo ayudarán a resolver los problemas que pueda encontrar.



Licencia

- [Solución de problemas de licencia](#): haga clic en este enlace para buscar soluciones a problemas relacionados con la activación o el cambio de licencia.
- [Cambiar la licencia](#): haga clic aquí para iniciar la ventana de activación y activar su producto. Si el dispositivo está [conectado a ESET HOME](#), elija una licencia de su cuenta ESET HOME o agregue una nueva.



Producto instalado

- [Novedades](#): haga clic aquí para abrir la ventana de información sobre características nuevas y mejoradas.
- [Acerca de ESET NOD32 Antivirus](#) – muestra información acerca de una copia de ESET NOD32 Antivirus.
- [Resolución de problemas del producto](#): haga clic en este enlace para buscar soluciones a los problemas más frecuentes.
- **Cambiar producto**: haga clic para ver si puede cambiar ESET NOD32 Antivirus a una [línea diferente de productos](#) con la licencia actual.



Página de ayuda – haga clic en este vínculo para abrir las páginas de ayuda de ESET NOD32 Antivirus.



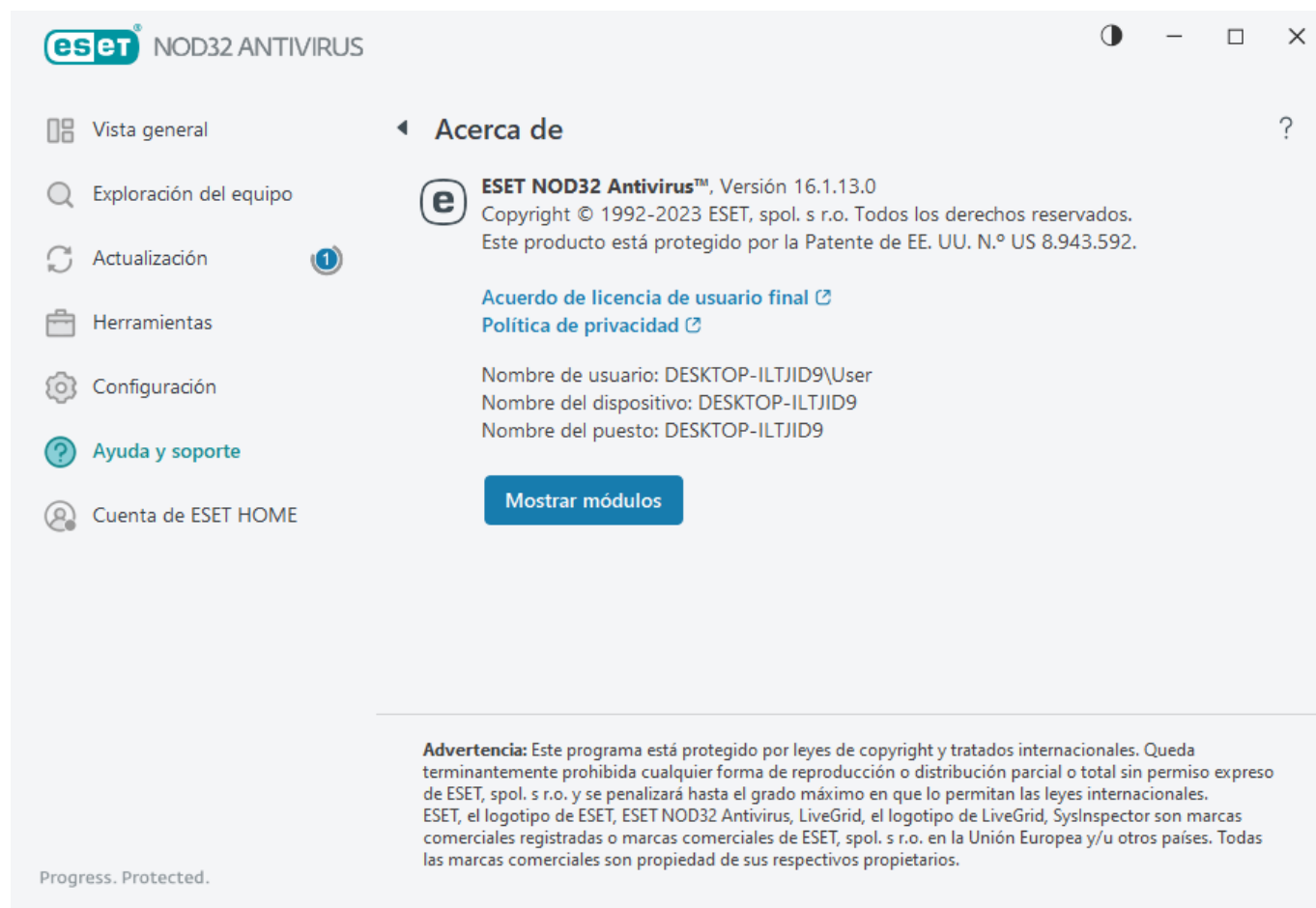
[Soporte técnico](#)



Base de conocimientos – la [base de conocimiento de ESET](#) contiene respuestas a las preguntas más frecuentes y soluciones recomendadas para varios problemas. La actualización regular por parte de los especialistas técnicos de ESET convierte a la base de conocimiento en la herramienta más potente para resolver varios problemas.

Acerca de ESET NOD32 Antivirus

Esta ventana brinda detalles sobre la versión instalada de ESET NOD32 Antivirus y su equipo.



Haga clic en **Mostrar módulos** para ver información sobre la lista de módulos del programa cargados.

- Puede copiar información sobre los módulos al portapapeles al hacer clic en **Copiar**. Esto puede resultar útil durante la resolución de problemas o al ponerse en contacto con el servicio de soporte técnico.
- Haga clic en **Motor de detección** en la ventana Módulos para abrir el radar de virus de ESET, que contiene información sobre cada versión del motor de detección de ESET.

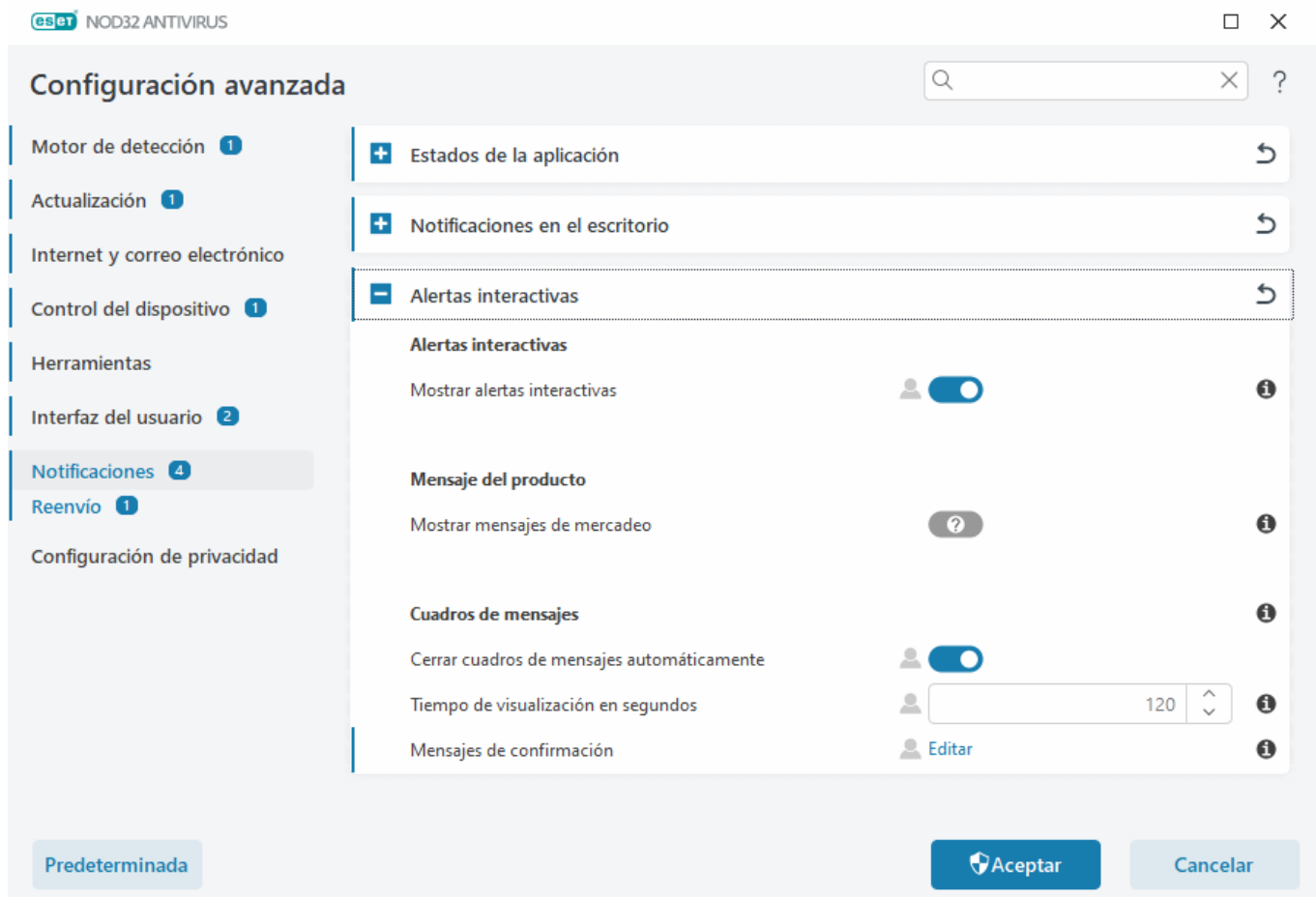
ESET Noticias

En esta ventana ESET NOD32 Antivirus le informan las noticias de ESET de forma regular.

La mensajería del producto ha sido diseñada para informar a los usuarios de ESET acerca de noticias y otras comunicaciones. El envío de mensajes de marketing requiere el consentimiento de un usuario. Los mensajes de marketing no se envían a un usuario de forma predeterminada (se muestra como un signo de interrogación). Al activar esta opción, acepta recibir mensajes de marketing de ESET. Si no está interesado en recibir material de marketing de ESET, desactive la opción **Mostrar mensajes de marketing**.

Para activar o desactivar la recepción de mensajes de marketing mediante una ventana de notificación, siga las instrucciones a continuación.

1. Abra la ventana principal de su producto ESET.
2. Presione la tecla **F5** para acceder a la **Configuración avanzada**.
3. Haga clic en **Notificaciones > Alertas interactivas**.
4. Modificar la opción **Mostrar mensajes de marketing**.



Enviar datos de configuración del sistema

Con el fin de proporcionar asistencia lo más rápido y con la mayor exactitud posible, ESET solicita información sobre la configuración de ESET NOD32 Antivirus, información detallada sobre el sistema y los procesos activos ([Archivos de registro ESET SysInspector](#)), y los datos de registro. ESET usará estos datos únicamente para proporcionar asistencia técnica al cliente.

Al enviar el [formulario web](#), los datos de configuración de su sistema se enviarán a ESET. Seleccione **Enviar siempre esta información** si desea recordar esta acción para este proceso. Para enviar el formulario sin enviar los datos, haga clic en **No enviar datos**, y puede contactar a Soporte Técnico de ESET mediante el formulario de soporte en línea.

Esta configuración también se puede establecer en **Configuración avanzada > Herramientas > Diagnóstico > Soporte técnico**.

i Si decidió enviar los datos del sistema, es necesario completar y enviar el formulario web. De lo contrario, no se creará su comprobante y se perderán los datos de su sistema.

Soporte técnico

En la [ventana principal del programa](#), haga clic en **Ayuda y soporte > Soporte técnico**.

Comuníquese con el Soporte técnico

Solicitar soporte: si no encuentra respuesta a su problema, puede usar este formulario del sitio web de ESET para ponerse rápidamente en contacto con el departamento de soporte técnico de ESET. En función de su configuración, se mostrará la ventana [Enviar los datos de configuración del sistema](#) antes de rellenar el formulario web.

Obtener información para soporte técnico

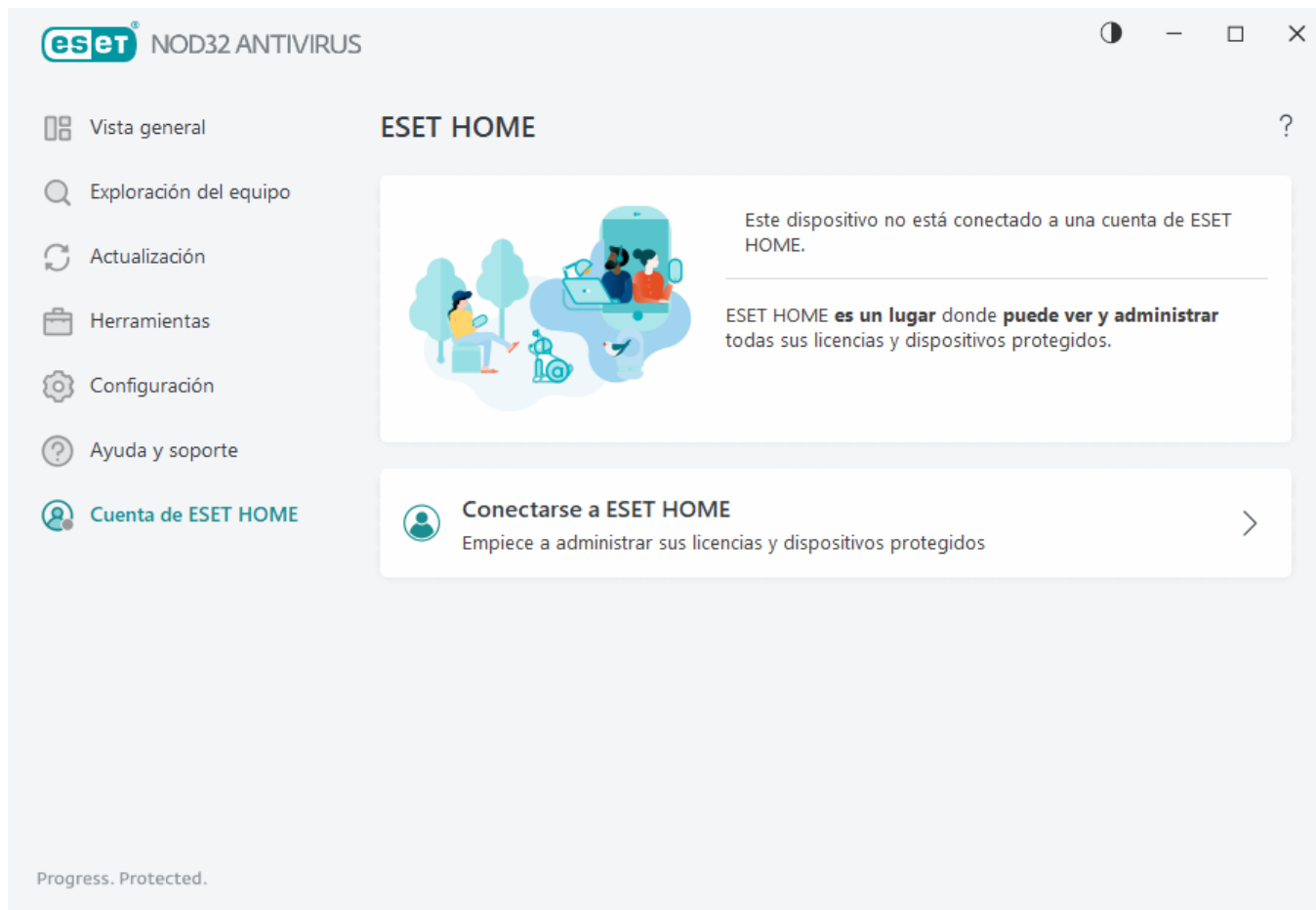
Detalles de soporte técnico: cuando se lo solicite, puede copiar y enviar información a Soporte técnico de ESET (como los detalles de la licencia, el nombre del producto, la versión del producto, el sistema operativo y la información del equipo).

ESET Log Collector - enlaza al artículo de la [Base de conocimiento de ESET](#), de donde puede descargar la utilidad ESET Log Collector, una aplicación que recopila información y registros automáticamente de un equipo para ayudar a resolver problemas más rápidamente. Para obtener más información, haga clic [ESET Log Collector aquí](#).

Haga clic en [Habilitar registros avanzados](#) para crear registros avanzados de todas las funciones disponibles a fin de ayudar a los desarrolladores a diagnosticar y resolver problemas. El detalle mínimo para los registros está ajustado en el nivel de Diagnóstico. El registro avanzado se desactivará automáticamente después de dos horas, a menos que lo detenga antes haciendo clic en Detener registro avanzado. Cuando se crean todos los registros, se muestra la ventana de notificación que proporciona acceso directo a la carpeta de Diagnóstico con los registros creados.

Cuenta ESET HOME

Puede revisar el estado de conexión de la cuenta ESET HOME en la [ventana principal del programa](#) > **cuenta ESET HOME**.



Este dispositivo no está conectado a una cuenta ESET HOME

Haga clic en [Conectar a ESET HOME](#) para conectar su dispositivo a [ESET HOME](#) y administrar sus licencias y dispositivos protegidos. Puede renovar, actualizar o ampliar la licencia y ver detalles importantes de ella. En el portal de administración o la aplicación para dispositivos móviles de ESET HOME, puede agregar diferentes licencias, descargar productos en sus dispositivos, comprobar el estado de seguridad del producto o compartir licencias por correo electrónico. Para obtener más información, visite [ayuda en línea de ESET HOME](#).

Este dispositivo está conectado a una cuenta ESET HOME

Puede administrar la seguridad de su dispositivo de forma remota con [el portal](#) o la aplicación para dispositivos móviles de ESET HOME. Haga clic en **App Store** o **Google Play** para mostrar un código QR que puede analizar con su teléfono móvil para descargar la aplicación para dispositivos móviles de ESET HOME de App Store o Google Play.

Cuenta de ESET HOME—nombre de su cuenta de ESET HOME.

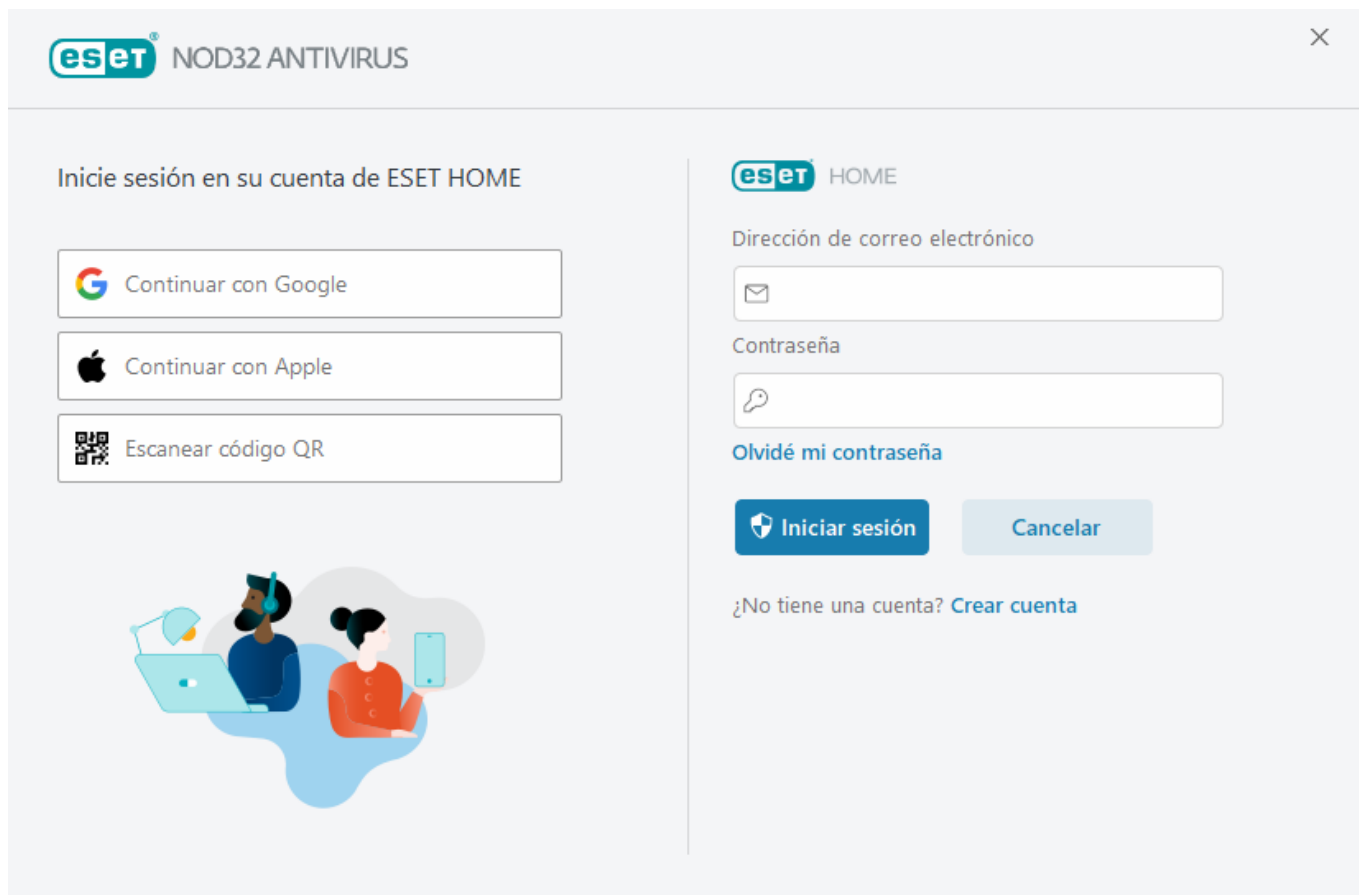
Nombre del dispositivo—nombre de este dispositivo que se muestra en la cuenta de ESET HOME.

Abrir ESET HOME—abre el portal de administración de ESET HOME.

Para desconectar el dispositivo de su ESET HOME cuenta, haga clic en **Desconectar de ESET HOME > Desconectar**. La licencia que se usa para la activación permanecerá activa y su dispositivo estará protegido.

Conectarse a ESET HOME

Conecte su dispositivo a [ESET HOME](#) para ver y administrar todas las licencias y los dispositivos de ESET activados. Puede renovar, actualizar o ampliar la licencia y ver detalles importantes de ella. En el portal de administración o la aplicación para dispositivos móviles de ESET HOME, puede agregar diferentes licencias, descargar productos en sus dispositivos, comprobar el estado de seguridad del producto o compartir licencias por correo electrónico. Para obtener más información, visite [ayuda en línea de ESET HOME](#).



