

# ESET Endpoint 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 Endpoint 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

<b>1 ESET Endpoint Antivirus</b>	<b>1</b>
<b>1.1 Novedades</b>	<b>2</b>
<b>1.2 Requisitos del sistema</b>	<b>2</b>
1.2 Idiomas compatibles	4
<b>1.3 Registro de cambios</b>	<b>5</b>
<b>1.4 Prevención</b>	<b>5</b>
<b>1.5 Estado de fin de ciclo de vida</b>	<b>6</b>
<b>1.6 Páginas de ayuda</b>	<b>9</b>
<b>2 Documentación para puntos de conexión administrados de forma remota</b>	<b>10</b>
<b>2.1 Introducción a ESET PROTECT</b>	<b>12</b>
<b>2.2 Introducción a ESET PROTECT Cloud</b>	<b>13</b>
<b>2.3 Configuración protegida por contraseña</b>	<b>13</b>
<b>2.4 ¿Qué son las políticas?</b>	<b>14</b>
2.4 Combinar políticas	15
<b>2.5 Cómo funcionan los indicadores</b>	<b>15</b>
<b>3 Instalación</b>	<b>16</b>
<b>3.1 Instalación con ESET AV Remover</b>	<b>17</b>
3.1 ESET AV Remover	17
3.1 La desinstalación con ESET AV Remover finalizó con un error	20
<b>3.2 Instalación (.exe)</b>	<b>20</b>
3.2 Cambiar la carpeta de instalación (.exe)	22
<b>3.3 Instalación (.msi)</b>	<b>22</b>
3.3 Instalación avanzada (.msi)	24
<b>3.4 Instalación de módulos mínimos</b>	<b>25</b>
<b>3.5 Instalación de línea de comando</b>	<b>25</b>
<b>3.6 Implementación a través de GPO o SCCM</b>	<b>30</b>
<b>3.7 Reemplazo a una versión más reciente</b>	<b>32</b>
3.7 Actualización automática de versión antigua del producto	33
<b>3.8 Actualizaciones de seguridad y estabilidad</b>	<b>33</b>
<b>3.9 Activación del producto</b>	<b>33</b>
3.9 Ingreso de su clave de licencia durante la activación	34
3.9 Cuenta ESET HUB	35
3.9 Procedimiento para usar credenciales de la licencia para activar un producto ESET Endpoint	35
3.9 Falló la activación	35
3.9 Registro	36
3.9 Progreso de la activación	36
3.9 La activación se completó correctamente.	36
<b>3.10 Problemas comunes de instalación</b>	<b>36</b>
<b>4 Guía para principiantes</b>	<b>36</b>
<b>4.1 Ícono de la bandeja del sistema</b>	<b>36</b>
<b>4.2 Accesos directos del teclado</b>	<b>37</b>
<b>4.3 Perfiles</b>	<b>37</b>
<b>4.4 Menú contextual</b>	<b>39</b>
<b>4.5 Configuración de la actualización</b>	<b>39</b>
<b>4.6 Configurar la protección de red</b>	<b>41</b>
<b>4.7 Hashes bloqueados</b>	<b>42</b>
<b>5 Trabajar con ESET Endpoint Antivirus</b>	<b>43</b>
<b>5.1 Estado de protección</b>	<b>44</b>
<b>5.2 Exploración del equipo</b>	<b>46</b>
5.2 Iniciador de la exploración personalizada	49

5.2 Progreso de la exploración .....	50
5.2 Registro de la exploración del equipo .....	53
<b>5.3 Actualización .....</b>	<b>54</b>
5.3 Cómo crear tareas de actualización .....	57
<b>5.4 Configuración .....</b>	<b>57</b>
5.4 Equipo .....	59
5.4 Se detecta una amenaza .....	60
5.4 Red .....	62
5.4 Solución de problemas de acceso a la red .....	63
5.4 Lista negra temporal de direcciones IP .....	64
5.4 Registros de protección de red .....	64
5.4 Solución de problemas con la protección de red de ESET .....	65
5.4 Registro y creación de reglas o excepciones desde el registro .....	65
5.4 Crear regla a partir del registro .....	65
5.4 Registro avanzado de protección de red .....	66
5.4 Resolución de problemas con el explorador de tráfico de red .....	66
5.4 Se bloqueó una amenaza de red .....	67
5.4 Web y correo electrónico .....	68
5.4 Protección antiphishing .....	69
5.4 Importación y exportación de una configuración .....	70
<b>5.5 Herramientas .....</b>	<b>71</b>
5.5 Archivos de registro .....	72
5.5 Filtrado de registros .....	75
5.5 Registros de auditorías .....	76
5.5 Procesos activos .....	77
5.5 Informe de seguridad .....	79
5.5 ESET SysInspector .....	80
5.5 Tareas programadas .....	81
5.5 Opciones de exploración programada .....	83
5.5 Resumen general de tareas programadas .....	84
5.5 Detalles de tarea .....	84
5.5 Programación de tarea .....	84
5.5 Sincronización de la tarea: una vez .....	85
5.5 Sincronización de la tarea: diariamente .....	85
5.5 Sincronización de la tarea: semanalmente .....	85
5.5 Sincronización de la tarea: desencadenada por un suceso .....	85
5.5 Omisión de una tarea .....	85
5.5 Detalles de la tarea: actualizar .....	86
5.5 Detalles de la tarea: ejecutar aplicación .....	86
5.5 Envío de muestras para su análisis .....	86
5.5 Seleccionar muestra para su análisis: archivo sospechoso .....	87
5.5 Seleccionar muestra para su análisis: sitio sospechoso .....	87
5.5 Seleccionar muestra para su análisis: archivo con falso positivo .....	88
5.5 Seleccionar muestra para su análisis: sitio de falso positivo .....	88
5.5 Seleccionar muestra para su análisis: otros .....	89
5.5 Cuarentena .....	89
<b>5.6 Ayuda y soporte .....</b>	<b>91</b>
5.6 Acerca de ESET Endpoint Antivirus .....	91
5.6 Enviar datos de configuración del sistema .....	92
5.6 Soporte técnico .....	93
<b>6 Configuración avanzada .....</b>	<b>93</b>

<b>6.1 Motor de detección</b>	94
6.1 Exclusiones	94
6.1 Exclusiones de rendimiento	95
6.1 Agregar o editar exclusión de rendimiento	96
6.1 Formato de las exclusiones de ruta	97
6.1 Exclusiones de la detección	98
6.1 Agregar o editar exclusiones de la detección	101
6.1 Asistente para crear exclusiones de la detección	102
6.1 Opciones avanzadas del motor de detección	102
6.1 Explorador del tráfico de red	102
6.1 Protección basada en la nube	103
6.1 Filtro de exclusión para la protección basada en la nube	106
6.1 Exploración de malware	107
6.1 Perfiles de exploración	107
6.1 Objetos para explorar	108
6.1 Exploración en estado inactivo	108
6.1 Detección en estado inactivo	109
6.1 Exploración en el inicio	109
6.1 Verificación de archivos de inicio automático	109
6.1 Medios extraíbles	110
6.1 Protección de documentos	111
6.1 HIPS: Sistema de prevención de intrusiones basado en el host	111
6.1 Exclusiones de HIPS	114
6.1 Configuración avanzada de HIPS	114
6.1 Controladores siempre permitidos para cargar	115
6.1 Ventana interactiva de HIPS	115
6.1 Se detectó un comportamiento ransomware potencial	116
6.1 Administración de reglas del HIPS	116
6.1 Configuración de reglas HIPS	117
6.1 Agregado de una aplicación/ruta de registro para HIPS	120
<b>6.2 Actualización</b>	120
6.2 Actualizar reversión	123
6.2 Actualizaciones del producto	125
6.2 Opciones de conexión	125
6.2 Mirror de actualización	127
6.2 Servidor HTTP y SSL para Mirror	129
6.2 Actualización desde el Mirror	129
6.2 Resolución de problemas de actualización desde el Mirror	131
<b>6.3 Protecciones</b>	132
6.3 Protección del sistema de archivos en tiempo real	136
6.3 Exclusiones de procesos	138
6.3 Agregado o edición de exclusiones de procesos	139
6.3 Cuándo modificar la configuración de la protección en tiempo real	139
6.3 Verificación de la protección en tiempo real	139
6.3 Qué hacer si la protección en tiempo real no funciona	139
6.3 Protección de acceso a la red	140
6.3 Perfiles de conexión de la red	141
6.3 Agregar o editar perfiles de conexión de red	142
6.3 Activadores	143
6.3 Conjuntos de IP	145
6.3 Editar conjuntos de IP	145

6.3 Protección contra ataques en la red (IDS)	146
6.3 Reglas IDS	147
6.3 Protección contra ataques de fuerza bruta	150
6.3 Reglas	150
6.3 Exclusiones	152
6.3 Opciones avanzadas	153
6.3 SSL/TLS	154
6.3 Reglas de la exploración de aplicaciones	156
6.3 Reglas de certificados	157
6.3 Tráfico de red cifrada	158
6.3 Protección del cliente de correo electrónico	158
6.3 Protección del transporte de correo electrónico	158
6.3 Aplicaciones excluidas	160
6.3 IP excluidas	161
6.3 Protección de la casilla de correo	162
6.3 Integraciones	163
6.3 Barra de herramientas de Microsoft Outlook	163
6.3 Cuadro de diálogo de confirmación	164
6.3 Volver a explorar los mensajes	164
6.3 Respuesta	164
6.3 ThreatSense	165
6.3 Protección del acceso a la Web	168
6.3 Aplicaciones excluidas	170
6.3 IP excluidas	170
6.3 Administración de la lista de URL	171
6.3 Lista de direcciones	172
6.3 Crear nueva lista de direcciones	173
6.3 Cómo agregar una máscara URL	174
6.3 Exploración del tráfico HTTP(S)	175
6.3 ThreatSense	175
6.3 Control de dispositivos	178
6.3 Editor de reglas del control del dispositivo	179
6.3 Dispositivos detectados	180
6.3 Agregado de reglas del control del dispositivo	180
6.3 Grupos de dispositivos	183
6.3 ThreatSense	184
6.3 Niveles de desinfección	187
6.3 Extensiones de archivos que no se analizarán	188
6.3 Parámetros adicionales de ThreatSense	189
<b>6.4 Herramientas</b>	<b>189</b>
6.4 Intervalos de tiempo	189
6.4 Actualización de Microsoft Windows	190
6.4 Ventana de diálogo: actualizaciones del sistema operativo	191
6.4 Información sobre la actualización	191
6.4 ESET CMD	191
6.4 Monitoreo y administración remotos	193
6.4 Línea de comandos de ERMM	194
6.4 Lista de los comandos ERMM JSON	196
6.4 Obtener estado de protección	196
6.4 Obtener información de la aplicación	197
6.4 Obtener información de licencia	199

6.4 Obtener registros .....	199
6.4 Obtener estado de activación .....	200
6.4 Obtener información de la exploración .....	201
6.4 Obtener configuración .....	202
6.4 Obtener estado de actualización .....	203
6.4 Comenzar exploración .....	204
6.4 Comenzar activación .....	204
6.4 Comenzar desactivación .....	205
6.4 Comenzar actualización .....	206
6.4 Establecer configuración .....	206
6.4 Verificación de intervalo de licencia .....	207
6.4 Archivos de registro .....	207
6.4 Modo de presentación .....	208
6.4 Diagnósticos .....	209
6.4 Soporte técnico .....	210
<b>6.5 Conectividad .....</b>	<b>211</b>
<b>6.6 Interfaz del usuario .....</b>	<b>212</b>
6.6 Elementos de la interfaz del usuario .....	213
6.6 Configuración del acceso .....	214
6.6 Contraseña para configuración avanzada .....	215
6.6 Contraseña .....	216
6.6 Modo seguro .....	216
<b>6.7 Notificaciones .....</b>	<b>216</b>
6.7 Estados de la aplicación .....	217
6.7 Notificaciones en el escritorio .....	218
6.7 Personalización de las notificaciones .....	220
6.7 Cuadro de diálogo: notificaciones en el escritorio .....	220
6.7 Alertas interactivas .....	221
6.7 Lista de alertas interactivas .....	222
6.7 Mensajes de confirmación .....	224
6.7 Error de conflicto de configuraciones avanzadas .....	225
6.7 Se requiere el reinicio .....	225
6.7 Se recomienda el reinicio .....	225
6.7 Reenvío .....	226
6.7 Restauración de todas las configuraciones a las predeterminadas .....	228
6.7 Restauración de todas las configuraciones en la sección actual .....	228
6.7 Error al guardar la configuración .....	228
<b>6.8 Exploración de la línea de comandos. ....</b>	<b>229</b>
<b>7 Preguntas habituales .....</b>	<b>231</b>
<b>7.1 Preguntas frecuentes sobre actualizaciones automáticas .....</b>	<b>232</b>
<b>7.2 Cómo actualizar ESET Endpoint Antivirus .....</b>	<b>235</b>
<b>7.3 Cómo quitar un virus del equipo .....</b>	<b>235</b>
<b>7.4 Cómo crear una nueva tarea en Tareas programadas .....</b>	<b>236</b>
7.4 Cómo programar una exploración semanal del equipo .....	237
<b>7.5 Cómo conectar ESET Endpoint Antivirus al ESET PROTECT .....</b>	<b>237</b>
7.5 Cómo utilizar el modo anulación .....	237
7.5 Procedimiento para aplicar una política recomendada para ESET Endpoint Antivirus .....	239
<b>7.6 Cómo configurar un servidor reflejado .....</b>	<b>241</b>
<b>7.7 Cómo actualizo a Windows 10 con ESET Endpoint Antivirus .....</b>	<b>242</b>
<b>7.8 Cómo activar el monitoreo y la administración remotos .....</b>	<b>242</b>
<b>7.9 Cómo bloquear la descarga de tipos específicos de archivos desde Internet .....</b>	<b>245</b>

7.10 Cómo minimizar la interfaz del usuario de ESET Endpoint Antivirus .....	246
8 Acuerdo de licencia de usuario final .....	247
9 Política de privacidad .....	254



# ESET Endpoint Antivirus

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

ESET Endpoint Antivirus es una solución de seguridad completa producida mediante un esfuerzo de largo plazo con el fin de combinar la protección máxima con un tamaño mínimo en el sistema. Las tecnologías avanzadas, basadas en la inteligencia artificial, son capaces de eliminar proactivamente las infiltraciones de [virus](#), spyware, troyanos, gusanos, adware, rootkits y otros ataques [provenientes de Internet](#) sin entorpecer el rendimiento del sistema ni perturbar el equipo.

ESET Endpoint Antivirus está diseñado principalmente para usar en estaciones de trabajo de un entorno de empresas.

En la sección [Instalación](#), encontrará temas de ayuda divididos en capítulos y subcapítulos para proporcionar una mejor orientación y más contexto, como [Descarga](#), [Instalación](#) y [Activación](#).

[Al usar ESET Endpoint Antivirus con ESET PROTECT](#) en un entorno corporativo, le permite administrar fácilmente cualquier cantidad de estaciones de trabajo del cliente, aplicar políticas y reglas, monitorear las detecciones y hacer configuraciones de forma remota de clientes desde cualquier equipo conectado en red.

El capítulo de [Preguntas frecuentes](#) abarca las preguntas más frecuentes y los problemas que se pueden encontrar.

---

## Características y beneficios

<b>Interfaz del usuario rediseñada</b>	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 Endpoint Antivirus y ofrece contenido de soporte actualizado en forma dinámica.
<b>Modo oscuro</b>	Una extensión que le ayuda a cambiar rápidamente la pantalla a un tema oscuro. Puede elegir su esquema de colores preferido en <a href="#">Elementos de la interfaz de usuario</a> .
<b>Antivirus y antispyware</b>	Detecta en forma proactiva y desinfecta más cantidad de amenazas conocidas y desconocidas, tales como virus, <a href="#">gusanos</a> , <a href="#">troyanos</a> y <a href="#">rootkits</a> . 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 <a href="#">Anti-Phishing</a> 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).
<b>Actualizaciones de rutina</b>	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.

<b>ESET LiveGrid® (Reputación basada en la nube)</b>	Usted podrá verificar la reputación de los procesos en ejecución y de los archivos directamente desde ESET Endpoint Antivirus.
<b>Gestión remota</b>	ESET PROTECT le permite administrar productos ESET en estaciones de trabajo, servidores y dispositivos móviles en un entorno en red desde una ubicación central. A través de la consola web de ESET PROTECT (Consola web de ESET PROTECT), puede implementar soluciones ESET, administrar tareas, aplicar políticas de seguridad, controlar el estado del sistema y responder rápidamente a problemas o amenazas en equipos remotos.
<b>Protección contra ataques de red</b>	Analiza el contenido del tráfico de la red y protege de ataques en la red. Todo tráfico considerado perjudicial será bloqueado.
<b>Control web (ESET Endpoint Security únicamente)</b>	El control web le permite bloquear las páginas web que puedan contener material potencialmente ofensivo. Además, los empleadores y los administradores de sistemas pueden prohibir el acceso a más de 27 categorías de sitios Web predefinidos y a más de 140 subcategorías.

## Novedades

### Novedades de ESET Endpoint Antivirus versión 11

#### Gestión de parches y vulnerabilidades

Función disponible en [ESET PROTECT Cloud](#) que analiza regularmente una estación de trabajo para detectar cualquier software instalado vulnerable a riesgos de seguridad. [La gestión de parches](#) comprueba si el espacio disponible coincide antes de iniciar la descarga (el valor predeterminado y mínimo es de 2 GB) y ayuda a corregir estos riesgos a través de actualizaciones de software automatizadas, para que los dispositivos se mantengan más seguros.

#### Estados de los productos al final del ciclo de vida

ESET Endpoint Antivirus en esta versión puede mostrar varios [estados de productos de fin de ciclo de vida](#). Puede configurar los estados de fin de ciclo de vida en [Notificaciones](#).

#### Varias soluciones de errores y mejoras en el rendimiento

## Requisitos del sistema

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


### 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


## Sistemas operativos

Microsoft® Windows® 11

Microsoft® Windows® 10

 Para obtener una lista detallada de las versiones de Microsoft® Windows® 10 y Microsoft® Windows® 11 compatibles, consulte la [política de compatibilidad del sistema operativo Windows](#).


 Siempre intente mantener su sistema operativo actualizado.

 La compatibilidad con Azure Code Signing debe estar instalada en todos los sistemas operativos Windows para instalar o actualizar los productos ESET lanzados después de julio de 2023. [Más información](#).

## Requisitos de características de ESET Endpoint Antivirus

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

Característica	Requisitos
Intel® Threat Detection Technology	Consulte los <a href="#">procesadores compatibles</a> .
Limpiador especializado	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.

 El instalador ESET Endpoint Antivirus creado en ESET PROTECT es compatible con Windows 10 Enterprise para escritorios virtuales y el modo de varias sesiones de Windows 10.

## Otros

- Se cumple con los requisitos del sistema operativo y otro software instalado en el equipo
- 0,3 GB de memoria libre en el sistema (consulte la Nota 1)
- 1 GB de memoria libre en el disco (consulte la Nota 2)
- Resolución de pantalla mínima de 1024 x 768
- Conexión a Internet o conexión a una red de área local a una fuente de actualizaciones del producto (consulte la Nota 3)
- 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

Aunque la instalación y ejecución del producto en sistemas que no cumplan estos requisitos podrían ser posibles, se recomienda realizar pruebas de usabilidad basadas en los requisitos de rendimiento.

- (1):** el producto podría usar memoria si esta estuviera sin uso en un equipo muy infectado o cuando se importan grandes listados de datos al producto (por ejemplo, listas blancas de URL).
- (2)** El espacio en disco es necesario para descargar el instalador, instalar el producto, guardar una copia del paquete de instalación en los datos del programa y guardar las copias de seguridad de las actualizaciones del producto para admitir la característica de reversión. El producto podría usar más espacio en disco en diferentes configuraciones (por ejemplo, cuando se almacenan más versiones de copias de seguridad de actualización del producto, volcados de memoria o grandes cantidades de registros) o en un equipo infectado (por ejemplo, debido a la característica de cuarentena). Se recomienda mantener suficiente espacio libre en el disco para admitir las actualizaciones del sistema operativo y los productos de ESET.
- (3)** Aunque no se recomienda, puede actualizar el producto manualmente desde un medio extraíble.

## Idiomas compatibles

ESET Endpoint Antivirus está disponible para instalación y descarga en los siguientes idiomas.

Idioma	Código de idioma	LCID
Inglés (Estados Unidos)	en-US	1033
Árabe (Egipto)	ar-EG	3073
Búlgaro	bg-BG	1026
Chino simplificado	zh-CN	2052
Chino tradicional	zh-TW	1028
Croata	hr-HR	1050
Checo	cs-CZ	1029
Estonio	et-EE	1061
Finlandés	fi-FI	1035
Francés (Francia)	fr-FR	1036
Francés (Canadá)	fr-CA	3084
Alemán (Alemania)	de-DE	1031
Griego	el-GR	1032
*Hebreo	he-IL	1037
Húngaro	hu-HU	1038
*Indonesio	id-ID	1057
Italiano	it-IT	1040
Japonés	ja-JP	1041
Kazajo	kk-KZ	1087
Coreano	ko-KR	1042
* Letón	lv-LV	1062
Lituano	lt-LT	1063
Nederlands	nl-NL	1043
Noruego	nb-NO	1044
Polaco	pl-PL	1045
Portuguese	pt-BR	1046
Rumano	ro-RO	1048

Idioma	Código de idioma	LCID
Ruso	ru-RU	1049
Español (Chile)	es-CL	13322
Español (España)	es-ES	3082
Sueco (Suecia)	sv-SE	1053
Eslovaco	sk-SK	1051
Esloveno	sl-SI	1060
Tailandés	th-TH	1054
Turco	tr-TR	1055
Ucraniano (Ucrania)	uk-UA	1058
*Vietnamita	vi-VN	1066

\* ESET Endpoint Antivirus está disponible en este idioma, pero la guía de usuario en línea no está disponible (lo redirige a la versión en inglés).

Para cambiar el idioma de esta guía de usuario en línea, consulte la casilla de selección de idioma (en la esquina superior derecha).

## Registro de cambios

## Prevención

Cuando usa su equipo y, en particular, cuando navega por Internet, recuerde que ningún sistema antivirus puede eliminar completamente el riesgo de las [detecciones](#) y de los [ataques remotos](#). Para ofrecer la máxima protección y conveniencia, debe usar 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 de ESET Virus Lab analizan estas amenazas a diario, y preparan y liberan actualizaciones continuamente para mejorar los niveles de protección a nuestros usuarios. Para garantizar la máxima eficacia, las actualizaciones deben estar correctamente configuradas 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 aumentar 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 Microsoft Edge, son ejemplos de los programas que publican actualizaciones de seguridad de manera periódica.

## Copia de seguridad de datos importantes

Normalmente, a los autores de malware no les importan las necesidades de los usuarios, y la actividad maliciosa del programa suele provocar un funcionamiento incorrecto del sistema operativo total y la pérdida de datos importantes. Es imprescindible realizar copias de seguridad habituales de los datos 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 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

La regla más útil y eficaz de todas es siempre ser precavido. Hoy en día, muchas infiltraciones requieren la interacción del usuario para ejecutarse y propagarse. Si es precavido al abrir nuevos archivos, ahorrará un tiempo y esfuerzo considerables, que se emplearían en limpiar 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.

## Estado de fin de ciclo de vida


ESET Endpoint Antivirus puede mostrar notificaciones o advertencias automáticas para notificarle sobre la próxima información del fin de ciclo de vida en varios lugares de la ventana principal del programa.

Más información acerca de:

- [Política sobre el fin de la vida útil \(productos para empresas\)](#)
- [Actualizaciones del producto](#)
- [Revisiones de seguridad y estabilidad](#)

Para obtener información adicional sobre los cambios en ESET Endpoint Antivirus, lea el siguiente [artículo de la base de conocimiento de ESET](#).

La siguiente tabla muestra algunos de los ejemplos de estados de productos y notificaciones con acciones basadas en categorías:

Categoría	Ventana de notificación o alerta	Página de actualización	Página de ayuda y soporte
Nueva actualización de funciones o mantenimiento disponible	 Nueva versión de disponible Hay una actualización disponible que contiene las correcciones de mantenimiento importantes requeridas por ESET Endpoint Antivirus. Actualice ahora para garantizar la protección más actualizada. <b>Acción:</b> Más información	 Hay una nueva versión de ESET Endpoint Antivirus disponible. Hay una nueva versión de ESET Endpoint Antivirus disponible. <b>Acciones:</b> Actualizar ahora/Habilitar actualizaciones automáticas	 Hay una nueva versión de ESET Endpoint Antivirus disponible Actualice ahora para obtener la última versión con nuevas funciones y mejoras. Compatible hasta: mm/dd/aaaa
	 Hay una actualización de mantenimiento disponible Hay una nueva versión de ESET Endpoint Antivirus disponible. Actualice ahora para obtener la última versión con nuevas funciones y mejoras. <b>Acción:</b> Más información	 Hay disponible una actualización de mantenimiento para ESET Endpoint Antivirus Número de versión instalada Compatible hasta: mm/dd/aaaa <b>Acción:</b> Más información	 Hay una actualización disponible que contiene las correcciones de mantenimiento importantes requeridas por ESET Endpoint Antivirus. Actualice ahora para garantizar la protección más actualizada. Compatible hasta: mm/dd/aaaa
	 Se recomienda reiniciar el dispositivo Hay una actualización disponible que contiene las correcciones de mantenimiento importantes requeridas por ESET Endpoint Antivirus. Actualice ahora para garantizar la protección más actualizada. <b>Acción:</b> Más información		Compatible hasta: mm/dd/aaaa
	 Hay una actualización de mantenimiento crítica disponible Hay una actualización disponible que contiene las correcciones de mantenimiento críticas requeridas por ESET Endpoint Antivirus. Actualice ahora para garantizar la protección más actualizada. <b>Acción:</b> Más información	 Hay disponible una actualización de mantenimiento crítica para ESET Endpoint Antivirus Número de versión instalada Compatible hasta: mm/dd/aaaa <b>Acción:</b> Más información	 Hay una actualización disponible que contiene las correcciones de mantenimiento críticas requeridas por ESET Endpoint Antivirus. Actualice ahora para garantizar la protección más actualizada. Compatible hasta: mm/dd/aaaa
	 Se necesita reiniciar el dispositivo Se ha descargado una actualización del número de versión, que contiene importantes correcciones de mantenimiento y estabilidad requeridas por su ESET Endpoint Antivirus. Actualice ahora para garantizar la protección más actualizada. <b>Acción:</b> Más información		Compatible hasta: mm/dd/aaaa

Categoría	Ventana de notificación o alerta	Página de actualización	Página de ayuda y soporte
Compatibilidad con la aplicación próxima a caducar	<p>! El soporte para la versión de la aplicación instalada finaliza el mm/dd/aaaa y su dispositivo pronto perderá la protección. Actualice ahora para mantenerse protegido.</p> <p><b>Acción:</b> Actualizar ahora</p>	<p>! Número de versión instalada/Compatible hasta: mm/dd/aaaa</p> <p><b>Acciones:</b> Actualizar ahora/Habilitar actualizaciones automáticas</p>	<p>! El soporte para la versión instalada de ESET Endpoint Antivirus finaliza pronto y su equipo perderá la protección. Actualice ahora para mantenerse protegido. Actualice ahora para mantenerse protegido. Compatible hasta: mm/dd/aaaa</p>
	<p>! El soporte extendido de ESET para la versión de la aplicación instalada finaliza el mm/dd/aaaa y su dispositivo pronto perderá la protección. Actualice ahora para mantenerse protegido.</p> <p><b>Acción:</b> Actualizar ahora</p>	<p>! Número de versión instalada/Compatible hasta: mm/dd/aaaa</p> <p><b>Acciones:</b> Actualizar ahora/Habilitar actualizaciones automáticas</p>	<p>! El soporte extendido de ESET para la versión instalada de ESET Endpoint Antivirus finaliza pronto y su dispositivo perderá la protección. Actualice ahora para mantenerse protegido. Actualice ahora para mantenerse protegido. Compatible hasta: mm/dd/aaaa</p>
	<p>! El sistema operativo instalado está desactualizado y la compatibilidad con la versión de la aplicación instalada finaliza el dd/mm/aaaa. Actualice su sistema operativo para obtener la última actualización de la aplicación y mantenerse protegido.</p> <p><b>Acciones:</b> Más información</p>	<p>! Número de versión instalada Compatible hasta: mm/dd/aaaa</p> <p><b>Acción:</b> Más información</p>	<p>! El soporte para la versión instalada de ESET Endpoint Antivirus finaliza pronto y su equipo perderá la protección. Actualice ahora para mantenerse protegido. Actualice ahora para mantenerse protegido. Compatible hasta: mm/dd/aaaa</p>
	<p>! El soporte extendido de ESET para la versión de la aplicación instalada finaliza pronto</p> <p>El sistema operativo instalado está desactualizado y la compatibilidad con la versión de la aplicación instalada finaliza el dd/mm/aaaa. Actualice su sistema operativo para obtener la última actualización de la aplicación y mantenerse protegido.</p> <p><b>Acción:</b> Más información</p>	<p>! El soporte extendido de ESET para la versión instalada de ESET Endpoint Antivirus finaliza pronto</p> <p>Número de versión instalada Compatible hasta: mm/dd/aaaa</p> <p><b>Acciones:</b> Más información</p>	<p>! El soporte extendido de ESET para la versión instalada de ESET Endpoint Antivirus finaliza pronto y su dispositivo perderá la protección. Actualice ahora para mantenerse protegido. Actualice ahora para mantenerse protegido.</p> <p>Compatible hasta: mm/dd/aaaa</p>



Categoría	Ventana de notificación o alerta	Página de actualización	Página de ayuda y soporte
La versión de la aplicación ya no es compatible	<p>⚠ La versión de la aplicación instalada ya no es compatible.</p> <p>El soporte para la versión de la aplicación instalada ha finalizado y es posible que el dispositivo no esté protegido. Actualice ahora para obtener protección.</p> <p><b>Acción:</b> Actualizar ahora</p>	<p>⚠ La versión instalada de ESET Endpoint Antivirus ya no es compatible</p> <p>Número de versión instalado/Compatible hasta: mm/dd/aaaa</p> <p><b>Acciones:</b> Actualizar ahora/Habilitar actualizaciones automáticas</p>	<p>⚠ Compatible hasta: mm/dd/aaaa</p>
	<p>⚠ La versión de la aplicación instalada ya no es compatible.</p> <p>El sistema operativo instalado está desactualizado y la compatibilidad con la versión de la aplicación instalada ha finalizado. Su equipo no está protegido. Actualice su sistema operativo para recibir la última actualización de la aplicación y obtener protección.</p> <p><b>Acción:</b> Más información</p>	<p>⚠ La versión instalada de ESET Endpoint Antivirus ya no es compatible</p> <p>Número de versión instalada Compatible hasta: mm/dd/aaaa</p> <p><b>Acción:</b> Más información</p>	<p>⚠ El soporte para la versión instalada de ESET Endpoint Antivirus ha finalizado y su equipo no está protegido. Actualice ahora para obtener protección. Actualice ahora para obtener protección. Compatible hasta: mm/dd/aaaa</p>
Actualización del sistema operativo requerida	<p>⚠ El sistema operativo instalado está desactualizado</p> <p>El sistema operativo instalado está desactualizado Actualice su sistema operativo para obtener la última actualización de la aplicación y mantenerse protegido.</p> <p><b>Acción:</b> Más información</p>	<p>✓ ESET Endpoint Antivirus</p> <p>Número de versión instalada</p>	<p>Compatible hasta: mm/dd/aaaa</p>

## Páginas de ayuda

Bienvenido a la guía de usuario de ESET Endpoint 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 empezar a usar ESET Endpoint Antivirus, tenga en cuenta que el producto se puede [gestionar de forma remota mediante ESET PROTECT](#). También recomendamos que se familiarice con los distintos [tipos de infiltraciones](#) y con los [ataques remotos](#) que puede encontrar al usar el equipo.

Consulte las [nuevas funciones](#) para obtener información acerca de las funciones que se presentan en esta versión de ESET Endpoint Antivirus. También preparamos una guía para ayudarlo a configurar y personalizar las opciones básicas de ESET Endpoint Antivirus.

## Cómo usar las páginas de ayuda de ESET Endpoint Antivirus

Los temas de ayuda se dividen en varios capítulos y subcapítulos, para proporcionar una mejor orientación y más contexto. Puede encontrar información relacionada si busca en la estructura de las páginas de ayuda.

Para obtener más información sobre cualquier ventana del programa, presione la tecla **F1**. Se mostrará la página de ayuda correspondiente a la ventana que está viendo actualmente.

Puede buscar en las páginas de ayuda por medio de palabras clave o al ingresar 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 en el contenido de todas las páginas y mostrará solo aquellas que contengan la palabra o frase buscada.

A fin de garantizar la consistencia y ayudar a evitar la confusión, la terminología que se usa en esta guía se basa en los nombres de parámetros de ESET Endpoint 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. En general, brinda información no crítica pero 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 entre paréntesis de advertencia, ya que hace referencia a configuraciones del sistema altamente sensibles o a algo arriesgado.



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
<b>En negrita</b>	Nombres de elementos de interfaces como cuadros y botones de opciones.
<i>En cursiva</i>	Referentes de 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.
<a href="#">Hervínculo</a>	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. La última versión de la Ayuda en línea se muestra de forma automática cuando tiene una conexión a Internet.

## Documentación para puntos de conexión administrados de forma remota

Los productos comerciales de ESET así como ESET Endpoint Antivirus pueden administrarse de forma remota en las estaciones de trabajo de cliente, servidores y dispositivos móviles en un entorno en red desde una ubicación central. Los administradores de sistemas que administran más de 10 estaciones de trabajo de cliente pueden considerar implementar una de las herramientas de administración remota de ESET para implementar soluciones de ESET, administrar tareas, aplicar [políticas de seguridad](#), supervisar el estado del sistema y responder rápidamente a problemas o amenazas en equipos remotos desde una ubicación central.

## Herramientas de administración remota de ESET

ESET Endpoint Antivirus puede administrarse de forma remota mediante ESET PROTECT o ESET PROTECT Cloud.

- [Introducción a ESET PROTECT](#)
- [Introducción a ESET PROTECT Cloud](#)
- [ESET HUB](#): puerta de enlace central a la plataforma de seguridad unificada de ESET PROTECT. Proporciona administración centralizada de identidades, suscripciones y usuarios para todos los módulos de la plataforma ESET. Consulte [Administración de licencias de ESET PROTECT](#) para obtener instrucciones sobre cómo activar el producto. ESET HUB reemplazará ESET Business Account y ESET MSP Administrator completamente.
- [ESET Business Account](#): es un portal de administración de licencias para productos empresariales de ESET. Consulte [ESET PROTECT Administración de licencias](#) para obtener instrucciones de activación del producto o consulte la [ESET Business Account ayuda en línea](#) para obtener más información sobre el uso de ESET Business Account. Si ya tiene un nombre usuario y contraseña emitidos por ESET que desea convertir en una clave de licencia, consulte la sección [Convertir credenciales de licencias heredadas](#).

## Productos de seguridad adicionales

- [ESET Inspect](#): un sistema integral de detección y respuesta de punto final que incluye características como: detección de incidentes, administración y respuesta ante incidentes, recolección de datos, indicadores de detección de riesgos potenciales, detección de anomalías, detección de comportamiento e incumplimientos de políticas.
- [ESET Endpoint Encryption](#): es una aplicación de seguridad integral diseñada para proteger sus datos en reposo y en tránsito. Al usar ESET Endpoint Encryption, puede cifrar archivos, carpetas y correos electrónicos o crear discos virtuales cifrados, comprimir archivos e incluir una trituradora de escritorio para la eliminación segura de archivos.

## Herramientas de administración remota de terceros

- [Monitoreo y administración remotos \(RMM\)](#)

## Prácticas recomendadas

- [Conectar todos los puntos de conexión con ESET Endpoint Antivirus a ESET PROTECT](#)
- Proteger la [Configuración avanzada](#) en equipos de cliente conectados para evitar modificaciones no autorizadas
- Aplicar [una política recomendada](#) para que se cumplan las características de seguridad disponibles
- [Minimizar la interfaz de usuario](#) : para reducir o limitar la interacción con ESET Endpoint Antivirus

## Guías de procedimientos

- [Cómo utilizar el modo anulación](#)
- [Procedimiento para implementar ESET Endpoint Antivirus con GPO o SCCM](#)

# Introducción a ESET PROTECT

ESET PROTECT le permite administrar productos ESET en estaciones de trabajo, servidores y dispositivos móviles en un entorno en red desde una ubicación central.

Con la consola web ESET PROTECT, puede implementar soluciones ESET, administrar tareas, aplicar [políticas de seguridad](#), supervisar el estado del sistema y responder rápidamente a problemas o amenazas en equipos remotos. Consulte también el resumen de elementos de arquitectura e infraestructura [ESET PROTECT](#), [Introducción a la consola web de ESET PROTECT](#) y [Entornos de aprovisionamiento de dispositivos de escritorio compatibles](#).

ESET PROTECT está compuesto por los siguientes componentes:

- [Servidor de ESET PROTECT](#): maneja la comunicación con los Agentes, y recoge y almacena los datos de la aplicación en la base de datos. Servidor de ESET PROTECT se puede instalar tanto en Windows como en Linux y también viene como un Dispositivo virtual.
- [Consola Web de ESET PROTECT](#): La consola web de es la interfaz principal que le permite administrar los equipos cliente en su entorno. Muestra una descripción general del estado de los clientes en la red y le permite implementar de forma remota soluciones de ESET en equipos no administrados. Después de instalar el Servidor ESET PROTECT (Servidor de ), puede acceder a la Consola Web mediante su navegador web. Si elige que el servidor web sea accesible desde Internet, puede usar ESET PROTECT desde cualquier lugar y dispositivo con conexión a Internet.
- [Agente ESET Management](#): facilita la comunicación entre el servidor ESET PROTECT y los equipos cliente. El Agente debe estar instalado en el equipo cliente para establecer comunicación entre ese equipo y el servidor ESET PROTECT. Dado que se ubica en el equipo cliente y puede almacenar diferentes escenarios de seguridad, el uso del Agente ESET Management disminuye significativamente el tiempo de reacción frente a nuevas detecciones. Al usar la consola web de ESET PROTECT puede [implementar el agente ESET Management](#) en equipos sin gestión reconocidos por Active Directory o ESET [Sensor de RD](#). También [puede instalar manualmente el Agente ESET Management](#) en equipos cliente, de ser necesario.
- [ESET Rogue Detection Sensor](#): detecta equipos no administrados en su red y envía su información al servidor de ESET PROTECT. Esto le permite administrar equipos cliente nuevos en ESET PROTECT sin necesidad de buscarlos y agregarlos manualmente. El Rogue Detection Sensor recuerda los equipos que han sido detectados y no enviará la misma información dos veces.
- [ESET Bridge](#): es un servicio que se puede usar junto con ESET PROTECT para:
  - Distribuir las actualizaciones a equipos clientes y paquetes de instalación para el agente ESET Management.
  - Enviar comunicación de agentes ESET Management al servidor ESET PROTECT.
- [Mobile Device Connector](#): es un componente que permite la Administración de dispositivos móviles con ESET PROTECT, que le permite gestionar dispositivos móviles (Android e iOS) y administrar ESET Endpoint Security para Android.
- [El dispositivo virtual de ESET PROTECT](#): está destinada para los usuarios que desean ejecutar ESET PROTECT en un ambiente virtualizado.
- [ESET PROTECT Virtual Agent Host](#): es un componente de ESET PROTECT que virtualiza entidades del agente para administrar máquinas virtuales sin agente. Esta solución permite la automatización, el uso de grupos dinámicos y el mismo nivel de administración de tareas que los Agente ESET Management en equipos físicos. El agente virtual recopila información de las máquinas virtuales y la envía al servidor ESET PROTECT.
- [Herramienta de replicación](#): es necesaria para las actualizaciones de los módulos fuera de línea. Si los equipos de su cliente no tienen conexión a Internet, puede usar la herramienta de replicación para descargar los archivos de actualización de los servidores de actualización de ESET y almacenarlos

localmente.

- [ESET Remote Deployment Tool](#): sirve para implementar paquetes todo en uno creados en la consola web de <%PRODUCT%>. Es una forma cómoda de distribuir el agente ESET Management con un producto ESET en equipos a través de una red.

**i** Para obtener más información, consulte [ESET PROTECT Ayuda en línea](#).

## Introducción a ESET PROTECT Cloud

ESET PROTECT Cloud le permite administrar los productos de ESET en estaciones de trabajo y servidores en un entorno de red desde una ubicación central sin el requisito de tener que contar con un servidor físico o virtual, como ESET PROTECT o . Al utilizar (Consola web de ESET PROTECT Cloud), puede implementar soluciones ESET, administrar tareas, aplicar políticas de seguridad, controlar el estado del sistema y responder rápidamente a problemas o amenazas en equipos remotos.

ESET PROTECT Cloud está compuesto por los siguientes componentes:

- [Instancia de ESET PROTECT Cloud](#): maneja la comunicación con los Agentes, y recoge y almacena los datos de la aplicación en la base de datos.
- [Consola Web de ESET PROTECT Cloud](#): La consola web de es la interfaz principal que le permite administrar los equipos cliente en su entorno. Muestra una descripción general del estado de los clientes en la red y le permite implementar de forma remota soluciones de ESET en equipos no administrados. Puede usar ESET PROTECT Cloud desde cualquier lugar o dispositivo con conexión a Internet.
- [Agente ESET Management](#): facilita la comunicación entre el ESET PROTECT Cloud y los equipos cliente. El Agente debe estar instalado en el equipo cliente para establecer comunicación entre ese equipo y el ESET PROTECT Cloud. Dado que se ubica en el equipo cliente y puede almacenar diferentes escenarios de seguridad, el uso del Agente ESET Management disminuye significativamente el tiempo de reacción frente a nuevas detecciones. Al usar la consola web de ESET PROTECT Cloud puede [implementar el agente ESET Management](#) en equipos sin gestión. También [puede instalar manualmente el Agente ESET Management](#) en equipos cliente, de ser necesario.
- [ESET Bridge](#): es un servicio que se puede usar junto con ESET PROTECT Cloud para:
  - Distribuir las actualizaciones a equipos clientes y paquetes de instalación para el agente ESET Management.
  - Enviar comunicación de agentes ESET Management al ESET PROTECT Cloud.
- [Administración de dispositivos móviles](#): es un componente que permite la Administración de dispositivos móviles con ESET PROTECT Cloud, que le permite gestionar dispositivos móviles (Android e iOS) y administrar ESET Endpoint Security para Android.
- [Gestión de parches y vulnerabilidades](#): función disponible en ESET PROTECT Cloud que explora regularmente una estación de trabajo para detectar cualquier software instalado que pueda ser vulnerable a los riesgos de seguridad. [La administración de parches](#) ayuda a corregir estos riesgos a través de actualizaciones de software automatizadas, manteniendo los dispositivos más seguros.

**i** Para obtener más información, consulte [ESET PROTECT Cloud Ayuda en línea](#).

## Configuración protegida por contraseña

Para proporcionar la máxima seguridad para su sistema, ESET Endpoint Antivirus debe estar configurado de forma correcta. Cualquier cambio o ajuste no calificado puede reducir la seguridad y el nivel de protección del cliente.

Para limitar el acceso del usuario a la configuración avanzada, un administrador puede proteger la configuración con una contraseña.

El administrador puede crear una política para proteger con contraseña la Configuración avanzada de ESET Endpoint Antivirus en los equipos de cliente conectados. Para crear una nueva política:

1. En la consola web de ESET PROTECT, haga clic en **Políticas** en el menú principal a la izquierda.
2. Haga clic en **Nueva política**.
3. Asigne un nombre a su nueva política y, si lo desea, escriba una breve descripción. Haga clic en el botón **Continuar**.
4. En la lista de productos, seleccione **ESET Endpoint para Windows**.
5. Haga clic en **Interfaz del usuario** en la lista de **Configuraciones** y expanda la **Configuración del acceso**.
6. De acuerdo con una versión de ESET Endpoint Antivirus, haga clic en la alternar para habilitar **Proteger la configuración por contraseña**. Tenga en cuenta que la versión 7 y versiones posteriores de los productos de ESET Endpoint ofrece protección mejorada. Si tiene la versión 7 y versiones posteriores y la versión 6 de los productos de Endpoint en la red, se recomienda crear dos políticas individuales con disitntas contraseñas para cada versión.
7. En la ventana de notificación, cree una nueva contraseña, confírmela y haga clic en **Aceptar**. Haga clic en **Continuar**.
8. Asigne la política a los clientes. Haga clic en **Asignar** y seleccione los equipos o grupos de equipos que desea proteger con contraseña. Haga clic en **Aceptar** para confirmar.
9. Compruebe que todos los equipos cliente deseados estén en la lista de destino y haga clic en **Continuar**.
10. Revise la configuración de la política en el resumen y haga clic en **Finalizar** para guardar su nueva política.

## ¿Qué son las políticas?

El administrador puede enviar configuraciones específicas a los productos de ESET que se ejecutan en equipos cliente utilizando políticas de la Consola Web de ESET PROTECT. Las políticas se pueden aplicar directamente a equipos individuales y a grupos de equipos. También puede asignar varias políticas a un equipo o a un grupo.

Un usuario debe tener los siguientes permisos para crear una nueva política: Permiso de **Lectura** para leer la lista de políticas, Permiso de **Uso** para asignar políticas a los equipos de destino y Permiso de **Escritura** para crear, modificar o editar políticas.

Las políticas se aplican en el orden de grupos estáticos. En el caso de los grupos dinámicos, las políticas se aplican primero a los grupos dinámicos secundarios. Esto le permite aplicar las políticas con mayor impacto a la parte superior del árbol de grupos y las más específicas a los subgrupos. Al usar [indicadores](#) un usuario de ESET Endpoint Antivirus con acceso a grupos que se encuentran en la parte superior del árbol puede anular las políticas de los grupos inferiores. Este algoritmo se explica en [Ayuda en línea del ESET PROTECT](#).

**i** Recomendamos que asigne políticas más genéricas (por ejemplo, la política del servidor de actualización) a grupos más elevados en el árbol de grupos. Las políticas más específicas (por ejemplo, la configuración del control de dispositivos) se deben asignar al grupo que se ubique en la parte inferior del árbol grupos. Las políticas inferiores suelen reemplazar las configuraciones de las superiores cuando se combinan (a menos que se defina lo contrario con [indicadores de políticas](#)).



# Combinar políticas

Una política aplicada a un cliente es generalmente el resultado de varias políticas que se fusionan en una política final. Las políticas se fusionan una por una. Al fusionar políticas, la regla general es que la última política siempre reemplaza la configuración establecida por la anterior. Para cambiar este comportamiento, puede utilizar [indicadores de políticas](#) (Disponible para cada configuración).

Al crear políticas, verá que algunas configuraciones tienen una regla adicional (reemplazar/agregar/preagregar) que puede configurar.

- **Reemplazar:** se reemplaza toda la lista, se añaden nuevos valores y se eliminan todos los anteriores.
- **Agregar:** se añaden elementos al final de la lista aplicada actualmente (debe ser otra política, la lista local siempre se sobrescribe).
- **Preagregar:** se añaden elementos al principio de la lista (la lista local se sobrescribe).

ESET Endpoint Antivirus es compatible con la fusión de la configuración local con las políticas remotas de una nueva manera. Si la configuración es una lista (por ejemplo, una lista de sitios web bloqueados) y la política remota entra en conflicto con una configuración local existente, la política remota la sobrescribe. Puede elegir cómo combinar listas locales y remotas al seleccionar las diferentes reglas de fusión para:




-  Configuración de fusión para políticas remotas.
-  Fusión de políticas remotas y locales: configuraciones locales con la resultante política remota.

Para obtener más información sobre la fusión de políticas, siga la [ESET PROTECT Guía para el usuario en línea](#) y vea el [ejemplo](#).

## Cómo funcionan los indicadores

Las políticas que se aplican a un equipo cliente suelen ser el resultado de varias políticas que se fusionan en una política final. Al fusionar políticas, puedes ajustar el comportamiento deseado de la política final, debido al orden de las políticas aplicadas, con el uso de indicadores de política. Los indicadores definen cómo la política manejará una configuración específica.

Para cada configuración, puede seleccionar uno de los siguientes indicadores:

 <b>No corresponde</b>	Cualquier configuración que tenga este indicador no está establecida por la política. Dado que la política no establece la configuración, se puede cambiar por otras políticas aplicadas posteriormente.
 <b>Aplicar</b>	La configuración con el indicador <b>Aplicar</b> se aplicará al equipo cliente. Sin embargo, al fusionar políticas, se pueden sobrescribir con otras políticas aplicadas posteriormente. Cuando se envía una política a un equipo cliente que contiene configuraciones marcadas con este indicador, dichas configuraciones cambiarán la configuración local del equipo cliente. Dado que la configuración no es forzada, todavía se puede modificar mediante otras políticas aplicadas posteriormente.
 <b>Forzar</b>	Las configuraciones con el indicador <b>Forzar</b> tienen prioridad y no se pueden sobrescribir con ninguna política aplicada posteriormente (incluso si también tiene un indicador de <b>Forzar</b> ). Esto asegura que otras políticas aplicadas posteriormente no podrán cambiar esta configuración durante la fusión. Cuando se envía una política a un equipo cliente que contiene configuraciones marcadas con este indicador, dichas configuraciones cambiarán la configuración local del equipo cliente.



**Escenario:** El *Administrador* desea permitir al usuario *John* crear o editar políticas en su grupo hogar y ver todas las políticas creadas por el *Administrador* incluyendo las Políticas que tienen indicadores de ⚡ Forzar. El *Administrador* quiere permitirle a *John* ver todas las políticas, pero que no pueda editar políticas ya existentes creadas por el *Administrador*. *John* solo puede crear o editar políticas dentro de su Grupo hogar, San Diego.

**Solución:** El *Administrador* tiene que seguir estos pasos:

#### Crear grupos estáticos personalizados y conjuntos de permisos

1. Crear un nuevo [Grupo estático](#) llamado *San Diego*.
2. Crear un nuevo [Conjunto de permisos](#) llamado *Todas las Políticas - John* con acceso al grupo estático *Todos* y permisos de **Lectura** para **Políticas**.
3. Crear un nuevo [Conjunto de permisos](#) llamado *Política John* con acceso al grupo estático *San Diego*, con acceso a funcionalidad y permiso de **Escritura** para **Grupo y equipos** y **Políticas**. Este conjunto de permisos permite a *John* crear o editar políticas en su Grupo hogar, *San Diego*.
4. Crear un nuevo [usuario](#) para *John* y, en la sección **Conjunto de permisos**, seleccionar *Todas las Políticas - John* y *Política John*.

#### Crear políticas

5. Crear una nueva [política](#) *Todos - Habilitar Firewall*, expandir la sección **Configuración**, seleccionar **ESET Endpoint para Windows**, ir a **Firewall personal > Básico** y aplicar todas las configuraciones mediante un indicador ⚡ **Forzar**. Expandir la sección **Asignar** y seleccionar el Grupo estático *Todos*.
6. Crear una nueva [política](#) *Grupo de John - Habilitar Firewall*, expandir la sección **Configuración**, seleccionar **ESET Endpoint para Windows**, ir a **Firewall personal > Básico** y aplicar todas las configuraciones mediante un indicador ● **Aplicar**. Expandir la sección **Asignar** y seleccionar el Grupo estático *San Diego*.

#### Resultado

Las Políticas creadas por el *Administrador* se aplicarán en primer lugar desde que se aplicaron los indicadores de ⚡ **Forzar** a la configuración de las políticas. La configuración con el indicador de Forzar aplicado tienen prioridad y no se pueden sobrescribir con otra política aplicada posteriormente. Las políticas creadas por el usuario *John* se aplicarán después de las políticas creadas por el Administrador. Para ver el orden final de las políticas, vaya a **Más > Grupos > San Diego**. Seleccione el equipo y seleccione **Mostrar detalles**. En la sección de **Configuración**, haga clic en **Políticas aplicadas**.

## Instalación

Hay varios métodos de instalación de ESET Endpoint Antivirus en una estación de trabajo de cliente, excepto que [implemente ESET Endpoint Antivirus de manera remota en estaciones de trabajo de clientes a través de ESET PROTECT o ESET PROTECT Cloud](#).



Puede actualizar desde ESET Endpoint Antivirus a ESET Endpoint Security ejecutando el instalador ESET Endpoint Security con ESET Endpoint Antivirus ya instalado. Sin embargo, debe instalar la misma versión o una versión posterior.

Métodos	Finalidad	Enlace de descarga
<a href="#">Instalación con ESET AV Remover</a>	La herramienta ESET AV Remover le ayudará a eliminar casi cualquier software antivirus que se haya instalado previamente en su sistema antes de seguir adelante con la instalación.	<a href="#">Descargar 64-bit</a> <a href="#">Descargar 32-bit</a>
*** <a href="#">Instalación (.exe)</a>	Proceso de instalación sin ESET AV Remover.	<a href="#">Descargar 64-bit</a> <a href="#">Descargar 32-bit</a>



Métodos	Finalidad	Enlace de descarga
<a href="#">Instalación (.msi)</a>	En entornos comerciales, el instalador .msi es el paquete de instalación de preferencia. Esto se debe principalmente a las implementaciones sin conexión y remotas que utilizan varias herramientas, como ESET PROTECT.	<a href="#">Descargar 64-bit</a> <a href="#">Descargar 32-bit</a>
<a href="#">Instalación de línea de comando</a>	ESET Endpoint Antivirus puede instalarse a nivel local utilizando la línea de comando o de manera remota utilizando una tarea de cliente desde ESET PROTECT.	N/A
<a href="#">Implementación a través de GPO o SCCM</a>	Use administración herramientas como GPO o SCCM para implementar ESET Management Agent y las estaciones de trabajo de cliente de ESET Endpoint Antivirus.	N/A
<a href="#">Implementación con herramientas de RMM</a>	Los complementos de ESET DEM para la herramienta Remote Management and Monitoring (RMM) le permiten implementar ESET Endpoint Antivirus en las estaciones de trabajo de cliente.	N/A

ESET Endpoint Antivirus está [disponible en más de 30 idiomas](#).

## Instalación con ESET AV Remover

Antes de que continúe con el proceso de instalación, es importante que desinstale todas las aplicaciones de seguridad del equipo. Seleccione la casilla de verificación junto a **Deseo desinstalar aplicaciones antivirus no deseadas con ESET AV Remover** para que ESET AV Remover explore el sistema y elimine todas las [aplicaciones de seguridad compatibles](#). Deje la casilla de verificación sin seleccionar y haga clic en **Continuar** para instalar ESET Endpoint Antivirus sin ejecutar ESET AV Remover.

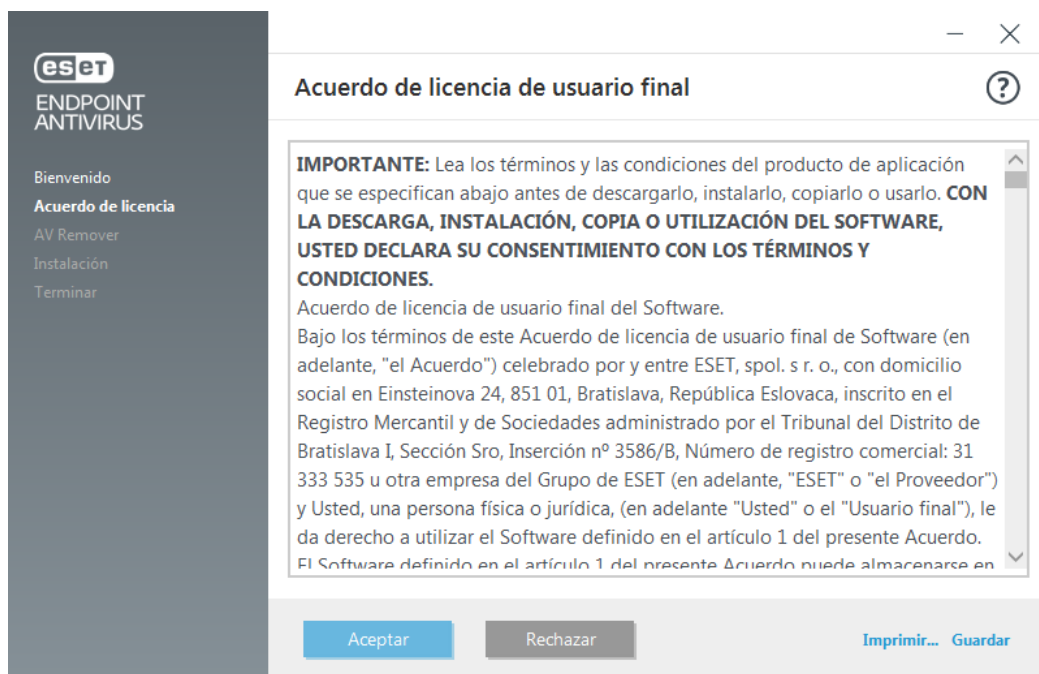


## ESET AV Remover

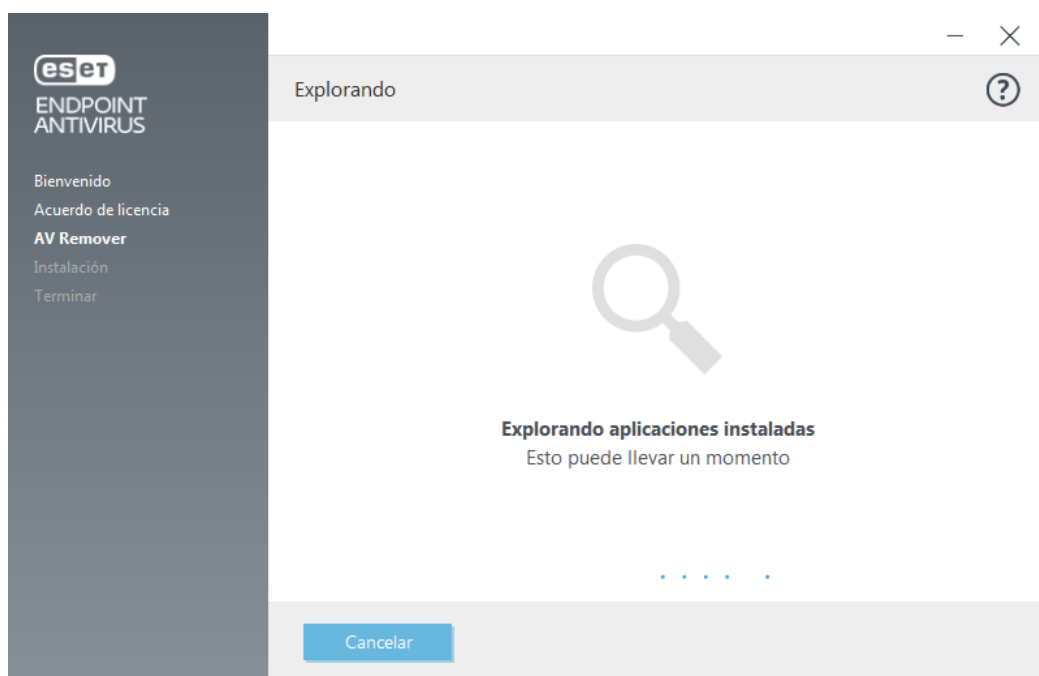
La herramienta ESET AV Remover le ayudará a quitar casi todo el software antivirus que haya instalado anteriormente en su sistema. Siga las instrucciones que se encuentran a continuación para eliminar un programa

antivirus existente mediante ESET AV Remover:

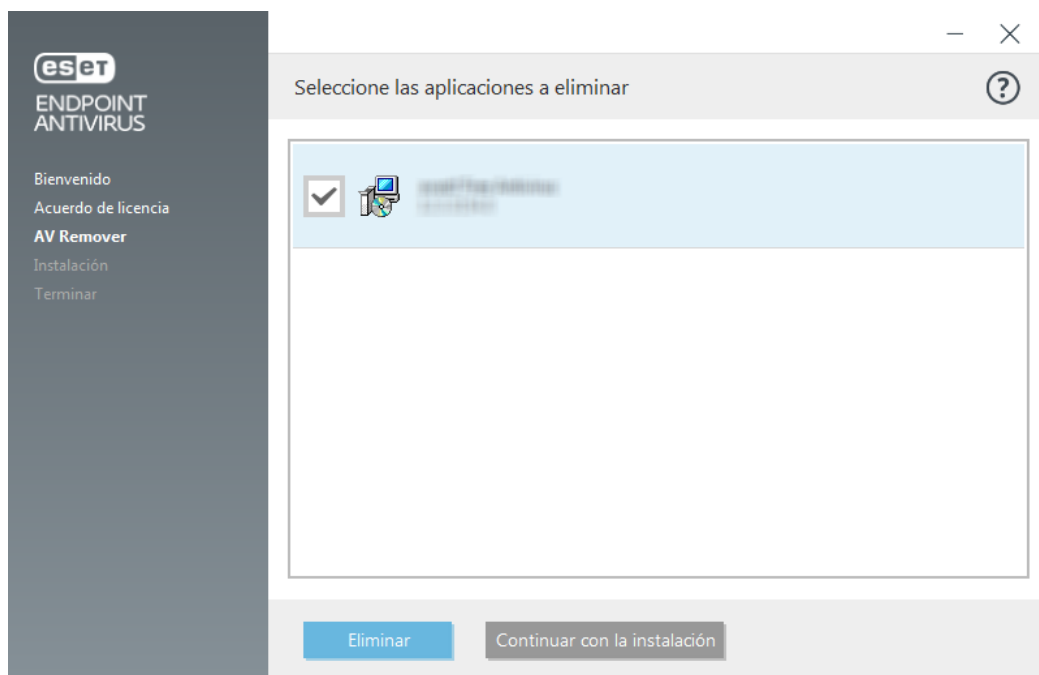
1. Para ver una lista de los software antivirus que ESET AV Remover puede eliminar, [visite el artículo de la base de conocimiento de ESET](#).
2. Lea el Acuerdo de licencia de usuario final y haga clic en **Aceptar** para dar su consentimiento. Si hace clic en **Rechazar**, procederá a la instalación de ESET Endpoint Antivirus sin eliminar la aplicación de seguridad existente en el equipo.