Conecte su dispositivo a ESET HOME:

- i** Si se conecta a ESET HOME durante la instalación o al seleccionar **Usar cuenta de ESET HOME** como método de activación, siga las instrucciones del tema [Usar cuenta de ESET HOME](#).
- i** Si ya ha instalado y activado ESET NOD32 Antivirus con una licencia añadida a su cuenta ESET HOME, puede conectar su dispositivo a ESET HOME mediante el portal ESET HOME. Siga las instrucciones en la [ESET HOME](#) [Guía de ayuda en línea](#) y [permita la conexión en ESET NOD32 Antivirus](#).

1. En la [ventana principal del programa](#), haga clic en **cuenta ESET HOME > Conectar a ESET HOME** o haga clic en **Conectar a ESET HOME** en la notificación **Conectar este dispositivo a una cuenta de ESET HOME**.
2. [Ingrese a su cuenta ESET HOME](#).

- i** Si no tiene una cuenta ESET HOME, haga clic en **Crear cuenta** para registrarse o consulte las instrucciones de la Ayuda en línea de [ESET HOME](#).
- i** Si olvidó su contraseña, haga clic en **Olvidé mi contraseña** y siga los pasos de la pantalla o consulte las instrucciones de la [Ayuda en línea de ESET HOME](#).

3. Defina un **Nombre del dispositivo** y haga clic en **Continuar**.

4. Tras una conexión correcta, se muestra una ventana de detalles. Haga clic en **Listo**.

Inicie sesión en ESET HOME

Hay varios métodos disponibles para iniciar sesión en su cuenta ESET HOME:

- **Usar su dirección de correo electrónico y contraseña de ESET HOME:** escriba la **dirección de correo electrónico** y la **contraseña** que usó para crear su cuenta ESET HOME y haga clic en **Iniciar sesión**.
- **Usar su cuenta de Google/AppleID:** haga clic en **Continuar con Google** o **Continuar con Apple** e inicie sesión en la cuenta correspondiente. Tras iniciar sesión correctamente, se lo redirigirá a la página web de confirmación de ESET HOME. Para continuar, vuelva a la ventana de su producto de ESET. Para obtener más información sobre la cuenta de Google o el inicio sesión de AppleID, consulte las instrucciones de la [Ayuda en línea de ESET HOME](#).
- **Analizar código QR:** haga clic en **Analizar código QR** para ver el código QR. Abra su aplicación móvil ESET HOME y escanee el código QR o apunte la cámara del dispositivo al código QR. Para obtener más información, consulte las instrucciones de la [Ayuda en línea de ESET HOME](#).



Si no tiene una cuenta ESET HOME, haga clic en **Crear cuenta** para registrarse o consulte las instrucciones de la Ayuda en línea de [ESET HOME](#).

Si olvidó su contraseña, haga clic en **Olvidé mi contraseña** y siga los pasos de la pantalla o consulte las instrucciones de la [Ayuda en línea de ESET HOME](#).

[Error de inicio de sesión: errores comunes.](#)

eset NOD32 ANTIVIRUS

Inicie sesión en su cuenta de ESET HOME

Continuar con Google

Continuar con Apple

Escanear código QR

eset HOME

Dirección de correo electrónico

Contraseña

[Olvidé mi contraseña](#)

Iniciar sesión

¿No tiene una cuenta? [Crear cuenta](#)

Error de inicio de sesión: errores comunes

No pudimos encontrar una cuenta que coincida con la dirección de correo electrónico ingresada

La dirección de correo electrónico que ha ingresado no coincide con ninguna cuenta ESET HOME. Haga clic en **Atrás** y escriba la dirección de correo electrónico y la contraseña correctas.

Para iniciar sesión debe crear una cuenta ESET HOME. Si no tiene una cuenta ESET HOME, haga clic en **Atrás > Crear cuenta** o consulte [Crear una nueva cuenta ESET HOME](#).

El nombre de usuario y la contraseña no coinciden

La contraseña ingresada no coincide con la dirección de correo electrónico ingresada. Haga clic en **Atrás**, escriba la contraseña correcta y asegúrese de que la dirección de correo electrónico ingresada sea correcta. Si no puede iniciar sesión, haga clic en **Atrás > ¿Olvidó su contraseña?** para restablecer su contraseña y siga los pasos de la pantalla o consulte [Olvidé mi contraseña de ESET HOME](#).

La opción de inicio de sesión seleccionada no coincide con su cuenta

Su cuenta está vinculada a su cuenta de redes sociales. Para iniciar sesión en ESET HOME, haga clic en **Continuar con Google** o **Continuar con Apple** e inicie sesión en la cuenta correspondiente. Tras iniciar sesión correctamente, se lo redirigirá a la página web de confirmación de ESET HOME. Puede desconectar su cuenta de redes sociales de su cuenta ESET HOME en el portal ESET HOME.

Contraseña incorrecta

Este error puede producirse si su ESET NOD32 Antivirus ya está conectado a ESET HOME y está realizando cambios que requieren que inicie sesión (por ejemplo, desactivar Anti-Theft) y la contraseña que ingresó no coincide con su cuenta. Haga clic en **Atrás** y escriba la contraseña correcta. Si no puede iniciar sesión, haga clic en **Atrás > ¿Olvidó su contraseña?** para restablecer su contraseña y siga los pasos de la pantalla o consulte [Olvidé mi contraseña de ESET HOME](#).

Agregar dispositivo en ESET HOME

Si ya ha instalado y activado ESET NOD32 Antivirus con una licencia añadida a su cuenta ESET HOME, puede conectar su dispositivo a ESET HOME mediante el portal ESET HOME:

1. [Envíe una solicitud de conexión a su dispositivo](#).
2. ESET NOD32 Antivirus muestra la ventana de diálogo **Conectar este dispositivo a una cuenta ESET HOME** con el nombre de su cuenta ESET HOME. Haga clic en **Permitir** para conectar el dispositivo a la cuenta ESET HOME mencionada.

i Si no hay interacción, la solicitud de conexión se cancelará automáticamente después de aproximadamente 30 minutos.

Interfaz del usuario

Para configurar el comportamiento de la interfaz gráfica de usuario (GUI) del programa, en la [ventana principal del programa](#), haga clic en **Configuración > Configuración avanzada (F5) > Interfaz de usuario**.

Puede ajustar el aspecto y los efectos visuales del programa en la pantalla Configuración avanzada de los [elementos de la interfaz del usuario](#).

Si desea disfrutar del máximo nivel de seguridad del software de seguridad, proteja la configuración con una contraseña para impedir la desinstalación o cualquier cambio no autorizado con la herramienta [Configuración de acceso](#).

i Para configurar el comportamiento de las notificaciones del sistema, las alertas de detección y los estados de la aplicación, consulte la sección [Notificaciones](#).

Elementos de la interfaz del usuario

Puede ajustar el entorno de trabajo (GUI) de ESET NOD32 Antivirus según sus necesidades en **Configuración avanzada (F5) > Interfaz del usuario > Elementos de la interfaz del usuario**.

Modo de color— seleccione el esquema de colores de la GUI de ESET NOD32 Antivirus en el menú desplegable:

- **Igual que el color del sistema**— define el esquema de colores de ESET NOD32 Antivirus según la configuración del sistema operativo.
- **Oscuro**—ESET NOD32 Antivirus tendrá un esquema de colores oscuros (modo oscuro).
- **Claro**—ESET NOD32 Antivirus tendrá un esquema de colores estándar y claro.

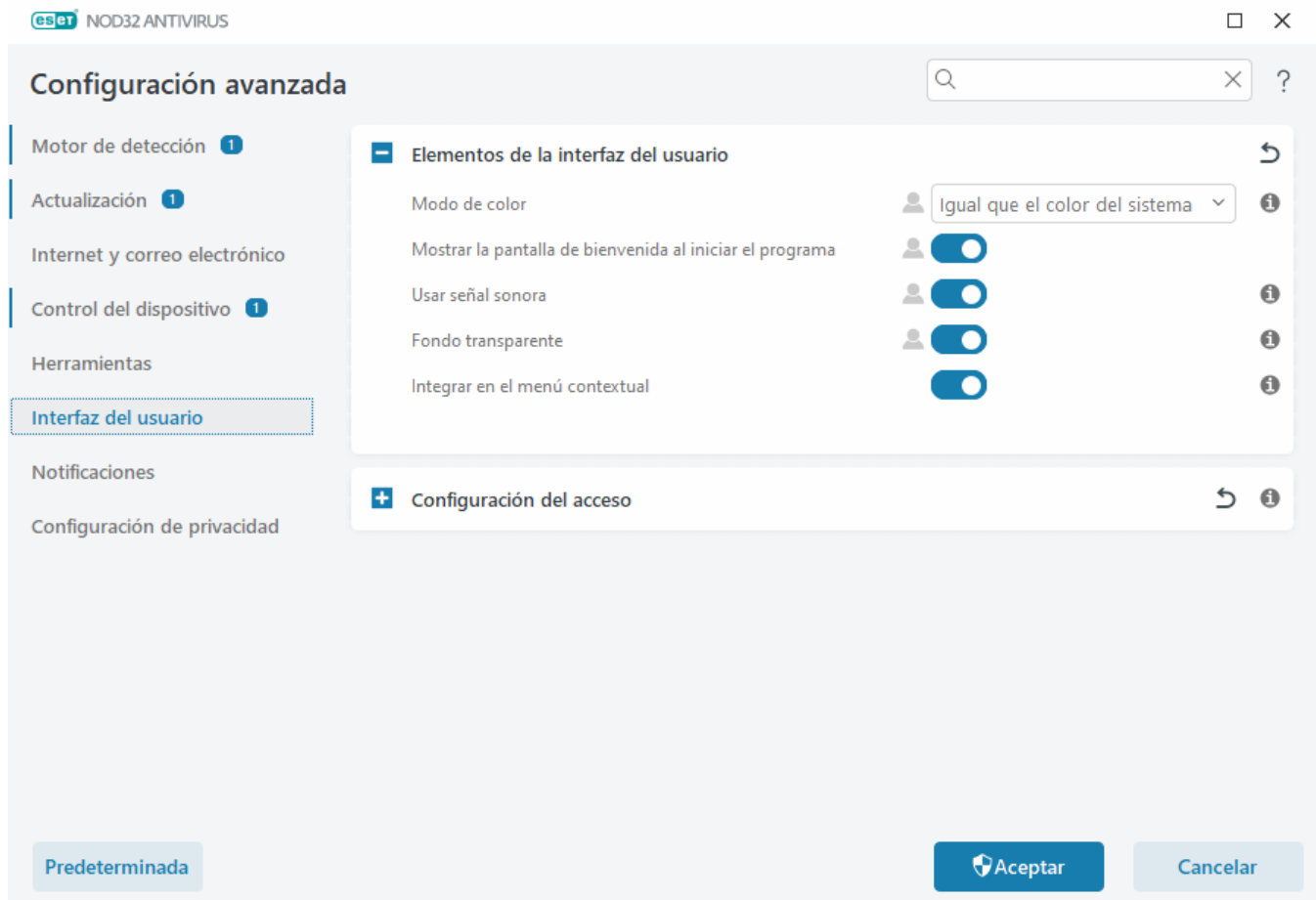
i También puede seleccionar el esquema de colores de la interfaz gráfica de usuario de ESET NOD32 Antivirus en la esquina superior derecha de la [ventana principal del programa](#).

Mostrar la pantalla de bienvenida al iniciar el programa – muestra la pantalla de bienvenida de ESET NOD32 Antivirus durante el inicio.

Usar señal acústica: reproduce un sonido cuando se producen eventos importantes durante una exploración, por ejemplo al detectar una amenaza o al finalizar la exploración.

Fondo transparente— habilita un efecto de fondo transparente para la [ventana principal del programa](#). El fondo transparente solo está disponible para las versiones más recientes de Windows (RS4 y posteriores).

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



Configuración del acceso

Las configuraciones ESET NOD32 Antivirus 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 evitar modificaciones no autorizadas, los parámetros de configuración y la desinstalación de ESET NOD32 Antivirus pueden protegerse con una contraseña.

Para establecer una contraseña para proteger los parámetros de configuración y desinstalación de ESET NOD32 Antivirus, haga clic en **Establecer** junto a **Proteger la configuración con una contraseña**.

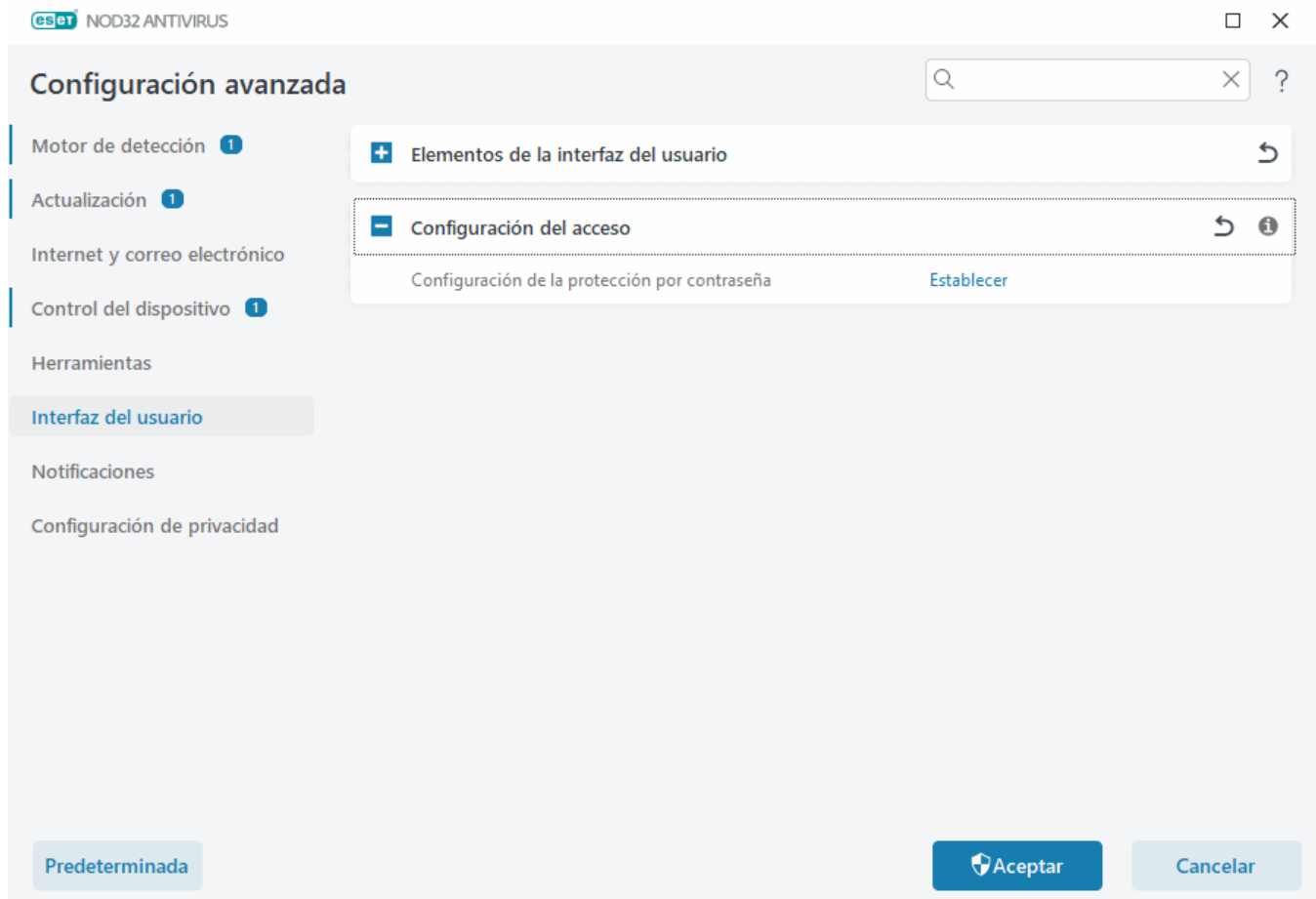


Cuando quiera acceder a la Configuración avanzada protegida, aparecerá la ventana para escribir la contraseña. Si no la recuerda o la pierde, haga clic en la opción **Restaurar contraseña** a continuación y escriba la dirección de correo electrónico que utilizó para el registro de la licencia. ESET le enviará un correo electrónico con el código de verificación y las instrucciones acerca de cómo restablecer su contraseña.

- [Cómo desbloquear la configuración avanzada](#)

Para cambiar la contraseña, haga clic en **Cambiar contraseña** junto a **Proteger la configuración con una contraseña**.

Para quitar la contraseña, haga clic en **Quitar** junto a **Proteger la configuración con una contraseña**.



Contraseña para configuración avanzada

Para proteger la Configuración avanzada de ESET NOD32 Antivirus y evitar modificaciones no autorizadas, ingrese su nueva contraseña en los campos **Nueva contraseña** y **Confirmar contraseña**. Haga clic en **Aceptar**.

Cuando desee cambiar una contraseña existente:


1. Escriba su contraseña anterior en el campo **Contraseña anterior**.
2. Ingrese su nueva contraseña en los campos **Nueva contraseña** y **Confirmar contraseña**.
3. Haga clic en **Aceptar**.

Esta contraseña será necesaria para acceder a Configuración avanzada.

Si olvidó su contraseña, consulte [Desbloquear su contraseña de configuración en productos para hogar de ESET](#).

Para recuperar la clave de licencia de ESET perdida, la fecha de caducidad de su licencia u otra información sobre la licencia de ESET NOD32 Antivirus, consulte [Perdí mi Clave de licencia](#).

Ícono de la bandeja del sistema

Algunas de las opciones de configuración y funciones más importantes están disponibles al hacer clic derecho en el ícono de la bandeja del sistema .

Detener la protección: muestra el cuadro de diálogo de confirmación que deshabilita el [Motor de detección](#), que protege ante ataques maliciosos al sistema mediante el control de los archivos, y las comunicaciones por medio de Internet y correo electrónico. En el menú desplegable **Intervalo de tiempo** puede especificar durante cuánto tiempo se deshabilitará la protección.



Configuración avanzada – abre la Configuración avanzada de ESET NOD32 Antivirus. Para abrir la Configuración avanzada desde la [ventana principal del producto](#), pulse F5 en el teclado o haga clic en **Configuración** > **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 detecciones.

Abrir ESET NOD32 Antivirus – abre la ventana [principal del programa](#) ESET NOD32 Antivirus

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

Modo de color—abre [la configuración de la interfaz de usuario](#), donde puede cambiar el color de la GUI.

Buscar actualizaciones – inicia un módulo o una actualización del producto para garantizar su protección. ESET NOD32 Antivirus busca actualizaciones automáticamente varias veces al día.

[Acerca de](#) – proporciona información del sistema, detalles sobre la versión instalada de ESET NOD32 Antivirus, los módulos del programa instalados e información sobre el sistema operativo y los recursos del sistema.

Asistencia para lectores de pantalla

ESET NOD32 Antivirus puede utilizarse junto con los lectores de pantalla para permitir que los usuarios de ESET con visión deficiente naveguen en el producto o configuren los ajustes. Los siguientes son los lectores de pantalla compatibles (JAWS, NVDA, Narrator).

Para garantizar que el software lector de pantalla pueda acceder a la GUI ESET NOD32 Antivirus correctamente, siga las instrucciones en el [Artículo de nuestra base de conocimiento](#).

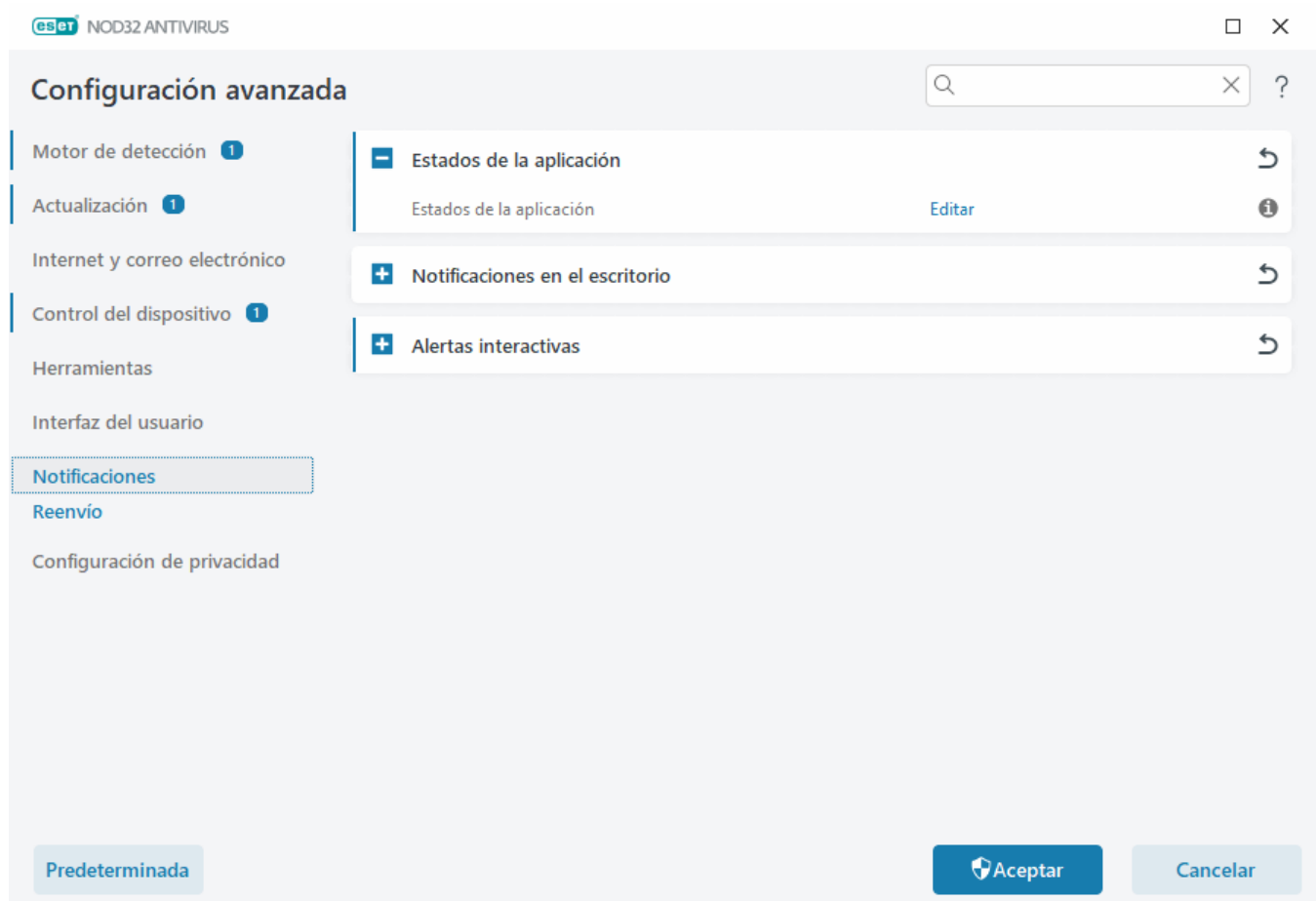
Notificaciones

Para administrar notificaciones de ESET NOD32 Antivirus, abra **Configuración avanzada** (F5) > **Notificaciones**. Puede configurar los siguientes tipos de notificaciones:

- Estados de la aplicación – notificaciones que se muestran en la [ventana principal del programa](#) > **Vista**

general.