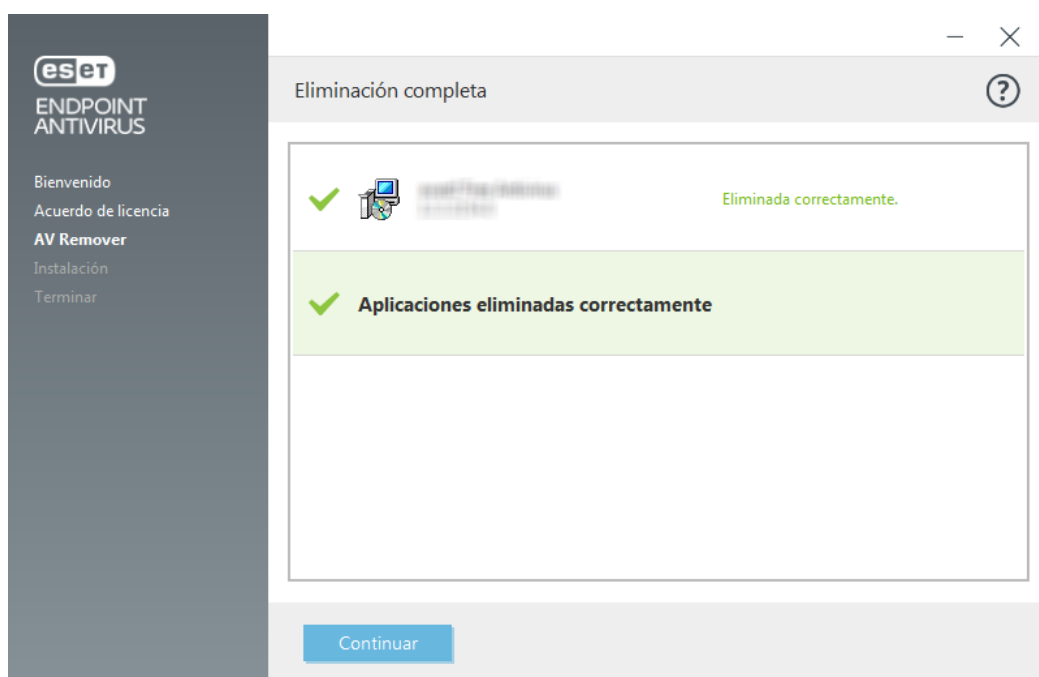
2. ESET AV Remover comenzará a buscar el software antivirus en el sistema.



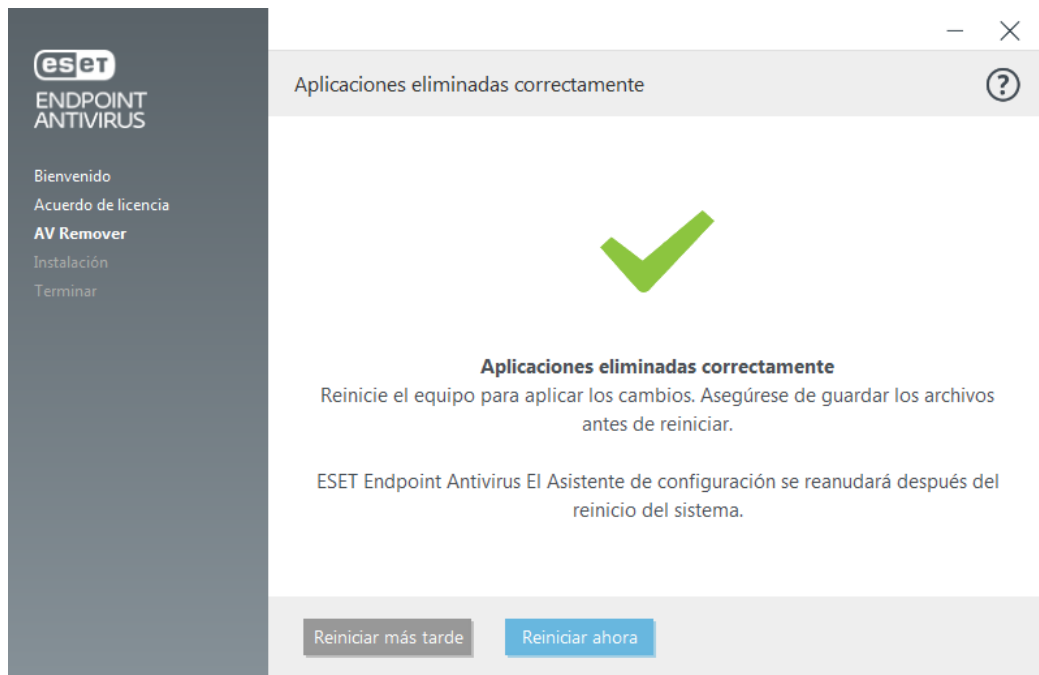
2. Seleccione cualquier aplicación de antivirus enumerada y haga clic en **Quitar**. La eliminación puede llevar unos minutos.



2. Cuando la eliminación se realice correctamente, haga clic en **Continuar**.



6. Reinicie el equipo para aplicar los cambios y continúe con la instalación de ESET Endpoint Antivirus. Si la desinstalación no ha finalizado correctamente, consulte la sección [Desinstalación con ESET AV Remover que ha finalizado con un error](#) de esta guía.



## La desinstalación con ESET AV Remover finalizó con un error

Si no puede quitar un programa antivirus con ESET AV Remover, recibirá una notificación que dirá que la aplicación que está tratando de quitar podría no ser compatible con ESET AV Remover. Para ver si este programa específico se puede quitar, visite la [lista de productos compatibles](#) o los [desinstaladores para software antivirus comunes de Windows](#) en la base de conocimiento de ESET.

Cuando falle la desinstalación de los productos de seguridad o cuando algunos de sus componentes se desinstale parcialmente, se le solicitará **Reiniciar y volver a explorar**. Confirme UAC luego del inicio y continúe con el proceso de exploración y desinstalación.

Si es necesario, póngase en contacto con el [Servicio de soporte técnico de ESET](#) para abrir una solicitud de soporte y tenga el archivo **AppRemover.log** disponible para ayudar a los técnicos de ESET. El archivo **AppRemover.log** se encuentra en la carpeta **eset**. Diríjase a `%TEMP%` en Windows Explorer para acceder a esta carpeta. Soporte técnico de ESET responderá tan rápido como sea posible para ayudarlo a resolver este problema.

## Instalación (.exe)

Una vez que haya iniciado el instalador .exe, el asistente de instalación lo guiará a través del proceso de instalación.



Asegúrese de que no haya otros programas antivirus instalados en el equipo. 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](#) para obtener una lista de herramientas del desinstalador para el software antivirus común (disponible en inglés y otros idiomas más).

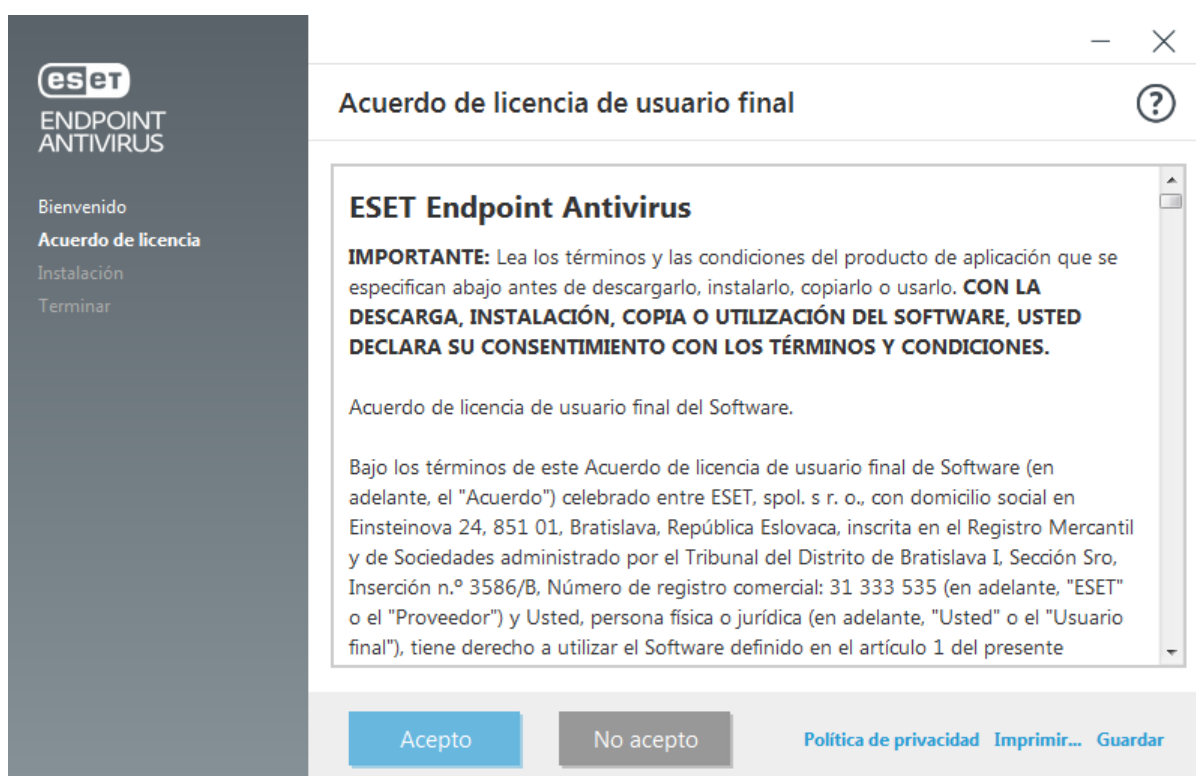


1. Seleccione su preferencia para las siguientes características, lea el [Acuerdo de licencia para el usuario final](#) y la [Política de privacidad](#) y haga clic en **Continuar** o haga clic en **Permitir todo** y continúe para activar todas las características:

- [Sistema de comentarios de ESET LiveGrid®](#)
- [Detección de aplicaciones potencialmente no deseadas](#)



Al hacer clic en **Continuar** o **Permitir todo** y continuar, acepta el Acuerdo de licencia para el usuario final y la Política de privacidad. Puede instalar ESET Endpoint Antivirus en una carpeta específica. Para ello, haga clic en [Cambiar la carpeta de instalación](#).



2. Una vez que se completa la instalación, se lo direccionará a [activar ESET Endpoint Antivirus](#).

## Cambiar la carpeta de instalación (.exe)

Durante la instalación, puede **cambiar la carpeta de instalación**. Seleccione una ubicación para la instalación de ESET Endpoint Antivirus. De forma predeterminada, el programa se instala en el siguiente directorio:

*C:\Program Files\ESET\ESET Security\*

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

*C:\Program Files\ESET\ESET Security\Modules\*

*C:\ProgramData\ESET\ESET Security\*

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

Haga clic en **Atrás** y, luego, continúe con el proceso de instalación.

## Instalación (.msi)

Una vez que haya iniciado el instalador .msi, el asistente de instalación lo guiará a través del proceso de instalación.



En entornos comerciales, el instalador .msi es el paquete de instalación de preferencia. Esto se debe principalmente a las implementaciones sin conexión y remotas que utilizan varias herramientas, como ESET PROTECT.



Asegúrese de que no haya otros programas antivirus instalados en el equipo. 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](#) para obtener una lista de herramientas del desinstalador para el software antivirus común (disponible en inglés y otros idiomas más).

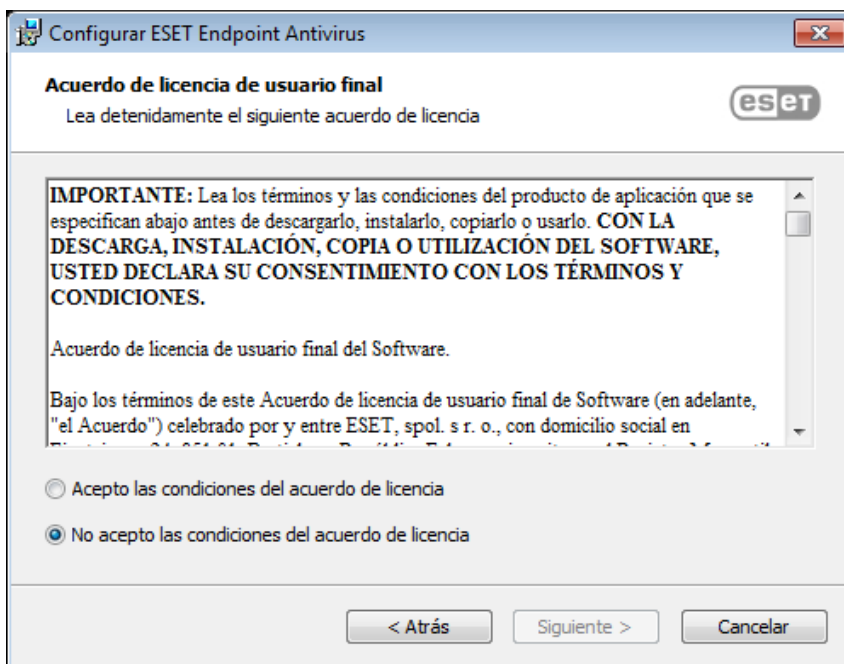


El instalador ESET Endpoint Antivirus creado en ESET PROTECT es compatible con Windows 10 Enterprise para escritorios virtuales y el modo de varias sesiones de Windows 10.

1. Seleccione un idioma deseado y haga clic en **Siguiente**.



2. Lea el Acuerdo de licencia de usuario final y haga clic en **Acepto los términos del contrato de licencia** para reconocer que acepta los términos del Acuerdo de licencia de usuario final. Haga clic en **Siguiente** para aceptar los términos y continuar con la instalación.



3. Seleccione su preferencia para el [sistema de retroalimentación de ESET LiveGrid®](#). ESET LiveGrid® ayuda a garantizar que a ESET se le informe en forma inmediata y continua sobre las nuevas infiltraciones, lo que nos permite proteger mejor a nuestros clientes. El sistema le permite enviar las nuevas amenazas al laboratorio de virus de ESET, donde se analizan, procesan y agregan al motor de detección. Haga clic en **Configuración avanzada** para [configurar parámetros de instalación adicionales](#).



4. El último paso es confirmar la instalación al hacer clic en **Instalar**. Una vez que se completa la instalación, se lo direccionará a [activar ESET Endpoint Antivirus](#).

## Instalación avanzada (.msi)

La instalación avanzada le permite personalizar los parámetros de instalación que no están disponibles al realizar una instalación típica.

1. Durante la instalación, puede **cambiar la carpeta de instalación**. Seleccione una ubicación para la instalación de ESET Endpoint Antivirus. De forma predeterminada, el programa se instala en el siguiente directorios:

*C:\Program Files\ESET\ESET Security\*

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

*C:\Program Files\ESET\ESET Security\Modules\*

*C:\ProgramData\ESET\ESET Security\*

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

2. Elija qué componentes del producto se instalarán. Puede seleccionar su preferencia para la [exploración del equipo](#) y todas las [protecciones](#) disponibles. El componente [Actualizar servidor reflejado](#) se puede utilizar para actualizar otros equipos en su red. [Monitoreo y administración remotos \(RMM\)](#) es el proceso que consiste en supervisar y controlar los sistemas de software mediante el uso de un agente instalado a nivel local al que se puede acceder mediante un proveedor de servicios de administración.
3. Haga clic en **Instalar** para iniciar el proceso de instalación.



# Instalación de módulos mínimos

Para reducir el tráfico de red relacionado con el tamaño del instalador y ahorrar recursos, el producto ESET incluye un instalador de módulos mínimos. El instalador solo contiene módulos esenciales, y el resto de los módulos se descargarán durante la actualización del módulo inicial después de la activación del producto. La principal ventaja es tener un instalador significativamente más pequeño, y descargar solo los módulos de la aplicación más recientes cuando activa el producto ESET Endpoint Antivirus.

El instalador de módulos mínimos no obstante contiene los siguientes módulos:

- Cargadores
- Comunicación Direct Cloud
- Soporte de traducción
- Configuración
- SSL

Tras la activación del producto, verá el estado de **Inicializando protección** que le informará sobre las características que se están inicializando.



Si se produce un problema con la descarga de los módulos (p. ej., configuración del proxy, sin red, etc.), se muestra el estado de alerta de la aplicación **Se requiere atención**. En la ventana principal del programa, haga clic en **Actualizar** > **Buscar actualizaciones** para iniciar el proceso de actualización de nuevo.



Tras varios intentos sin éxito, se muestra el estado de la aplicación **Error en la configuración de la protección** en color rojo. Haga clic en **Inténtelo de nuevo** para volver a iniciar la configuración de la protección. Si el proceso de inicialización falla y sigue sin poder descargar los módulos, [descargue los instaladores MSI completos](#).



Si sus ordenadores cliente no tienen una conexión a Internet o funcionan sin conexión y necesitan actualizaciones, utilice los siguientes métodos para descargar archivos de actualización de los servidores de actualización de ESET:

- [Actualización desde el Mirror](#)
- [Uso de la herramienta Mirror](#)

# Instalación de línea de comando

Puede instalar ESET Endpoint Antivirus de forma local mediante la línea de comandos o de forma remota mediante una tarea de cliente desde ESET PROTECT.

## Parámetros admitidos

**APPDIR=<path>**

- Ruta - Ruta de directorio válida.
- Directorio de instalación de aplicación.

**APPDATADIR=<path>**

- Ruta - Ruta de directorio válida.
- Directorio de instalación de los datos de la aplicación.

## MODULEDIR=<path>

- Ruta - Ruta de directorio válida.
- Directorio de instalación del módulo.

## ADDLOCAL=<list>

- Instalación de componente: lista de características no obligatorias que se instalarán en forma local.
- Uso con paquetes de .msi de ESET: `ees_nt64_ENU.msi /qn ADDLOCAL=<list>`
- Para obtener más información acerca de la propiedad **ADDLOCAL** vea <http://msdn.microsoft.com/en-us/library/aa367536%28v=vs.85%29.aspx>

## ADDEXCLUDE=<list>

- La lista de ADDEXCLUDE es una lista separada por comas de los nombres de todas las características que se instalarán, como un reemplazo para REMOVE obsoleta.
- Cuando selecciona una característica que no desea instalar, la ruta completa (es decir, todas las características secundarias) y las características invisibles relacionadas se deben incluir explícitamente en la lista.
- Uso con paquetes de .msi de ESET: `ees_nt64_enu.msi /qn ADDEXCLUDE=Firewall,Network`

**i** ADDEXCLUDE no se puede usar junto con **ADDLOCAL**.

Consulte la [documentación](#) para la versión de **msiexec** usada para los cambios correspondientes de la línea de comandos.

## Reglas

- El **ADDLOCAL** list es una lista separada por comas de todos los nombres de las características que se instalarán.
- Al seleccionar una característica para instalar, toda la ruta (todas las características principales) deberá incluirse de forma explícita en la lista.
- Vea reglas adicionales para utilizarlo correctamente.

## Componentes y características

**i** La instalación de componentes con los parámetros ADDLOCAL/ADDEXCLUDE no funcionará con ESET Endpoint Antivirus.

Las características se dividen en 4 categorías:

- **Obligatoria:** la característica se instalará siempre.
- **Opcional:** se puede anular la selección de la característica para que no se instale.
- **Invisible:** función lógica obligatorio para que otras características funcionen correctamente
- **Marcador:** característica que no tiene ningún efecto en el producto, pero debe figurar con las subfunciones

El conjunto de características de ESET Endpoint Antivirus es el siguiente:

Descripción	Nombre de característica	Característica principal	Presencia
Componentes básicos del programa	Computer		Marcador

Descripción	Nombre de característica	Característica principal	Presencia
Motor de detección	Antivirus	Computer	Obligatoria
Motor de detección/Exploración de malware	Scan	Computer	Obligatoria
Motor de detección/Protección del sistema de archivos en tiempo real	RealtimeProtection	Computer	Obligatoria
Motor de detección/Exploración de malware/Protección de documentos	DocumentProtection	Antivirus	Opcional
Control del dispositivo	DeviceControl	Computer	Opcional
Protección de la red	Network		Marcador
Protección de la red/Firewall	Firewall	Network	Opcional
Protección de la red/Protección contra ataques en la red/...	IdsAndBotnetProtection	Network	Opcional
Navegador seguro	OnlinePaymentProtection	WebAndEmail	Opcional
Web y correo electrónico	WebAndEmail		Marcador
Internet y correo electrónico/Filtrado de protocolos	ProtocolFiltering	WebAndEmail	Invisible
Internet y correo electrónico/Protección de acceso a la Web	WebAccessProtection	WebAndEmail	Opcional
Internet y correo electrónico/Protección del cliente de correo electrónico	EmailClientProtection	WebAndEmail	Opcional
Internet y correo electrónico/Protección del cliente de correo electrónico/Cientes de correo electrónico	MailPlugins	EmailClientProtection	Invisible
Internet y correo electrónico/Protección del cliente de correo electrónico/Web y correo electrónico	Antispam	EmailClientProtection	Opcional
Internet y correo electrónico/Control web	WebControl	WebAndEmail	Opcional
Herramientas/ESET RMM	Rmm		Opcional
Actualización/Perfiles/Replicación de actualización	UpdateMirror		Opcional
<a href="#">Complemento de ESET Inspect</a>	EnterpriseInspector		Invisible

Conjunto de características grupales:

Descripción	Nombre de característica	Presencia de característica
Todas las características obligatorias	_Base	Invisible
Todas las características disponibles	ALL	Invisible

## Reglas adicionales

- Si se selecciona alguna de las características de **WebAndEmail** para la instalación, se debe incluir la

característica invisible **ProtocolFiltering** en la lista.

- Los nombres de todas las características distinguen entre mayúsculas y minúsculas, por ejemplo, UpdateMirror no es lo mismo que UPDATERMIRROR.

## Lista de propiedades de configuración

Propiedad	Valor	Característica
CFG_POTENTIALLYUNWANTED_ENABLED=	0: Deshabilitado 1: Habilitado	<a href="#">Detección de aplicaciones potencialmente no deseadas (PUA)</a>
CFG_LIVEGRID_ENABLED=	<a href="#">Ver a continuación</a>	Consulte la propiedad <a href="#">LiveGrid</a> a continuación
FIRSTSCAN_ENABLE=	0: Deshabilitado 1: Habilitado	Programe y ejecute una <a href="#">Exploración del equipo</a> después de la instalación
CFG_PROXY_ENABLED=	0: Deshabilitado 1: Habilitado	Configuración del servidor proxy
CFG_PROXY_ADDRESS=	<ip>	Dirección IP del servidor proxy
CFG_PROXY_PORT=	<port>	Número de puerto del servidor proxy
CFG_PROXY_USERNAME=	<username>	Nombre de usuario para la autenticación
CFG_PROXY_PASSWORD=	<password>	Contraseña para la autenticación
ACTIVATION_DATA=	<a href="#">Ver a continuación</a>	Activación del producto, clave de licencia o archivo de licencia sin conexión
ACTIVATION_DLG_SUPPRESS=	0: Deshabilitado 1: Habilitado	Cuando lo establezca en "1", no se mostrará el cuadro de diálogo de activación del producto después del primer inicio
ADMINCFG=	<path>	Ruta a la <a href="#">configuración XML exportada</a> (valor predeterminado <i>cfg.xml</i> )

### Propiedad de [LiveGrid®](#)

Al instalar ESET Endpoint Antivirus conCFG\_LIVEGRID\_ENABLED, el comportamiento del producto después de la instalación será el siguiente:

Característica	CFG_LIVEGRID_ENABLED=0	CFG_LIVEGRID_ENABLED=1
<b>Sistema de reputación de ESET LiveGrid®</b>	Activado	Activado
<b>Sistema de comentarios de ESET LiveGrid®</b>	Desactivado	Activado
<b>Enviar estadísticas anónimas</b>	Desactivado	Activado

### Propiedad ACTIVATION\_DATA

Formato	Métodos
ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE	<a href="#">Activación con Clave de licencia de ESET</a> (La conexión a Internet debe estar activa)
ACTIVATION_DATA=offline:C:\ProgramData\ESET\ESET Security\license.lf	<a href="#">Activación con un archivo de licencia sin conexión</a>

## Propiedades de idioma


Idioma de ESET Endpoint Antivirus (debe especificar ambas propiedades).

Propiedad	Valor
PRODUCT_LANG=	Decimal LCID (Identificación de configuración regional), por ejemplo, 1033 para inglés (Estados Unidos de América). Consulte la <a href="#">lista de códigos de idioma</a> .
PRODUCT_LANG_CODE=	Cadena LCID (Nombre cultural del idioma) en minúscula, por ejemplo en-us para inglés (Estados Unidos de América). Consulte la <a href="#">lista de códigos de idioma</a> .

## Propiedades de reinicio


Especifique los siguientes parámetros para reiniciar el equipo después de la instalación:


Propiedad	Valor	Característica
REBOOT_WHEN_NEEDED=	0: Deshabilitado 1: Habilitado	Si esta opción está activada, tras la instalación, el equipo se reiniciará.
REBOOT_CANCELABLE=	0: Deshabilitado 1: Habilitado	Si esta opción está activada, el usuario puede cancelar el reinicio del equipo.
REBOOT_POSTPONE=	valor en segundos	Tiempo máximo en segundos para que el usuario posponga el reinicio del equipo.


 REBOOT\_CANCELABLE y REBOOT\_POSTPONE solo están disponibles si REBOOT\_WHEN\_NEEDED está activado.

## Ejemplos de instalación desde la línea de comandos


 Asegúrese de leer el [Acuerdo de licencia de usuario final](#) y de obtener privilegios administrativos antes de ejecutar la instalación.


 Excluya la sección **NetworkProtection** de la instalación (debe especificar también todas las características secundarias):  
`msiexec /qn /i ees_nt64.msi ADDEXCLUDE=Network,Firewall,IdsAndBotnetProtection`

 Si desea que su ESET Endpoint Antivirus se configure automáticamente después de la instalación, puede especificar parámetros de configuración básicos dentro del comando de instalación.  
Instale ESET Endpoint Antivirus con ESET LiveGrid® habilitado:  
`msiexec /qn /i ees_nt64.msi CFG_LIVEGRID_ENABLED=1`

 Instale en un directorio de instalación de aplicaciones diferente al [predeterminado](#).  
`msiexec /qn /i ees_nt64_enu.msi APPDIR=C:\ESET\`

 Instale y active ESET Endpoint Antivirus con su clave de licencia de ESET.  
`msiexec /qn /i ees_nt64_enu.msi ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE`

 Instalación silenciosa con registro detallado (útil para la resolución de problemas) y RMM solo con componentes obligatorios:  
`msiexec /qn /i ees_nt64.msi /l*xv msi.log ADDLOCAL=_Base,Rmm`

 Instalación completa silenciosa forzada con un [idioma especificado](#).  
`msiexec /qn /i ees_nt64.msi ADDLOCAL=ALL PRODUCT_LANG=1033 PRODUCT_LANG_CODE=en-us`

## Opciones de la línea de comandos posteriores a la instalación

- [ESET CMD](#): importar un archivo de configuración de .xml o activar/desactivar una característica de seguridad
- [Explorador de la línea de comandos](#) : ejecutar una exploración del equipo desde la línea de comandos

## Implementación a través de GPO o SCCM

Además de la [instalación directa de ESET Endpoint Antivirus en una estación de trabajo del cliente](#), también puede usar herramientas de administración como Objeto de política de grupo (GPO), Software Center Configuration Manager (SCCM), Symantec Altiris o Puppet.