- [Notificaciones en el escritorio](#): pequeñas ventanas de notificación junto a la barra de tareas del sistema.
- [Alertas interactivas](#): ventanas de alerta y cuadros de mensajes que requieren la intervención del usuario.
- [Reenvío](#) (Notificaciones por correo electrónico): las notificaciones por correo electrónico se envían a la dirección de correo electrónico especificada.



[-] Estados de la aplicación

Estados de la aplicación: haga clic en **Modificar** para seleccionar los estados de la aplicación que se mostrarán en la sección de inicio de la [ventana principal del programa](#) > **Vista general**.

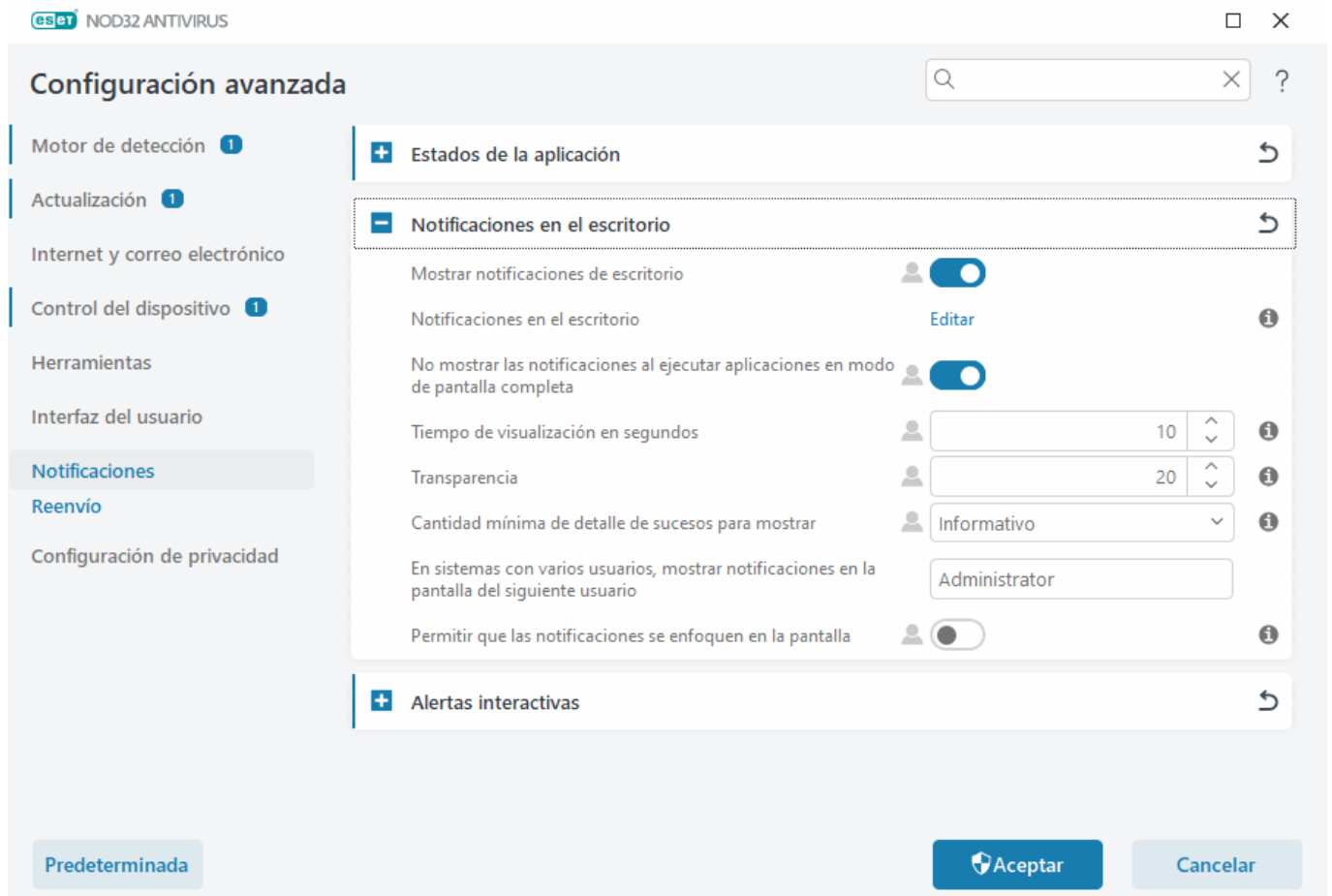
Ventana de diálogo: estados de la aplicación

En este cuadro de diálogo, puede seleccionar los estados de aplicación que se mostrarán. Por ejemplo, cuando pone en pausa la protección antivirus y antispyware o activa el modo de juego.

El estado de la aplicación también se mostrará si su producto no está activado o si la licencia ha vencido.

Notificaciones en el escritorio

Las notificaciones en el escritorio se representan mediante una pequeña ventana de notificación junto a la barra de tareas del sistema. De forma predeterminada, se muestra durante 10 segundos y, a continuación, desaparece lentamente. Entre las notificaciones se incluyen actualizaciones correctas del producto, conexión de nuevos dispositivos, finalización de tareas de análisis de virus o nuevas amenazas encontradas.



Mostrar notificaciones en el escritorio: recomendamos mantener esta opción activada, para que el producto pueda informarle cuando ocurra un suceso nuevo.

Notificaciones en el escritorio: haga clic en **Editar** para activar o desactivar las [Notificaciones en el escritorio](#) específicas.

No mostrar las notificaciones al ejecutar aplicaciones en modo de pantalla completa: elimina todas las notificaciones que no son interactivas al ejecutar aplicaciones en modo de pantalla completa.

Tiempo de espera: defina la duración de visibilidad de la notificación. El valor debe estar entre 3 y 30 segundos.

Transparencia: defina el porcentaje de transparencia de la notificación. El intervalo admitido es de 0 (sin transparencia) a 80 (transparencia muy alta).

Nivel mínimo de detalle de los eventos a mostrar: defina el nivel de gravedad de la notificación inicial mostrado. Seleccione una de las siguientes opciones en el menú desplegable:

o **Diagnóstico** – muestra la información necesaria para ajustar el programa y todos los historiales antes mencionados.

0Informativo – muestra los mensajes de información, como los eventos de red no estándar, que incluyen los mensajes de actualizaciones correctas, y todos los registros antes mencionados.

0Advertencias: muestra mensajes de advertencia, errores y errores graves (por ejemplo, falló la actualización).

0Errores: muestra errores (por ejemplo, la protección de documentos no iniciada) y errores graves.

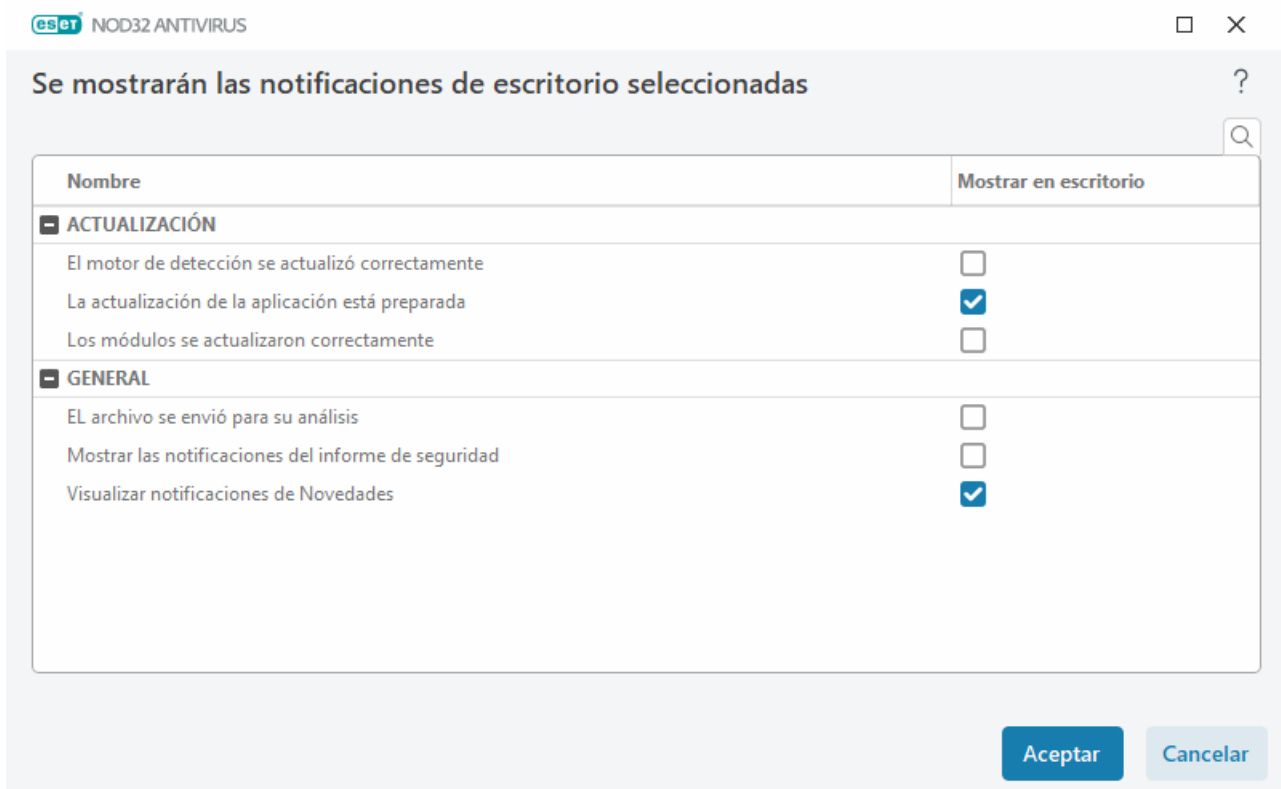
0Crítico: muestra solo los errores críticos (error al iniciar la protección antivirus o sistema infectado, etc.).

En sistemas con varios usuarios, mostrar notificaciones en la pantalla de este usuario: permite que la cuenta seleccionada reciba notificaciones en el escritorio. Por ejemplo, si no utiliza la cuenta de administrador, escriba el nombre completo de la cuenta y se mostrarán las notificaciones en el escritorio de la cuenta especificada. Solo puede recibir notificaciones en el escritorio una cuenta de usuario.

Permitir que las notificaciones se enfoquen en la pantalla: permite que las notificaciones se enfoquen en la pantalla; se puede acceder a esta opción en el menú **ALT + Tab**.

Lista de notificaciones en el escritorio

Para ajustar la visibilidad de las notificaciones en el escritorio (mostradas en la parte inferior derecha de la pantalla), abra **Configuración avanzada (F5) > Notificaciones > Notificaciones en el escritorio**. Haga clic en **Modificar** junto a **Notificaciones en el escritorio** y marque la casilla de verificación **Mostrar** correspondiente.



Nombre	Mostrar en escritorio
ACTUALIZACIÓN	
El motor de detección se actualizó correctamente	<input type="checkbox"/>
La actualización de la aplicación está preparada	<input checked="" type="checkbox"/>
Los módulos se actualizaron correctamente	<input type="checkbox"/>
GENERAL	
EL archivo se envió para su análisis	<input type="checkbox"/>
Mostrar las notificaciones del informe de seguridad	<input type="checkbox"/>
Visualizar notificaciones de Novedades	<input checked="" type="checkbox"/>

Acceptar Cancelar

General

Mostrar las notificaciones del informe de seguridad: reciba una notificación cuando se genera un nuevo [Informe de seguridad](#).

Mostrar las notificaciones de novedades: notificaciones sobre todas las características nuevas y mejoradas de la versión más reciente del producto.

El archivo se ha enviado para su análisis: reciba una notificación cada vez que ESET NOD32 Antivirus envía un archivo para su análisis.

Actualización

Se prepara la actualización de la aplicación: reciba una notificación cuando haya una actualización de una nueva versión de ESET NOD32 Antivirus preparada.

El Motor de detección se ha actualizado correctamente: reciba una notificación cuando el producto actualiza los módulos del Motor de detección.

Los módulos se han actualizado correctamente: reciba una notificación cuando el producto actualiza los componentes del programa.

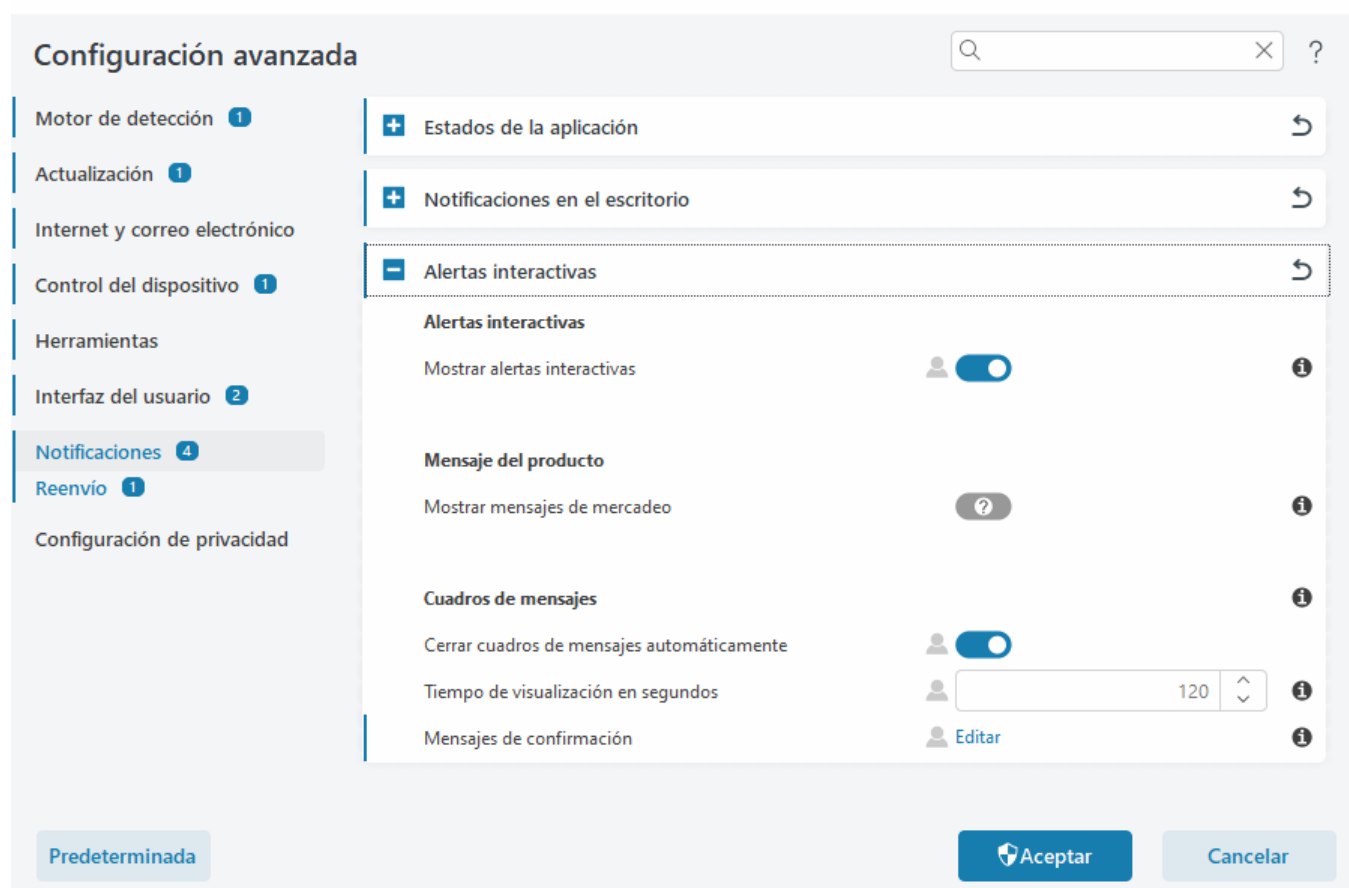
Para definir las configuraciones generales de las notificaciones de escritorio, por ejemplo, durante cuánto tiempo se mostrará un mensaje o la cantidad mínima de detalles para mostrar de los sucesos, consulte [Notificaciones de escritorio](#) en **Configuración avanzada (F5) > Notificaciones**.

Alertas interactivas

¿Necesita información sobre alertas y notificaciones comunes?

- [Amenaza detectada](#)
- [La dirección se ha bloqueado](#)
- [Producto no activado](#)
- [Cambiar a un producto con más funciones](#)
- [Cambiar a un producto con menos funciones](#)
- [Está disponible la actualización](#)
- [La información sobre la actualización no es consistente](#)
- [Resolución de problemas para el mensaje «error de actualización de módulos»](#)
- [Resolver errores de actualización de módulos](#)
- [Certificado de sitio web revocado](#)

La sección **Alertas interactivas** de **Configuración avanzada (F5) > Notificaciones** le permite configurar cómo gestiona ESET NOD32 Antivirus los cuadros de mensajes y las alertas interactivas para detecciones (por ejemplo, un sitio web potencial de phishing) cuando un usuario debe tomar una decisión.



Alertas interactivas

Si desactiva la opción **Mostrar alertas interactivas**, se ocultarán todas las ventanas de alerta y los cuadros de diálogo del navegador. Solo es adecuado para una serie de situaciones muy específicas. Recomendamos mantener esta opción activada.

Mensajería del producto

La mensajería del producto ha sido diseñada para informar a los usuarios de ESET acerca de noticias y otras comunicaciones. El envío de mensajes de marketing requiere el consentimiento de un usuario. Los mensajes de marketing no se envían a un usuario de forma predeterminada (se muestra como un signo de interrogación). Al activar esta opción, acepta recibir mensajes de marketing de ESET. Si no está interesado en recibir material de marketing de ESET, desactive la opción **Mostrar mensajes de marketing**.

Cuadros de mensajes

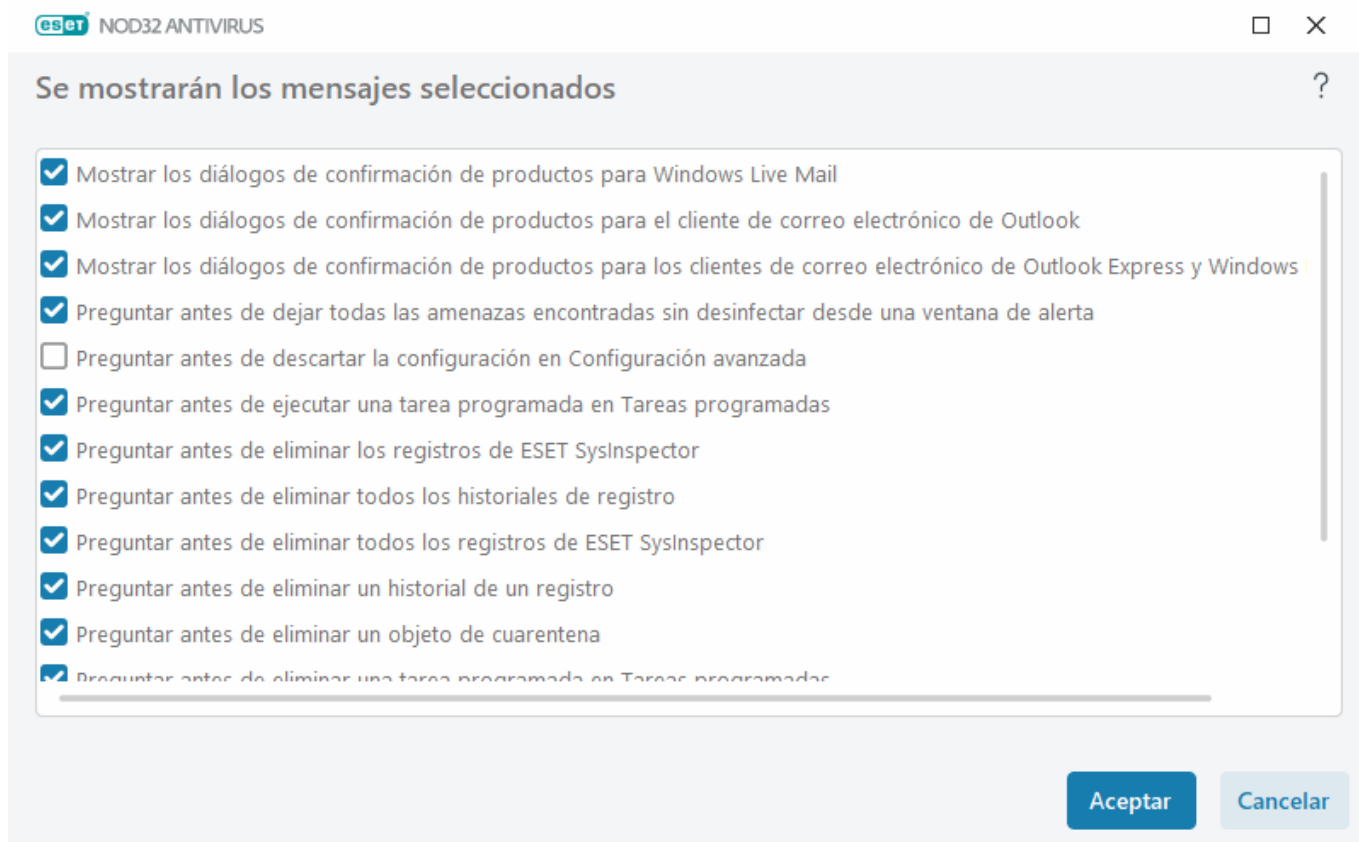
Para cerrar las casillas de mensajes automáticamente después de un período de tiempo determinado, seleccione **Cerrar cuadros de mensajes automáticamente**. Si no se cierran manualmente, las ventanas de alerta se cerrarán automáticamente una vez que transcurra el tiempo especificado.