### Administrado (recomendado)

Para equipos administrados, primero instalamos el agente ESET Management, luego implementamos ESET Endpoint Antivirus a través de ESET PROTECT. Debe tener ESET PROTECT instalado en su red.

1. Descargue el [instalador independiente](#) para el agente ESET Management.
2. [Prepare el script de implementación remota GPO/SCCM](#).
3. Implemente el agente ESET Management con GPO o SCCM.
4. Asegúrese de que los [equipos cliente](#) se hayan agregado a ESET PROTECT.
5. [Implemente y active ESET Endpoint Antivirus en sus equipos cliente](#).



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

- [Implemente ESET Management Agent a través de SCCM o GPO](#)
- [Implemente ESET Management Agent con un Objeto de política de grupo \(GPO\)](#)

### Sin administración

Para equipos no administrados, puede implementar ESET Endpoint Antivirus directamente en las estaciones de trabajo de cliente. Esto no se recomienda ya que no podrá supervisar ni aplicar las políticas para todos sus productos de punto de conexión de ESET en las estaciones de trabajo.

De manera predeterminada, ESET Endpoint Antivirus no se activa después de la instalación y, por lo tanto, no es funcional.

### Opción 1 (Instalación del software)

1. [Descargue el instalador .msi](#) para ESET Endpoint Antivirus.
2. Cree un paquete de transformación .mst del archivo .msi (por ejemplo, mediante el uso del editor Orca .msi) para incluir la propiedad de activación del producto (consulte ACTIVATION\_DATA en [Instalación de línea de comandos de](#)).



[Mostrar pasos para la creación de .mst en Orca](#)

1. Abrir Orca.
2. Haga clic en **File > Open** para cargar el instalador .msi.
3. Haga clic en **Transform > New Transform**.
4. Haga clic en **Property** en la sección **Tables** y luego en el menú **Tables > Add row**.
5. En las ventanas **Add Row** escriba ACTIVATION\_DATA como **Property** y la información de la licencia como **Value**.

ees\_nt32.msi (transformed by act.mst) - Orca

File Edit Tables Transform Tools View Help

Tables	Property	Value
CreateFolder	ACTIVATION_DATA	key:AAAA-BBBB-CCCC-DDDD-EEEE
CustomAction	ACTIVATION_DLG_SUPPRESS	0
Dialog	ALLUSERS	1
Directory	ARPNOREPAIR	1
Error	ARPPRODUCTICON	Icon_Product
EventMapping	ApplicationCode	33686273
Feature	CHECK_NEW_VERSION	0
FeatureComponents	CLOUD_AGREE	1
File	CompatibleProductTypes	eav;eis;ess;essp;eea;ees;eavbe;essbe
Icon	DataDir	ESET\ESET Security\
InstallExecuteSequence	DefaultUIFont	DlgStdFont
InstallUISequence	EPFW_PROXY_ENABLED	1
LaunchCondition	ERAProductCategory	1
ListBox	EULATAG	4a25ec5f3fae5a774466f5f9991524b438c942bf
Media	EULATAG_1026	4ff82b074b311d037fe051eadf6d42d2de00abf4
MoveFile	EULATAG_1028	205fb56b27259a729eced47de74a82ed6d80ba82
MsiEmbeddedUI	EULATAG_1029	014f233417984a324eadcab90b7ea46b2fc72414
MsiFileHash	EULATAG_1030	c75483d80bdcb8381984918b8c0406fec55247fc
MsiShortcutProperty	EULATAG_1031	3cf6614563807ce122021482475c01882de1d20a
Property	EULATAG_1032	7f64744d3e9acfa7634af832b3f32bccd95c33d1
RadioButton	EULATAG_1033	e27bcea9073de912ce9e72c3176f1495410901f5
ReqLocator	EULATAG_1035	b6a3cbdf825e409b2dd7c9dda3d5558db3492158
Registry	EULATAG_1036	3f953a8ff495167510d22df1b289c5a0f6faf3b2
RemoveFile	EULATAG_1037	5cb62b1988ec4b5667a6c9a3067a3efca6421735
ServiceControl	EULATAG_1038	df1b69e526fbd9c06fa10d79547b88b495ba4306
ServiceInstall	EULATAG_1040	cb63d6d62b38a9b50f3396cf1681b9eade12fa86
Shortcut	EULATAG_1041	01f931f203068d0a47d54f5ee9738c58ff82aff3
Signature	EULATAG_1042	44fde07b99660d4d28dafbb4d275693fd0a90b80
TextStyle		

Tables: 45      Property - 87 rows      Value - Localizable[0]

6. Haga clic en **Transformar > Generar transformación** para guardar el archivo .mst.

1. Opcional: Para [importar](#) su archivo de configuración ESET Endpoint Antivirus .xml personalizado (por ejemplo, para habilitar RMM o ajustar la configuración del servidor proxy), coloque el archivo cfg.xml en la misma ubicación que el instalador .msi.
2. Implemente el instalador .msi con el archivo .mst de forma remota mediante GPO (a través de la instalación de software) o SCCM.

## Opción 2 (con una tarea programada)

1. [Descargue el instalador .msi](#) para ESET Endpoint Antivirus.
2. Prepare un script de [instalación de línea de comandos](#) para incluir la propiedad de activación del producto (consulte ACTIVATION\_DATA).
3. Haga que el instalador .msi y el script .cmd estén disponibles en la red para todas las estaciones de trabajo.
4. Opcional: Para [importar](#) su archivo de configuración ESET Endpoint Antivirus .xml personalizado (por ejemplo, para habilitar RMM o ajustar la configuración del servidor proxy), coloque el archivo cfg.xml en la misma ubicación que el instalador .msi.
5. Aplique un script de instalación de línea de comandos mediante GPO o SCCM.
  - Para GPO, use Preferencias de política de grupo > Tareas programadas de política de grupo > Tarea inmediata



Si no desea usar ESET PROTECT para administrar sus productos de punto de conexión de ESET de forma remota, ESET Endpoint Antivirus contiene el complemento de ESET para RMM que le permite supervisar y controlar los sistemas de software mediante un agente instalado de forma local al que se puede acceder a través de un proveedor de servicios de administración. [Más información](#)

## Reemplazo a una versión más reciente

Las versiones nuevas de ESET Endpoint Antivirus se emiten para implementar mejoras o resolver problemas que no se pueden solucionar mediante la actualización automática de los módulos del programa.

El reemplazo a una versión más reciente se puede realizar de varias maneras:

1. De manera automática, utilice ESET PROTECT, o ESET PROTECT Cloud.
2. Automáticamente, [mediante el uso de GPO o SCCM](#).
3. Automáticamente, mediante una actualización del programa.  
Dado que la actualización del programa se distribuye a todos los usuarios y puede afectar ciertas configuraciones del sistema, se emite luego de un largo período de prueba para asegurarse de que funciona con todas las configuraciones posibles del 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 **Modo de actualización** en [Configuración avanzada](#) > **Actualización** > **Perfiles** > **Actualizaciones del producto**.
4. En forma manual, mediante la descarga e [instalación de la versión más reciente](#) sobre la instalación previa.

## Escenarios de actualización recomendados

### Administro o deseo administrar mis productos ESET de manera remota

Si administra más de 10 productos de ESET Endpoint, analice administrar las actualizaciones con ESET PROTECT o ESET PROTECT Cloud. Consulte la siguiente documentación:

- [ESET PROTECT | Actualizar el software de ESET mediante la tarea del cliente](#)
- [ESET PROTECT | Guía para empresas de pequeñas a medianas que administran hasta 250 productos ESET Endpoint de Windows](#)
- [Introducción a ESET PROTECT Cloud](#)

### Cómo actualizar manualmente en una estación de trabajo del cliente

Para actualizar ESET Endpoint Antivirus en estaciones de trabajo cliente individuales manualmente:

1. Compruebe que [la versión que tiene instalada actualmente sea compatible](#).
2. Compruebe que su sistema operativo sea [compatible](#).
2. Descargue e [instale la versión más reciente](#) sobre la versión anterior.



No se garantiza la instalación correcta de la versión más reciente sobre la anterior en versiones con nivel de soporte de "Fin de la vida útil". Consulte la [política sobre el fin de la vida útil](#) para revisar el nivel de soporte de ESET Endpoint Antivirus.


Para actualizar desde versiones no compatibles, desinstale primero ESET Endpoint Antivirus. Para obtener información adicional sobre la actualización de ESET Endpoint Antivirus en una estación de trabajo cliente, lea el siguiente artículo de la [base de conocimiento de 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](#)

 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 comentarios de ESET LiveGrid®](#) 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 de inicio. 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.

## Actualizaciones de seguridad y estabilidad


La actualización de ESET Endpoint Antivirus es una parte fundamental para mantener una protección completa contra códigos maliciosos. Cada nueva versión de ESET Endpoint Antivirus presenta nuevas mejoras y reparaciones de errores. Recomendamos realizar actualizaciones periódicas de ESET Endpoint Antivirus para evitar vulnerabilidades y amenazas de seguridad. ESET Endpoint Antivirus encaja en una etapa específica del ciclo de vida del producto como cualquiera de los demás productos ESET.

Más información acerca de:

[Política sobre el fin de la vida útil \(productos para empresas\)](#)

 [Actualizaciones del producto](#)  
[Revisiones de seguridad y estabilidad](#)

Para obtener más información sobre los cambios en ESET Endpoint Antivirus, lea el siguiente [artículo de la base de conocimiento de ESET](#).

 Las actualizaciones automáticas garantizan la máxima seguridad y estabilidad de su producto. Las actualizaciones de seguridad y estabilidad no se pueden deshabilitar.

## Activación del producto

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

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

ESET, tipo de instalador .msi o .exe, etc.).

Puede activar ESET Endpoint Antivirus en la [ventana principal del programa](#) > **Ayuda y soporte** > **Activar producto** o **Estado de protección** > **Activar producto**.

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

- **Use una clave de licencia que compró:** una cadena única en el formato XXXX-XXXX-XXXX-XXXX-XXXX que se utiliza para la identificación del propietario de la licencia y para la activación de la licencia.
- **ESET HUB:** Una [cuenta de ESET HUB](#) que tiene que crear. ESET HUB es una puerta de enlace central a la plataforma de seguridad unificada de ESET PROTECT. Proporciona administración centralizada de identidades, suscripciones y usuarios para todos los módulos de la plataforma ESET. Puede usar esta opción para activar ESET Endpoint Antivirus también con herramientas de administración de licencias más antiguas: [ESET Business Account](#) o [ESET MSP Administrator](#).
- **Licencia sin conexión:** un archivo generado automáticamente que será transferido al producto ESET para brindar información sobre la licencia. Si una licencia le permite descargar un archivo de licencia sin conexión (.lf), ese archivo puede utilizarse para realizar una activación sin conexión. La cantidad de licencias sin conexión se restará de la cantidad total de licencias disponibles. Para mayor información sobre la generación de un archivo sin conexión, consulte la [ESET Business Account Guía para el usuario](#).

Haga clic en **Activar más tarde** si su equipo es miembro de una red administrada, y su administrador realizará la activación remota a través de ESET PROTECT. También puede utilizar esta opción si desea activar este cliente más tarde.

Si tiene un nombre de usuario y una contraseña que usó para activaciones anteriores de productos de ESET, [convierta sus credenciales anteriores en una clave de licencia](#).

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



ESET PROTECT puede activar equipos cliente de manera silenciosa con el uso de licencias que el administrador pone a disposición. Para obtener instrucciones, consulte la [ayuda en línea de ESET PROTECT](#).

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

## Ingreso de su clave de licencia durante la activación

Las actualizaciones automáticas son importantes para su seguridad. ESET Endpoint Antivirus solo recibirá actualizaciones después de activarlas mediante su **Clave de licencia**.

Si no ingresó su Clave de licencia luego de la instalación, el producto no se activará. Puede cambiar su licencia en la ventana principal del programa. Para ello, haga clic en **Ayuda y soporte**, > **Activar la licencia** e ingrese los datos de la licencia que recibió con el producto de seguridad de ESET en la ventana de activación del producto.

Al ingresar 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.

## Cuenta ESET HUB

ESET HUB es una puerta de enlace central a la plataforma de seguridad unificada de ESET PROTECT. Proporciona administración centralizada de identidades, suscripciones y usuarios para todos los módulos de la plataforma ESET. Al usar ESET HUB, usted puede:

- Obtener información general sobre las suscripciones de seguridad
- Comprobar el uso y los estados de los servicios a los que está suscrito
- Asignar y controlar el acceso granular a plataformas ESET individuales
- Inicio de sesión único para todas las plataformas ESET vinculadas y accesibles

Puede usar esta opción de activación para activar ESET Endpoint Antivirus también con herramientas de administración de licencias más antiguas: [ESET Business Account](#) o [ESET MSP Administrator](#).

Puede [crear una cuenta de ESET HUB](#) e iniciar sesión con su **dirección de correo electrónico** y **contraseña**.

Si ha olvidado su contraseña, haga clic en **¿Olvidó su contraseña?** y se lo redireccionará al ESET HUB. Ingrese su dirección de correo electrónico y haga clic en **Iniciar sesión** para confirmar. A continuación, obtendrá un mensaje con instrucciones sobre cómo restablecer su contraseña.

## Procedimiento para usar credenciales de la licencia para activar un producto ESET Endpoint

Si ya tiene su Nombre de usuario y Contraseña, y le gustaría recibir una Clave de licencia, visite el [portal de ESET Business Account](#), donde puede convertir sus credenciales en una nueva Clave de licencia.

## Falló la activación

Si la activación de ESET Endpoint 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.

Asegúrese de haber ingresado la Clave de licencia apropiada o haber adjuntado una Licencia sin conexión para volver a activar.

Si no puede activar el producto, nuestro paquete de bienvenida lo guiará a través de preguntas, errores y problemas comunes acerca de la activación y las licencias (disponible en inglés y otros idiomas).

- [Iniciar resolución de problemas de activación del producto de ESET](#)

# Registro

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

## Progreso de la activación

ESET Endpoint Antivirus no se activa, puede demorar un momento.

## La activación se completó correctamente.

La activación se completó correctamente y ESET Endpoint Antivirus ahora está activado. A partir de este momento, ESET Endpoint Antivirus recibirá actualizaciones regularmente para identificar las últimas amenazas y mantener su equipo seguro. Haga clic en **Listo** para finalizar con la activación del producto.

## Problemas comunes 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](#).

## Guía para principiantes

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

## 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 .

**i** Para acceder al menú del ícono de la bandeja del sistema (área de notificación de Windows), asegúrese de que el modo inicio de [Elementos de la interfaz de usuario](#) esté configurado en set to Completo.

**Detener la protección:** muestra el cuadro de diálogo de confirmación que deshabilita el [Motor de detección](#), que protege ante ataques mediante el control de los archivos, 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 Endpoint Antivirus. Para abrir la Configuración avanzada desde la [ventana principal del programa](#), 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 Endpoint Antivirus:** abre la [ventana principal del programa](#) de ESET Endpoint Antivirus desde el ícono de la bandeja (área de notificación de Windows).

**Restablecer disposición de la ventana:** restablece la ventana de ESET Endpoint 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 interfaz gráfica de usuario.

**Buscar actualizaciones** — inicia un módulo o una actualización del producto para garantizar su protección. ESET Endpoint Antivirus busca actualizaciones automáticamente varias veces al día.

**Acerca de** — proporciona información del sistema, detalles sobre la versión instalada de ESET Endpoint Antivirus, los módulos del programa instalados e información sobre el sistema operativo y los recursos del sistema.

## Accesos directos del teclado

Para mejorar la navegación en ESET Endpoint Antivirus, puede utilizar los siguientes accesos directos del teclado:

Accesos directos desde teclado	Acción
F1	abre las páginas de ayuda
F5	abre la <a href="#">Configuración avanzada</a>
Flecha arriba/flecha abajo	navegación en elementos del menú desplegable
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.

## Perfiles

El administrador de perfiles se usa en dos partes de ESET Endpoint Antivirus — en la sección **Exploración bajo demanda** y en **Actualización**.

## Exploración del equipo

Hay cuatro perfiles de exploración predefinidos en ESET Endpoint 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 [Configuración avanzada](#) > **Motor de detección** > **Exploración de malware** > **Exploración a demanda** > **Lista de perfiles** > **Editar**. 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 [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 [configuración de la actualización](#) permite 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.

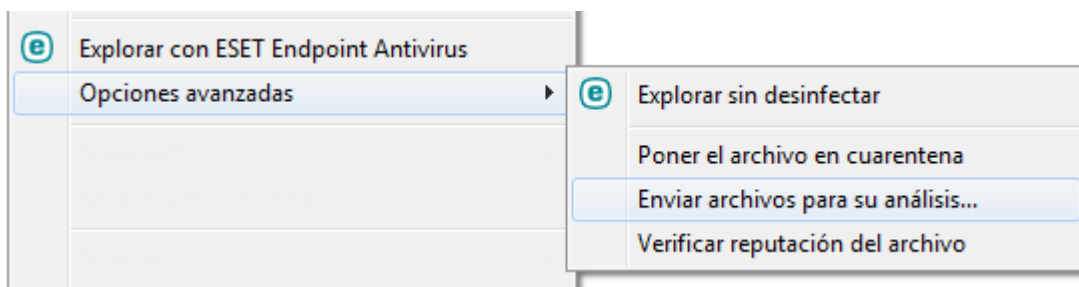
**Lista de perfiles** – cree perfiles nuevos o elimine perfiles de actualización existentes.

## Menú contextual

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

Puede integrar elementos de control de ESET Endpoint Antivirus en el menú contextual. Las opciones de configuración para esta función están disponibles en [Configuración avanzada](#) > **Interfaz del usuario** > **Elementos de la interfaz del usuario**.

**Integrar en el menú contextual** – integrar los elementos de control de ESET Endpoint Antivirus al menú contextual.

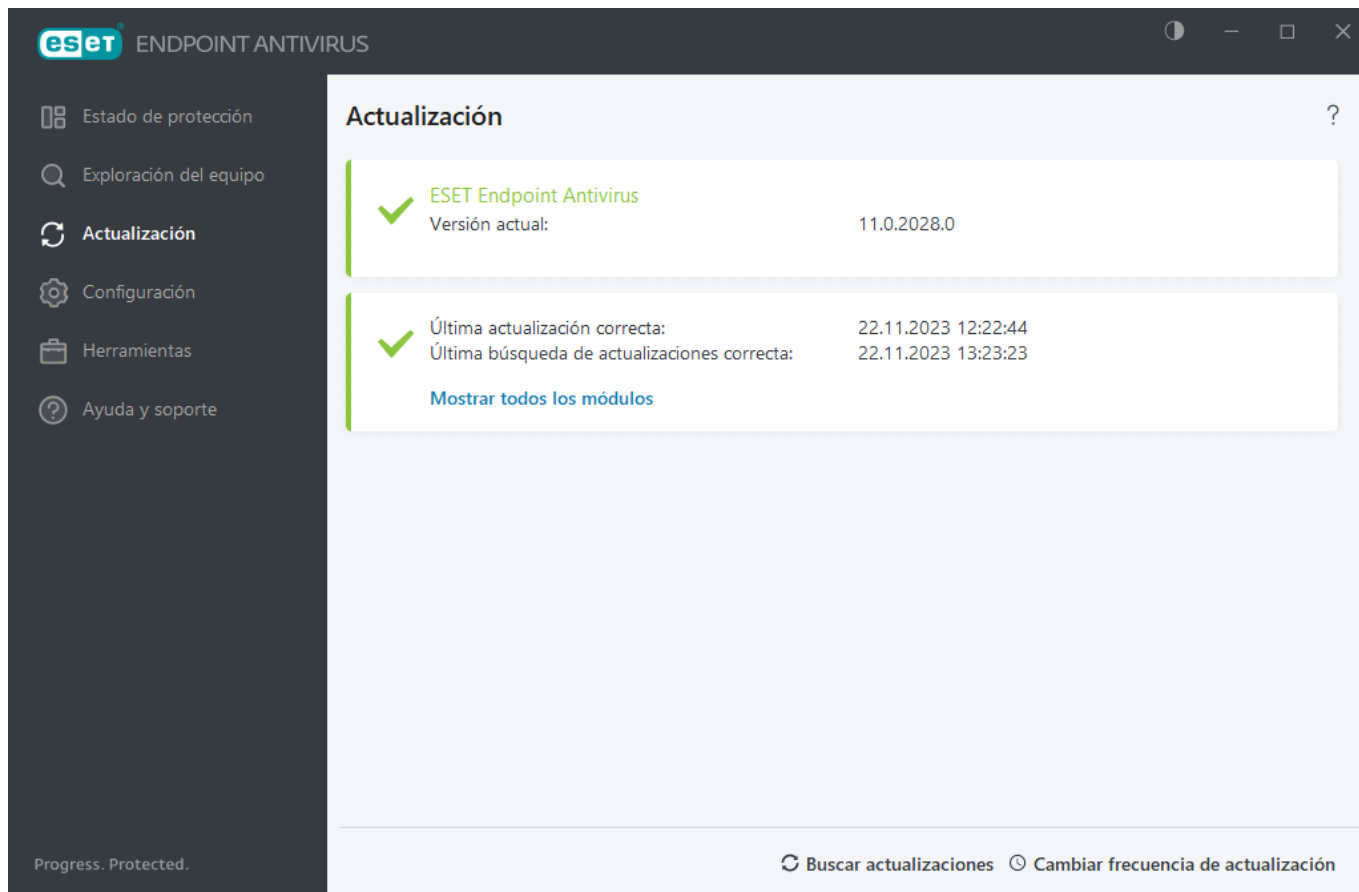


## Configuración de la actualización

La actualización periódica de ESET Endpoint Antivirus es el mejor método para ofrecer la máxima 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.

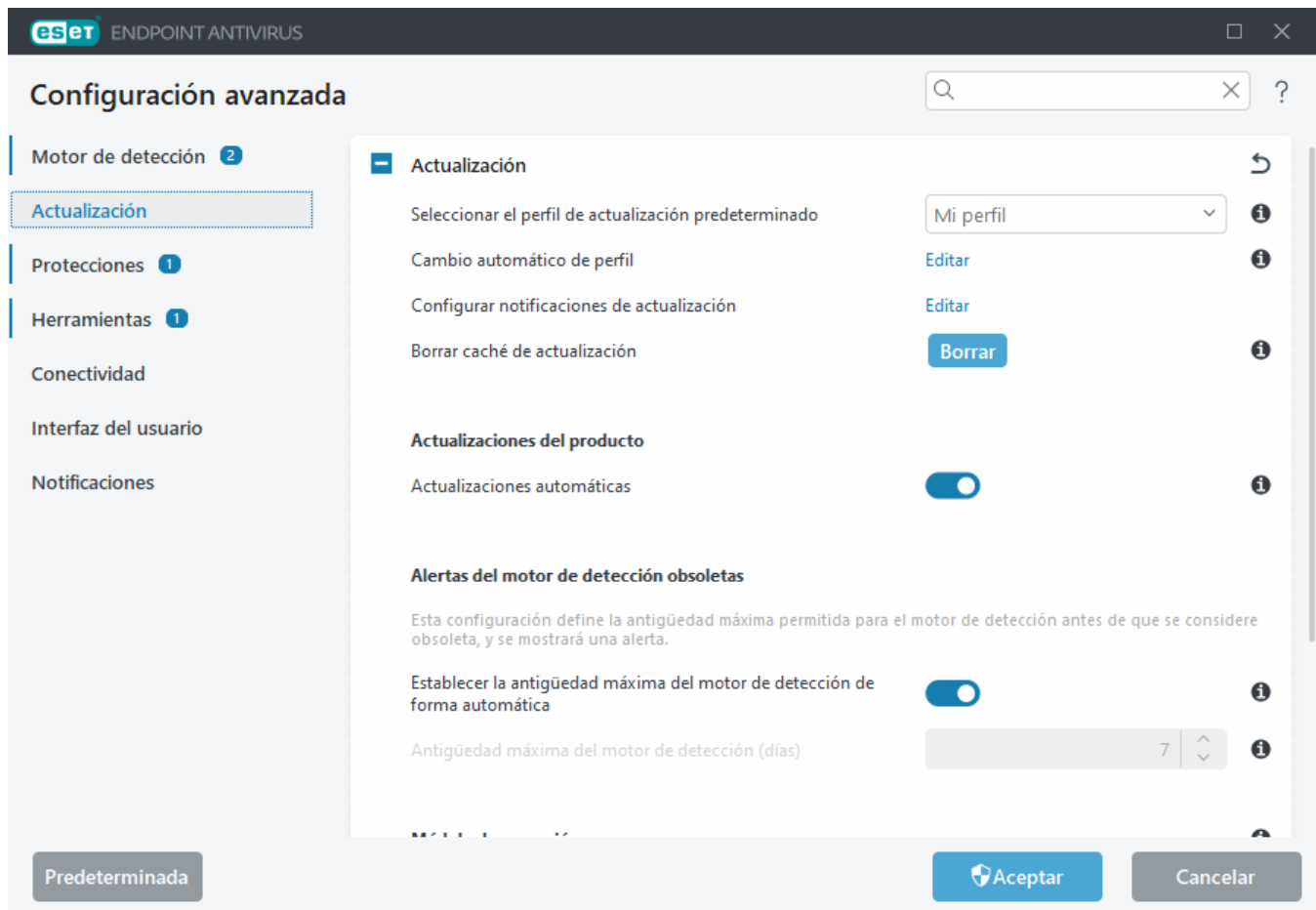
Además de las actualizaciones automáticas, puede hacer clic en **Buscar actualizaciones** para activar una actualización manual.



[Configuración avanzada](#) > **Actualización** contiene opciones de actualización adicionales, como el modo de actualización, el acceso al servidor proxy y las conexiones LAN.

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”](#).



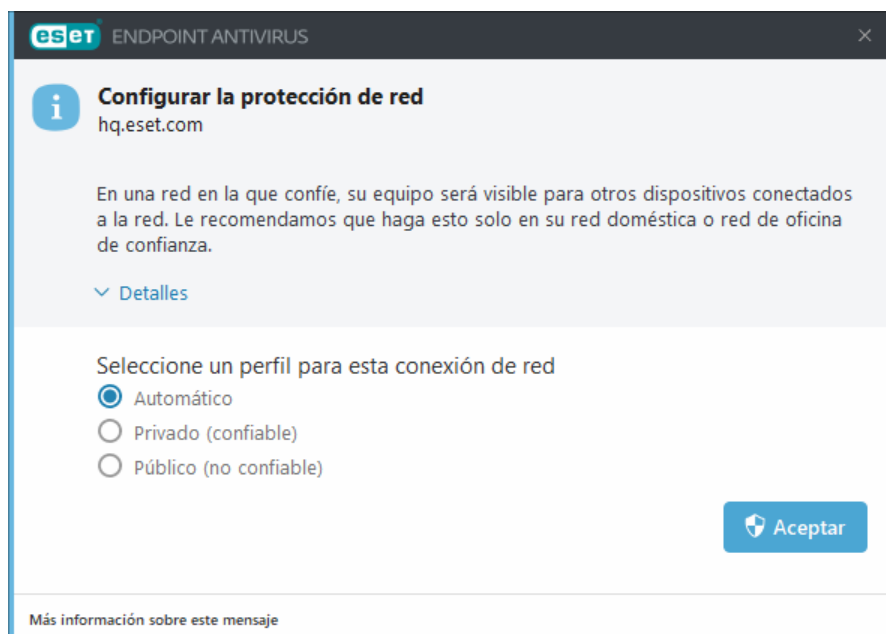


La opción **Elegir de manera automática** en [Configuración avanzada](#) > **Actualización** > **Perfiles** > **Actualizaciones** > **Actualizaciones de los módulos** se encuentra habilitada de manera predeterminada. Al usar un servidor de actualización de ESET para recibir actualizaciones, le recomendamos que deje esta configuración tal como está.

Para lograr una funcionalidad óptima, el programa debe actualizarse automáticamente. Las actualizaciones automáticas solo pueden ocurrir si se ingresa la clave de licencia correcta en **Ayuda y soporte** > **Activar el producto**. Si no ingresó su Clave de licencia luego de la instalación, puede hacerlo en cualquier momento. Para obtener información más detallada sobre la activación, consulte [Cómo activar ESET Endpoint Antivirus](#).

## Configurar la protección de red

De manera predeterminada, ESET Endpoint Antivirus utiliza la configuración de Windows cuando se detecta una nueva conexión de red. Para mostrar una ventana de diálogo cuando se detecta una nueva red, cambie la [asignación del perfil de protección de red](#) a **Preguntar**. La configuración de la protección de red se mostrará cada vez que el equipo se conecte a una nueva red.




Puede seleccionar entre los siguientes [perfiles de conexión de red](#):

**Automático:** ESET Endpoint Antivirus seleccionará el perfil automáticamente, en función de los [Activadores](#) configurados para cada perfil.

**Privado:** para redes confiables (red doméstica o de oficina). Su equipo y los archivos compartidos almacenados en su equipo están visibles para otros usuarios en la red y estos pueden acceder a los recursos del equipo (el acceso a archivos e impresoras compartidos está habilitado, la comunicación entrante RPC está habilitada y el uso compartido de escritorio remoto está disponible). Recomendamos el uso de esta configuración al acceder a una red local segura. Este perfil se asigna automáticamente a una conexión de red si está configurado como Dominio o Red privada en Windows.

**Público:** para redes no confiables (red pública). Los archivos y las carpetas en su equipo no se comparten con otros usuarios en la red o no están visibles para ellos, y el uso compartido de recursos del equipo está desactivado. Recomendamos el uso de esta configuración al acceder a redes inalámbricas. Este perfil se asigna automáticamente a cualquier conexión de red que no esté configurada como Dominio o Red privada en Windows.

**Perfil definido por el usuario:** puede seleccionar un [perfil que haya creado](#) en el menú desplegable. Esta opción solo está disponible si ha creado al menos un perfil personalizado.