Tiempo de espera en segundos: define la duración de la visibilidad de la alerta. El valor debe estar entre 10 y 999 segundos.

Mensajes de confirmación: haga clic en **Modificar** para mostrar una [lista de mensajes de confirmación](#) que se pueden seleccionar para que se muestren o no.

Mensajes de confirmación

Para ajustar los mensajes de confirmación, vaya a **Configuración avanzada** (F5) > **Notificaciones** > **Alertas interactivas** y haga clic en **Modificar** junto a **Mensajes de confirmación**.



Esta ventana de diálogo muestra mensajes de confirmación que ESET NOD32 Antivirus mostrará antes de que se realice alguna acción. Seleccione o anule la selección de la casilla de verificación junto a cada mensaje de confirmación para permitirlo o deshabilitarlo.

Obtenga más información sobre la función específica relacionada con los mensajes de confirmación:

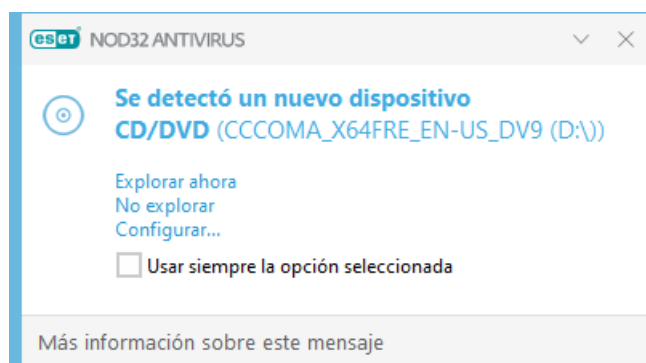
- [Preguntar antes de eliminar ESET SysInspector registros](#)
- [Preguntar antes de eliminar todos los ESET SysInspector registros](#)
- [Preguntar antes de eliminar un objeto de cuarentena](#)
- Preguntar antes de descartar la configuración en Configuración avanzada
- [Preguntar antes de dejar todas las amenazas encontradas sin desinfectar desde una ventana de alerta](#)
- [Preguntar antes de eliminar un historial de un registro](#)
- [Preguntar antes de eliminar una tarea programada en Tareas programadas](#)
- [Preguntar antes de eliminar todos los historiales de registro](#)
- [Preguntar antes de restablecer las estadísticas](#)

- [Preguntar antes de restaurar un objeto de cuarentena](#)
- [Preguntar antes de restaurar objetos de cuarentena y excluirlos de la exploración](#)
- [Preguntar antes de ejecutar una tarea programada en Tareas programadas](#)
- [Mostrar cuadros de diálogo de confirmación del producto para los clientes de correo electrónico de Outlook Express y Windows Mail](#)
- [Mostrar cuadros de diálogo de confirmación del producto para Windows Live Mail](#)
- [Mostrar cuadros de diálogo de confirmación del producto para el cliente de correo electrónico de Outlook](#)

Medios extraíbles

ESET NOD32 Antivirus proporciona la exploración automática de los medios extraíbles (CD/DVD/USB/...) al insertarlos en un equipo. Resulta útil si el administrador del equipo desea prevenir que los usuarios utilicen medios extraíbles con contenido no solicitado.

Cuando se inserten medios extraíbles y se configure **Mostrar las opciones de exploración** en ESET NOD32 Antivirus, se mostrará el siguiente cuadro de diálogo:



Opciones para este diálogo:

- **Explorar ahora** – desencadenará la exploración de los medios extraíbles.
- **No explorar:** no se explorarán los medios extraíbles.
- **Configuración:** abre la sección **Configuración avanzada**.
- **Usar siempre la opción seleccionada** – de seleccionarse, se llevará a cabo la misma acción cuando se inserte un medio extraíble en el futuro.

Además, ESET NOD32 Antivirus presenta la funcionalidad de Control del dispositivo, que le permite definir las reglas para el uso de dispositivos externos en un equipo determinado. Se pueden encontrar más detalles sobre el Control del dispositivo en la sección [Control del dispositivo](#).

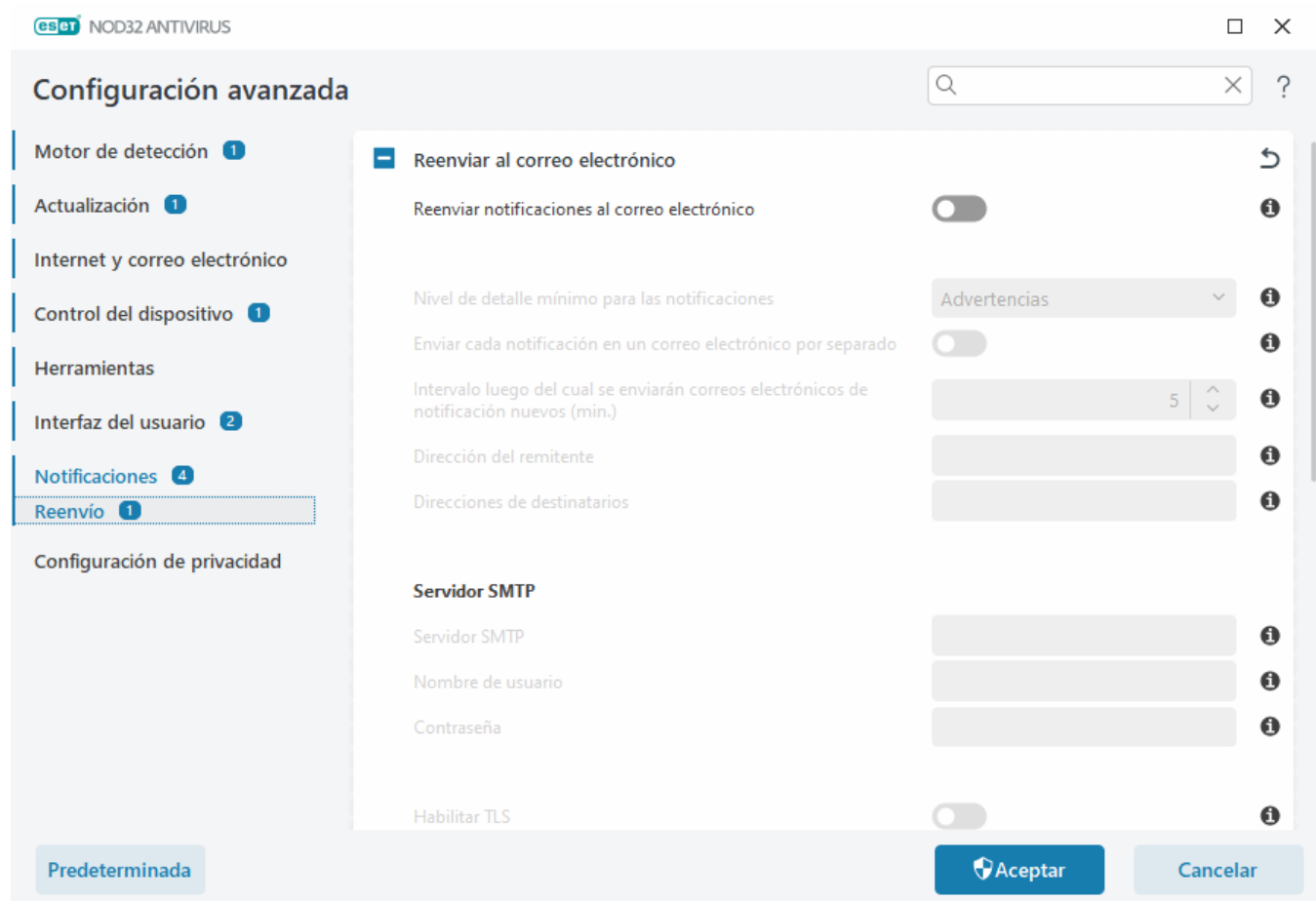
Para acceder a la configuración de la exploración de medios extraíbles, abra Configuración avanzada (**F5**) > **Motor de detección** > **Exploraciones de malware** > **Medios extraíbles**.

Acción para realizar tras insertar un medio: seleccione la acción predeterminada que se realizará cuando se inserte un medio extraíble en el equipo (CD/DVD/USB). Seleccione la acción deseada luego de insertar un medio extraíble en un equipo:

- **No explorar:** no se realizará ninguna acción y no se abrirá la ventana **Se detectó un nuevo dispositivo**.
- **Exploración automática del dispositivo:** se llevará a cabo una exploración del equipo en los dispositivos de medios extraíbles insertados.
- **Mostrar las opciones de exploración** – abre la sección de configuración de **medios extraíbles**.

Reenvío

ESET NOD32 Antivirus puede enviar correos electrónicos de forma automática si se produce un suceso con el nivel de detalle seleccionado. Abra la **Configuración avanzada** (F5) **Notificaciones** > **Reenviar** y habilite la opción **Reenviar notificaciones al correo electrónico** para activar las notificaciones por correo electrónico.



En el menú desplegable **Nivel de detalle mínimo para las notificaciones**, puede seleccionar el nivel de gravedad a partir del cual se enviarán las notificaciones.

- **Diagnóstico** – registra la información necesaria para ajustar el programa y todos los historiales antes mencionados.
- **Informativo** – registra los mensajes de información, como los eventos de red no estándar, que incluyen los mensajes de actualizaciones correctas, y todos los registros antes mencionados.

- **Advertencias** – registra los errores críticos y los mensajes de advertencia (por ejemplo, falló la actualización).
- **Errores** – se registrarán los errores (no se inició la protección de documentos) y los errores críticos.
- **Crítico**: registra únicamente los errores graves (por ejemplo, Error al iniciar la protección antivirus o Amenaza encontrada).

Enviar cada notificación en un correo electrónico distinto: si esta opción está activada, el destinatario recibirá un correo electrónico nuevo para cada notificación. Esto podría provocar que muchos mensajes de correo electrónico se reciban en un breve periodo de tiempo.

Intervalo luego del cual se enviarán correos electrónicos de notificación nuevos (min.) – intervalo en minutos luego del cual se enviarán notificaciones nuevas al correo electrónico. Si establece este valor en 0, las notificaciones se enviarán inmediatamente.

Dirección del remitente – define la dirección del remitente que se mostrará en el encabezado de los correos electrónicos de notificación.

Direcciones de destinatarios: defina las direcciones de destinatarios mostradas en el encabezado de los mensajes de correo electrónico de notificación. Se admiten varios valores. Utilice punto y coma como separador.

Servidor SMTP

SMTP servidor: el SMTP servidor utilizado para enviar notificaciones (p. ej., smtp.provider.com:587, el puerto predeterminado es 25).

 Los servidores SMTP con cifrado TLS son admitidos por ESET NOD32 Antivirus.

Nombre de usuario y contraseña – si el servidor SMTP requiere autenticación, se deben completar estos campos con un nombre de usuario y una contraseña válidos para acceder al servidor SMTP.

Habilitar TLS: Secure Alert y notificaciones con cifrado TLS.

Probar conexión SMTP: se enviará un correo electrónico de prueba a la dirección de correo electrónico del destinatario. Se debe completar el servidor SMTP, el nombre de usuario, la contraseña, la dirección del remitente y las direcciones del destinatario.

Formato de mensajes

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 de sucesos.

Formato de mensajes de sucesos – formato de los mensajes de sucesos que se muestran en los equipos remotos.

Formato de mensajes de advertencias sobre amenazas: los mensajes de notificación y alerta de amenazas tienen un formato predefinido de forma predeterminada. Recomendamos mantener el formato predefinido. No obstante, en algunas circunstancias (por ejemplo, si tiene un sistema automatizado de procesamiento de correo electrónico), es posible que deba cambiar el formato de los mensajes.

Conjunto de caracteres – convierte un mensaje de correo electrónico en una codificación de caracteres ANSI en base a la configuración regional de Windows (por ejemplo, windows-1250, Unicode (UTF-8), ACSII 7-bit, o japonés (ISO-2022-JP)). Por lo tanto, "á" se cambiará por "a" y un símbolo desconocido por "?".

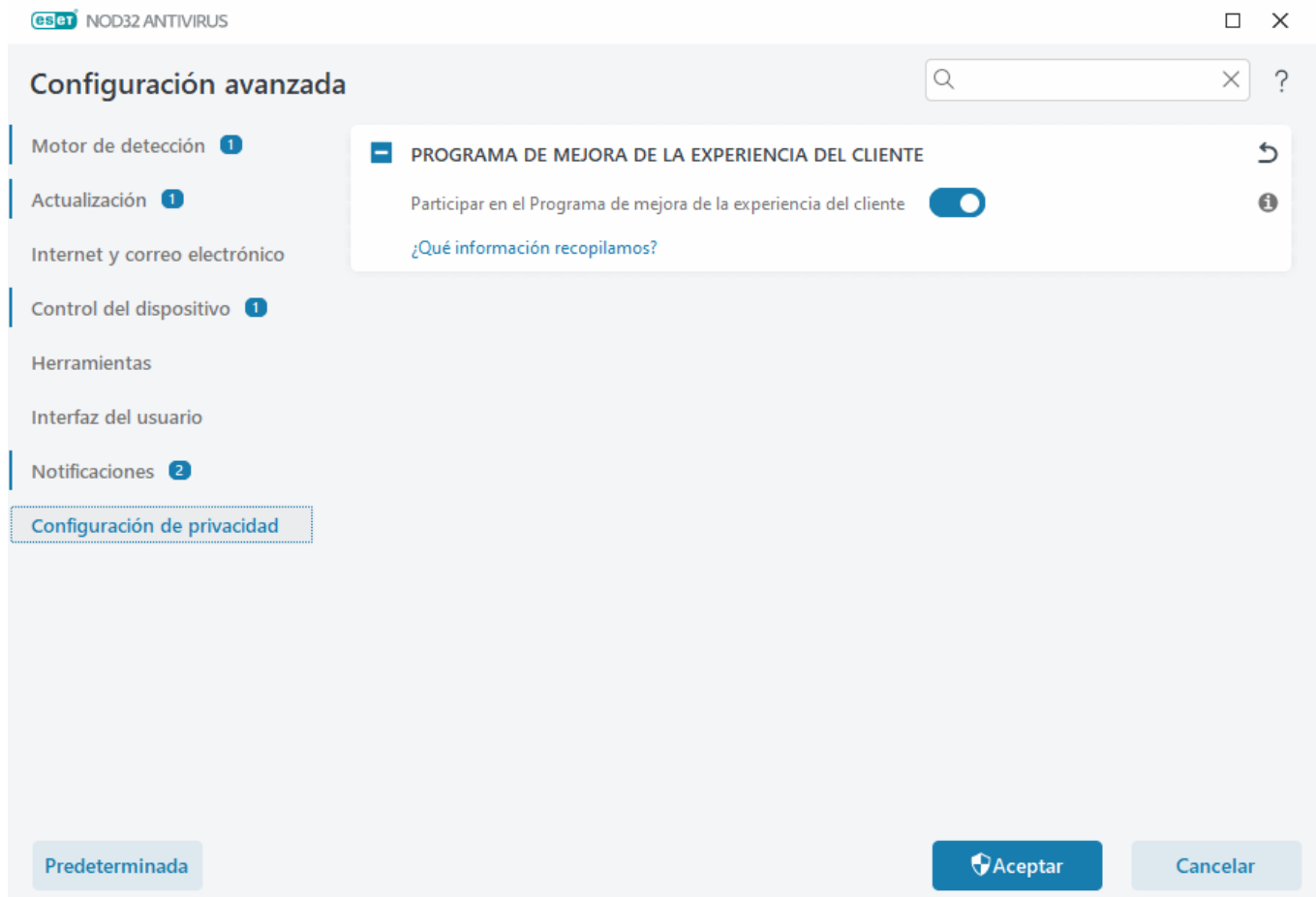
Usar la codificación de Entrecomillado imprimible: el origen del mensaje de correo electrónico se codificará en el formato Entrecomillado imprimible ((QP)) que usa los caracteres de ASCII y puede transmitir correctamente los caracteres nacionales especiales por correo electrónico en el formato de 8 bits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

- **%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., infectados.
- **%VirusName%:** identificación de la infección
- **%Action% :** Acción tomada sobre la infiltración
- **%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.

Configuración de privacidad

En la [ventana principal del programa](#), haga clic en **Configuración > Configuración avanzada (F5) > Configuración de privacidad**.



Programa de mejora de la experiencia del cliente

Active la barra deslizante junto a **Participar en el Programa de mejora de la experiencia del cliente** para unirse al Programa de mejora de la experiencia del cliente. Al unirse, le proporcionará a ESET información anónima relativa al uso de productos de ESET. Los datos recopilados nos ayudarán a mejorar su experiencia y nunca se compartirán con terceros. [¿Qué información recopilamos?](#)

Perfiles

El administrador de perfiles se usa en dos partes de ESET NOD32 Antivirus – en la sección **Exploración del equipo a pedido** y en **Actualización**.

Exploración del equipo

Hay cuatro perfiles de exploración predefinidos en ESET NOD32 Antivirus:

- **Análisis inteligente** – Es el perfil de exploración avanzada predeterminado. El perfil de análisis inteligente utiliza la tecnología de optimización inteligente, que excluye los archivos que se encontraron limpios en una exploración anterior y que no se han modificado desde esa exploración. Esto permite tener tiempos de exploración más bajos con un impacto mínimo en la seguridad del sistema.
- **Exploración del menú contextual** – Puede iniciar la exploración del menú contextual de cualquier archivo desde el menú contextual. El perfil de exploración del menú contextual le permite definir una configuración de exploración que se utilizará cuando se ejecuta la exploración de esta manera.

- **Exploración exhaustiva** – El perfil de exploración exhaustiva no utiliza la optimización inteligente de forma predeterminada, por lo que no se excluye ningún archivo de la exploración mediante este perfil.
- **Exploración del equipo** – Es el perfil predeterminado utilizado en la exploración estándar 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 **Motor de detección > Escaneos de malware > exploración bajo demanda > Lista de perfiles**. La ventana **Administrador de perfiles** 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.

i Suponga que desea crear su propio perfil de exploración y la configuración de **Explore su equipo** es parcialmente adecuada, pero no desea explorar [empaquetadores en tiempo real](#) o [aplicaciones potencialmente no seguras](#) y, además, quiere aplicar una **Reparar siempre la detección**. Ingrese el nombre de su nuevo perfil en la ventana **Administrador de perfiles** y haga clic en **Agregar**. Seleccione su nuevo perfil desde el menú desplegable **Perfil seleccionado** y ajuste los parámetros restantes para cumplir con sus requisitos, y haga clic en **Aceptar** para guardar 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 use 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 usar 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.

Actualizar perfil – El perfil de actualización utilizado actualmente. Para cambiarlo, elija un perfil del menú desplegable.

Lista de perfiles – cree perfiles nuevos o elimine perfiles de actualización existentes.

Accesos directos del teclado

Para mejorar la navegación en ESET NOD32 Antivirus, puede utilizar los siguientes accesos directos del teclado:

Accesos directos desde teclado	Acción
F1	abre las páginas de ayuda
F5	abre la configuración avanzada
Flecha arriba/flecha abajo	navegación en elementos del menú desplegable

Accesos directos desde teclado	Acción
TAB	mover al siguiente elemento de la interfaz gráfica de usuario de una ventana
Shift+TAB	mover al elemento de la interfaz gráfica de usuario anterior en una ventana
ESC	cierra la ventana de diálogo activa
Ctrl+U	Muestra información sobre la licencia de ESET (detalles para Soporte técnico)
Ctrl+R	restablece la ventana del producto a su tamaño y posición predeterminados en la pantalla
ALT + Flecha izquierda	volver
ALT + Flecha derecha	avanzar
ALT+Home	ir al inicio

También puede utilizar los botones del mouse hacia atrás o hacia delante para la navegación.

Diagnósticos

Los diagnósticos proporcionan el volcado de memoria de los procesos de ESET (por ejemplo, ekrrn). Si una aplicación se bloquea, se generará un volcado. Esto puede ayudar a los desarrolladores a depurar y reparar distintos problemas ESET NOD32 Antivirus.

Haga clic en el menú desplegable junto a **Tipo de volcado** y seleccione una de las tres opciones disponibles:

- Seleccione **Deshabilitar** para deshabilitar esta característica.
- **Mini** (predeterminado): 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 ser útil cuando el espacio sea limitado. Sin embargo, debido a la cantidad limitada de información incluida, es posible que los errores que no se hayan provocado directamente por el subproceso activo en el momento del problema no se descubran al analizar este archivo.
- **Completo**: registra todo el contenido de la memoria del sistema cuando la 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.

Directorio de destino – ubicación donde se va a generar la volcado de memoria durante el bloqueo.

Abrir carpeta de diagnósticos: haga clic en **Abrir** para abrir este directorio dentro de una nueva ventana del *Explorador de Windows*.

Crear volcado de diagnóstico: haga clic en **Crear** para crear archivos de volcado de diagnóstico en el **Directorio de destino**.

Registro avanzado

Activar registro avanzado en mensajes de marketing: registrar todos los eventos relacionados con los mensajes de marketing del producto.

Habilitar el registro avanzado de exploración: registra todos los eventos que tienen lugar durante la exploración de archivos y carpetas mediante la exploración del equipo.

Habilitar el registro avanzado del control parental: registra todos los eventos que ocurren en Control del dispositivo. Esto puede ayudar a los desarrolladores a diagnosticar y corregir problemas relacionados al control del dispositivo.

Habilitar el registro avanzado de Direct Cloud: registra todos los eventos que ocurren en ESET LiveGrid®. Esto puede ayudar a los desarrolladores a diagnosticar y corregir problemas relacionados con ESET LiveGrid®.

Habilitar el registro avanzado de protección de documentos: graba todos los eventos que ocurren en la protección de documentos para diagnosticar y solucionar problemas.

Activar registro avanzado de protección del cliente de correo electrónico: registra todos los sucesos que tienen lugar en la Protección del cliente de correo electrónico y el complemento del cliente de correo electrónico para permitir diagnosticar y resolver problemas.

Activar registro avanzado del núcleo: registra todos los eventos que tienen lugar en el núcleo de ESET (ekrn).