 Una configuración de red incorrecta puede suponer un riesgo para la seguridad de su equipo.

## Hashes bloqueados

El uso de ESET Inspect en su entorno permite a los administradores bloquear el acceso a ejecutables especificados en función de su hash. Si el administrador bloquea el acceso a un archivo ejecutable e intenta acceder a él, ESET Endpoint Antivirus muestra esta notificación:

**Acceso a archivo bloqueado:** la aplicación (se muestra el nombre de la aplicación) intentó acceder a un archivo que no está permitido por el administrador.

Si es el administrador y desea permitir el acceso a la aplicación especificada en la notificación, consulte [Hashes bloqueados](#) en la ayuda en línea de ESET Inspect. Si es un usuario y desea cambiar el comportamiento de la

aplicación, póngase en contacto con el administrador.

## Trabajar con ESET Endpoint Antivirus

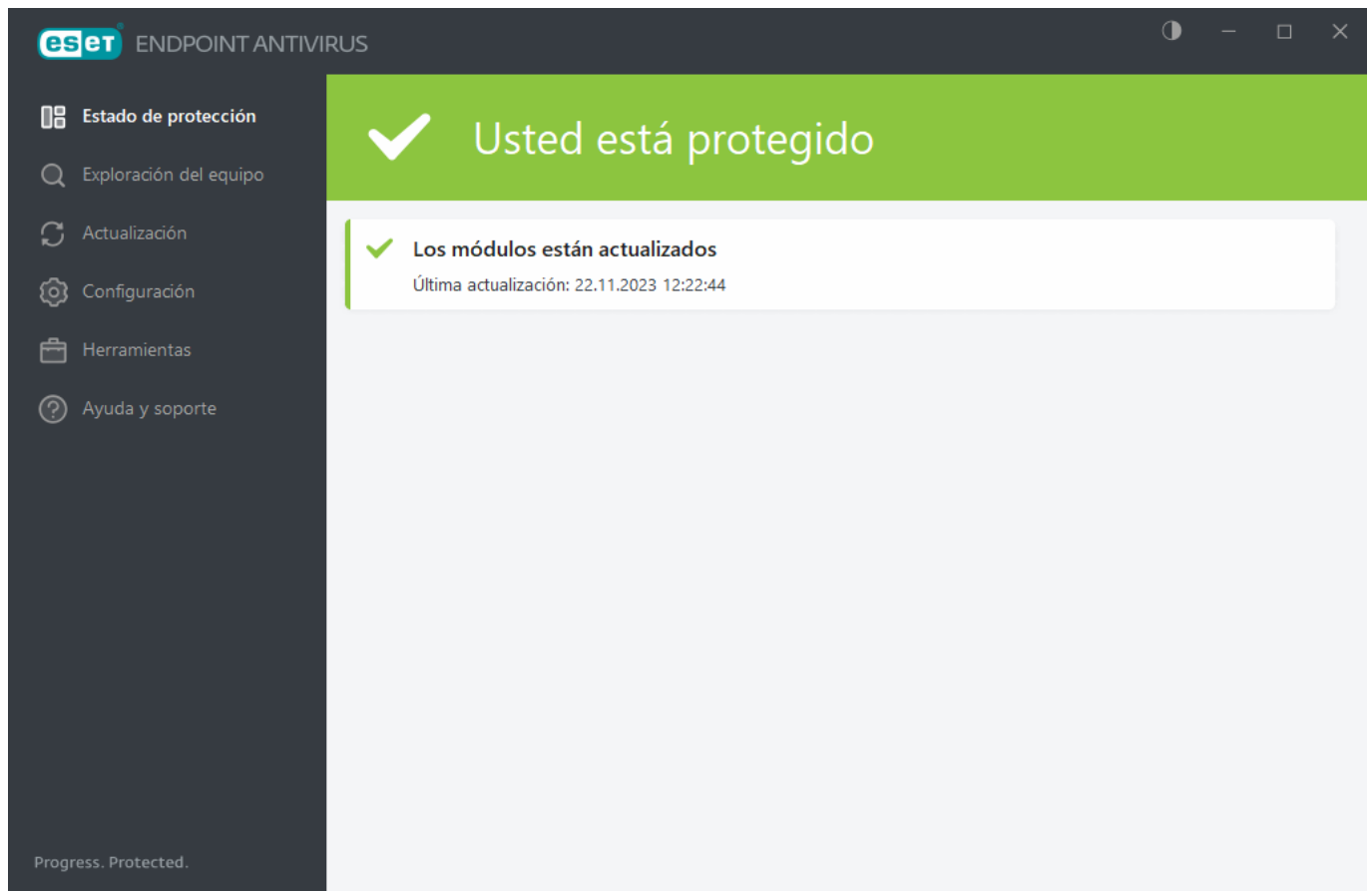
La ventana principal del programa de ESET Endpoint Antivirus se divide en dos secciones. La ventana primaria que está a la derecha muestra información correspondiente a la opción seleccionada en el menú principal de la izquierda.

### 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 Endpoint 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 Endpoint Antivirus según la configuración del sistema operativo.
- **Oscuro**— ESET Endpoint Antivirus tendrá un esquema de colores oscuros (modo oscuro).
- **Claro**— ESET Endpoint Antivirus tendrá un esquema de colores estándar y claro.



Opciones del menú principal:

[Estado de protección](#) – proporciona información sobre el estado de protección de ESET Endpoint 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](#) – Características que ayudan a simplificar la administración del programa y ofrece opciones adicionales para usuarios avanzados.

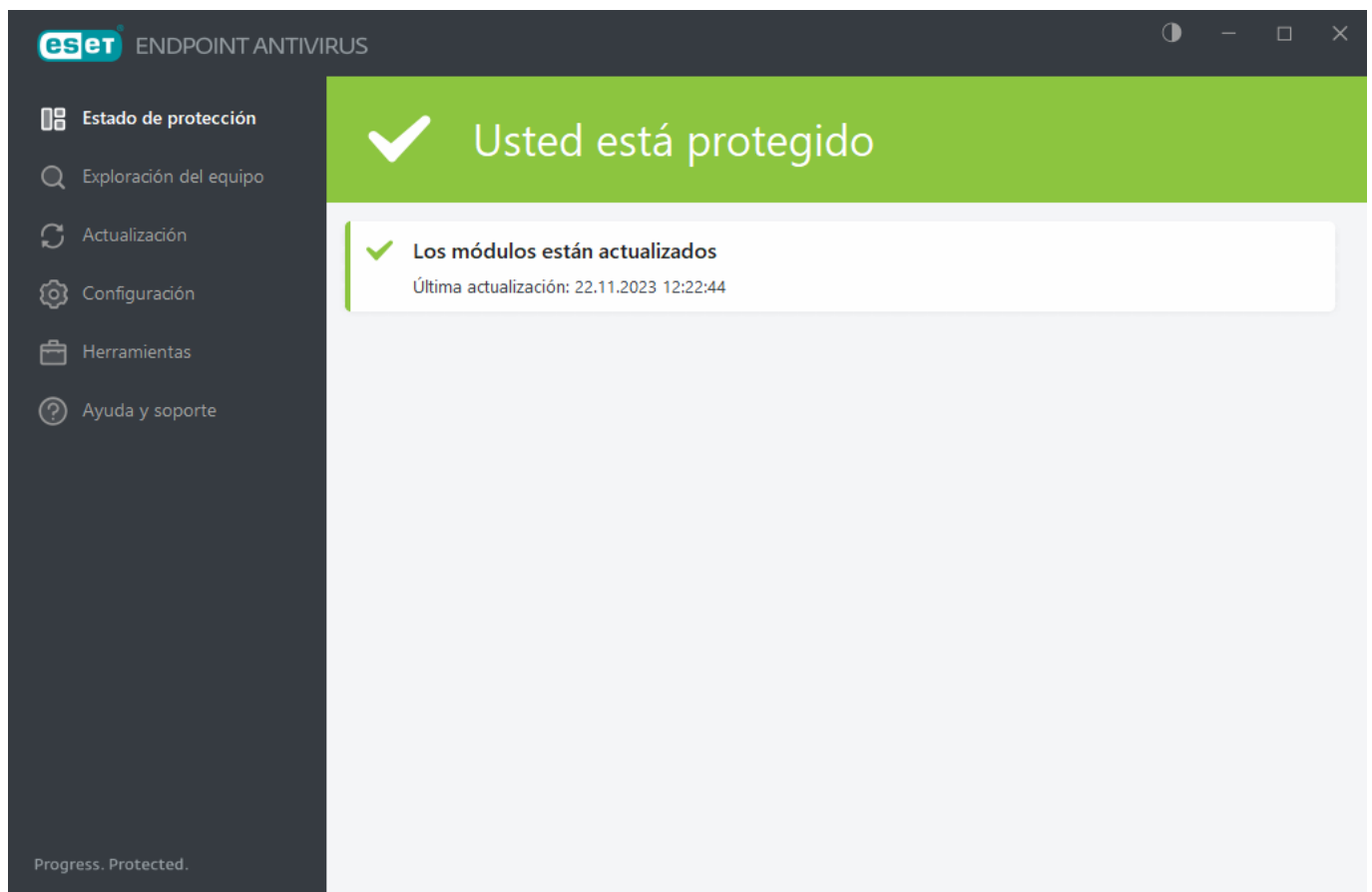
[Configuración](#): ofrece opciones de configuración para las funciones de protección de ESET Endpoint Antivirus y acceso a [Configuración avanzada](#).

[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](#).

## Estado de protección

La ventana **Estado de protección** muestra información sobre la protección actual del equipo y la última actualización. El estado **Protección máxima**, en color verde, indica que la máxima protección está asegurada.

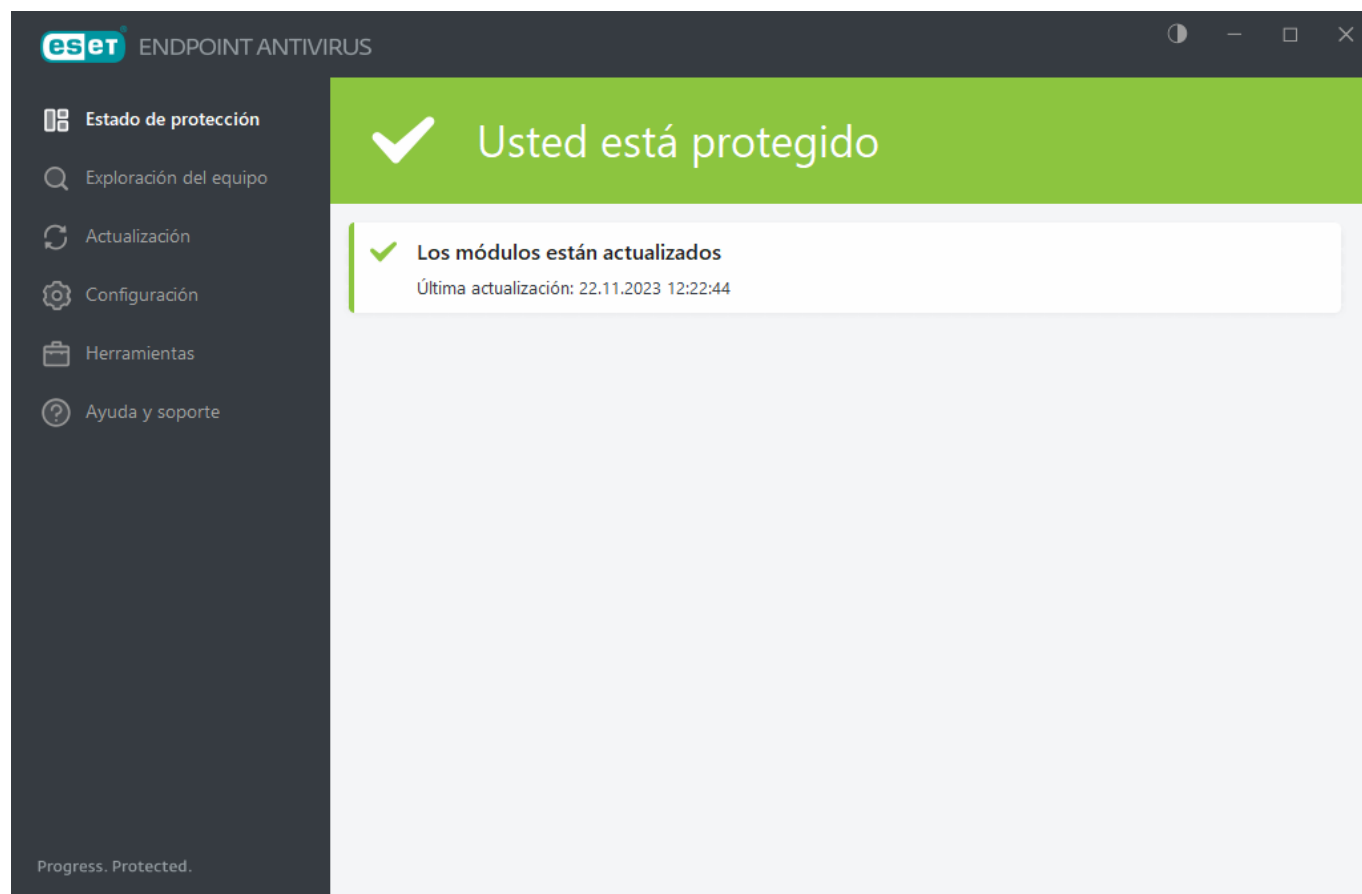
En la ventana **Estado de protección** se muestran [notificaciones](#) con información detallada y soluciones recomendadas para mejorar la seguridad de ESET Endpoint Antivirus, activar funciones adicionales o garantizar la máxima protección.



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

## Qué hacer si el programa no funciona correctamente

Se verá un tilde verde al lado de todos los módulos del programa que son completamente funcionales. Se mostrará un signo de exclamación rojo o un ícono de notificación naranja si un módulo necesitara atención. En la parte superior de la ventana se muestra información adicional sobre el módulo, incluida nuestras recomendaciones sobre cómo restaurar la funcionalidad completa. Para cambiar el estado de un módulo, haga clic en **Configuración** en el menú principal y luego en el módulo deseado.



El ícono rojo con un signo de exclamación (!) indica que la máxima protección del equipo no está asegurada. Puede encontrarse con este tipo de notificación en los siguientes escenarios:

- **La protección antivirus y antispyware está pausada** – Haga clic en **Iniciar todos los módulos de protección antivirus y antispyware** para volver a habilitar la protección antivirus y antispyware en el panel **Estado de la protección** o bien **Habilite la protección antivirus y antispyware** en el panel **Configuración** en la ventana principal del programa.
- **La protección antivirus no es funcional** – Falló la inicialización de escaneo de virus. La mayoría ESET Endpoint Antivirus de los módulos no funcionará correctamente.
- **La protección Anti-Phishing no es funcional** – Esta característica no es funcional porque otros módulos requeridos del programa no están activos.
- **El motor de detección está desactualizado** – Este error aparecerá luego de varios intentos insatisfactorios de actualizar el motor de detección (antes denominado la base de datos de firmas de virus). Es recomendable verificar la configuración de la actualización. El motivo más común de este error es el ingreso incorrecto de los [datos de autenticación](#) o la configuración incorrecta de las [opciones de conexión](#).
- **El producto no está activado o Su 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.

- **Se inhabilitó el Sistema de prevención de intrusiones basado en el host (HIPS, por su sigla en inglés)** – Se indica este problema cuando se inhabilita HIPS. Su computadora no está protegida contra algunos tipos de amenazas y debe volver a habilitarse la protección inmediatamente haciendo clic en **Habilitar HIPS**.
- **No se programaron actualizaciones regulares** – ESET Endpoint Antivirus no buscará o recibirá actualizaciones importantes a menos que usted programe la tarea de actualización.
- **Acceso a la red bloqueado** – Se muestra cuando se activa la tarea de cliente **Aislar equipo de la red** de esta estación de trabajo desde ESET PROTECT. Comuníquese con el administrador para obtener más información.
- **Se pausó la protección del sistema de archivos en tiempo real** – El usuario inhabilitó la protección en tiempo real. Su computadora no está protegida contra amenazas. Haga clic en **Habilitar protección en tiempo real** para volver a habilitar esta funcionalidad.



La «i» en naranja indica que su producto ESET requiere atención por un problema que no es crítico. Las razones posibles incluyen:

- **La protección del acceso a la Web está inhabilitada** – Haga clic en la notificación de seguridad para volver a habilitar la protección del acceso a la Web y luego haga clic en **Habilitar protección del acceso a la Web**.
- **La licencia se vencerá pronto/Su licencia vence hoy:** se indica mediante un ícono de estado de protección y un signo de exclamación. Una vez que se vence la licencia, el programa no podrá actualizarse y el ícono de estado de protección se pondrá rojo.
- **El antispam del cliente de correo electrónico está en pausa:** haga clic en **Habilitar el antispam del cliente de correo electrónico** para volver a habilitar esta función.
- **Se pausó el control Web** – Haga clic en **Habilitar control Web para volver a habilitar esta característica**.
- **Anulación de política activa**– La configuración establecida por la política se encuentra temporalmente anulada, posiblemente hasta finalizar la resolución de problemas. Solo el usuario autorizado puede anular la configuración de la política. Para obtener más información, consulte [Cómo utilizar el modo Anulación](#).
- **Se pausó el control del dispositivo** – Haga clic en **Habilitar control del dispositivo** para volver a habilitar esta característica.

Para ajustar la visibilidad en los estados del producto en el primer panel de ESET Endpoint Antivirus, consulte [Estados de la aplicación](#).

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 solicitud de soporte técnico de ESET. El Soporte técnico de ESET responderá rápidamente a sus preguntas y lo ayudará a encontrar una resolución.

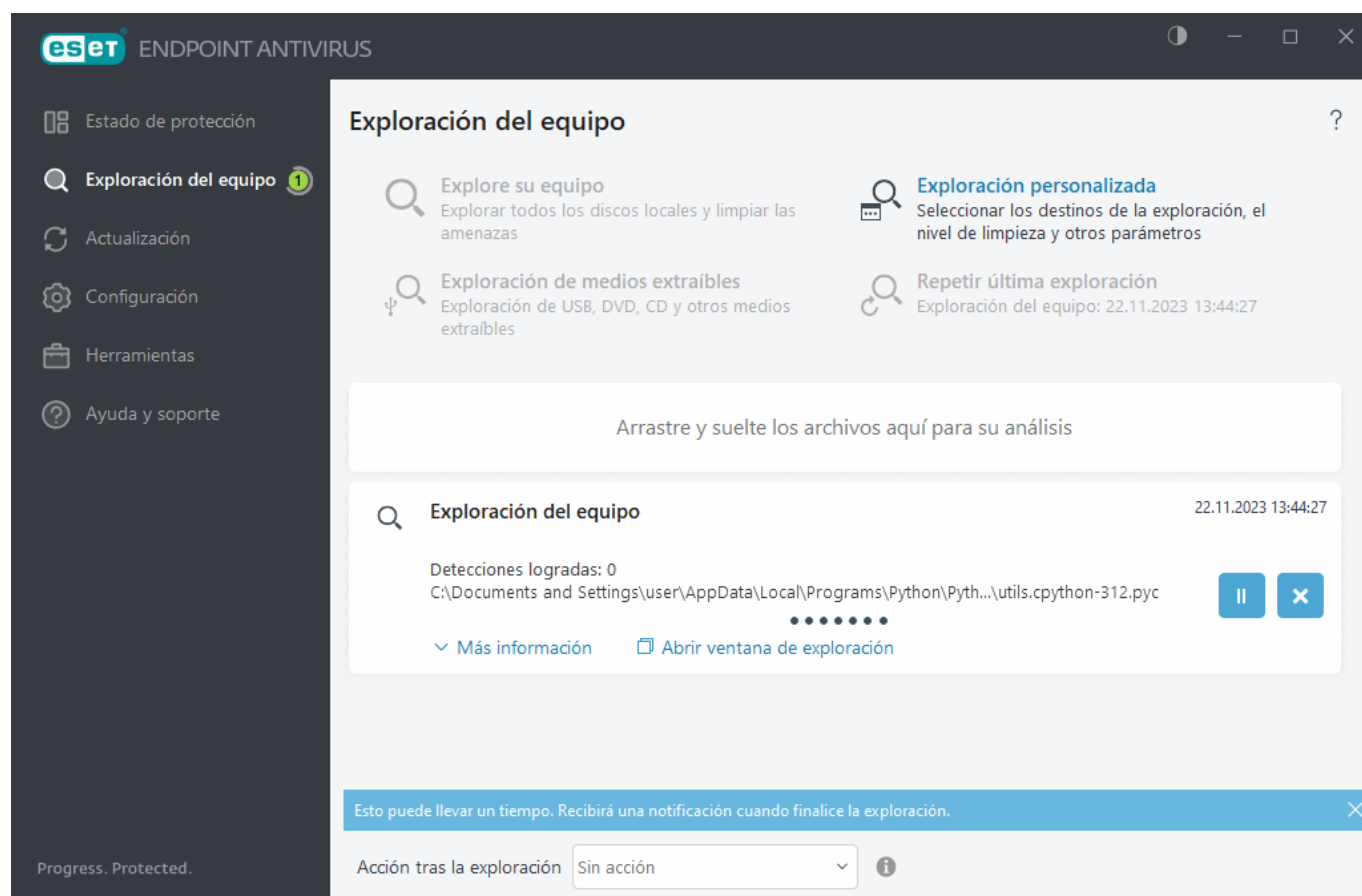


Si un estado pertenece a una característica bloqueada por la política ESET PROTECT, no se podrá hacer clic en el enlace.

## Exploración del equipo

El módulo de exploración bajo demanda es una parte importante de ESET Endpoint Antivirus. Se usa para realizar la exploración de los archivos y las carpetas del equipo. Desde el punto de vista de la seguridad, es esencial que las exploraciones del equipo no se ejecuten solo cuando existen sospechas de una infección, sino en forma habitual como parte de una medida de seguridad de rutina. Recomendamos que realice exploraciones profundas de manera regular (por ejemplo, una vez al mes) en su sistema para detectar los virus que no haya detectado la [Protección del sistema de archivos en tiempo real](#). Esto puede ocurrir si la Protección del sistema de archivos en tiempo real se deshabilitó en algún momento, si el motor de detección era obsoleto o si el archivo no se detectó

como virus cuando se guardó en el disco.



Se encuentran disponibles dos tipos de **Exploración del equipo**. **Exploración del equipo** explora rápidamente el sistema sin necesidad de realizar configuraciones adicionales de los parámetros de exploración. La **Exploración personalizada** le permite seleccionar cualquiera de los perfiles de exploración predefinidos y definir objetos específicos para la exploración.

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

## 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** le permite especificar los parámetros de la exploración, como objetivos y métodos de exploración. 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.



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).

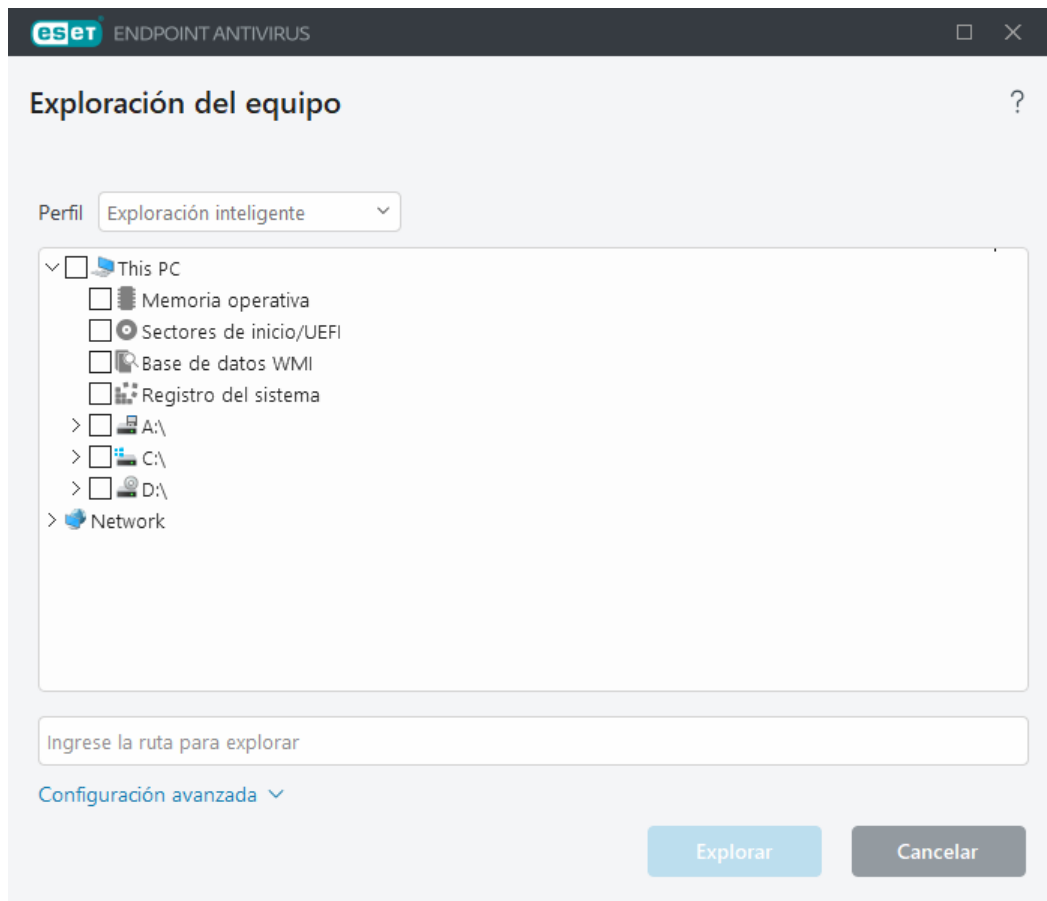
En el menú desplegable **Perfil**, puede elegir un perfil que podrá usar al explorar objetos específicos. El perfil predeterminado es **Análisis inteligente**. Hay otros tres perfiles de exploración predefinidos denominados **Exploración exhaustiva**, **Exploración del menú contextual** y **Exploración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



Puede configurar los parámetros de limpieza para la exploración en [Configuración avanzada](#) > **Motor de detección** > **Exploración de malware** > **Exploración a demanda** > **ThreatSense** > **Desinfección**. 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. Puede encontrar más detalles en nuestro [artículo de la base de conocimiento](#).



## Cómo programar una exploración semanal del equipo

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

**Progreso de la exploración:** la barra de progreso muestra el estado de la exploración en ejecución.

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

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

Haga clic en Más información para mostrar la siguiente información:

- **Usuario:** nombre de la cuenta de usuario que inició la exploración.
- **Objetos explorados:** cantidad de objetos ya explorados.
- **Duración:** tiempo transcurrido.

Icono de pausa: pausa una exploración.

Reanudar: esta opción se muestra cuando el progreso de la exploración está en pausa. Haga clic en el icono para continuar explorando.

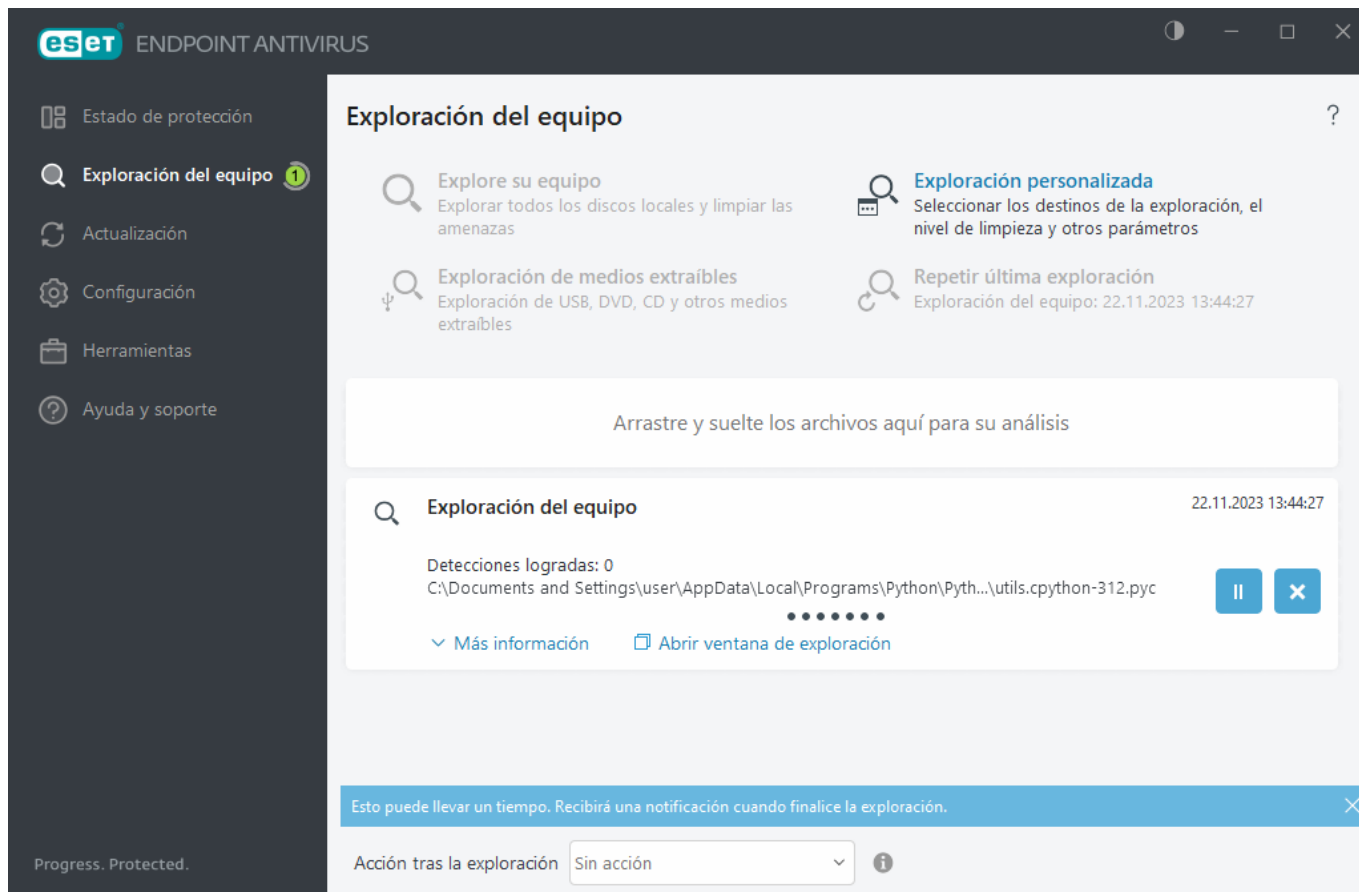
Icono de detención: finaliza la exploración.