Habilitar el registro avanzado de licencias: registra todas las comunicaciones del producto con la activación de ESET o los servidores de ESET License Manager.

Habilitar seguimiento de memoria: registra todos los eventos que ayudarán a los desarrolladores a diagnosticar pérdidas de memoria.

Habilitar el registro avanzado de sistemas operativos: registra información adicional acerca del sistema operativo, como los procesos en ejecución, actividad del CPU y operaciones de disco. Esto puede ayudar a los desarrolladores a diagnosticar y solucionar problemas relacionados con el producto ESET ejecutado en su sistema operativo.

Habilitar el registro avanzado del filtrado de protocolos: registra todos los datos que pasan a través del motor de filtrado de protocolos con el formato PCAP para ayudar a los desarrolladores a diagnosticar y solucionar problemas relacionados con el filtrado de protocolos.

Activar registro avanzado de la mensajería push: registrar todos los sucesos que tienen lugar durante la mensajería push.

Habilitar el registro avanzado de protección del sistema de archivos en tiempo real: registra todos los eventos que tienen lugar durante la exploración de archivos y carpetas mediante la protección del sistema de archivos en tiempo real.

Habilitar el registro avanzado del motor de actualización: registra todos los eventos que ocurren durante el proceso de actualización. Esto puede ayudar a los desarrolladores a diagnosticar y solucionar problemas relacionados con el motor de actualizaciones.

Los archivos de registro se encuentran en *C:\ProgramData\ESET\ESET Security\Diagnostics*.

Soporte técnico

Al [ponerse en contacto con el soporte técnico de ESET](#) desde ESET NOD32 Antivirus, puede enviar datos de configuración del sistema. Seleccione **Enviar siempre** desde el menú desplegable **Enviar datos de configuración del sistema** para enviar los datos automáticamente, o bien, seleccione **Preguntar antes de enviar** para que se le solicite el envío antes de que se envíen los datos.

Importación y exportación de una configuración

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

Instrucciones ilustradas

i Consulte [Importar o exportar los ajustes de configuración de ESET con un archivo .xml](#) para obtener instrucciones ilustradas disponibles en inglés y en otros idiomas.

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. Puede importar fácilmente un archivo .xml para transferir estas configuraciones.

Para importar una configuración, en la [ventana principal del programa](#), haga clic en **Configuración > Importar/Exportar configuración** y seleccione **Importar configuración**. Ingrese el nombre del archivo de configuración o haga clic en el botón ... para buscar el archivo de configuración que desea importar.

Para importar una configuración, en la [ventana principal del programa](#), haga clic en **Configuración > Importar/Exportar configuración**. Seleccione **Importar configuración** e ingrese la ruta completa del archivo con el nombre. Haga clic en ... para navegar hasta una ubicación en su equipo para guardar el archivo de configuración.


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



The screenshot shows the 'Importar y exportar una configuración' dialog box in the ESET NOD32 ANTIVIRUS application. The dialog has a title bar with the ESET logo and 'NOD32 ANTIVIRUS'. Below the title bar, the title 'Importar y exportar una configuración' is displayed. A message states: 'Se puede guardar la configuración actual en un archivo XML y restaurar más tarde cuando sea necesario.' There are two radio buttons: 'Importar la configuración' (selected) and 'Exportar la configuración'. Below these is a text field labeled 'Ruta completa del archivo con nombre:' followed by a button with three dots (...). At the bottom, there are two buttons: 'Importar' and 'Cerrar'.

Restauración de todas las configuraciones en la sección

actual

Haga clic en la flecha curva  para restaurar todas las configuraciones de la sección actual a los valores predeterminados definidos por ESET.

Tenga en cuenta que cualquier cambio que se haya hecho se perderá después de hacer clic en **Revertir a predeterminado**.

Restaurar el contenido de las tablas – cuando se habilitan, las reglas, las tareas o los perfiles que se hayan agregado de manera manual o automática se perderán.

Consulte también [Importar y exportar configuración](#).

Revertir a la configuración predeterminada

En **Configuración avanzada** (F5), haga clic en **Predeterminada** para revertir toda la configuración del programa para todos los módulos. Se restablecerá el estado que tendrían después de una nueva instalación.

Consulte también [Importar y exportar configuración](#).

Error al guardar la configuración

Este mensaje de error indica que la configuración no se guardó correctamente debido a un error.

Por lo general, esto significa que el usuario que intentó modificar los parámetros del programa:

- tiene derechos de acceso insuficientes o no tiene los privilegios del sistema operativo necesarios para modificar los archivos de configuración y el registro del sistema.
> Para realizar las modificaciones deseadas, el administrador del sistema debe iniciar sesión.
- recientemente habilitó el Modo de aprendizaje en HIPS o Firewall e intentó hacer cambios en Configuración avanzada.
> Para guardar la configuración y evitar el conflicto de configuración, cierre Configuración avanzada sin guardar y vuelva a intentar hacer los cambios deseados.

La segunda causa más común puede ser que el programa ya no funcione correctamente, que esté dañado y que deba reinstalarse.

Exploración de la 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 de la 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=CARPETA	cargar módulos desde FOLDER
/quar-dir=CARPETA	FOLDER de cuarentena
/exclude=MÁSCARA	excluir de la exploración los archivos que coinciden con MASK
/subdir	explorar las subcarpetas (predeterminado)
/no-subdir	no explorar las subcarpetas
/max-subdir-level=NIVEL	subnivel máximo de carpetas dentro de las carpetas que se van a explorar
/symlink	seguir los vínculos simbólicos (predeterminado)
/no-symlink	saltear los vínculos simbólicos
/ads	explorar ADS (predeterminado)
/no-ads	no explorar ADS
/log-file=ARCHIVO	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=TAMAÑO	solo explorar los archivos menores que SIZE megabytes (predeterminado 0 = ilimitado)
/max-arch-level=NIVEL	subnivel máximo de archivos comprimidos dentro de los archivos comprimidos (anidados) que se van a explorar
/scan-timeout=LÍMITE	explorar los archivos comprimidos durante LIMIT segundos como máximo
/max-arch-size=TAMAÑO	solo explorar los archivos en un archivo comprimido si son menores que SIZE (predeterminado 0 = ilimitado)
/max-sfx-size=TAMAÑO	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-exclude=EXTENSIONES	excluir de la exploración las EXTENSIONES de archivos delimitadas por dos puntos
/clean-mode=MODO	<p>usar el MODO de desinfección para objetos infectados</p> <p>Se encuentran disponibles las siguientes opciones:</p> <ul style="list-style-type: none"> • none (predeterminado): no se realizará desinfección automática alguna. • standard: 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

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

ESET CMD

Esta es una característica que habilita los comandos avanzados `ecmd`. Le permite exportar e importar la configuración mediante la línea de comando (`ecmd.exe`). Hasta ahora, solo era posible exportar configuraciones usando la interfaz gráfica del usuario, [GUI](#). ESET NOD32 Antivirus la configuración puede exportarse al archivo `.xml`.

Cuando haya habilitado ESET CMD, existen dos métodos de autorización disponibles:

- **Ninguno** – sin autorización. No le recomendamos este método porque permite la importación de cualquier configuración no firmada, lo cuál es un riesgo potencial.
- **Contraseña de configuración avanzada**: se requiere una contraseña para importar una configuración de un archivo `.xml`, este archivo debe estar firmado (consulte la firma del archivo de configuración `.xml` más abajo). La contraseña especificada en [Configuración de acceso](#) se debe brindar antes de poder importar una nueva configuración. Si no tiene acceso a la configuración habilitada, su contraseña no coincide o el archivo de configuración `.xml` no está firmado, la configuración no se importará.

Una vez habilitado ESET CMD, puede usar la línea de comandos para exportar/importar ESET NOD32 Antivirus configuraciones. Puede hacerlo manualmente o crear una secuencia de comandos con fines de automatización.




Para utilizar comandos avanzados de `ecmd`, debe ejecutarlos con privilegios de administrador o abrir el Símbolo de comandos de Windows (`cmd`) utilizando **Ejecutar como administrador**. Caso contrario, obtendrá el mensaje **Error executing command**. Además, al exportar una configuración, debe existir la carpeta de destino. El comando de exportar sigue funcionando cuando la configuración ESET CMD se encuentra apagada.



Exportar comando de configuración:
`ecmd /getcfg c:\config\settings.xml`

Importar comando de configuración:
`ecmd /setcfg c:\config\settings.xml`

 Los comandos `ecmd` avanzados solo pueden ejecutarse localmente.

Firmar un archivo de configuración `.xml`:

1. Descargar el [XmlSignTool](#) ejecutable.

2. Abra el símbolo del sistema de Windows (cmd) mediante **Ejecutar como administrador**.
3. Navegar a la ubicación de guardar de `xmlsigntool.exe`
4. Ejecute un comando para firmar el archivo de configuración.xml, uso: `xmlsigntool /version 1|2 <xml_file_path>`



El valor del `/version` parámetro depende de su versión de ESET NOD32 Antivirus. Use `/version 1` para versiones anteriores de ESET NOD32 Antivirus que 11.1. Use `/version 2` para la versión actual de ESET NOD32 Antivirus.

5. Ingrese y vuelva a ingresar su contraseña de [Configuración avanzada](#) cuando XmlSignTool lo solicite. Su archivo de configuración.xml/ahora se encuentra firmado y se podrá utilizar para importar en otra instancia de ESET NOD32 Antivirus con ESET CMD utilizando el método de autorización con contraseña.

Firme el comando de archivo de configuración exportado:
`xmlsigntool /version 2 c:\config\settings.xml`

```
C:\Windows\system32\cmd.exe
C:\XmlSignTool>xmlsigntool /version 1 c:\config\settings.xml
Enter Advanced Setup Password:
Re-enter Password:
C:\XmlSignTool>_
```



Si cambia su contraseña de la [Configuración de acceso](#) y desea importar la configuración firmada anteriormente con una contraseña antigua, necesita volver a firmar el archivo de configuración .xml/ usando la contraseña actual. Esto le permite usar un archivo de configuración anterior sin exportarlo a otro equipo que ejecute ESET NOD32 Antivirus antes de la importación.



No se recomienda habilitar ESET CMD sin una autorización, ya que esto permitirá la importación de cualquier configuración no firmada. Establezca la contraseña en **Configuración avanzada > Interfaz de usuario > Configuración de acceso** para evitar las modificaciones no autorizadas de los usuarios.

Detección en estado inactivo

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

- Pantalla apagada o protector de pantalla
- Bloqueo de equipo

- **Cierre de sesión de usuario**

Use las barras deslizantes de cada estado correspondiente para habilitar o deshabilitar los desencadenantes de la detección en estado inactivo.

Preguntas habituales

A continuación, encontrará algunas de las preguntas más frecuentes y los problemas más comunes. Haga clic en el título del tema para obtener información sobre cómo solucionar el problema:

- [Cómo actualizar ESET NOD32 Antivirus](#)
- [Cómo quitar un virus del equipo](#)
- [Cómo crear una nueva tarea en Tareas programadas](#)
- [Cómo programar una tarea de exploración \(semanal\)](#)
- [Cómo desbloquear la configuración avanzada](#)
- [Cómo resolver la desactivación del producto desde ESET HOME](#)

Si su problema no está incluido en la lista anterior, intente buscar en la Ayuda en línea de ESET NOD32 Antivirus.

Si no encuentra una solución a su problema o pregunta en la Ayuda en línea de ESET NOD32 Antivirus, puede visitar nuestra [Base de conocimiento de ESET](#), la cual se actualiza regularmente. A continuación, se incluyen vínculos a nuestros artículos de la base de conocimiento más populares:

- [¿Cómo renovar mi licencia?](#)
- [Recibí un error de activación mientras se instalaba el producto de ESET. ¿Qué significa esto?](#)
- [Activar mi producto hogareño de ESET Windows con la clave de licencia](#)
- [Desinstalar o volver a instalar mi producto hogareño de ESET](#)
- [Recibo el mensaje de que mi instalación de ESET finalizó de manera prematura](#)
- [¿Qué necesito hacer luego de renovar mi licencia? \(Usuarios locales\)](#)
- [¿Qué sucede si cambio mi dirección de correo electrónico?](#)
- [Transferir mi producto ESET a un nuevo equipo o dispositivo](#)
- [Cómo iniciar Windows en Modo seguro o Modo seguro con conexión de red](#)
- [Impedir que se bloquee un sitio web seguro](#)
- [Permita que el software de los lectores de pantalla acceda a la GUI de ESET](#)

En caso de ser necesario, también puede ponerse en contacto con [Soporte técnico](#) para consultar sus preguntas o problemas.

Cómo actualizar ESET NOD32 Antivirus

La actualización de ESET NOD32 Antivirus se puede realizar en forma manual o automática. Para iniciar la actualización, haga clic en **Actualizar** en la [ventana del programa principal](#) y luego haga clic en **Comprobar si hay actualizaciones**.

La configuración predeterminada de la instalación crea una tarea de actualización automática que se ejecuta a cada hora. Si necesita cambiar dicho intervalo, vaya a **Herramientas** > [Tareas programadas](#).

Cómo quitar un virus del equipo

Si su equipo muestra síntomas de infección por malware; por ejemplo, funciona más lento o con frecuencia no responde, se recomienda hacer lo siguiente:

1. Desde la [ventana principal del programa](#), haga clic en **Exploración del equipo**.
2. Haga clic en **Explorar el equipo** para iniciar la exploración del sistema.
3. Una vez finalizada la exploración, consulte el registro con la cantidad de archivos explorados, infectados y desinfectados.
4. Si solo quiere explorar una parte seleccionada del disco, haga clic en **Exploración personalizada** y seleccione los objetos para explorar en busca de virus.

Para obtener más información, consulte nuestro [artículo de la base de conocimiento de ESET](#), que se actualiza en forma regular.

Cómo crear una nueva tarea en Tareas programadas

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

- **Ejecutar aplicación externa** – programa la ejecución de una aplicación externa.
- **Mantenimiento de registros** – los archivos de registro también contienen remanentes de historiales eliminados. Esta tarea optimiza los historiales de los archivos de registro en forma habitual para que funcionen eficazmente.
- **Verificación de archivos de inicio del sistema**: verifica los archivos que tienen permiso para ejecutarse al iniciar el sistema o tras el registro del usuario.
- **Crear una instantánea de estado del equipo**: crea una instantánea del equipo de ESET SysInspector, que recopila información detallada sobre los componentes del sistema (por ejemplo, controladores, aplicaciones) y evalúa el nivel de riesgo de cada componente.
- **Exploración del equipo a pedido**: realiza una exploración del equipo de los archivos y las carpetas de su equipo.
- **Actualización**: programa una tarea de actualización mediante la actualización de módulos.

Dado que la **Actualización** es una de las tareas programadas de uso frecuente, a continuación se explicará cómo agregar una nueva tarea de actualización.

En el menú desplegable **Tarea programada**, seleccione **Actualización**. Ingrese el nombre de la tarea en el campo **Nombre de la tarea** y haga clic en **Siguiente**. Seleccione la frecuencia de la tarea. Se encuentran disponibles las siguientes opciones: **Una vez**, **Reiteradamente**, **Diariamente**, **Semanalmente** y **Cuando se cumpla la condición**. Seleccione **Omitir tarea al ejecutar con alimentación de la batería** para reducir los recursos del sistema mientras un equipo portátil se ejecuta con alimentación de la batería. La tarea se ejecutará en la fecha y hora especificadas en los campos de **Ejecución de la tarea**. A continuación, defina la acción a tomar en caso de que la tarea no se pueda realizar o completar a la hora programada. Se encuentran disponibles las siguientes opciones:

- **A la próxima hora programada**
- **Lo antes posible**
- **Inmediatamente, si el tiempo desde la última ejecución excede un valor específico** (el intervalo se puede definir con el uso del cuadro de desplazamiento del **Tiempo desde la última ejecución [horas]**)

En el siguiente paso, se muestra una ventana de resumen con información acerca de la tarea actual programada. Haga clic en **Finalizar** cuando haya terminado de realizar los cambios.

Aparecerá una ventana de diálogo desde donde se le permite seleccionar los perfiles que se usarán para la tarea programada. Aquí puede configurar el perfil principal y el alternativo. El perfil alternativo se utiliza si la tarea no se puede completar con el perfil principal. Confirme haciendo clic en **Finalizar** y la nueva tarea programada se agregará a la lista de tareas actualmente programadas.

Cómo programar una exploración semanal del equipo

Para programar una tarea de rutina, abra la [ventana principal del programa](#) y haga clic en **Herramientas > Tareas programadas**. La siguiente guía le indicará cómo programar una tarea que explorará sus unidades locales todas las semanas. Lea nuestro [artículo de la base de conocimiento](#) para obtener instrucciones más detalladas.

Para programar una tarea de exploración:

1. Haga clic en **Agregar** en la pantalla principal de Tareas programadas.
2. Escriba un nombre para la tarea y seleccione **Exploración del equipo a pedido** desde el menú desplegable **Tipo de tarea**.
3. Seleccione **Semanalmente** para establecer la frecuencia.
4. Configure el día y la hora en que se ejecutará la tarea.
5. Seleccione **Ejecutar la tarea lo antes posible** para realizar la tarea más tarde en caso de que su ejecución no se haya iniciado por algún motivo (por ejemplo, porque el equipo estaba apagado).
6. Revise el resumen de la tarea programada y haga clic en **Finalizar**.
7. En el menú desplegable **Destino**, seleccione **Unidades locales**.
8. Haga clic en **Finalizar** para aplicar la tarea.

Cómo desbloquear la configuración avanzada protegida por contraseña

Cuando quiera acceder a la Configuración avanzada protegida, aparecerá la ventana para escribir la contraseña. Si no la recuerda o la pierde, haga clic en **Restaurar contraseña** y escriba la dirección de correo electrónico que usó para el registro de la licencia. ESET le enviará un correo electrónico con el código de verificación. Escriba el código de verificación y luego ingrese y confirme la nueva contraseña. El código de verificación tiene una validez de siete días.

Restaurar la contraseña a través de su cuenta ESET HOME: use esta opción si la licencia que se usa para la activación está asociada a su cuenta ESET HOME. Escriba la dirección de correo electrónico que usa para iniciar sesión en su cuenta [ESET HOME](#).

Si no recuerda su dirección de correo electrónico o tiene dificultades para restablecer la contraseña, haga clic en **Ponerse en contacto con el servicio de soporte técnico**. Se lo redirigirá al sitio web de ESET para que se ponga en contacto con nuestro Departamento de Soporte Técnico.

Generar código para soporte técnico: esta opción generará un código para Soporte Técnico. Copie el código proporcionado por Soporte Técnico y haga clic en **Tengo un código de verificación**. Escriba el código de verificación y, a continuación, ingrese y confirme la nueva contraseña. El código de verificación tiene una validez de siete días.

Para obtener más información, consulte [Desbloquear su contraseña de configuración en productos hogareños de Windows ESET](#).

Cómo resolver la desactivación del producto desde ESET HOME

Producto no activado

Este mensaje de error aparece cuando el propietario de la licencia desactiva ESET NOD32 Antivirus desde el portal ESET HOME o la licencia compartida con su cuenta ESET HOME ya no se ha compartido. Para resolver este problema:

- Haga clic en **Activar** y utilice uno de los [Métodos de activación](#) para activar ESET NOD32 Antivirus.
- Póngase en contacto con el propietario de la licencia si tiene información de que el propietario de la licencia ha desactivado su ESET NOD32 Antivirus o que ya no se comparte la licencia con usted. El propietario puede resolver el problema en [ESET HOME](#).

Producto desactivado, dispositivo desconectado

Este mensaje de error aparece después de [quitar un dispositivo de la cuenta ESET HOME](#). Para resolver este problema:

- Haga clic en **Activar** y utilice uno de los [Métodos de activación](#) para activar ESET NOD32 Antivirus.

- Póngase en contacto con el propietario de la licencia si tiene información de que se ha desactivado su ESET NOD32 Antivirus y que el dispositivo se ha desconectado de ESET HOME.
- Si es el propietario de la licencia y no tiene conocimiento de estos cambios, consulte la fuente de actividades de [ESET HOME](#). Si encuentra alguna actividad sospechosa, [cambie la contraseña de su cuenta ESET HOME](#) y [póngase en contacto con el servicio de soporte técnico de ESET](#).

Producto desactivado, dispositivo desconectado

Este mensaje de error aparece después de [quitar un dispositivo de la cuenta ESET HOME](#). Para resolver este problema:

- Haga clic en **Activar** y utilice uno de los [Métodos de activación](#) para activar ESET NOD32 Antivirus.
- Póngase en contacto con el propietario de la licencia si tiene información de que se ha desactivado su ESET NOD32 Antivirus y que el dispositivo se ha desconectado de ESET HOME.
- Si es el propietario de la licencia y no tiene conocimiento de estos cambios, consulte la fuente de actividades de [ESET HOME](#). Si encuentra alguna actividad sospechosa, [cambie la contraseña de su cuenta ESET HOME](#) y [póngase en contacto con el servicio de soporte técnico de ESET](#).

Producto no activado

Este mensaje de error aparece cuando el propietario de la licencia desactiva ESET NOD32 Antivirus desde el portal ESET HOME o la licencia compartida con su cuenta ESET HOME ya no se ha compartido. Para resolver este problema:

- Haga clic en **Activar** y utilice uno de los [Métodos de activación](#) para activar ESET NOD32 Antivirus.
- Póngase en contacto con el propietario de la licencia si tiene información de que el propietario de la licencia ha desactivado su ESET NOD32 Antivirus o que ya no se comparte la licencia con usted. El propietario puede resolver el problema en [ESET HOME](#).

Programa de mejora de la experiencia del cliente

Al unirse a nuestro Programa de mejora de la experiencia del cliente, usted le provee a ESET información anónima relacionada con el uso de nuestros productos. Para obtener más información sobre el procesamiento de datos, consulte nuestra Política de privacidad.

Su consentimiento

La participación en el Programa es voluntaria y se basa en su consentimiento. Luego de unirse, la participación es pasiva, lo que significa que no se requiere ninguna acción de su parte. Usted podrá revocar su consentimiento al modificar la configuración del producto cuando lo desee. Al hacerlo, evitará que sigamos procesando sus datos anónimos.

Puede revocar su consentimiento en cualquier momento al cambiar la configuración del producto:

- [Cambia la configuración del Programa de mejora de la experiencia del cliente en los productos hogareños](#)

¿Qué tipo de información recolectamos?