Haga clic en la **ventana Abrir exploración** para abrir el [registro de escaneo del equipo](#) con más detalles sobre 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**.



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 exploración del equipo

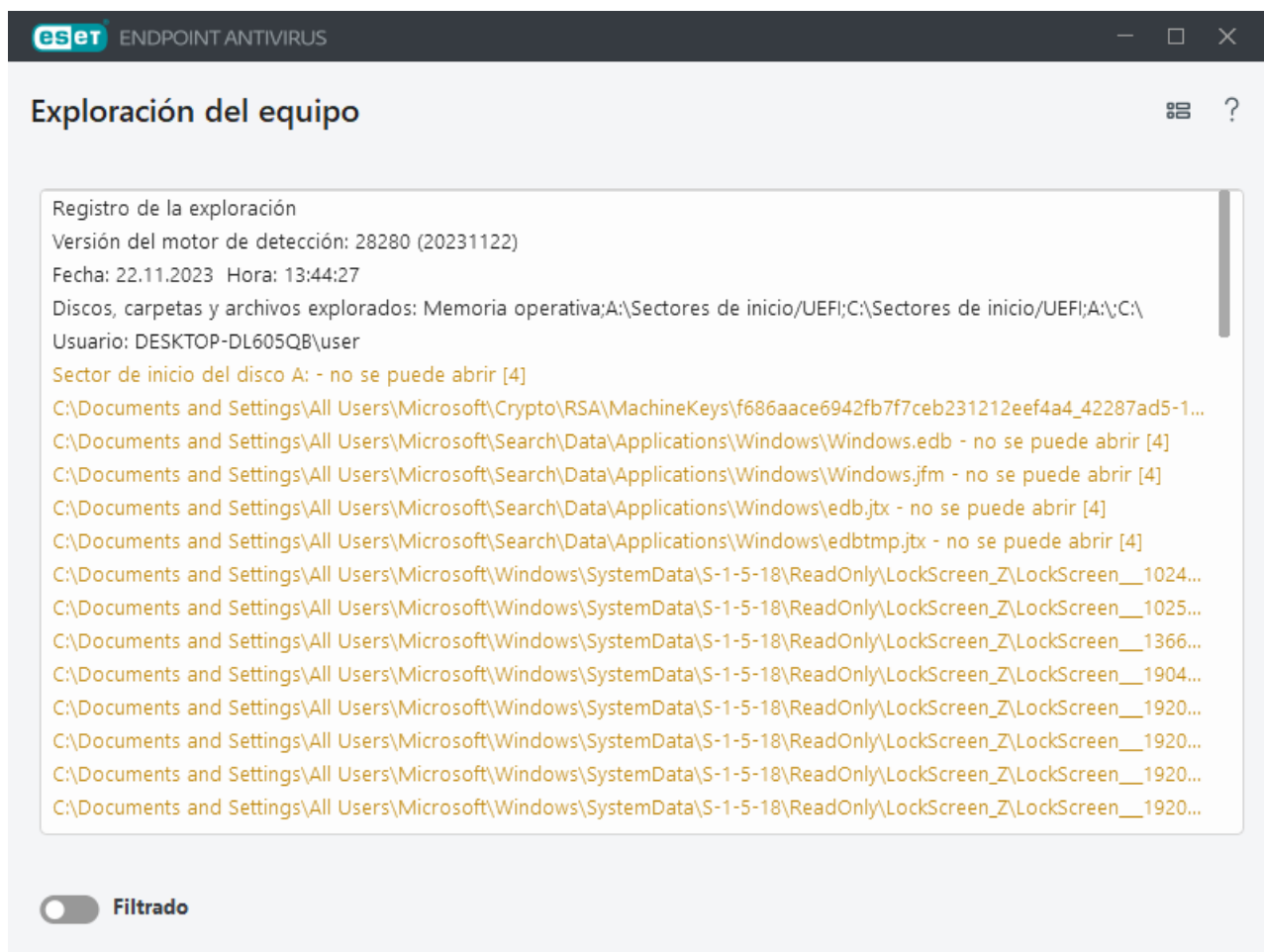
Puede ver información detallada relacionada con una exploración específica en [Archivos de registro](#). El registro la exploración contiene la siguiente información:

- 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](#))
- Usuario que inició la exploración.
- 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.



**i** 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 del interruptor  **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: <b>Ctrl+Shift+F</b>
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: <b>Ctrl+C</b>
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.

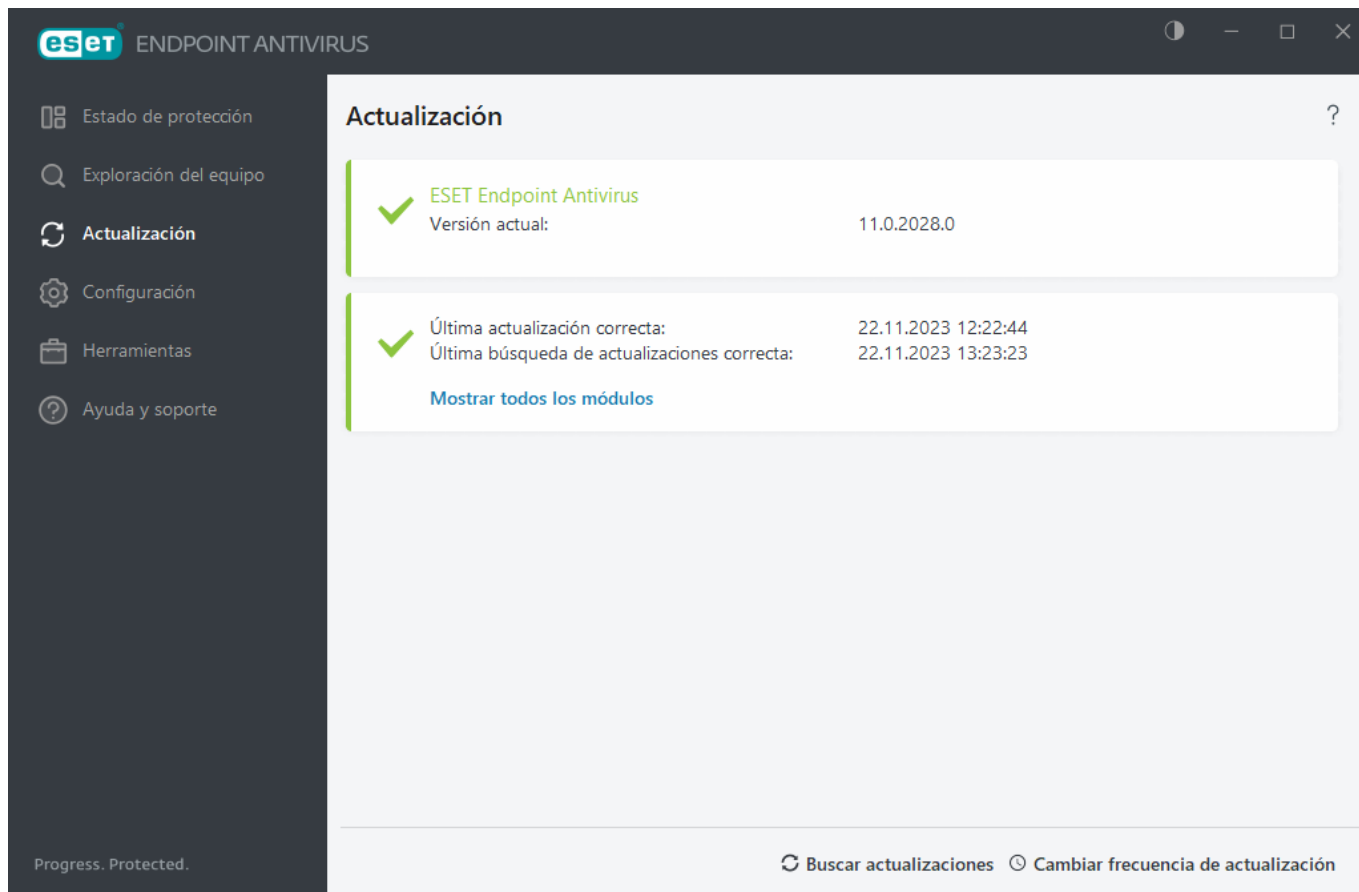
## Actualización

La actualización habitual de ESET Endpoint 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 [activar ESET Endpoint Antivirus](#) 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 Endpoint Antivirus.

Si activa ESET Endpoint Antivirus con un archivo de licencia sin conexión y sin nombre de usuario ni contraseña, y trata de realizar una actualización, la información de color rojo **La actualización de los módulos finalizó con un error** le indica que solo puede descargar actualizaciones desde el mirror.



**Versión actual** – el ESET Endpoint Antivirus número de compilación.

**Última actualización exitosa:** la fecha y hora de la última actualización exitosa. Asegúrese de que la fecha sea reciente, lo que significa que el motor de detección está al día.

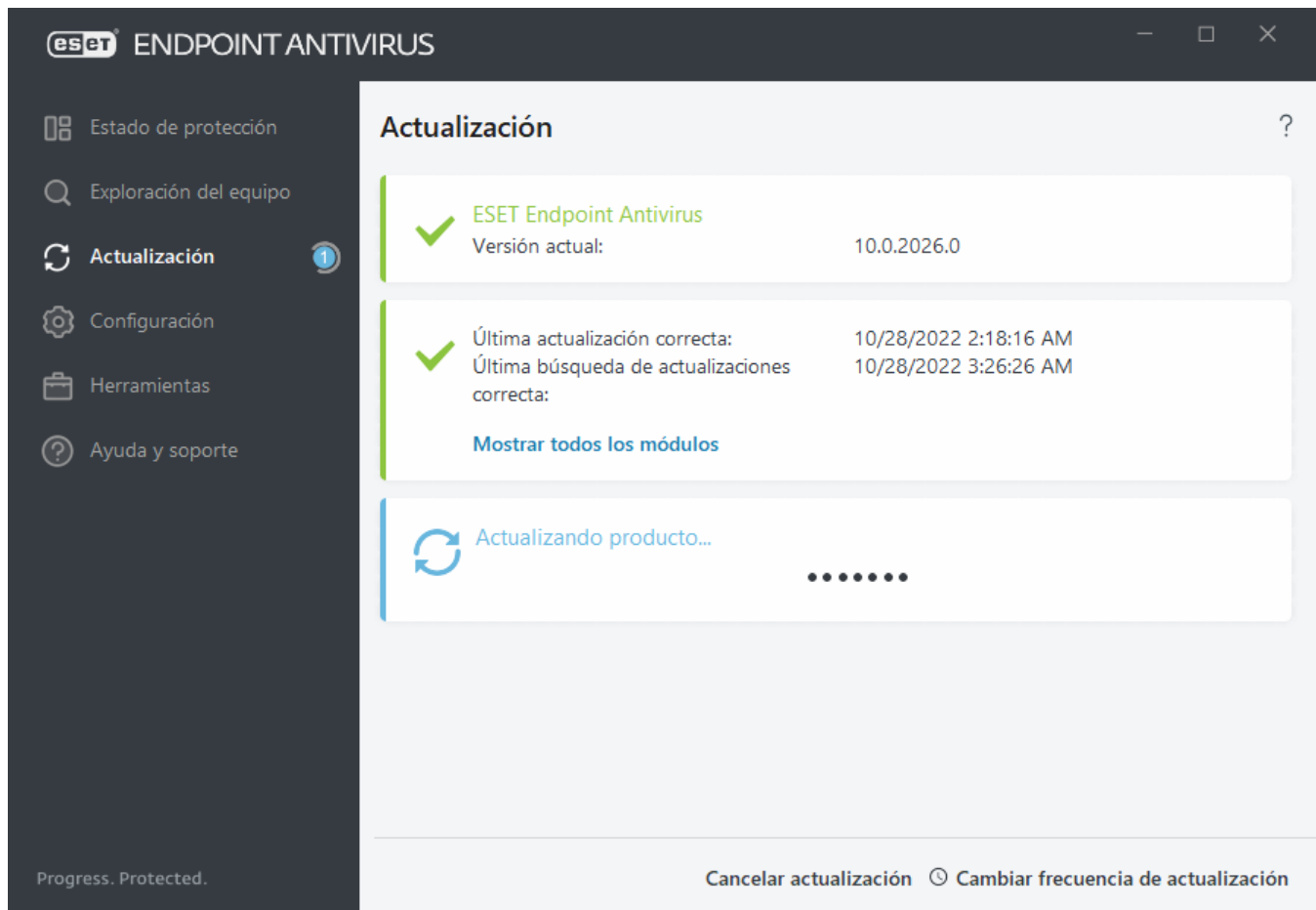
**Última búsqueda exitosa de actualizaciones:** es la fecha y hora del último intento de actualización de módulos exitoso.

**Mostrar todos los módulos** – haga clic en el enlace para abrir la lista de módulos instalados y comprobar la versión y la última actualización de un módulo.

---

## 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.

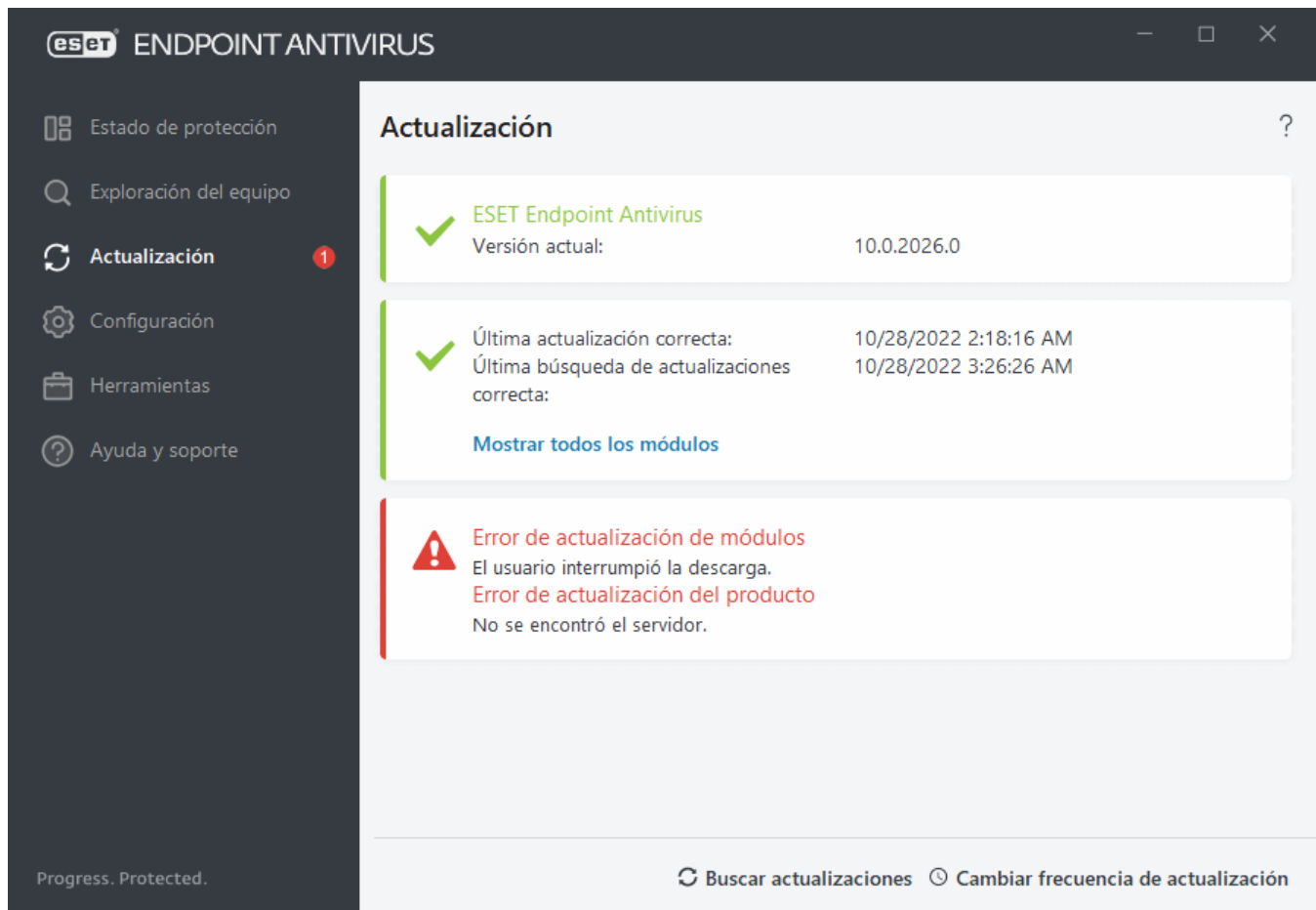
## Última actualización exitosa

**El motor de detección está desactualizado:** este error aparecerá luego de varios intentos insatisfactorios de actualizar los módulos. 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](#).

La notificación anterior está relacionada con los dos mensajes siguientes **Falló la actualización de los módulos** sobre actualizaciones insatisfactorias que se detallan a continuación:

1. **Licencia no válida:** su licencia no está activa. Recomendamos que verifique sus datos de autenticación. Haga clic en **Ayuda y soporte > Administrar licencia** en el menú principal para ingresar una clave de licencia nueva.
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. Asegúrese de tener una conexión a Internet activa desde su Proveedor de servicios de Internet (ISP).





 Para obtener más información, consulte el [artículo de la base de conocimiento de ESET](#).

## 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 de actualización se encuentran activas en forma predeterminada en ESET Endpoint Antivirus:

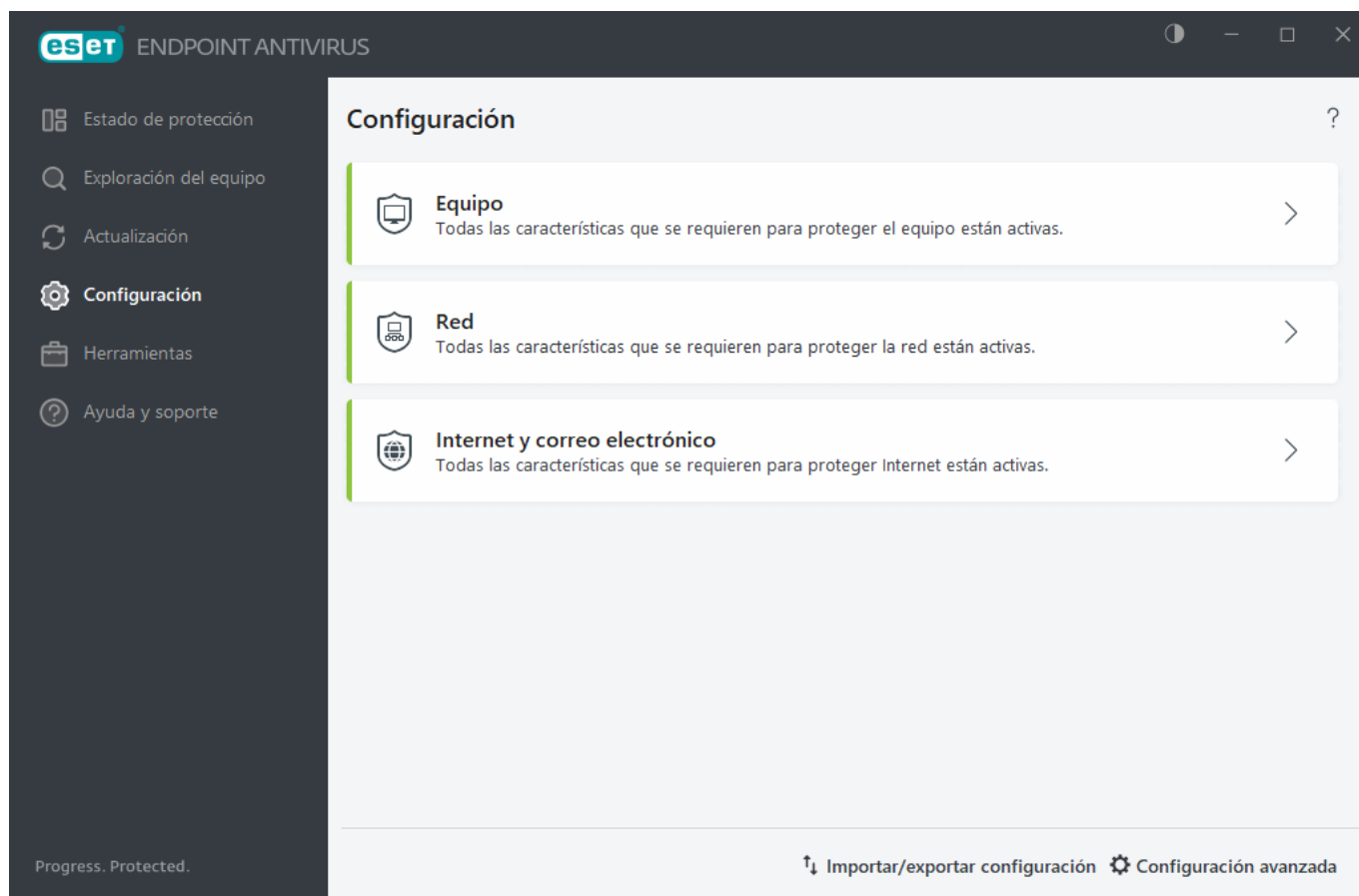
- **Actualización automática de rutina**
- **Actualización automática luego del registro del usuario**

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](#).

## Configuración

Puede encontrar grupos de funciones de protección disponibles en la [ventana principal del programa > Configuración](#).

**i** Cuando cree una política desde la Consola Web de ESET PROTECT, puede seleccionar el indicador para cada configuración. Las configuraciones con el indicador Forzar tienen prioridad y no se pueden sobrescribir por una política posterior (incluso si la política posterior tiene un indicador Forzar). Esto garantiza que no se modificarán las configuraciones (por ejemplo, por el usuario o por políticas posteriores durante una fusión). Para obtener más información, consulte [Indicadores en la Ayuda en línea de ESET PROTECT](#).




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

[Equipo](#)

[Red](#)

[Internet y correo electrónico](#)

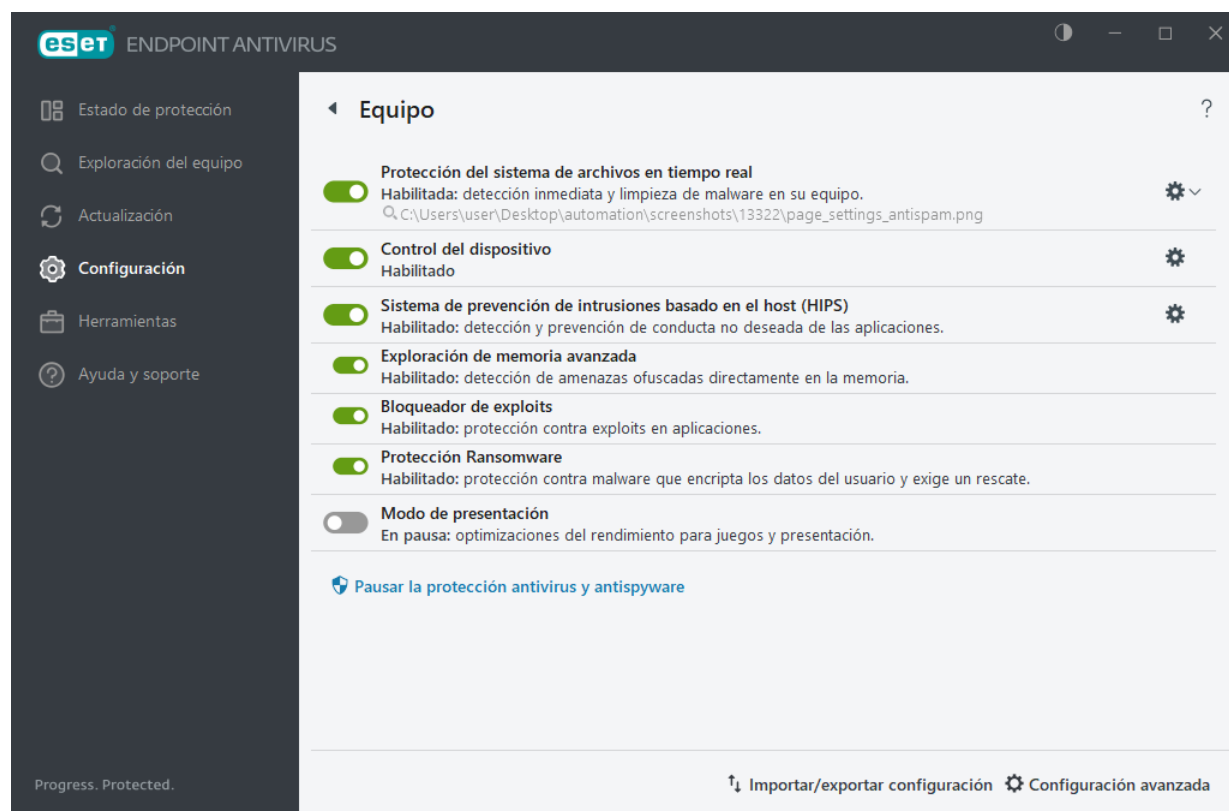
Cuando se aplique la política de ESET PROTECT, verá el ícono de candado  al lado de un componente específico. La política aplicada por ESET PROTECT puede anularse localmente tras la autenticación por el usuario registrado (p. ej. administrador). Para obtener más información, consulte [ESET PROTECT Ayuda en línea](#).

**i** Todas las medidas de protección que se deshabiliten de esta forma, se volverán a habilitar luego del reinicio del equipo.


Hay opciones adicionales disponibles en la parte inferior de la ventana de configuración. Haga clic en [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](#).

# Equipo

Haga clic en **Equipo** en la [ventana del programa principal](#) > **Configuración** para ver una descripción general de todos los módulos de protección:




En la sección **Equipo** puede habilitar o deshabilitar los siguientes componentes:

- [Protección del sistema de archivos en tiempo real](#) – se exploran todos los archivos en busca de códigos maliciosos cuando se abren, crean o ejecutan en el equipo. Haga clic en la icono de engranaje  junto a Protección del sistema de archivos en tiempo real y haga clic en Editar exclusiones para abrir la [Ventana de configuración de exclusiones](#), que le permite excluir archivos y carpetas de la exploración. Para abrir la configuración avanzada de la Protección del sistema de archivos en tiempo real, haga clic en Configurar.
- [Control del dispositivo](#): 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.
- [Host Intrusion Prevention System \(HIPS\)](#) – el sistema [HIPS](#) monitorea los sucesos que ocurren dentro del sistema operativo y reacciona a ellos según un grupo de reglas personalizado.
- La **Exploración de memoria avanzada**: 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](#).
- **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](#).
- **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](#).
- [Modo de presentación](#) – una función para los usuarios que requieren usar el software en forma

ininterrumpida, que no desean que las ventanas emergentes los molesten y que quieren minimizar el uso de la CPU. Recibirá un mensaje de advertencia (riesgo potencial en la seguridad) y la ventana principal del programa se pondrá de color naranja una vez habilitado el [Modo de presentación](#).

**Pausar la protección antivirus y antispyware** – cuando deshabilite temporalmente la protección antivirus y antispyware, puede seleccionar el periodo de tiempo por el que desea que el componente seleccionado esté deshabilitado mediante el uso del menú desplegable y, luego, haga clic en **Aplicar** para deshabilitar el componente de seguridad. Para volver a habilitar la protección, haga clic en **Habilitar la protección antivirus y antispyware**.

Para pausar o desactivar módulos de protección individuales, haga clic en el ícono de interruptor .

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

## Se detecta una amenaza

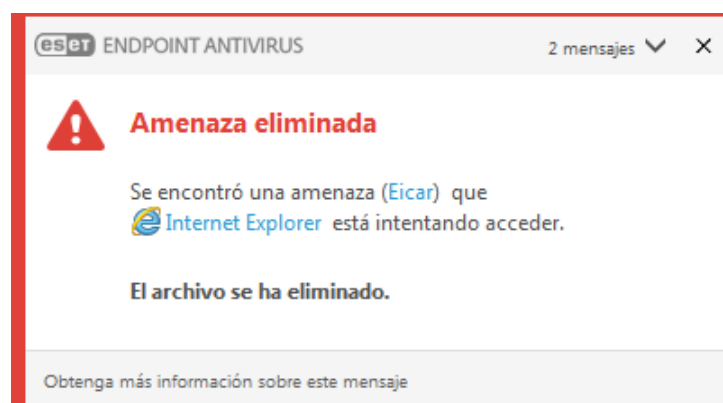
Las infiltraciones pueden llegar al sistema desde diversos puntos de entrada, como [páginas Web](#), carpetas compartidas, correo electrónico o [dispositivos extraíbles](#) (USB, discos externos, CD, DVD, etc.).

## Conducta estándar

Como ejemplo general de la forma en que ESET Endpoint 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 [Desinfección](#).



## Desinfección y eliminación:

Si no hay ninguna acción predefinida para la protección del sistema de archivos en tiempo real, el programa le

pedirá que seleccione una opción en una ventana de alerta. Por lo general están disponibles las opciones **Desinfectar**, **Eliminar** y **Sin acción**. No se recomienda seleccionar **Sin acción**, ya que esto dejará los archivos infectados sin desinfectar. La excepción a este consejo es cuando usted está seguro de que un archivo es inofensivo y fue detectado por error.