Datos de la interacción con el producto

Estos datos nos informan sobre cómo se utilizan nuestros productos. Gracias a esto sabemos, por ejemplo, cuáles funcionalidades se utilizan frecuentemente, qué configuraciones modifican los usuarios o cuánto tiempo pasan utilizando nuestros productos.

Datos acerca de dispositivos

Recopilamos esta información para comprender en qué dispositivos y dónde se utilizan nuestros productos. Algunos ejemplos típicos son el modelo de dispositivo, el país, la versión y el nombre del sistema operativo.

Datos de diagnóstico de errores

También se recopilan datos acerca del error y de la situación de la falla. Por ejemplo, qué error se ha producido y qué acciones derivaron en él.

¿Por qué recopilamos esta información?

Estos datos anónimos nos hacen posible mejorar nuestros productos para usted, el usuario. Además, nos ayudan a convertirlos en más relevantes, fáciles de usar y sin fallas como sea posible.

¿Quién controla esta información?

ESET, spol. s r.o. es el único controlador de los datos recopilados en el programa. Esta información no se comparte con terceros.

Acuerdo de licencia de usuario final

Vigente a partir del 19 de octubre de 2021.

IMPORTANTE: Lea los términos y las condiciones del producto de aplicación que se especifican abajo antes de descargarlo, instalarlo, copiarlo o usarlo. **AL DESCARGAR, INSTALAR, COPIAR O UTILIZAR EL SOFTWARE, USTED DECLARA SU CONSENTIMIENTO CON LOS TÉRMINOS Y CONDICIONES Y RECONOCE QUE HA LEÍDO LA [POLÍTICA DE PRIVACIDAD](#).**

Acuerdo de Licencia de Usuario Final

Los términos de este Acuerdo de licencia para el usuario final ("Acuerdo") ejecutado por y entre ESET, spol. s r. o., con domicilio social en Einsteinova 24, 85101 Bratislava, Slovak Republic, registrado en el Registro Mercantil administrado por el tribunal de distrito de Bratislava I, sección Sro, n.º de entrada 3586/B, número de registro de negocio: 31333532 ("ESET" o el "Proveedor") y usted, una persona física o jurídica ("Usted" o el "Usuario final"), tienen derecho a usar el Software definido en el Artículo 1 de este Acuerdo. El Software definido en este artículo puede almacenarse en un soporte digital, enviarse mediante correo electrónico, descargarse de Internet, descargarse de servidores del Proveedor u obtenerse de otras fuentes bajo los términos y condiciones mencionados más adelante.

ESTO ES UN ACUERDO SOBRE LOS DERECHOS DEL USUARIO FINAL; NO UN CONTRATO DE COMPRA PARA ARGENTINA. El Proveedor sigue siendo el propietario de la copia del Software y del soporte físico en el que el Software se suministra en paquete comercial, así como de todas las demás copias a las que el Usuario final está autorizado a hacer en virtud de este Acuerdo.

Al hacer clic en las opciones "Acepto" o "Acepto..." durante la instalación, descarga, copia o uso del Software, acepta los términos y condiciones de este Acuerdo y la Política de privacidad. Si no acepta todos los términos y condiciones de este Acuerdo o la Política de privacidad, de inmediato haga clic en la opción de cancelación, cancele la instalación o descarga o destruya o devuelva el Software, el soporte de instalación, la documentación adjunta y el recibo de compra al Proveedor o al lugar donde haya adquirido el Software.

USTED ACEPTA QUE LA UTILIZACIÓN DEL SOFTWARE INDICA QUE HA LEÍDO ESTE ACUERDO, QUE LO COMPRENDE Y QUE CONSIENTE OBLIGARSE POR SUS TÉRMINOS Y CONDICIONES.

1. Software. Tal como se utiliza en este Acuerdo, el término "Software" significa: (i) el programa informático que acompaña a este Acuerdo y todos sus componentes; (ii) todos los contenidos de los discos, CD-ROMs, DVDs, correos electrónicos y cualquier adjunto, u otros medios con los cuales se provee este Acuerdo, incluyendo el formulario del código objeto del software provisto en soporte digital, por medio de correo electrónico o descargado a través de la Internet; (iii) cualquier material escrito explicativo relacionado y cualquier otra documentación posible relacionada con el Software, sobre todo cualquier descripción del Software, sus especificaciones, cualquier descripción de las propiedades u operación del software, cualquier descripción del ambiente operativo en el cual se utiliza el Software, instrucciones de uso o instalación del Software o cualquier descripción del modo de uso del Software ("Documentación"); (iv) copias del Software, parches para posibles errores del Software, adiciones al Software, extensiones del Software, versiones modificadas del Software y actualizaciones de los componentes del Software, si existieran, con la autorización que le da a Usted el Proveedor con arreglo al Artículo 3 de este Acuerdo. El Software será provisto exclusivamente en la forma de código objeto ejecutable.

2. Instalación, equipo y clave de licencia. El Software suministrado en un soporte digital, enviado por correo electrónico, descargado de Internet, descargado de los servidores del Proveedor u obtenido de otras fuentes requiere instalación. El Software debe instalarse en un equipo correctamente configurado que cumpla, como mínimo, con los requisitos especificados en la Documentación. La metodología de instalación se describe en la Documentación. No puede haber ningún programa informático ni Hardware que pudiera afectar al Software instalado en el equipo en el que instala el Software. El equipo hace referencia al Hardware que incluye, pero no se limita, a equipos personales, equipos portátiles, estaciones de trabajo, equipos de bolsillo, teléfonos inteligentes, dispositivos electrónicos portátiles o cualquier otro dispositivo para el que se diseñe el Software y en el que vaya a instalarse y/o utilizarse. La clave de licencia se refiere a una secuencia única de símbolos, letras números o caracteres especiales que se le brinda al Usuario final para permitirle el uso del Software de manera legal, así como de una versión específica de este o para brindarle una extensión de los términos de la Licencia en conformidad con el presente Acuerdo.

3. Licencia. Siempre que haya aceptado los términos de este Acuerdo y cumpla con todos los términos y condiciones aquí especificados, el Proveedor le concederá los siguientes derechos (la "Licencia"):

a) **Instalación y uso.** Usted tendrá el derecho no exclusivo y no transferible de instalar el Software en el disco rígido de un equipo o soporte similar para un almacenamiento permanente de datos, instalar y almacenar el Software en la memoria de un sistema informático e implementar, almacenar y mostrar el Software.

b) **Disposición sobre la cantidad de licencias.** El derecho a utilizar el Software estará sujeto a la cantidad de Usuarios finales. Un "Usuario final" se refiere a lo siguiente: (i) instalación del Software en un sistema informático, o (ii) si el alcance de una licencia está vinculado a la cantidad de buzones de correo, un Usuario final se referirá a un usuario informático que acepta correo electrónico a través de un Agente de usuario de correo ("AUC"). Si un

AUC acepta el correo electrónico y lo distribuye posteriormente en forma automática a varios usuarios, la cantidad de Usuarios finales se determinará conforme a la cantidad real de usuarios para los que se distribuyó el correo electrónico. Si un servidor de correo cumple la función de una pasarela de correo, la cantidad de Usuarios finales será equivalente a la cantidad de usuarios de servidores de correo a los que dicha pasarela presta servicios. Si se envía una cantidad no especificada de direcciones de correo electrónico (por ejemplo, con alias) a un usuario y el usuario las acepta, y el cliente no distribuye automáticamente los mensajes a más usuarios, se requiere la Licencia únicamente para un equipo. No debe usar la misma Licencia en más de un equipo al mismo tiempo. El Usuario final solo tiene derecho a introducir la Clave de licencia en el Software en la medida en que el Usuario final tenga derecho a usar el Software de acuerdo con la limitación derivada del número de Licencias otorgadas por el Proveedor. Se considera que la clave de Licencia es confidencial. No puede compartirla con terceros ni puede permitirles que la utilicen a menos que el presente Acuerdo o el Proveedor indique lo contrario. Si su clave de Licencia se encuentra en riesgo notifique al Proveedor de inmediato.

c) **Home/Business Edition.** La versión Home Edition del Software solo se usará en entornos privados o no comerciales para uso en el hogar y familiar exclusivamente. Debe obtener una versión Business Edition del software para poder usarla en un entorno comercial, así como en servidores, transmisores y puertas de enlace de correo o de Internet.

d) **Término de la Licencia.** El derecho a utilizar el Software tendrá un límite de tiempo.

e) **Software de OEM.** El software clasificado como "OEM" solo se puede usar en el equipo con el que se ha obtenido. No puede transferirse a otro equipo.

f) **Software NFR y versión de prueba.** Al Software clasificado como "No apto para la reventa", "NFR" o "Versión de prueba" no se le podrá asignar un pago y puede utilizarse únicamente para hacer demostraciones o evaluar las características del Software.

g) **Rescisión de la Licencia.** La Licencia se rescindirá automáticamente al finalizar el período para el cual fue otorgada. Si Usted no cumple con alguna de las disposiciones de este Acuerdo, el Proveedor tendrá el derecho de anular el Acuerdo, sin perjuicio de cualquier derecho o recurso judicial disponible para el Proveedor en dichas eventualidades. En el caso de cancelación de la Licencia, Usted deberá borrar, destruir o devolver de inmediato por su propia cuenta el Software y todas las copias de seguridad a ESET o al punto de venta donde obtuvo el Software. Tras la finalización de la Licencia, el Proveedor podrá cancelar el derecho del Usuario Final a utilizar las funciones del Software que requieran conexión a los servidores del Proveedor o de terceros.

4. Funciones con recopilación de información y requisitos para la conexión a Internet. Para que funcione de manera correcta, el Software requiere conexión a Internet y debe conectarse a intervalos regulares a los servidores del Proveedor o de terceros y debe recopilar información en conformidad con la Política de Privacidad. La conexión a Internet y la recopilación de datos son necesarias para llevar a cabo las siguientes funciones del Software:

a) **Actualizaciones del Software.** El Proveedor podrá publicar periódicamente actualizaciones o actualizaciones del Software ("Actualizaciones"), aunque no está obligado a proporcionarlas. Esta función se activa en la sección de configuración estándar del Software y las Actualizaciones se instalan automáticamente, a menos que el Usuario final haya desactivado la instalación automática de Actualizaciones. Para aprovisionar Actualizaciones, es necesario verificar la autenticidad de la Licencia, lo que incluye información sobre el equipo o la plataforma en los que está instalado el Software, de acuerdo con la Política de Privacidad.

La entrega de todas las actualizaciones puede estar sujeta a la Política de fin de la vida útil ("Política EOL"), disponible en https://go.eset.com/eol_home. No se proporcionarán actualizaciones una vez que el Software o cualquiera de sus funciones lleguen a la fecha de fin de su vida útil, como se define en la Política EOL.

b) **Envío de infiltraciones e información al Proveedor.** El Software contiene funciones que reúnen muestras de

virus informáticos, otros programas informáticos dañinos y objetos sospechosos, problemáticos, potencialmente no deseados o potencialmente no seguros como archivos, URL, paquetes de IP y marcos de Ethernet (“Infiltraciones”) y luego los envía al Proveedor, incluidas, entre otras, la información sobre el proceso de instalación, el equipo o la plataforma en los cuales se instala el Software y la información sobre las operaciones y la funcionalidad del Software (“Información”). La Información y las Infiltraciones pueden contener datos (incluidos datos personales obtenidos aleatoriamente o accidentalmente) sobre el Usuario Final u otros usuarios del equipo en el cual se encuentra instalado el Software, y archivos afectados por Infiltraciones con metadatos asociados.

La Información y las Infiltraciones pueden ser recopiladas por las siguientes funciones del Software:

- i. La función Sistema de reputación de LiveGride incluye la recopilación y el envío de hashes de una vía relacionados a Infiltraciones al Proveedor. Esta función se activa con la configuración estándar del Software.
- ii. La función del sistema de comentarios de LiveGrid es recopilar información acerca de las infiltraciones con metadatos relacionados para enviársela al Proveedor. El Usuario final debe activar esta función durante la instalación del Software.

El proveedor solo debe hacer uso de la información y de las infiltraciones que recibe para analizar y para investigar las infiltraciones, para mejorar el Software y el proceso de verificación de la autenticidad de la Licencia. Asimismo, debe tomar las medidas correspondientes para garantizar la seguridad de las infiltraciones y de la información que recibe. Si se activa esta función del Software, el Proveedor deberá recopilar y procesar las infiltraciones y la información tal como se especifica en la Política de Privacidad y en conformidad con las normas legales vigentes. Puede desactivar estas funciones en cualquier momento.

A los efectos de este Acuerdo, es necesario recopilar, procesar y almacenar información que permita al Proveedor identificarlo en conformidad con la Política de Privacidad. Por medio del presente, reconoce que el Proveedor utiliza sus propios medios para verificar si Usted hace uso del Software de acuerdo con las disposiciones del Acuerdo. Asimismo, reconoce que, a los efectos de este Acuerdo, es necesario que su información se transfiera durante las comunicaciones entre el Software y los sistemas informáticos del Proveedor o de sus socios comerciales como parte de la red de distribución y soporte del Proveedor a fin de garantizar la funcionalidad del Software, de autorizar el uso del Software y proteger los derechos del Proveedor.

Tras la finalización de este Acuerdo, el Proveedor o cualquiera de sus socios comerciales tendrán el derecho de transferir, procesar y almacenar datos esenciales que lo identifiquen, con el propósito de realizar la facturación y para la ejecución del presente Acuerdo y para transmitir notificaciones a su equipo.

Los detalles sobre la privacidad, la protección de la información personal y sus derechos como parte interesada pueden encontrarse en la Política de Privacidad, disponible en el sitio web del Proveedor y a la que se puede acceder de manera directa desde el proceso de instalación. También puede acceder a ella desde la sección de ayuda del Software.

5. Ejercicio de los derechos del Usuario final. Debe ejercer los derechos del Usuario final en persona o a través de sus empleados. Tiene derecho a utilizar el Software solamente para asegurar sus operaciones y proteger los sistemas informáticos para los que ha obtenido una Licencia.

6. Restricciones de los derechos. No puede copiar, distribuir, extraer componentes o crear versiones derivadas del Software. Al usar el Software, Usted tiene la obligación de cumplir con las siguientes restricciones:

- a) Puede crear una copia del Software en un soporte de almacenamiento permanente de datos como una copia de seguridad para archivar, siempre que su copia de seguridad para archivar no esté instalada ni se utilice en ningún equipo. Cualquier otra copia que realice del Software constituirá un incumplimiento de este Acuerdo.
- b) No puede utilizar, modificar, traducir ni reproducir el Software, o transferir los derechos de su uso o copias

realizadas del Software de ninguna otra forma a lo establecido en este Acuerdo.

c) No puede vender, sublicenciar, arrendar o alquilar el Software, ni usarlo para suministrar servicios comerciales.

d) No puede aplicar técnicas de ingeniería inversa, descompilar o desmontar el Software, ni intentar obtener el código fuente del Software de ninguna otra forma, salvo en la medida en que esta restricción esté explícitamente prohibida por la ley.

e) Usted acepta que solo usará el Software de forma que se cumplan todas las leyes aplicables en la jurisdicción en la que lo utilice, incluyendo, pero sin limitarse a, las restricciones aplicables relacionadas con el copyright y otros derechos de propiedad intelectual.

f) Usted acepta que solamente usará el Software y sus funciones de una manera que no limite las posibilidades de otros Usuarios finales para acceder a estos servicios. El Proveedor se reserva el derecho de limitar el alcance los servicios proporcionados a Usuarios finales individuales, para activar el uso de los servicios por parte de la mayor cantidad posible de Usuarios finales. La limitación del alcance de los servicios también significará la terminación completa de la posibilidad de usar cualquiera de las funciones del Software y la eliminación de los Datos y de la información de los servidores de los Proveedores o de los servidores de terceros relacionados con una función específica del Software.

g) Usted acepta no ejercer ninguna actividad que implique el uso de la clave de Licencia de manera contraria a los términos de este Acuerdo ni que implique proporcionar la clave de Licencia a personas que no estén autorizadas a hacer uso del Software, como la transferencia de la clave de Licencia usada o no, en cualquier forma, así como la reproducción no autorizada, o la distribución de claves de Licencia duplicadas o generadas. Asimismo, no utilizará el Software como resultado del uso de una clave de Licencia obtenida de una fuente que no sea el Proveedor.

7. Copyright. El Software y todos los derechos, incluyendo, pero sin limitarse a, los derechos de propiedad y los derechos de propiedad intelectual, son propiedad de ESET y/o sus licenciarios. Están protegidos por las disposiciones de tratados internacionales y por todas las demás leyes nacionales aplicables del país en el que se utiliza el Software. La estructura, la organización y el código del Software son valiosos secretos comerciales e información confidencial de ESET y/o sus licenciarios. No puede copiar el Software, a excepción de lo especificado en el artículo 6 (a). Todas las copias que este Acuerdo le permita hacer deberán incluir el mismo copyright y los demás avisos legales de propiedad que aparezcan en el Software. Si aplica técnicas de ingeniería inversa, descompila o desmonta el Software, o intenta obtener el código fuente del Software de alguna otra forma, en incumplimiento de las disposiciones de este Acuerdo, por este medio Usted acepta que toda la información obtenida de ese modo se considerará automática e irrevocablemente transferida al Proveedor o poseída por el Proveedor de forma completa desde el momento de su origen, más allá de los derechos del Proveedor en relación con el incumplimiento de este Acuerdo.

8. Reserva de derechos. Por este medio, el Proveedor se reserva todos los derechos del Software, excepto por los derechos concedidos expresamente bajo los términos de este Acuerdo a Usted como el Usuario final del Software.

9. Versiones en varios idiomas, software en medios duales, varias copias. En caso de que el Software sea compatible con varias plataformas o idiomas, o si Usted obtuvo varias copias del Software, solo puede usar el Software para la cantidad de sistemas informáticos y para las versiones correspondientes a la Licencia adquirida. No puede vender, arrendar, alquilar, sublicenciar, prestar o transferir ninguna versión o copias del Software no utilizado por Usted.

10. Comienzo y rescisión del Acuerdo. Este Acuerdo es efectivo desde la fecha en que Usted acepta los términos de la Licencia. Puede poner fin a este Acuerdo en cualquier momento. Para ello, desinstale, destruya o devuelva permanentemente y por cuenta propia el Software, todas las copias de seguridad, y todos los materiales relacionados suministrados por el Proveedor o sus socios comerciales. Su derecho a usar el Software y cualquiera

de sus funciones puede estar sujeto a la Política EOL. Cuando el Software o cualquiera de sus funciones lleguen a la fecha de fin de su vida útil definida en la Política EOL, se terminará su derecho a usar el Software. Más allá de la forma de rescisión de este Acuerdo, las disposiciones de los artículos 7, 8, 11, 13, 19 y 21 seguirán siendo aplicables por tiempo ilimitado.

11. DECLARACIONES DEL USUARIO FINAL. COMO USUARIO FINAL, USTED RECONOCE QUE EL SOFTWARE SE SUMINISTRA EN UNA CONDICIÓN "TAL CUAL ES", SIN UNA GARANTÍA EXPRESA O IMPLÍCITA DE NINGÚN TIPO Y HASTA EL ALCANCE MÁXIMO PERMITIDO POR LAS LEYES APLICABLES. NI EL PROVEEDOR, SUS LICENCIATARIOS, SUS AFILIADOS NI LOS TITULARES DEL COPYRIGHT PUEDEN HACER NINGUNA REPRESENTACIÓN O GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, PERO SIN LIMITARSE A, LAS GARANTÍAS DE COMERCIABILIDAD O ADECUACIÓN PARA UN FIN ESPECÍFICO O GARANTÍAS DE QUE EL SOFTWARE NO INFRINGIRÁ UNA PATENTE, DERECHOS DE PROPIEDAD INTELECTUAL, MARCAS COMERCIALES U OTROS DERECHOS. NO EXISTE NINGUNA GARANTÍA DEL PROVEEDOR NI DE NINGUNA OTRA PARTE DE QUE LAS FUNCIONES CONTENIDAS EN EL SOFTWARE CUMPLIRÁN CON SUS REQUISITOS O DE QUE LA OPERACIÓN DEL SOFTWARE SERÁ ININTERRUMPIDA O ESTARÁ LIBRE DE ERRORES. USTED ASUME TODA LA RESPONSABILIDAD Y EL RIESGO POR LA ELECCIÓN DEL SOFTWARE PARA LOGRAR SUS RESULTADOS DESEADOS Y POR LA INSTALACIÓN, EL USO Y LOS RESULTADOS QUE OBTENGA DEL MISMO.

12. Sin más obligaciones. Este Acuerdo no crea obligaciones del lado del Proveedor y sus licenciarios, excepto las obligaciones específicamente indicadas en este Acuerdo.

13. LIMITACIÓN DE RESPONSABILIDAD. EN LA MEDIDA EN QUE LO PERMITA LA LEGISLACIÓN APLICABLE, EN NINGÚN CASO EL PROVEEDOR, SUS EMPLEADOS O LICENCIADORES SERÁN RESPONSABLES DE PÉRDIDAS DE INGRESOS, GANANCIAS, VENTAS, DATOS O COSTOS DE ADQUISICIÓN DE BIENES O SERVICIOS SUSTITUIDOS, DAÑOS A LA PROPIEDAD, DAÑOS PERSONALES, INTERRUPCIÓN DEL NEGOCIO, PÉRDIDA DE INFORMACIÓN COMERCIAL O DE CUALQUIER VALOR ESPECIAL, DIRECTO, INSONDADO, ACCIDENTAL, ECONÓMICO, DE COBERTURA, DAÑOS PUNITIVOS, ESPECIALES O CONSECUENCIALES, QUE SIN EMBARGO DERIVEN O SURJAN POR CONTRATO, AGRAVIOS, NEGLIGENCIA U OTRA TEORÍA DE RESPONSABILIDAD QUE DERIVE DE LA INSTALACIÓN, EL USO O LA INCAPACIDAD DE USAR EL SOFTWARE, AUNQUE EL PROVEEDOR, SUS LICENCIADORES O FILIALES RECIBAN INFORMACIÓN DE LA POSIBILIDAD DE DICHOS DAÑOS. DADO QUE DETERMINADOS PAÍSES Y JURISDICIONES NO PERMITEN LA EXCLUSIÓN DE RESPONSABILIDAD, PERO PUEDEN PERMITIR LA LIMITACIÓN DE RESPONSABILIDAD, EN DICHOS CASOS, LA RESPONSABILIDAD DEL PROVEEDOR, SUS EMPLEADOS, LICENCIATARIOS O AFILIADOS SE LIMITARÁ AL PRECIO QUE USTED PAGÓ POR LA LICENCIA.

14. Nada de lo contenido en este Acuerdo perjudicará los derechos estatutarios de ninguna parte que actúe en calidad de consumidor si infringe dicho Acuerdo.

15. Soporte técnico. ESET o los terceros autorizados por ESET suministrarán soporte técnico a discreción propia, sin ninguna garantía ni declaración. Cuando el software o cualquiera de sus funciones lleguen a la fecha de fin de la vida útil definida en la Política EOL, no se proporcionará soporte técnico. El Usuario final deberá crear una copia de seguridad de todos los datos existentes, software y prestaciones de los programas en forma previa al suministro de soporte técnico. ESET y/o los terceros autorizados por ESET no pueden aceptar la responsabilidad por el daño o pérdida de datos, propiedad, software o hardware, o pérdida de beneficios debido al suministro de soporte técnico. ESET y/o los terceros autorizados por ESET se reservan el derecho de decidir si la solución del problema excede el alcance del soporte técnico. ESET se reserva el derecho de rechazar, suspender o dar por finalizado el suministro de soporte técnico a discreción propia. Se puede solicitar información sobre la Licencia y cualquier otro tipo de información a fin de brindar soporte técnico conforme a la Política de Privacidad.

16. Transferencia de la Licencia. El Software puede transferirse de un sistema informático a otro, a menos que esta acción infrinja los términos del presente Acuerdo. Si no infringe los términos del Acuerdo, el Usuario final solamente tendrá derecho a transferir en forma permanente la Licencia y todos los derechos derivados de este Acuerdo a otro Usuario final con el consentimiento del Proveedor, sujeto a las siguientes condiciones: (i) que el

Usuario final original no se quede con ninguna copia del Software; (ii) que la transferencia de los derechos sea directa, es decir, del Usuario final original al nuevo Usuario final; (iii) que el nuevo Usuario final asuma todos los derechos y obligaciones pertinentes al Usuario final original bajo los términos de este Acuerdo; (iv) que el Usuario final original le proporcione al nuevo Usuario final la Documentación que habilita la verificación de la autenticidad del Software, como se especifica en el artículo 17.

17. Verificación de la autenticidad del Software. El Usuario final puede demostrar su derecho a usar el Software en una de las siguientes maneras: (i) a través de un certificado de licencia emitido por el Proveedor o por un tercero designado por el Proveedor; (ii) a través de un acuerdo de licencia por escrito, en caso de haberse establecido dicho acuerdo; (iii) a través de la presentación de un correo electrónico enviado por el Proveedor donde se incluyan los detalles de la Licencia (nombre de usuario y contraseña). Se puede solicitar información sobre la Licencia y datos sobre el Usuario final a para llevar a cabo la verificación de la autenticidad del Software conforme a la Política de Privacidad.

18. Licencias para autoridades públicas y el gobierno de los Estados Unidos. Se deberá suministrar el Software a las autoridades públicas, incluyendo el gobierno argentino, con los derechos de la Licencia y las restricciones descritas en este Acuerdo.

19. Cumplimiento del control comercial.

a) Usted no podrá, ya sea directa o indirectamente, exportar, reexportar o transferir el Software, o de alguna otra forma ponerlo a disposición de ninguna persona, o utilizarlo de ninguna manera, o participar de ningún acto, que pueda ocasionar que ESET o sus compañías controladoras, sus empresas subsidiarias y las subsidiarias de cualquiera de sus compañías controladoras, así como también las entidades controladas por sus compañías controladoras ("Afiliadas") violen, o queden sujetas a las consecuencias negativas de las Leyes de Control Comercial, las cuales incluyen

i. toda ley que controle, restrinja o imponga requisitos de licencia a la exportación, reexportación o transferencia de productos, software, tecnología o servicios, establecida o adoptada por cualquier gobierno, estado o autoridad reguladora de los Estados Unidos de América, Singapur, el Reino Unido, la Unión Europea o cualquiera de sus Estados Miembro, o cualquier país donde deban cumplirse las obligaciones conforme al Acuerdo, o donde ESET o cualquiera de sus Afiliadas operen o estén constituidas y

ii. cualquier sanción, restricción, embargo, prohibición de exportación o importación, prohibición de transferencia de fondos o activos o prohibición de prestación de servicios, ya sea de índole económica, financiera, comercial o de otro tipo, o toda medida equivalente impuesta por cualquier gobierno, estado o autoridad reguladora de los Estados Unidos de América, Singapur, el Reino Unido, la Unión Europea o cualquiera de sus Estados Miembro, o cualquier país donde deban cumplirse las obligaciones conforme al Acuerdo, o donde ESET o cualquiera de sus Afiliadas operen o estén constituidas.

(actos legales mencionados en los puntos i y ii. anteriormente, denominados "Leyes de control comercial").

b) ESET tendrá el derecho de suspender sus obligaciones conforme a estos Términos o terminar el Acuerdo, con efecto inmediato, en los siguientes casos:

i. ESET determina que, en su razonable opinión, el Usuario ha violado o podría violar la disposición del Artículo 19 a) del Acuerdo; o

ii. el Usuario final o el Software quedan sujetos a las Leyes de Control Comercial y, en consecuencia, ESET determina que, en su razonable opinión, el cumplimiento continuo de sus obligaciones conforme al Acuerdo podría ocasionar que ESET o sus Afiliadas incurriesen en la violación de las Leyes de Control Comercial o quedasen sujetas a las consecuencias negativas de estas.

c) Ninguna de las estipulaciones del Acuerdo tiene por objeto inducir o exigir, ni debe interpretarse como una intención de inducir o exigir a ninguna de las partes actuar o abstenerse de actuar (o acordar actuar o abstenerse de actuar) de ninguna manera que resulte inconsistente con las Leyes de Control Comercial aplicables, o se encuentre penalizada o prohibida por estas.

20. Avisos. Todos los avisos y devoluciones de software o documentación deben entregarse a: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, sin perjuicio del derecho de ESET a comunicarle cualquier cambio de este Acuerdo, las Políticas de privacidad, la Política de EOL y la Documentación de acuerdo con el artículo. 22 del Acuerdo. ESET puede enviarle correos electrónicos, notificaciones en la aplicación a través del Software o publicar la comunicación en nuestro sitio web. Acepta recibir comunicaciones legales de ESET de forma electrónica, lo que incluye comunicaciones sobre cambios de Términos, Términos especiales o Políticas de privacidad, cualquier contrato de trabajo o aceptación o invitación a tratar, avisos u otras comunicaciones legales. Dicha comunicación electrónica se considerará recibida por escrito, a menos que la legislación aplicable requiera específicamente una forma de comunicación diferente.

21. Legislación aplicable. Este Acuerdo se registrará e interpretará conforme a la legislación de la República Eslovaca. En el presente Acuerdo, el Usuario final y el Proveedor aceptan que los principios del conflicto de leyes y la Convención de las Naciones Unidas sobre los Contratos de Venta Internacional de Bienes no serán aplicables. Acepta expresamente que cualquier disputa o demanda derivada del presente Acuerdo con respecto al Proveedor o relativa al uso del Software deberá resolverse por el Tribunal del Distrito de Bratislava I., Eslovaquia; asimismo, Usted acepta expresamente el ejercicio de la jurisdicción del Tribunal mencionado.

22. Disposiciones generales. Si alguna disposición de este Acuerdo no es válida o aplicable, no afectará la validez de las demás disposiciones del Acuerdo, que seguirán siendo válidas y ejecutables bajo las condiciones aquí estipuladas. Este acuerdo se ha ejecutado en inglés. En el caso de que se prepare cualquier traducción del acuerdo para su comodidad o con cualquier otro fin, o en caso de discrepancia entre las versiones en diferentes idiomas de este acuerdo, prevalecerá la versión en inglés.

ESET se reserva el derecho de realizar cambios en el Software, así como de revisar los términos de este Acuerdo, sus Anexos, la Política de privacidad, la Política y la Documentación de EOL o cualquier parte de ellos, en cualquier momento mediante la actualización del documento pertinente (i) para reflejar cambios del Software o el comportamiento comercial de ESET, (ii) por cuestiones legales, normativas o de seguridad; o (iii) para evitar abusos o daños. Se le notificará cualquier revisión del Acuerdo por correo electrónico, notificación en la aplicación o por otros medios electrónicos. Si no está de acuerdo con los cambios de texto del Acuerdo, puede rescindir el acuerdo con el Artículo 10 en el plazo de 30 días después de recibir un aviso del cambio. A menos que rescinda el Acuerdo dentro de este límite de tiempo, los cambios de texto se considerarán aceptados y estarán vigentes para Usted a partir de la fecha en que reciba un aviso del cambio.

Este es el acuerdo entero entre el proveedor y Usted relacionado con el Software y reemplaza a cualquier representación, discusión, garantía, comunicación o publicidad previa relacionadas con el Software.

ANEXO AL ACUERDO

Evaluación de seguridad de los dispositivos conectados a la red. Se aplican disposiciones adicionales a la Evaluación de seguridad de los dispositivos conectados a la red como se muestra a continuación:

El Software contiene una función para verificar la seguridad de la red local del Usuario final y la seguridad de los dispositivos en la red local, lo que requiere el nombre de la red local e información acerca de los dispositivos en la red local, como presencia, tipo, nombre, dirección IP y dirección MAC en conexión con la información de licencia. La información también incluye tipo de seguridad inalámbrica y tipo de cifrado inalámbrico para los dispositivos del enrutador. Esta función también puede proporcionar información relacionada con la disponibilidad de la solución de software de seguridad para asegurar los dispositivos en la red local.

Protección contra el uso indebido de datos. Se aplican disposiciones adicionales a la protección contra el uso indebido de datos como se muestra a continuación:

El Software contiene una función que evita la pérdida o el uso indebido de datos críticos directamente relacionados con el robo de un equipo. Esta función se puede desactivar en los parámetros predeterminados del Software. Hay que crear una Cuenta ESET HOME para activarla, a través de la cual se activa la recopilación de datos en caso de robo del equipo. Si activa esta función del Software, se recopilará la información acerca del equipo robado y se enviará al Proveedor. Esta información puede incluir datos relacionados con la ubicación de red del equipo, datos relacionados con el contenido que se muestra en la pantalla del equipo, datos acerca de la configuración del equipo o datos grabados mediante una cámara conectada al equipo (en adelante denominados "Datos"). El Usuario final podrá usar los Datos obtenidos por esta función y proporcionados a través de la Cuenta ESET HOME exclusivamente para rectificar una situación adversa causada por el robo de un equipo. Para la única finalidad de esta función, el Proveedor procesa los Datos según se especifica en la Política de Privacidad y conforme a los reglamentos legales pertinentes. El Proveedor permitirá al Usuario final acceder a los Datos durante el período requerido para alcanzar el objetivo para el que se obtuvieron los datos, que no podrá superar el período de retención especificado en la Política de Privacidad. La protección contra el uso indebido de datos será usada exclusivamente con equipos y cuentas para los que el Usuario final tenga acceso legítimo. Cualquier uso ilegal será informado a la autoridad competente. El Proveedor cumplirá con las leyes relevantes y asistirá a las autoridades encargadas del cumplimiento de la ley en caso de uso indebido. Usted acepta y reconoce que es responsable de proteger la contraseña de acceso a la Cuenta ESET HOME y acuerda no divulgar la contraseña a un tercero. El Usuario Final es responsable por cualquier actividad realizada la función de protección contra el uso indebido de datos de la Cuenta ESET HOME, ya sea autorizada o no. Si su cuenta de ESET HOME se ve comprometida, notifíquelo inmediatamente al Proveedor. Las disposiciones adicionales para la protección contra el uso indebido de datos solo podrán aplicarse a los usuarios finales de ESET Internet Security y ESET Smart Security Premium.

ESET Secure Data. Se aplican disposiciones adicionales a ESET Secure Data como se muestra a continuación:

1. Definiciones. En estas disposiciones adicionales de ESET Secure Data, los términos a continuación significan lo siguiente:

- a) "Información" Todo tipo de datos que se cifran o descifran mediante el uso del software.
- b) "Productos" el software y la documentación de ESET Secure Data;
- c) "ESET Secure Data", el software que se usa para el cifrado y descifrado de datos electrónicos;

Toda referencia al plural deberá incluir el singular, así como toda referencia al género masculino deberá incluir el femenino y el neutro, y viceversa. Las palabras que no tengan una definición específica deberán utilizarse en conformidad con las definiciones estipuladas por este Acuerdo.

2. Declaración de Usuario final adicional. Usted reconoce y acepta que:

- a) Es su responsabilidad proteger, mantener y realizar copias de seguridad de la Información;
- b) Debe realizar copias de seguridad completas de toda la información y los datos (incluidos, por ejemplo, información y datos críticos) en su equipo antes de instalar del ESET Secure Data;
- c) Debe conservar un registro seguro de las contraseñas y demás información que se usa para la configuración y uso del ESET Secure Data. También debe realizar copias de seguridad de todas las claves de cifrado, códigos de licencia, archivos clave y demás datos generados en un medio de almacenamiento separado;
- d) Usted es responsable del uso de los Productos. El Proveedor no será responsable por pérdidas, reclamos o

daños sufridos como consecuencia de cualquier cifrado o descifrado no autorizado o equivocado de información o datos independientemente del lugar o del modo en que se almacena dicha información o dichos datos;

e) A pesar de que el Proveedor siguió todos los pasos posibles para garantizar la integridad y seguridad de ESET Secure Data, los Productos (o cualquiera de ellos) no se deben usar en áreas que sean dependientes de un nivel de seguridad a prueba de fallos o que sean potencialmente peligrosas o riesgosas, incluso, por ejemplo, instalaciones nucleares, navegación aérea, sistemas de control o comunicación, sistemas de armas o defensa y sistemas de soporte vital o control vital;

f) Es su responsabilidad garantizar que el nivel de seguridad y cifrado provisto por el producto sea adecuado para sus requisitos;

g) Usted es responsable del uso de los Productos o cualquiera de ellos, que incluyen, pero no se limitan a, asegurar que dicho uso cumpla con las leyes y normativas vigentes de la República Eslovaca o de otro país, región o estado donde se utiliza el producto. Antes de usar los productos, debe asegurarse de que no constituye una contravención de un embargo gubernamental (en la República Eslovaca o en otro país);

h) ESET Secure Data puede contactar al Proveedor en distintas oportunidades para verificar la información de la licencia, parches disponibles, paquetes de servicio y otras actualizaciones que pueden mejorar, modificar o realizar la operación de ESET Secure Data. El software puede enviar información general del sistema relacionada con la funcionalidad del software en conformidad con la Política de Privacidad.

i) El Proveedor no será responsable por pérdidas, daños, gastos o reclamos generados por pérdidas, robos, mal uso, corrupción, daños o destrucciones de contraseñas, información de configuración, claves de cifrado, códigos de activación de licencias o demás datos generados o almacenados durante el uso del software.

Las disposiciones adicionales de ESET Secure Data solo se podrán aplicar a los usuarios finales de ESET Smart Security Premium.

Password Manager Software. Se aplican disposiciones adicionales al software Password Manager como se muestra a continuación:

1. Declaración de Usuario final adicional. Usted reconoce y acepta que no:

a) Utilizará el software de Password Manager para operar cualquier aplicación de misión crítica donde pudiera estar en peligro la vida humana o las propiedades. Usted comprende que el software de Password Manager no está diseñado para dichos propósitos y que su falla en dichos casos podría llevar a la muerte, lesiones personales o daños graves a la propiedad o el medio ambiente por los cuales el Proveedor no será responsable.

EL SOFTWARE DE PASSWORD MANAGER NO ESTÁ DISEÑADO, LICENCIADO NI ES APTO PARA SU USO EN ENTORNOS PELIGROSOS QUE REQUIEREN CONTROLES A PRUEBA DE FALLAS, INCLUIDOS, POR EJEMPLO, EL DISEÑO, LA CONSTRUCCIÓN, EL MANTENIMIENTO O LA OPERACIÓN DE INSTALACIONES NUCLEARES, SISTEMAS DE NAVEGACIÓN O COMUNICACIÓN AÉREOS, CONTROL DE TRÁFICO AÉREO Y SISTEMAS DE SOPORTE VITAL O DE ARMAS. EL PROVEEDOR ESPECÍFICAMENTE NIEGA TODA GARANTÍA EXPRESA O IMPLÍCITA DE IDONEIDAD PARA DICHOS PROPÓSITOS.

b) Utilizará el software de Password Manager de manera que viole este acuerdo o las leyes de la República Eslovaca o su jurisdicción. En concreto, no puede usar el software Password Manager para crear ni promover contenido ilegal, lo que incluye la carga de datos de contenido dañino o que pueda usarse para actividades ilegales o que infrinjan de algún modo la ley o los derechos de terceros (incluidos todos los derechos de propiedad intelectual), lo que incluye, entre otras cosas, cualquier intento de acceder a las cuentas del Almacenamiento (a los efectos de estos términos adicionales del software Password Manager, por "Almacenamiento" se hace referencia al espacio de almacenamiento de datos administrado por el Proveedor o un

tercero que no sea el Proveedor y el Usuario a efectos de activar la sincronización y copia de seguridad de los datos del usuario) o cualquier cuenta y datos de otros usuarios del software Password Manager o del Almacenamiento. Si usted viola cualquiera de estas disposiciones, el Proveedor tiene derecho a finalizar inmediatamente este acuerdo y trasladarle los costos de cualquier acción, como así también a tomar las medidas necesarias para evitar que Usted continúe usando el software de Password Manager sin la posibilidad de reembolso.

2. LIMITACIÓN DE RESPONSABILIDAD. EL SOFTWARE DE PASSWORD MANAGER ES PROVISTO "COMO ESTÁ". NO SE EXPRESA NI IMPLICA NINGÚN TIPO DE GARANTÍA. USTED USA EL SOFTWARE BAJO SU PROPIO RIESGO. EL PRODUCTOR NO ES RESPONSABLE POR PÉRDIDAS DE DATOS, DAÑOS, LIMITACIÓN DE DISPONIBILIDAD DE SERVICIO, INCLUIDOS DATOS ENVIADOS POR EL SOFTWARE DE PASSWORD MANAGER A UN ALMACENAMIENTO EXTERNO POR PROPÓSITOS DE SINCRONIZACIÓN Y COPIA DE SEGURIDAD DE DATOS. EL CIFRADO DE DATOS CON EL USO DEL SOFTWARE DE PASSWORD MANAGER NO IMPLICA NINGUNA RESPONSABILIDAD DEL PROVEEDOR RESPECTO A LA SEGURIDAD DE DICHOS DATOS. USTED ACUERDA EXPRESAMENTE QUE LOS DATOS ADQUIRIDOS, USADOS, CIFRADOS, ALMACENADOS, SINCRONIZADOS O ENVIADOS MEDIANTE EL SOFTWARE DE PASSWORD MANAGER TAMBIÉN PUEDEN ALMACENARSE EN SERVIDORES DE TERCEROS (SE APLICA SOLO AL USO DEL SOFTWARE DE PASSWORD MANAGER DONDE LOS SERVICIOS DE SINCRONIZACIÓN Y COPIA DE SEGURIDAD FUERON HABILITADOS). SI EL PROVEEDOR, A SU PROPIA DISCRECIÓN, SELECCIONA USAR DICHO ALMACENAMIENTO, SITIOS WEB, PORTAL WEB, SERVIDOR O SERVICIO DE TERCEROS, EL PROVEEDOR NO ES RESPONSABLE POR LA CALIDAD, SEGURIDAD O DISPONIBILIDAD DE DICHO SERVICIO DE TERCEROS Y EN NINGÚN CASO SERÁ EL PROVEEDOR RESPONSABLE ANTE USTED POR CUALQUIER INCUMPLIMIENTO DE LAS OBLIGACIONES CONTRACTUALES O LEGALES POR PARTE DEL TERCERO NI POR DAÑOS, PÉRDIDA DE GANANCIAS, DAÑOS ECONÓMICOS O NO ECONÓMICOS O CUALQUIER OTRO TIPO DE PÉRDIDA DURANTE EL USO DE ESTE SOFTWARE. EL PROVEEDOR NO ES RESPONSABLE DEL CONTENIDO DE LOS DATOS ADQUIRIDOS, USADOS, CIFRADOS, ALMACENADOS, SINCRONIZADOS O ENVIADOS MEDIANTE EL SOFTWARE DE PASSWORD MANAGER O EN EL ALMACENAMIENTO. USTED RECONOCE QUE EL PROVEEDOR NO TIENE ACCESO AL CONTENIDO DE LOS DATOS ALMACENADOS Y NO PUEDE CONTROLARLOS O ELIMINAR EL CONTENIDO LEGALMENTE DAÑINO.

El proveedor posee todos los derechos de mejoras, actualizaciones y arreglos relacionados con el software de Password MANAGER ("Mejoras"), incluso en el caso de que dichas mejoras hayan sido creadas a partir de comentarios, ideas o sugerencias enviados por usted en cualquier formato. Usted no tendrá derecho a compensación, incluidas regalías relacionadas con dichas Mejoras.

LAS ENTIDADES O LICENCIADORES DEL PROVEEDOR NO SERÁN RESPONSABLES ANTE USTED POR RECLAMOS Y RESPONSABILIDADES DE CUALQUIER TIPO QUE SURJAN O ESTÉN DE ALGUNA MANERA RELACIONADAS AL USO DEL SOFTWARE DE PASSWORD MANAGER POR PARTE SUYA O DE TERCEROS, AL USO O NO USO DE FIRMAS O PROVEEDORES DE CORRETAJE O A LA VENTA O COMPRA DE CUALQUIER SEGURIDAD, INDEPENDIENTEMENTE DE QUE DICHOS RECLAMOS Y RESPONSABILIDADES SE BASEN EN UNA TEORÍA LEGAL O EQUITATIVA.