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

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

## Restauración desde Cuarentena

Para acceder a la cuarentena, diríjase a la ventana principal del programa ESET Endpoint 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 la acción para dichos archivos.

## Eliminación de archivos en archivos comprimidos

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


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


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


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

## Red

Abra la [ventana del programa principal](#) > **Configuración** > **Red** para configurar las opciones básicas de protección de red o solucionar problemas de comunicación.

Para pausar o desactivar módulos de protección individuales, haga clic en el ícono de interruptor .

 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.

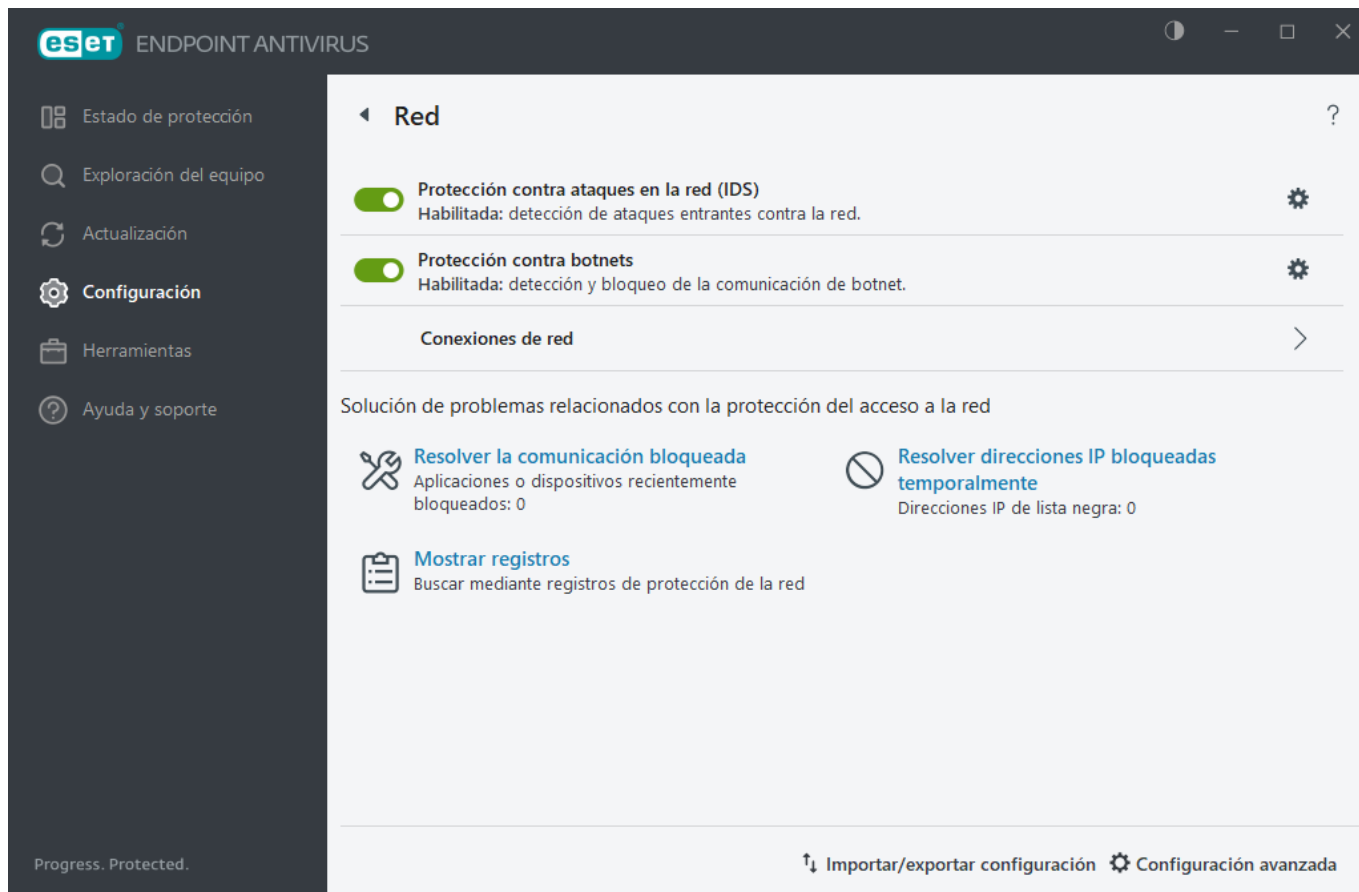
[Protección contra ataques a la red \(IDS\)](#) – Analiza el contenido del tráfico de red y protege de ataques en la red. Se bloquea cualquier tráfico considerado perjudicial. ESET Endpoint Antivirus le informa cuando se conecta a una red inalámbrica desprotegida o a una red con protección débil.

**Protección contra Botnet:** identifica de manera rápida y precisa el malware en el sistema.

**Resolver la comunicación bloqueada** – le ayuda a resolver los problemas de conectividad causados por el firewall de ESET. Para obtener información más detallada, consulte el [Asistente para solución de problemas](#).

**Resolver direcciones IP bloqueadas temporalmente** – ver una [lista de direcciones IP que han sido detectadas como la fuente de ataques y agregadas a la lista negra](#) para bloquear la conexión durante cierto período de tiempo.

**Mostrar registros:** abre el [archivo Registro](#) de la Protección de red.



## Solución de problemas de acceso a la red

El Asistente para la resolución de problemas le ayuda a resolver problemas de conectividad causados por el Firewall. La **solución de problemas de acceso a la red** se puede encontrar en la [ventana del programa principal](#) > **Configuración** > **Red** > **Resolver comunicación bloqueada**.

Seleccione si desea mostrar la comunicación bloqueada para **aplicaciones locales** o la comunicación bloqueada desde **dispositivos remotos**.

Desde el menú desplegable, seleccione el tiempo durante el que la comunicación se ha bloqueado. El listado de comunicaciones bloqueadas recientemente le brinda una vista general del tipo de aplicación o dispositivo, reputación y cantidad total de aplicaciones y dispositivos bloqueados durante dicho período. Para más detalles sobre comunicaciones bloqueadas, haga clic en **Detalles**. El siguiente paso es desbloquear la aplicación o dispositivo con el que está experimentando problemas de conectividad.

Al hacer clic en **Desbloquear**, se permitirá la comunicación que estaba bloqueada. Si los problemas con una aplicación continúan o si su dispositivo no funciona como debería, haga clic en **crear otra regla** y se permitirán todas las comunicaciones para ese dispositivo que estaban bloqueadas. Si el problema persiste, reinicie el equipo.



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

- [Agregar una excepción mediante el Asistente para solución de problemas](#)



Si no se puede crear la regla, recibirá un mensaje de error. Haga clic en **Intentar de nuevo** y repita el proceso para desbloquear la comunicación o cree otra regla de la lista de comunicaciones bloqueadas.

# Lista negra temporal de direcciones IP

Las direcciones IP que han sido detectadas como fuentes de ataques son agregadas a la Lista negra para prevenir la conexión durante un cierto período de tiempo, abra [ventana del programa principal](#) > **Configuración** > **Protección de red** > **Resolver direcciones IP bloqueadas temporalmente**. Las direcciones IP bloqueadas de manera temporal se bloquean durante 1 hora.

## Columnas

**Direcciones IP:** muestra las direcciones IP que han sido bloqueadas.

**Motivo del bloqueo:** muestra el tipo de ataque que se ha prevenido de la dirección (por ejemplo, ataque de exploración de puerto TCP).

**Tiempo de espera:** muestra la hora y fecha en la cual la dirección expirará de la lista negra.

## Elementos de control

**Eliminar:** haga clic para eliminar una dirección de la lista negra antes de que expire.

**Quitar todas:** haga clic para quitar todas las direcciones de la lista negra inmediatamente.

**Agregar excepción:** haga clic para agregar una excepción del firewall al filtrado de IDS.

# Registros de protección de red

La protección de red ESET Endpoint Antivirus guarda todos los eventos importantes en un archivo de registro. Para ver el archivo de registro, abra [ventana del programa principal](#) > **Configuración** > **Red** > **Mostrar registros**.

Los archivos de registro se pueden usar para detectar errores y revelar intrusiones en el sistema. Los registros de protección de red contienen los siguientes datos:

- Fecha y la hora del suceso
- Nombre del suceso
- Fuente
- Dirección de red de destino
- Protocolo de comunicación de red
- La regla aplicada o, si se identificó el gusano, su nombre
- Ruta de la aplicación y nombre
- Hash
- Usuario
- Firmante de la aplicación (editor)
- Nombre del paquete
- Nombre del servicio

Un análisis completo de estos datos puede ayudar a detectar intentos de comprometer la seguridad del sistema. Existen muchos otros factores que indican riesgos de seguridad potenciales y permiten minimizar su impacto: conexiones frecuentes desde ubicaciones remotas, intentos reiterados de establecer conexiones, comunicaciones de aplicaciones desconocidas o el uso de números de puerto inusuales.



### Explotación de la vulnerabilidad de la seguridad



El mensaje de ataque de vulnerabilidad a la seguridad se registra incluso cuando se soluciona la vulnerabilidad específica, ya que se detecta el intento de ataque y se lo bloquea a nivel de la red antes de que el ataque real pueda tener lugar.

## Solución de problemas con la protección de red de ESET

Si experimenta problemas de conectividad con ESET Endpoint Antivirus instalado, existen varias maneras de identificar si el Protección de la red de ESET es el causante del problema. Además, el Protección de la red puede ayudarle a crear nuevas reglas o excepciones para resolver los problemas de conectividad.

Consulte los siguientes temas de ayuda para resolver los problemas con el Protección de la red de ESET:

- [Solución de problemas de acceso a la red](#)
- [Registro y creación de reglas o excepciones desde el registro](#)
- [Registro avanzado de protección de red](#)
- [Resolución de problemas con el explorador de tráfico de red](#)

## Registro y creación de reglas o excepciones desde el registro

De forma predeterminada, el Firewall de ESET no registra todas las conexiones bloqueadas. Si desea ver lo que bloqueó la protección de red, abra [Configuración avanzada](#) > **Herramientas** > **Diagnósticos** > **Registro avanzado** y habilite **Habilitar el registro avanzado de la protección de red**. Si ve algo en el registro que no desea que el Firewall bloquee, puede crear una regla o una regla del sistema de detección de intrusiones al hacer clic derecho en ese elemento y seleccionar **No bloquear eventos similares en el futuro**. Tenga en cuenta que el registro de todas las conexiones bloqueadas puede contener miles de elementos y es posible que sea difícil encontrar una conexión específica en este registro. Puede desactivar el registro luego de haber solucionado su problema.

Para obtener más información acerca del registro consulte los [Archivos de registro](#).



Use los registros para ver el orden en que el Protección de red bloqueó las conexiones específicas. Además, la creación de reglas desde los registros le permite crear reglas que hagan exactamente lo que usted desee.

## Crear regla a partir del registro

La nueva versión de ESET Endpoint Antivirus le permite crear una regla a partir del registro. Desde el menú principal, haga clic en **Herramientas** > **Archivos de registro**. Elija **Protección de la red** del menú desplegable, haga clic derecho en la entrada de registro deseada y seleccione **No bloquear sucesos similares en el futuro** del menú contextual. Una ventana de notificación mostrará su regla nueva.

Para permitir la creación de reglas nuevas a partir del registro, ESET Endpoint Antivirus debe establecerse con las siguientes configuraciones:

1. Ajustar el nivel de detalle mínimo para los registros a **Diagnóstico** en [Configuración avanzada](#) > **Herramientas** > **Archivos de registro**.
2. Active **Mostrar notificaciones para ataques entrantes frente a agujeros de seguridad** en [Configuración](#)

## Registro avanzado de protección de red

Esta característica tiene como propósito brindar archivos de registro más complejos para el soporte técnico de ESET. Use esta característica solo cuando el soporte al cliente de ESET se lo solicite, ya que puede generar un archivo de registro inmenso y así ralentizar su equipo.

1. Abrir [Configuración avanzada](#) > **Herramientas** > **Diagnósticos** y active **Habilitar el registro avanzado de protección de red**.
2. Intente reproducir el problema que está experimentando.
3. Deshabilite el registro avanzado de protección de red.
4. El archivo de registro PCAP creado por el registro avanzado de protección de red se puede encontrar en el mismo directorio donde se generan los volcados de memoria de diagnóstico: `C:\ProgramData\ESET\ESET Security\Diagnostics\`

## Resolución de problemas con el explorador de tráfico de red

Si experimenta problemas con su navegador o cliente de correo electrónico, el primer paso es determinar si el responsable es el explorador de tráfico de red. Para hacer eso, intente deshabilitar temporalmente la exploración del tráfico de red en [Configuración avanzada](#) > **Motor de detección** > **Explorador de tráfico de red** (recuerde activarlo nuevamente una vez finalizado ya que, de lo contrario, su navegador y cliente de correo electrónico permanecerán desprotegidos). Si el problema desaparece una vez desactivado, aquí hay una lista de problemas comunes y formas para resolverlos:

### Actualizar o asegurar problemas de comunicación

Si su aplicación se queja de la incapacidad de actualizar o de que un canal de comunicación no es seguro:

- Si tiene [SSL/TLS](#) habilitado, intente desactivarlo temporalmente. Si eso ayuda, puede continuar utilizando SSL/TLS y hacer que la actualización funcione al excluir la comunicación problemática:  
Deshabilitar SSL/TLS. Vuelva a ejecutar la actualización. Debería aparecer un cuadro de diálogo para informarle acerca del tráfico de red cifrado. Asegúrese de que la aplicación se ajuste a la que está intentando resolver y que el certificado parezca que proviene del servidor del que se está actualizando. Luego, elija recordar la acción para este certificado y haga clic en ignorar. Si no se muestran más cuadros de diálogo relevantes, puede cambiar el modo de filtrado a automático y el problema debería resolverse.
- Si la aplicación en cuestión no es un navegador o cliente de correo electrónico, puede excluirla por completo de [protección de acceso a la web](#) (hacer esto en el navegador o cliente de correo electrónico lo dejaría expuesto). Cualquier aplicación cuya comunicación haya sido filtrada en el pasado debería estar en la lista provista a usted cuando agrega la excepción, por lo que agregar una de forma manual no debería ser necesario.

## Problema para acceder a un dispositivo de su red

Si no puede usar ninguna funcionalidad de un dispositivo en su red (esto podría significar abrir una página web de su cámara web o reproducir un video en un reproductor multimedia doméstico), intente agregar sus direcciones IPv4 y IPv6 a la lista de direcciones excluidas.

## Problemas con un sitio Web específico

Puede excluir sitios Web específicos de la [protección de acceso a la web](#) con la gestión de direcciones URL. Por ejemplo, si no puede acceder a <https://www.gmail.com/intl/en/mail/help/about.html>, intente agregar \*gmail.com\* a la lista de direcciones excluidas.

## Error “Algunas de las aplicaciones aptas para importar el certificado raíz siguen activas”

Cuando habilita SSL/TLS, ESET Endpoint Antivirus se asegura de que las aplicaciones instaladas confían en la forma en que se filtra el protocolo SSL al importar un certificado a su almacén de certificados. Es posible que algunas aplicaciones requieran un reinicio para importar un certificado. Esto incluye a Firefox y Opera. Asegúrese de que ninguna de ellas esté activa (la mejor manera de hacer esto es abrir el Administrador de tareas y asegurarse de que firefox.exe u opera.exe no estén en la pestaña de Procesos), luego vuelva a intentarlo.

## Error acerca de un emisor no confiable o de una firma no válida

Lo más probable es que esto signifique que falló la importación antes mencionada. Primero, asegúrese de que ninguna de las aplicaciones mencionadas esté activa. A continuación, desactive SSL/TLS y vuelva a activarlo. Esto vuelve a ejecutar la importación.

## Se bloqueó una amenaza de red

Esta situación puede ocurrir cuando una aplicación en su equipo está intentando transmitir tráfico malicioso a otro dispositivo en la red, está explotando una vulnerabilidad de seguridad o incluso si se detecta un intento de exploración de los puertos en su sistema.

Puede encontrar el tipo de amenaza y la dirección IP del dispositivo relacionado en la notificación. Haga clic en **Cambiar el manejo de esta amenaza** para mostrar las siguientes opciones:

**Continuar con el bloqueo:** bloquea la amenaza detectada. Si desea dejar de recibir notificaciones sobre este tipo de amenaza desde la dirección remota específica, seleccione el botón de opción situado junto a **No notificar** antes de hacer clic en **Continuar con el bloqueo**. Al hacerlo, se creará una [regla de servicio de detección de intrusiones \(IDS\)](#) con la siguiente configuración: **Bloquear** - predeterminado, **Notificar** - no, **Registrar** - no.

**Permitir:** crea una [regla de servicio de detección de intrusiones \(IDS\)](#) para permitir la amenaza detectada. Seleccione una de las siguientes opciones antes de hacer clic en **Permitir** para especificar la configuración de la regla:

- **Notificar únicamente cuando se bloquea esta amenaza** — Configuración de la regla: **Bloquear** - no, **Notificar** - no, **Registrar** - no.
- **Notificar siempre que esta amenaza ocurra** — Configuración de la regla: **Bloquear** - no, **Notificar** -

predeterminado, **Registrar** - predeterminado.

- **No notificar** — Configuración de la regla: **Bloquear** - no, **Notificar** - no, **Registrar** - no.


La información que se muestre en la ventana de notificación puede variar en base al tipo de amenaza detectada.

**i** Para obtener más información acerca de las amenazas y otros términos relacionados, consulte [Tipos de ataques remotos](#) o [Tipos de detecciones](#).

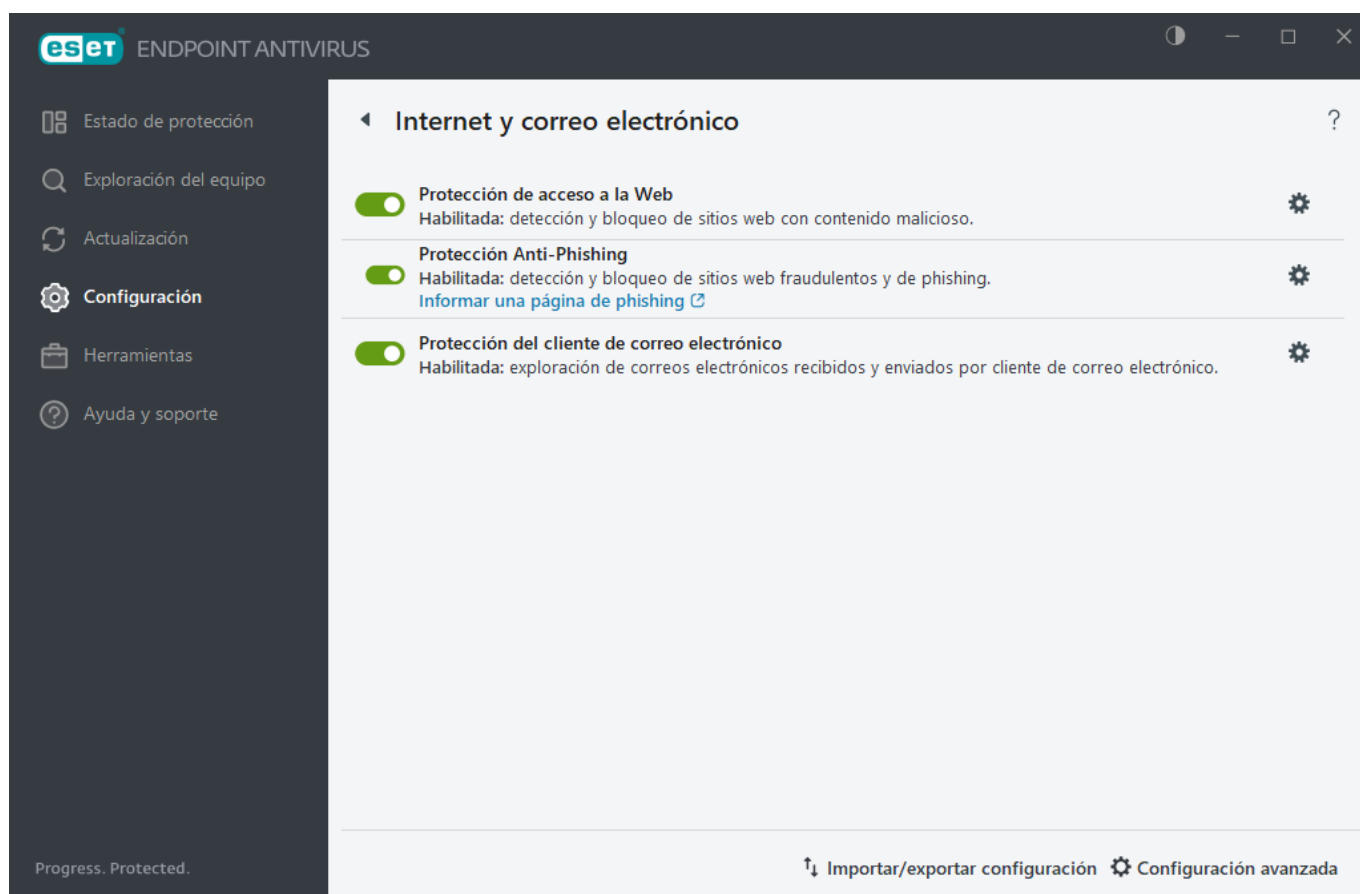
Para resolver el evento **Direcciones de IP duplicadas en la red**, consulte nuestro [artículo de la Base de conocimiento de ESET](#).


## Web y correo electrónico

La conectividad a Internet es una función estándar en un equipo personal, pero también el medio principal para transferir código malicioso. Abra la [ventana principal del programa](#) > **Configuración** > **Internet y correo electrónico** para configurar las funciones de ESET Endpoint Antivirus que aumenten la protección de Internet.

Para pausar o desactivar módulos de protección individuales, haga clic en el ícono de interruptor .

**⚠** 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 protección de acceso a la Web](#) explora la comunicación HTTP/HTTPS para detectar malware y phishing. La protección de acceso a la web solo debe desactivarse para solucionar problemas.

[Protección antiphishing](#) le permite bloquear las páginas Web conocidas por distribuir contenido phishing. Se

recomienda firmemente que deje Anti-Phishing habilitada.

**Informar una página de phishing:** informa un sitio web malicioso/de phishing a ESET para su análisis.



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](#).

[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 Endpoint Antivirus proporciona el control de todas las comunicaciones desde el cliente de correo electrónico.

## Protección antiphishing

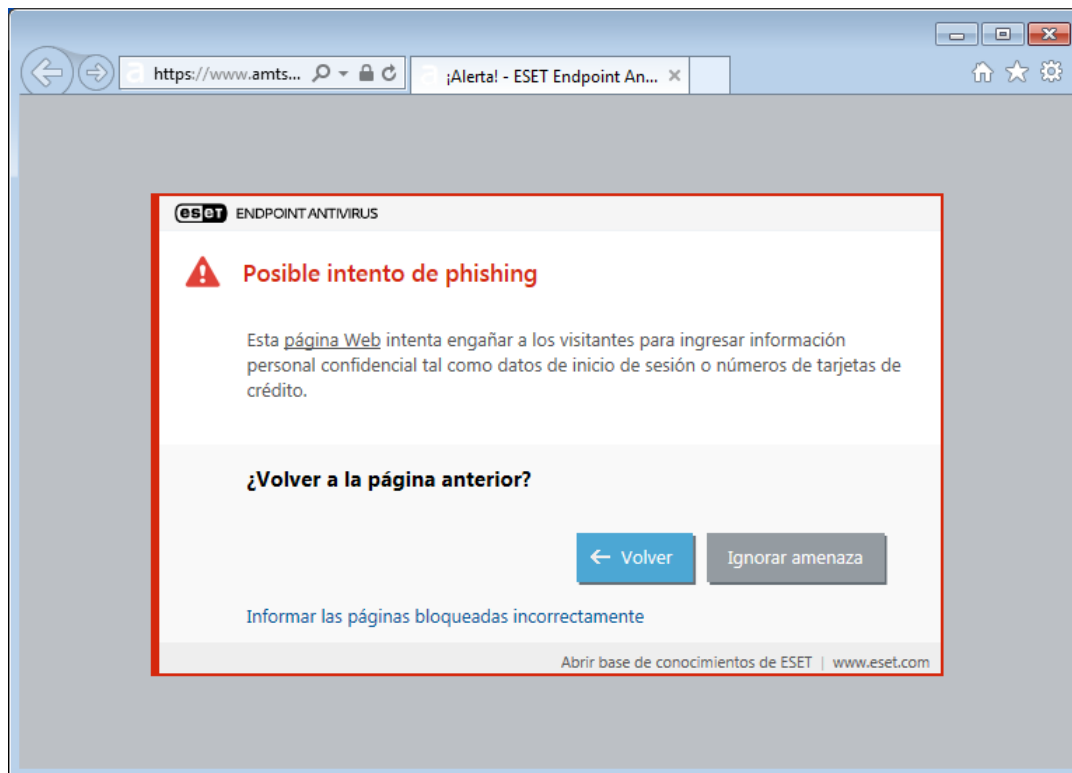
El phishing es una actividad delictiva que usa la ingeniería social (manipulación de usuarios para obtener información confidencial). El phishing se utiliza para acceder a datos confidenciales, como números de cuentas bancarias, códigos PIN, etc. Obtenga más información sobre esta actividad en el [glosario](#).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

La protección antiphishing está activada de forma predeterminada. Esta opción se puede configurar en **Configuración avanzada** > [Protecciones](#) > **Protección de acceso a la web**.

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



**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](#) > **Protecciones** > **Protección de 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 enlace **Informar una página bloqueada incorrectamente** le permite informar un sitio Web que se detecta incorrectamente como una amenaza.

Como alternativa, puede enviar el sitio Web por correo electrónico. Envíe su correo electrónico a [samples@eset.com](mailto: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.).

## Importación y exportación de una configuración

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

**i** **Instrucciones ilustradas**  
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 Endpoint 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.

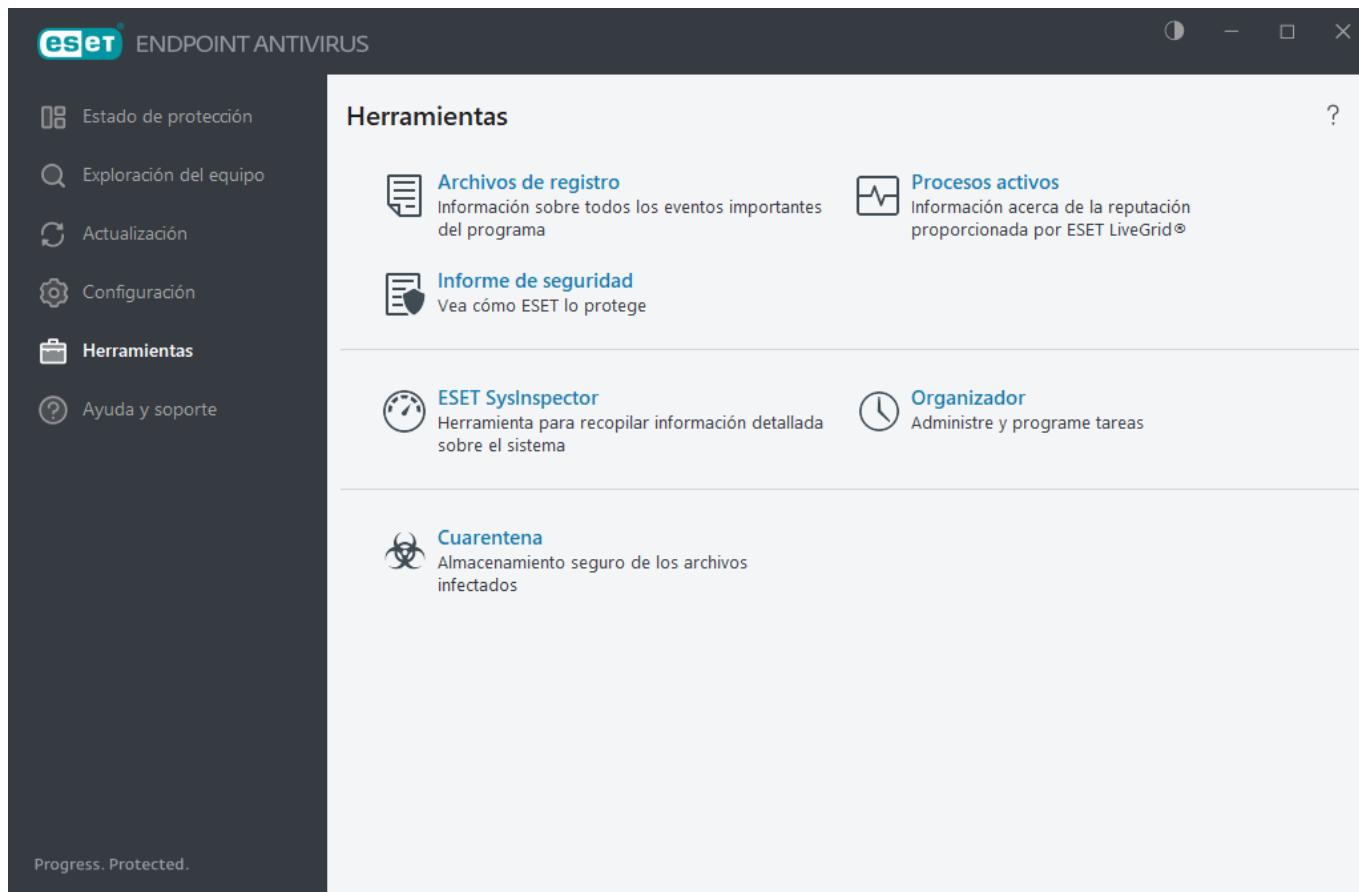
**i** Es probable que encuentre un error mientras exporta las configuraciones, si no tiene suficientes derechos para escribir el archivo exportado en el directorio especificado.



## Herramientas

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

- [Archivos de registro](#)
- [Procesos activos](#) (si ESET LiveGrid® está habilitado en ESET Endpoint Antivirus )
- [Informe de seguridad](#) (para puntos de conexión no administrados)
- [ESET SysInspector](#)
- [Tareas programadas](#)
- [Enviar muestra para su análisis](#): le permite enviar un archivo sospechoso al laboratorio de investigación de ESET para que se analice (es posible que no esté disponible según la configuración de ESET LiveGrid® que usted tenga).
- [Cuarentena](#)



## Archivos de registro

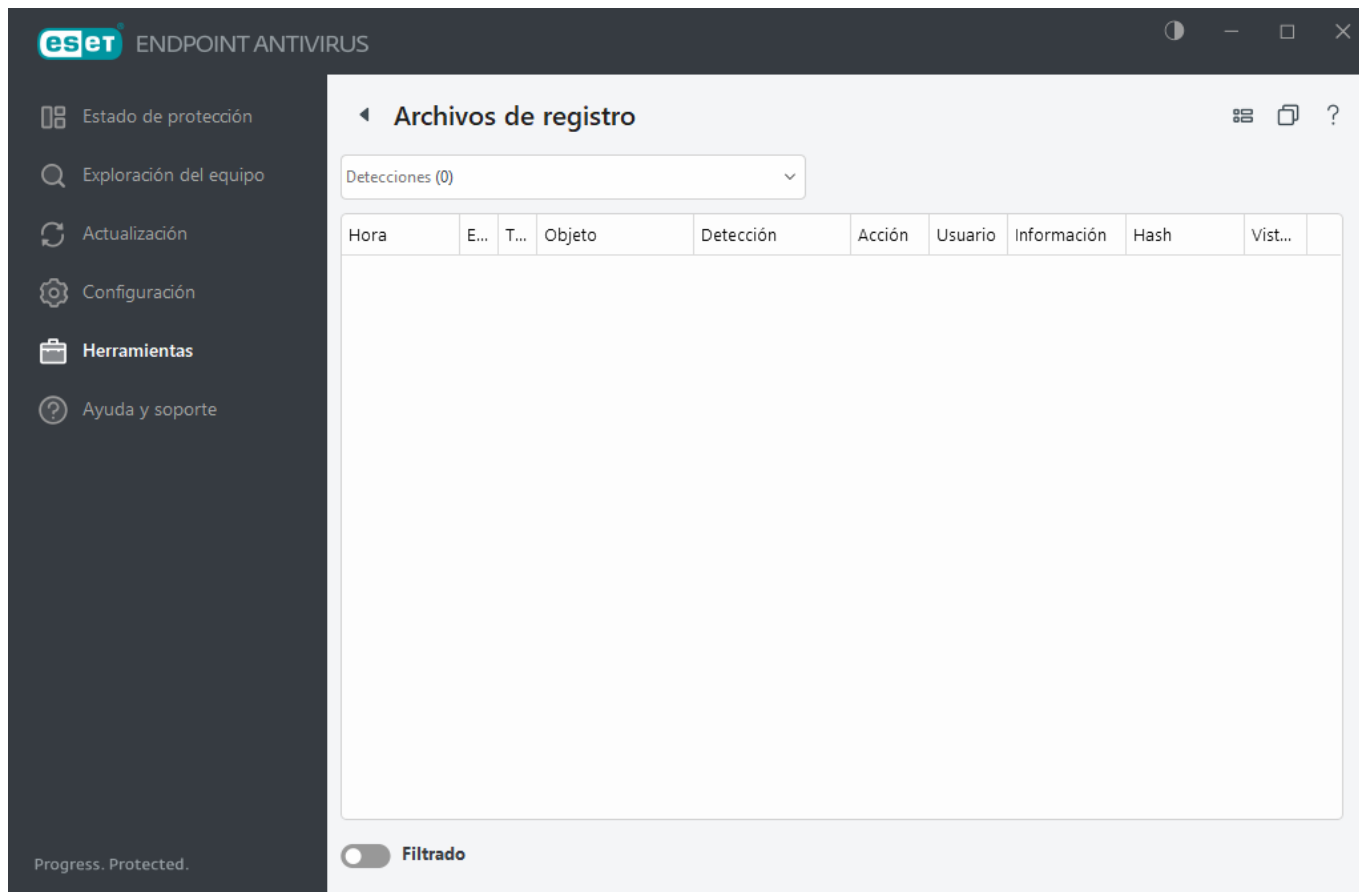
Los archivos de registro contienen información sobre todos los sucesos importantes del programa que se llevaron a cabo y proporcionan una visión general de las amenazas detectadas. Los registros constituyen una herramienta esencial en el análisis del sistema, la detección de amenazas y la resolución 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. Puede ver los mensajes de texto y los registros directamente desde el entorno de ESET Endpoint Antivirus. También es posible guardar los archivos de registro.

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

- **Amenazas detectadas:** el registro de amenazas ofrece información detallada sobre las infiltraciones y amenazas detectadas por ESET Endpoint Antivirus. La información de registro incluye la hora de la detección, el nombre de la infiltración, la ubicación, la acción realizada y el nombre del usuario registrado cuando se detectó la infiltración. Haga doble clic en la entrada de cualquier registro para mostrar sus detalles en una ventana separada. 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 Endpoint 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 resolver problemas. Con frecuencia, la información aquí incluida puede ayudarlo a encontrar una solución a un problema que ocurra en el programa.



- **Exploración del equipo** – todos los resultados de la exploración se muestran en esta ventana. Cada línea corresponde a un único control del equipo. Haga doble clic en cualquier entrada para visualizar los detalles de la exploración respectiva.
- **Archivos bloqueados:** contiene registros de archivos que se bloquearon y a los que no se pudo acceder al estar conectado a ESET Enterprise Inspector. El protocolo muestra el motivo y el módulo de origen que bloquearon el archivo, así como la aplicación y el usuario que ejecutaron el archivo. Para obtener más información, consulte la Guía para el usuario en línea de [ESET Enterprise Inspector](#).
- **Archivos enviados:** contiene registros de archivos que se enviaron a ESET LiveGrid® o [ESET LiveGuard](#) para su análisis.
- **Registros de auditorías:** cada registro contiene información sobre la fecha y la hora en que se llevó a cabo la modificación, el tipo de modificación, la descripción, el origen y el usuario. Consulte [Registros de auditoría](#) para obtener más información.
- **HIPS** – contiene historiales de las reglas específicas que se marcan para su inclusión en el registro. El protocolo muestra la aplicación que desencadenó la operación, el resultado (si la regla se permitió o prohibió) y el nombre de la regla creada.
- **Protección de red:** el registro del firewall muestra todos los ataques remotos detectados por la [protección contra ataques a la red \(IDS\)](#). Aquí encontrará información sobre todos los ataques a su equipo. En la columna Suceso, se muestra una lista de los ataques detectados. La columna Origen da más información sobre el atacante. La columna Protocolo revela el protocolo de comunicación utilizado en el ataque. Un análisis del registro de protección de red puede ayudarlo a detectar a tiempo los intentos de infiltraciones en el sistema para prevenir el acceso no autorizado. Para obtener más información sobre los ataques de red, consulte [IDS y opciones avanzadas](#).
- **Sitios web filtrados:** esta lista es útil si desea ver una lista de sitios web bloqueados por la [protección de acceso a la Web](#). En estos registros puede ver la hora, la URL, el usuario y la aplicación que abrió una conexión con el sitio Web en particular.
- **Control del dispositivo:** contiene registros de medios o dispositivos extraíbles que se conectaron al equipo. Solo los dispositivos con una Regla de control del dispositivo se registrarán en el archivo de registro. Si la regla no coincide con un dispositivo conectado, se creará una entrada del registro para un dispositivo conectado. Aquí también puede ver detalles tales como el tipo de dispositivo, número de serie, nombre del proveedor y tamaño del medio (si está disponible).



Seleccione los contenidos de cualquier registro y presione **Ctrl + C** para copiarlo al portapapeles. Mantenga presionado **Ctrl + 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, puede definir los criterios de filtrado para entradas de registros específicas en la [ventana de filtrado de registros](#).
- **Habilitar filtro** — activa las configuraciones de los filtros.
- **Deshabilitar el filtro** — borra todas las configuraciones del filtro (descritas arriba).
- **Copiar/Copiar todo** — copia la información sobre todos los historiales que aparecen en la ventana.
- **Copiar celda**— copia el contenido de la celda en la que se hace clic con el botón derecho.
- **Eliminar/Eliminar todo** — elimina los historiales seleccionados o todos los historiales mostrados (esta acción requiere privilegios de administrador).
- **Exportar** — exporta información sobre los historiales en formato XML.
- **Exportar todo** — exporta información sobre 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.
- **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.

## Registros de auditorías

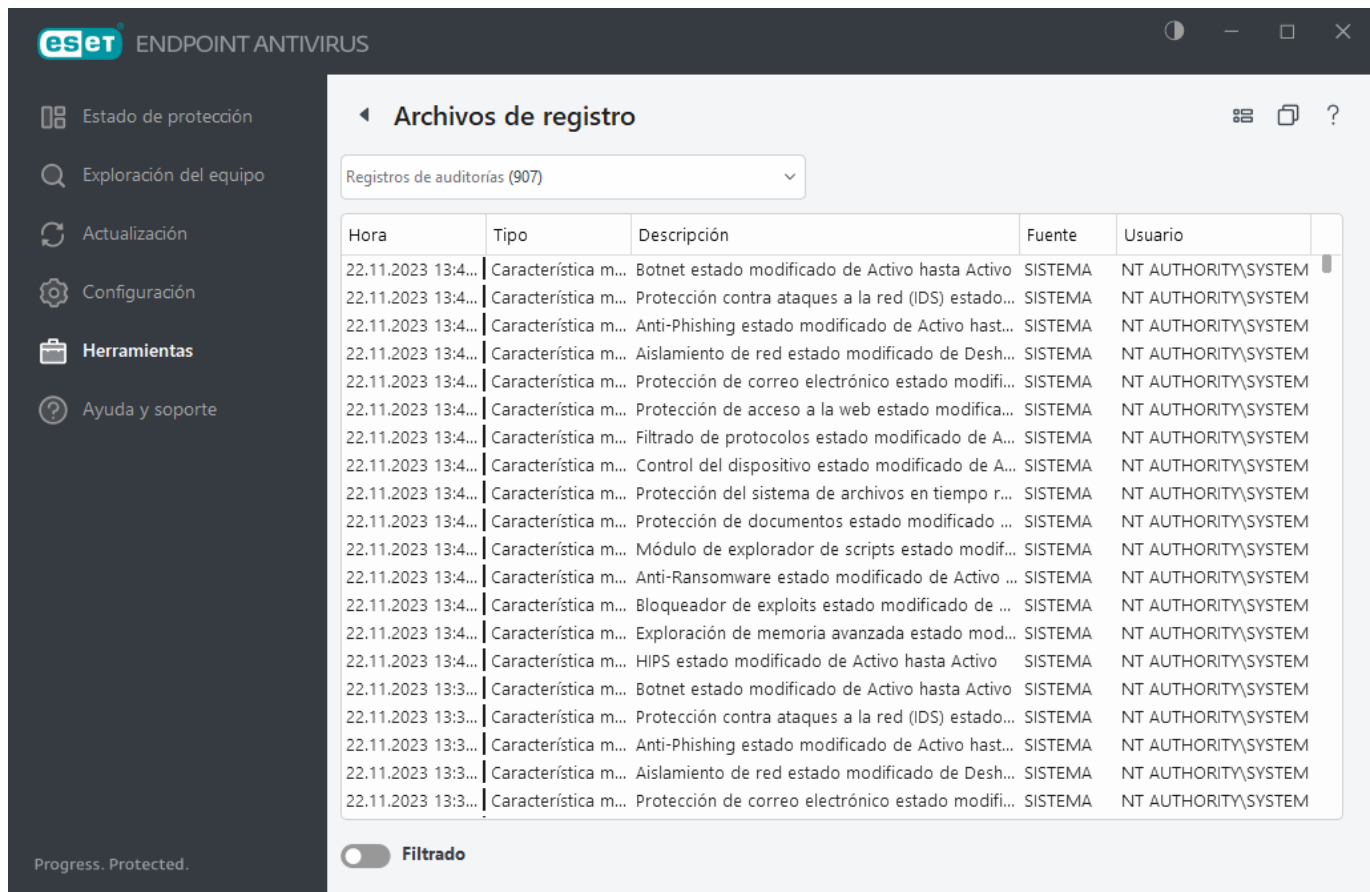
En un entorno empresarial, suele haber varios usuarios con derechos de acceso definidos para configurar puntos de conexión. Debido a que la modificación en la configuración del producto puede afectar de manera significativa su modo de funcionamiento, resulta fundamental que los administradores lleven un registro de los cambios hechos por los usuarios para ayudar a los administradores a identificar, resolver y, también, evitar con rapidez que ocurran los mismos problemas, o problemas similares, en el futuro.

El registro de auditoría es un nuevo tipo de registro para la identificación del origen del problema. En los registros de auditoría, se lleva un registro de los cambios en la configuración o en el estado de protección, y se graban capturas de pantalla para posterior referencia.

Para ver el **registro de auditoría**, haga clic en **Herramientas** en el menú principal y, luego, en **Archivos de registro** y seleccione **Registros de auditorías** del menú desplegable.

El registro de auditoría contiene información sobre:

- **Horario** : cuándo se realizó el cambio
- **Tipo**: qué tipo de configuración o función se modificó
- **Descripción**: qué se modificó exactamente y qué parte de la configuración se cambió junto con la cantidad de configuraciones modificadas
- **Origen**: ubicación del origen del cambio
- **Usuario**: quién aplicó el cambio



Haga clic con el botón secundario en cualquiera de los tipos de registro de auditoría **Configuración modificada** en la ventana Archivos de registro y seleccione **Mostrar cambios** en el menú de contexto para mostrar información detallada sobre el cambio implementado. Además, puede restablecer el cambio de configuración. Para ello, haga clic en **Restablecer** en el menú de contexto (no disponible para productos administrados por ESET PROTECT). Si selecciona **Quitar todo** del menú de contexto, se creará un registro con la información sobre esta acción.

Si selecciona la opción **Optimizar archivos de registros de manera automática** habilitada en [Configuración avanzada](#) > **Herramientas** > **Archivos de registro**, los registros de auditoría se desfragmentarán de manera automática como otros registros.

Si selecciona la opción **Eliminar registros de manera automática anteriores a (días)** habilitada en [Configuración avanzada](#) > **Herramientas** > **Archivos de registro**, las entradas de registros anteriores a la cantidad de días especificados se quitarán de manera automática.

## 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 Endpoint Antivirus proporciona información detallada sobre los procesos activos para proteger a los usuarios con la tecnología **ESET LiveGrid®** habilitada.

**ENDPOINT ANTIVIRUS**

Estado de protección

Exploración del equipo

Actualización

Configuración

Herramientas

Ayuda y soporte

Progress. Protected.

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 u...	Tiempo de ...	Nombre de la aplicación
	smss.exe	344		hace 2 sema...	Microsoft® Windows® Op...
	csrss.exe	464		hace 2 sema...	Microsoft® Windows® Op...
	wininit.exe	612		hace 2 sema...	Microsoft® Windows® Op...
	winlogon.exe	660		hace 2 sema...	Microsoft® Windows® Op...
	services.exe	732		hace 2 sema...	Microsoft® Windows® Op...
	lsass.exe	752		hace 2 sema...	Microsoft® Windows® Op...
	svchost.exe	880		hace 2 sema...	Microsoft® Windows® Op...
	fontdrvhost.exe	908		hace 2 sema...	Microsoft® Windows® Op...
	dwm.exe	584		hace 2 sema...	Microsoft® Windows® Op...
	efwd.exe	1576		hace 2 sema...	ESET Security
	spoolsv.exe	3024		hace 2 sema...	Microsoft® Windows® Op...
	vmtoolsd.exe	3360		hace 3 meses	VMware Tools
	vgauthservice.exe	3368		hace 3 meses	VMware Guest Authentication
	vm3dservice.exe	3384		hace 1 mes	VMware SVGA 3D
	mpdefendercoreservice.exe	3412		hace 2 sema...	Microsoft® Windows® Op...
	dllhost.exe	744		hace 2 sema...	Microsoft® Windows® Op...
	msdtc.exe	4108		hace 2 sema...	Microsoft® Windows® Op...
	wmiprvse.exe	4184		hace 2 sema...	Microsoft® Windows® Op...
	searchindexer.exe	4712		hace 2 sema...	Windows® Search
	sihost.exe	5160		hace 2 sema...	Microsoft® Windows® Op...

**Reputación** – en la mayoría de los casos, la tecnología ESET Endpoint 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 reputación desde el valor 9: Mejor reputación (en color verde) hasta 0: Peor reputación (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. Puede abrir el Administrador de tareas al hacer clic derecho en un área vacía de la barra de tareas seleccionado, posteriormente, el Administrador de tareas, o al presionar **Ctrl+Shift+Esc** en su teclado.

**PID** – es un identificador de procesos activos en los sistemas operativos de Windows.

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

**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.

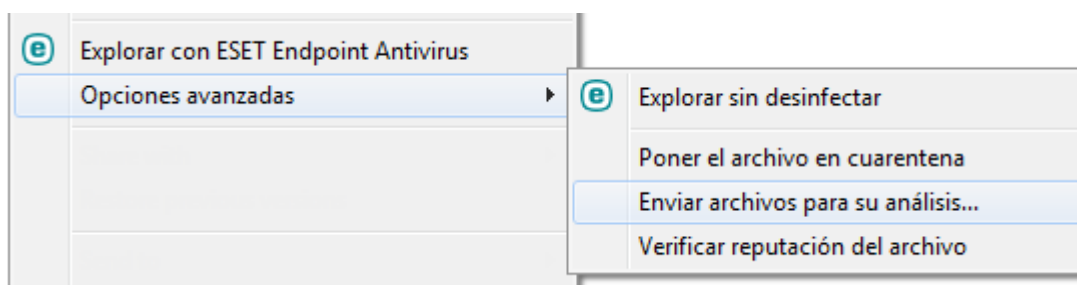
**i** Si una aplicación está marcada como nivel de seguridad desconocido (naranja), no significa necesariamente que sea software malicioso. Por lo general, solo se trata de una aplicación nueva. Si no está seguro con respecto al archivo, use la función [enviar el archivo para su análisis](#) para enviar el archivo al laboratorio de virus de ESET. Si el archivo resulta ser una aplicación maliciosa, se agregará su detección en una de las próximas actualizaciones del motor de búsqueda.

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

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

- **Ruta** – ubicación de una aplicación en su equipo.
- **Descripción** – características del archivo según la descripción proporcionada por el sistema operativo.
- **Versión** – información proporcionada por el desarrollador de la aplicación.
- **Empresa** – nombre del proveedor o del proceso de la aplicación.
- **Producto** – nombre de la aplicación y/o nombre comercial.
- **Tamaño** – tamaño del archivo ya sea en kB (kilobytes) o MB (megabytes).
- **Creada el** – fecha y hora de la creación de una aplicación.
- **Modificada el:** última fecha y hora en que se modificó una aplicación.

**i** La reputación también se puede verificar en archivos que no sean programas o procesos activos. Para ello, marque los archivos que desea verificar, haga un clic derecho en ellos y, desde el [menú contextual](#), seleccione **Opciones avanzadas > Verificar la reputación de archivos mediante ESET LiveGrid®**.




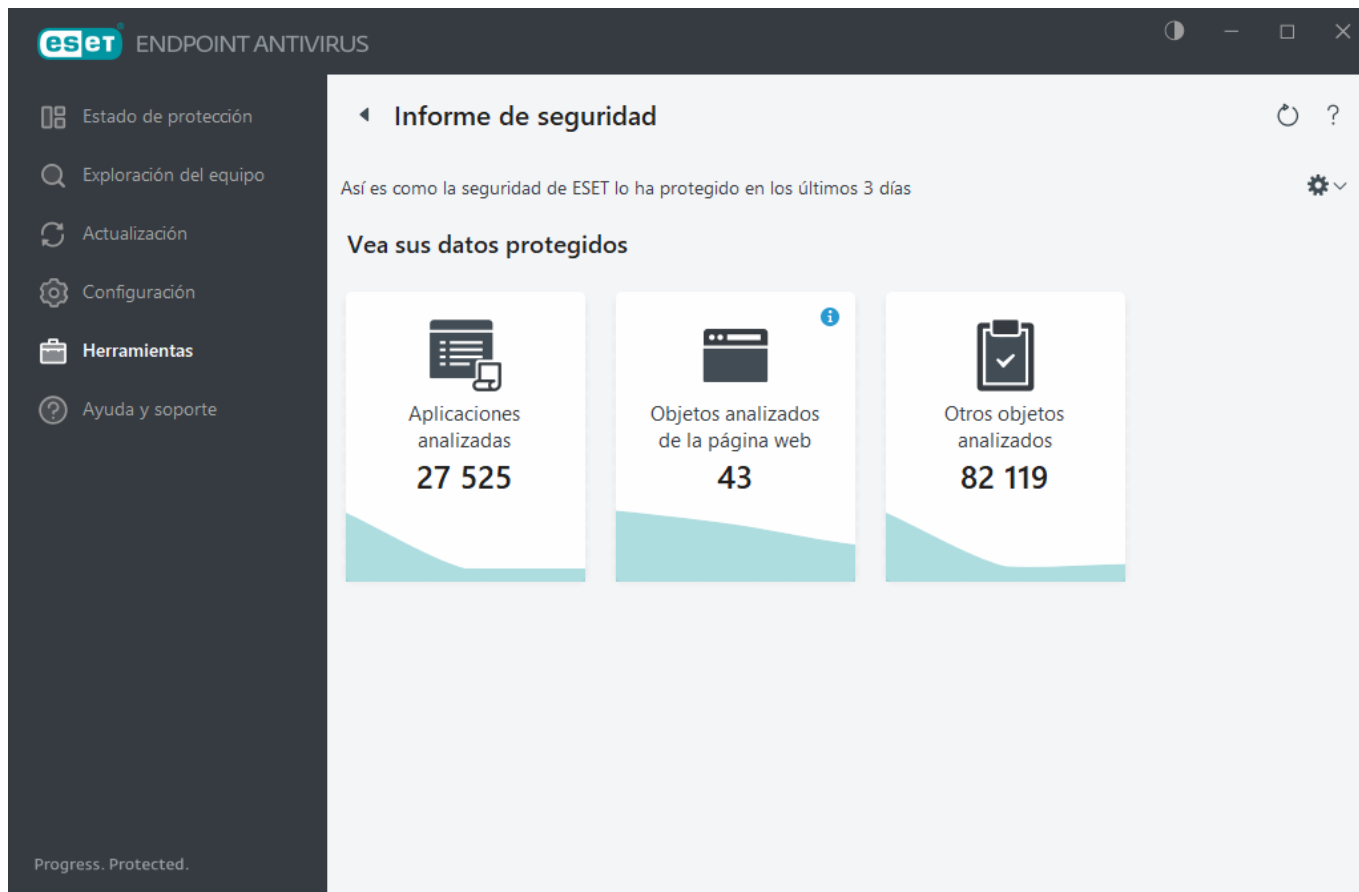
## Informe de seguridad

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 explorados**: muestra el número de objetos de documento explorados.
- **Aplicaciones exploradas**: muestra el número de objetos ejecutables explorados.
- **Otros objetos explorados**: 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.

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 Endpoint 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**.

## 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. El registro se guarda en C:\ProgramData\ESET\ESET Security\SysInspector.



- **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 (equivalente 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.

## 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 Endpoint 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: actualización del motor de detección, tarea de exploración, verificación de archivos de inicio del sistema y 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). 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.

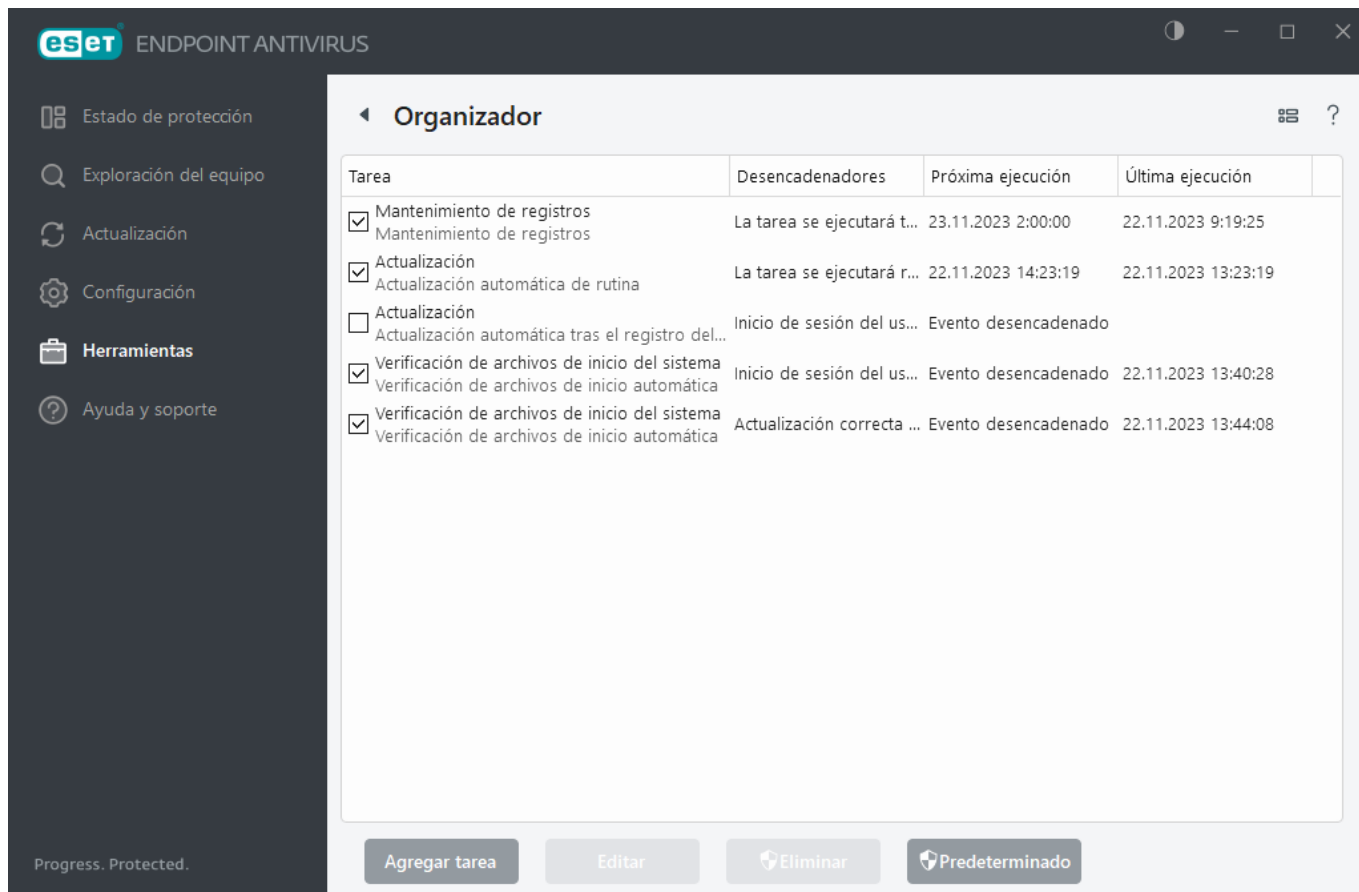
En forma predeterminada, se muestran las siguientes **tareas programadas**:

- **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)
- **Verificación de archivos de inicio automática** (después de la actualización del módulo exitosa)

**i**

En ESET PROTECT, los retrasos de la ejecución de la tarea aleatoria se pueden utilizar para reducir la carga del servidor al ejecutar las tareas, especialmente en redes más grandes. Esta opción permite definir el período durante el cual una tarea se debe ejecutar en toda la red, de manera opuesta a ejecutar una tarea en todas las estaciones de trabajo, en toda la red al mismo tiempo. Cuando se ejecuta una tarea, el valor del tiempo establecido se segmenta de forma aleatoria para asignar un tiempo de ejecución de una tarea única a cada estación de trabajo en la red. Esto ayuda a evitar sobrecargas en el servidor y problemas relacionados (por ej., algunos servidores pueden informar un [ataque de DoS](#) al realizar una actualización masiva simultánea en las estaciones de trabajo a través de toda la red).

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



## Agregar una nueva tarea

- Haga clic en **Agregar tarea** en el sector inferior de la ventana.
- Escriba el nombre de la tarea.
- 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 del motor de detección y los módulos del programa.
- Encienda el interruptor de **Habilitado** si desea 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 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**)

Para revisar la tarea programada, haga clic con el botón derecho en la tarea y, a continuación, 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.

En el menú desplegable, puede definir la acción que desea realizar automáticamente cuando finaliza la 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** – cierra todos los programas abiertos, y reinicia el equipo luego 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.
- **Forzar reinicio**: fuerza el cierre de todos los programas abiertos sin esperar la intervención del usuario y reinicia el equipo cuando finaliza la exploración.
- **Forzar reinicio si es necesario**: el equipo se reinicia solo si es necesario para completar la limpieza de las amenazas detectadas.
- **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.



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.

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.

## Envío de muestras 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).

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).

El envío de una muestra le permite enviar un archivo o un sitio web para que ESET lo analice por medio de uno de

estos métodos:

1. En **Herramientas > Enviar muestra para su análisis** encontrará una muestra del diálogo de envío.
2. Como alternativa, puede enviar el archivo por correo electrónico. Si prefiere esta opción, comprima el archivo utilizando WinRAR/ZIP, proteja el archivo con la contraseña “infected” y envíelo a [samples@eset.com](mailto:samples@eset.com).
3. Para reportar spam o falsos positivos de spam, consulte nuestro artículo en la [Base de conocimiento de ESET](#).

Con la opción **Seleccionar muestra para su análisis** abierta, seleccione **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),
- [Archivo falso positivo](#) (un archivo que se detecta como una infección pero no está infectado),
- [Sitio falso positivo