LAS ENTIDADES O LICENCIADORES DEL PROVEEDOR NO SON RESPONSABLES ANTE USTED POR CUALQUIER DAÑO DIRECTO, ACCIDENTAL, ESPECIAL, INDIRECTO O CONSECUENTE DERIVADO O RELACIONADO A CUALQUIER SOFTWARE DE TERCEROS, CUALQUIER DATO AL QUE SE ACCEDE A TRAVÉS DEL SOFTWARE DE PASSWORD MANAGER, SU USO O IMPOSIBILIDAD DE USO O ACCESO AL SOFTWARE DE PASSWORD MANAGER O A CUALQUIER DATO PROVISTO A TRAVÉS DEL SOFTWARE DE PASSWORD MANAGER, INDEPENDIENTEMENTE DE QUE DICHOS RECLAMOS POR DAÑOS SE GENEREN BAJO UNA TEORÍA DE LEY O EQUITAD. LOS DAÑOS EXCLUIDOS POR ESTA CLÁUSULA INCLUYEN, POR EJEMPLO, AQUELLOS DE PÉRDIDAS DE GANANCIAS COMERCIALES, LESIÓN A PERSONAS O DAÑOS MATERIALES, INTERRUPCIÓN DE NEGOCIOS, PÉRDIDA DE INFORMACIÓN COMERCIAL O PERSONAL. ALGUNAS JURISDICCIONES NO PERMITEN LA LIMITACIÓN DE DAÑOS ACCIDENTALES O CONSECUENTES, POR LO QUE ESTA RESTRICCIÓN PODRÍA NO APLICARSE A USTED. EN DICHO CASO, EL GRADO DE RESPONSABILIDAD DEL PROVEEDOR SERÁ EL MÍNIMO PERMITIDO POR LA LEY EN VIGOR.

LA INFORMACIÓN PROVISTA A TRAVÉS DEL SOFTWARE DE PASSWORD MANAGER, INCLUIDAS COTIZACIONES DE

ACCIONES, ANÁLISIS, INFORMACIÓN DE MERCADO, NOTICIAS Y DATOS ECONÓMICOS PUEDE ESTAR RETRASADA, SER IMPRECISA O CONTENER ERRORES U OMISIONES, Y LAS ENTIDADES Y LICENCIADORES DEL PROVEEDOR NO SERÁN RESPONSABLES RESPECTO A LA MISMA. EL PROVEEDOR PUEDE CAMBIAR O DISCONTINUAR CUALQUIER ASPECTO O FUNCIÓN DEL SOFTWARE DE PASSWORD MANAGER O EL USO DE TODAS O ALGUNAS DE LAS FUNCIONES O LA TECNOLOGÍA DEL SOFTWARE DE PASSWORD MANAGER EN CUALQUIER MOMENTO SIN PREVIO AVISO.

SI LAS DISPOSICIONES DE ESTE ARTÍCULO SON NULAS POR CUALQUIER MOTIVO O SI EL PROVEEDOR ES CONSIDERADO RESPONSABLE POR PÉRDIDAS, DAÑOS, ETC. EN EL MARCO DE LAS LEYES VIGENTES, LAS PARTES ACUERDAN QUE LA RESPONSABILIDAD DEL PROVEEDOR ANTE USTED SE LIMITARÁ AL MONTO TOTAL DE DERECHOS DE LICENCIA QUE HA PAGADO.

USTED ACUERDA INDEMNIZAR, DEFENDER Y EXONERAR AL PROVEEDOR Y A SUS EMPLEADOS, SUBSIDIARIAS, AFILIADOS, REPOSICIONAMIENTO DE MARCA Y DEMÁS SOCIOS CONTRA TODO RECLAMO, RESPONSABILIDAD, DAÑO, PÉRDIDA, COSTO, GASTO Y TARIFA DE TERCEROS (INCLUIDOS LOS PROPIETARIOS DEL DISPOSITIVO O LAS PARTES CUYOS DERECHOS FUERON AFECTADOS POR LOS DATOS USADOS EN EL SOFTWARE DE PASSWORD MANAGER O EN EL ALMACENAMIENTO) QUE DICHAS PARTES PUDIERAN INCURRIR COMO RESULTADO DE SU USO DEL SOFTWARE DE PASSWORD MANAGER.

3. Datos en el software de Password Manager. A menos que usted lo seleccione de manera explícita, todos los datos ingresados por usted que sean guardados en una base de datos del software de Password Manager se almacenan en un formato cifrado en su equipo u otro dispositivo de almacenamiento que haya definido. Usted comprende que en el caso de eliminación de cualquier base de datos u otros archivos del software de Password Manager o la eliminación de estos, todos los datos contenidos en los mismos se perderán irreversiblemente y usted comprende y acepta el riesgo de dicha pérdida. El hecho de que sus datos personales estén almacenados en un formato cifrado en el equipo no significa que la información no pueda ser robada o usada de forma errónea por alguien que descubra la Contraseña maestra u obtenga acceso al dispositivo de activación definido por el usuario para abrir la base de datos. Usted es responsable de mantener la seguridad de todos los métodos de acceso.

4. Transmisión de datos personales al proveedor o al almacenamiento. Si elige hacerlo, y con el único propósito de garantizar una sincronización y copia de seguridad oportunas, el software de Password Manager transmite o envía datos personales desde la base de datos del software de Password Manager (principalmente contraseñas, información de inicio de sesión, Cuentas e Identidades) a través de Internet hacia el Almacenamiento. Los datos se transfieren exclusivamente en forma cifrada. El uso del software de Password Manager para completar formularios en línea con contraseñas, inicios de sesión u otros datos puede requerir el envío de información a través de Internet al sitio web que identifica. Esta transmisión de datos no se inicia en el software de Password Manager y, por lo tanto, el Proveedor no puede ser responsable por la seguridad de dichas interacciones con cualquier sitio web admitido por los diversos proveedores. Cualquier transacción a través de Internet, ya sea en conjunto o no con el software de Password Manager, se realiza bajo su propia discreción y riesgo y usted será el único responsable por los daños en su sistema informático o pérdidas de datos resultantes de la descarga y/o uso de cualquier material o servicio mencionado. Para minimizar el riesgo de pérdidas de datos valiosos, el Proveedor recomienda que los clientes realicen una copia de seguridad periódica de la base de datos y de los demás archivos importantes en unidades externas. El Proveedor no puede proveerle asistencia en la recuperación de datos perdidos o dañados. Si el Proveedor le proporciona servicios de copia de seguridad de los archivos de la base de datos del usuario en caso de daños o eliminaciones de los archivos en las PC del usuario, dicho servicio de copia de seguridad se provee sin garantías y no implica que el Proveedor tenga responsabilidad alguna ante usted.

Al utilizar el software de Password Manager, Usted acepta que el software puede contactar a los servidores del Proveedor en distintas oportunidades para verificar la información de la licencia, parches disponibles, paquetes de servicio y otras actualizaciones que pueden mejorar, mantener, modificar o realzar la operación del software de Password Manager. El software puede enviar información general del sistema relacionada con la funcionalidad

del software de Password Manager en conformidad con la Política de Privacidad.

5. Información e instrucciones de desinstalación. Toda la información que desee retener de la base de datos se debe exportar antes de desinstalar el software de Password Manager.

Las disposiciones adicionales del software Password Manager solo se podrán aplicar a los usuarios finales de ESET Smart Security Premium.

ESET LiveGuard. Se aplican disposiciones adicionales a ESET LiveGuard como se muestra a continuación:

El Software incluye una función de análisis adicional de los archivos enviados por el Usuario final. El Proveedor solo podrá usar los archivos enviados por el Usuario final y los resultados del análisis de acuerdo con la Política de Privacidad y la normativa legal relevante.

Las disposiciones adicionales de ESET LiveGuard solo se podrán aplicar a los usuarios finales de ESET Smart Security Premium.

EULAID: EULA-PRODUCT-LG-EHSW; 3537.0

Política de privacidad

La protección de los datos personales reviste especial importancia para ESET, spol. s r. o., con domicilio social en Einsteinova 24, 851 01 Bratislava, Slovak Republic, inscrita en el Registro comercial del Tribunal de Distrito de Bratislava I, Sección Sro, Registro N.º 3586/B, Número de registro de empresa: 31333532 como controlador de datos ("ESET" o "Nosotros"). Queremos cumplir con el requisito de transparencia de acuerdo con el Reglamento General de Protección de Datos de la Unión Europea ("RGPD"). A fin de cumplir con el objetivo, publicamos la presente Política de privacidad con el único propósito de informar a nuestros clientes ("Usuario final" o "Usted"), en carácter de interesados, acerca de los siguientes temas relativos a la protección de los datos personales:

- Fundamento jurídico para el procesamiento de datos personales.
- Intercambio y confidencialidad de los datos.
- Seguridad de los datos.
- Sus derechos como interesado.
- Procesamiento de sus datos personales.
- Información de contacto.

Fundamento jurídico para el procesamiento de datos personales

Existen solo unas pocas bases legales para el procesamiento de datos que usamos de acuerdo con el marco legislativo aplicable en relación con la protección de datos personales. En ESET, el procesamiento de datos personales es necesario principalmente a fin de cumplir con el [Acuerdo de Licencia de Usuario Final](#) ("EULA") con el Usuario final [Art. 6 (1) (b) del Reglamento General de Protección de Datos (RGPD)], que rige la prestación de productos o servicios de ESET, a menos que se indique algo distinto explícitamente, p. ej.:

- El fundamento jurídico del interés legítimo, conforme al Art. 6 (1) (f) del RGPD, que nos permite procesar los datos sobre cómo nuestros clientes usan nuestros Servicios y su satisfacción a fin de ofrecerles a nuestros usuarios el máximo nivel posible en protección, soporte y experiencia. Incluso la legislación aplicable reconoce

el marketing como un interés legítimo. Por lo tanto, solemos confiar en este concepto cuando se trata de la comunicación de marketing con nuestros clientes.

- El consentimiento, conforme al Art. 6 (1) (a) del RGPD, que podemos solicitarle a Usted en situaciones específicas en las que consideramos que este fundamento jurídico es el más adecuado o si lo exige la ley.
- El cumplimiento de una obligación legal, conforme al Art. 6 (1) (c) del RGPD, por ejemplo, una que estipula los requisitos para la comunicación electrónica o la retención de documentos de facturación o cobranza.

Intercambio y confidencialidad de los datos

No compartimos sus datos con terceros. Sin embargo, ESET es una compañía que opera globalmente a través de entidades afiliadas o socios como parte de nuestra red de venta, servicio y soporte. La información sobre licencias, facturación y soporte técnico que procesa ESET puede ser transferida desde las entidades afiliadas o los socios o hacia ellos a fin de ejecutar el EULA, por ejemplo, para la prestación de servicios o soporte.

ESET prefiere procesar sus datos en la Unión Europea (UE). Sin embargo, según su ubicación (el uso de nuestros productos o servicios fuera de la UE) o el servicio que elija, puede que sea necesario transmitir sus datos a un país ubicado fuera de la UE. Por ejemplo, usamos servicios de terceros en conexión con la informática en la nube. En estos casos, seleccionamos cuidadosamente a nuestros proveedores de servicios y garantizamos un nivel adecuado de protección de los datos mediante medidas contractuales, técnicas y organizativas. Por regla general, pactamos las cláusulas contractuales estándar de la UE, si es necesario, con normas contractuales complementarias.

En el caso de algunos países fuera de la UE, como Reino Unido y Suiza, la UE ya ha determinado un nivel de protección de datos equivalente. Debido a este nivel de protección de datos equivalente, la transferencia de datos hacia estos países no requiere ninguna autorización ni acuerdo especial.

Seguridad de los datos

ESET implementa medidas técnicas y de organización para asegurar un nivel de seguridad apropiado ante riesgos potenciales. Hacemos todo lo posible para garantizar una continua confidencialidad, integridad, disponibilidad y resistencia de los sistemas operativos y servicios. Sin embargo, si ocurre una filtración de datos que genera un riesgo para sus derechos y libertades, estamos preparados para notificar a la autoridad supervisora pertinente, como también a los Usuarios finales afectados que actúen en carácter de interesados.

Derechos de la persona registrada

Los derechos de los Usuarios finales son importantes. Queremos informarle que cada Usuario final (de cualquier país, dentro y fuera de la Unión Europea) tiene los siguientes derechos, que ESET garantiza. Para ejercer los derechos de los interesados, puede comunicarse con nosotros a través del formulario de soporte o por correo electrónico a la siguiente dirección: dpo@eset.sk. A fin de poder identificarlo, le solicitamos la siguiente información: Nombre, dirección de correo electrónico y, de estar disponible, clave de licencia o número de cliente y empresa de afiliación. No debe enviarnos ningún otro dato personal, como la fecha de nacimiento. Queremos señalar que, para poder procesar su solicitud, así como con fines de identificación, procesaremos sus datos personales.

Derecho a retirar el consentimiento. El derecho a retirar el consentimiento resulta aplicable únicamente cuando nuestro procesamiento requiera su consentimiento. Si procesamos sus datos personales en razón de su consentimiento, tiene derecho a retirarlo en cualquier momento sin expresión de causa. Solo podrá retirar su consentimiento con efectos para el futuro, lo que no afectará la legitimidad de los datos procesados con

anterioridad.

Derecho a oponerse. El derecho a oponerse al procesamiento resulta aplicable únicamente cuando nuestro procesamiento esté basado en el interés legítimo de ESET o un tercero. Si procesamos sus datos personales en pos de un interés legítimo, Usted, como interesado, tiene derecho a oponerse, en cualquier momento, al interés legítimo que designemos y al procesamiento de sus datos personales. Solo podrá oponerse al procesamiento con efectos para el futuro, lo que no afectará la legitimidad de los datos procesados con anterioridad. Si procesamos sus datos personales con fines de marketing directo, no es necesario que exprese una causa. Esto también se aplica a la elaboración de perfiles, ya que se relaciona con el marketing directo. En todos los demás casos, le solicitamos que nos informe, de forma breve, sus quejas en contra del interés legítimo de ESET para el procesamiento de sus datos personales.

Tenga en cuenta que, en algunos casos, a pesar de que haya retirado su consentimiento, tenemos derecho a continuar procesando sus datos personales en función de algún otro fundamento jurídico, por ejemplo, para el cumplimiento de un contrato.

Derecho de acceso. En carácter de interesado, Usted tiene derecho a obtener información de los datos que almacene ESET sobre usted de forma gratuita, en cualquier momento.

Derecho a solicitar una rectificación. En caso de que procesemos de forma involuntaria datos personales incorrectos sobre Usted, tiene derecho a que se corrija esta información.

Derecho a solicitar el borrado de los datos y la restricción en el procesamiento. En carácter de interesado, Usted tiene derecho a solicitar el borrado de sus datos personales o una restricción en su procesamiento. Si procesamos sus datos personales, por ejemplo, con su consentimiento, Usted lo retira y no hay ningún otro fundamento jurídico (como un contrato), eliminaremos sus datos personales de inmediato. También eliminaremos sus datos personales en cuanto ya no sean necesarios para los fines indicados cuando finalice nuestro período de retención.

Si usamos sus datos personales únicamente con el fin de marketing directo y Usted ha retirado su consentimiento o se ha opuesto al interés legítimo subyacente de ESET, restringiremos el procesamiento de sus datos personales, lo que implicará que sus datos de contacto se incluyan en nuestra lista negra interna para evitar el contacto no solicitado. De lo contrario, sus datos personales serán eliminados.

Tenga en cuenta que podemos tener la obligación de almacenar sus datos hasta que finalicen los períodos y las obligaciones de retención determinados por el legislador o las autoridades supervisoras. La legislación eslovaca también podría determinar períodos y obligaciones de retención. A partir de su finalización, los datos correspondientes se eliminarán de forma rutinaria.

Derecho a la portabilidad de datos. Nos complace proporcionarle a Usted, en carácter de interesado, los datos personales que procese ESET en formato xls.

Derecho a presentar una queja. Como interesado, Usted tiene el derecho de presentar una queja a una autoridad supervisora en cualquier momento. ESET se encuentra sujeto a la regulación de las leyes eslovacas y Nosotros cumplimos con la ley de protección de datos como parte de la Unión Europea. La autoridad supervisora competente en materia de datos es la Oficina de Protección de Datos Personales de la República de Eslovaquia, con sede en Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Procesamiento de sus datos personales

Los servicios prestados por ESET implementados en nuestro producto se prestan de acuerdo con los términos del [EULA](#), pero algunos pueden requerir atención especial. Quisiéramos brindarle más detalles sobre la recolección de datos relacionada a la provisión de nuestros servicios. Prestamos diversos servicios descritos en el EULA y la

[documentación](#). Para hacer que todo funcione, necesitamos recolectar la siguiente información:

Datos de facturación y licencia. ESET recopila y procesa el nombre, la dirección de correo electrónico, la clave de licencia y, si corresponde, la dirección, la empresa de afiliación y los datos de pago para facilitar la activación de la licencia, la entrega de la clave de licencia, los recordatorios sobre caducidad, las solicitudes de soporte, la verificación de la autenticidad de la licencia, la prestación de nuestro servicio y otras notificaciones, como mensajes de marketing acordes a la legislación aplicable o Su consentimiento. ESET tiene la obligación legal de conservar la información de facturación durante un plazo de 10 años, pero la información sobre licencias se anonimiza a más tardar 12 meses después de la caducidad de la licencia.

Actualización y otras estadísticas. La información procesada comprende información relacionada con el proceso de instalación y su equipo, lo que incluye la plataforma en la que está instalado nuestro producto e información sobre las operaciones y la funcionalidad de nuestros productos, como el sistema operativo, información sobre el hardware, identificadores de instalación, identificadores de licencias, dirección IP, dirección MAC o ajustes de configuración del producto. Esta información se procesa con el fin de prestar servicios de actualización y a efectos del mantenimiento, la seguridad y la mejora de nuestra infraestructura de backend.

Esta información se encuentra separada de la información de identificación necesaria para las licencias y la facturación, ya que no requiere la identificación del Usuario final. El período de retención es de hasta cuatro años.

Sistema de reputación de **ESET LiveGrid®**. Las funciones hash unidireccionales relativas a infiltraciones se procesan a efectos del sistema de reputación de ESET LiveGrid®, que mejora la eficiencia de nuestras soluciones de protección contra malware comparando archivos analizados con una base de datos de elementos en listas blancas y negras en la nube. Durante este proceso, no se identifica al Usuario final.

Sistema de comentarios de **ESET LiveGrid®**. Muestras y metadatos sospechosos de la circulación, parte del sistema de realimentación de ESET LiveGrid®, que permite a ESET reaccionar de forma inmediata ante las necesidades de sus usuarios finales y responder a las amenazas más recientes. Nosotros dependemos de que Usted nos envíe:

- Infiltraciones como muestras potenciales de virus y otros programas malignos y sospechosos; objetos problemáticos o potencialmente no deseados o inseguros, como archivos ejecutables, mensajes de correo electrónico que haya clasificado, como correo no deseado o que nuestro producto haya marcado;
- Información relativa al uso de Internet, como dirección IP e información geográfica, paquetes IP, URL y marcos de Ethernet;
- Archivos de volcado de memoria y la información que contienen.

No necesitamos recopilar datos por fuera de este ámbito. Sin embargo, en algunas ocasiones no podemos evitarlo. Los datos recopilados accidentalmente pueden incluirse como malware y Nosotros no pretendemos que sean parte de nuestros sistemas o procesarlos para el cumplimiento de los objetivos detallados en la presente Política de privacidad.

Toda la información obtenida y procesada a través del sistema de comentarios de ESET LiveGrid® ha de utilizarse sin la identificación de Usuario final.

Evaluación de seguridad de los dispositivos conectados a la red. A fin de proporcionar la función de evaluación de seguridad, procesamos el nombre de la red local y la información acerca de los dispositivos en la red local, como presencia, tipo, nombre, dirección IP y dirección MAC en conexión con la información de licencia. La información también incluye tipo de seguridad inalámbrica y tipo de cifrado inalámbrico para los dispositivos del enrutador. La información de licencia que identifique al Usuario final se anonimiza a más tardar 12 meses después de la caducidad de la licencia.

Soporte técnico. Se puede solicitar la información de contacto, la información de licencia y los datos incluidos en sus solicitudes de soporte para brindar asistencia. Basados en el medio que Usted eligió para comunicarse con Nosotros, podemos recopilar su correo electrónico, número de teléfono, datos de licencia, detalles del producto y descripción de su caso de asistencia. Podemos solicitarle que proporcione datos adicionales para facilitar la prestación del servicio de soporte. Los datos procesados a los fines del soporte técnico se almacenan durante cuatro años.

Protección contra el uso indebido de datos. Si el Usuario final crea una Cuenta de ESET HOME en <https://home.eset.com> y activa esta función en caso de robo del equipo, se recopilará y procesará la siguiente información: datos sobre la ubicación, capturas de pantalla, datos sobre la configuración del equipo y datos grabados mediante la cámara del equipo. Los datos recopilados se almacenan en nuestros servidores o en los servidores de nuestros proveedores de servicios durante un período de retención de tres meses.

Password Manager. Si elige activar la función de Password Manager, la información relativa a sus datos de acceso se almacena de forma cifrada solo en su equipo o en otro dispositivo designado. Si activa el servicio de sincronización, los datos cifrados se almacenan en nuestros servidores o en los servidores de nuestros proveedores de servicios. Ni ESET ni el proveedor de servicios tienen acceso a los datos cifrados. Solo usted tiene la clave para descifrar los datos. Los datos se eliminarán una vez que desactive la función.

ESET LiveGuard. Si elige activar la función de ESET LiveGuard, se requiere el envío de muestras, como archivos predefinidos y seleccionados por el Usuario final. Las muestras que elija para el análisis remoto se cargarán en el servicio de ESET, y el resultado del análisis se enviará a su equipo. Las muestras sospechosas se procesan como información recopilada por el sistema de comentarios de ESET LiveGrid®.

Programa de mejora de la experiencia del cliente. Si optó por activar [Programa de mejora de la experiencia del cliente](#), se recopilará y usará la información de telemetría anónima relativa al uso de nuestros productos, en función de su consentimiento.

Tenga en cuenta que, si la persona que usa nuestros productos y servicios no es el Usuario final que ha adquirido el producto o el servicio y celebrado el EULA con Nosotros (por ejemplo, un empleado del Usuario final, un familiar o una persona autorizada por el Usuario final de otra forma a usar el producto o el servicio de acuerdo con el EULA), el procesamiento de los datos se lleva a cabo en pos del interés legítimo de ESET en virtud del Artículo 6 (1) (f) del RGPD, a fin de permitir que el usuario autorizado por el Usuario final use los productos y servicios prestados por Nosotros en virtud del EULA.

Información de contacto

Si desea ejercer su derecho como persona registrada o tiene una consulta o preocupación, envíenos un mensaje a:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk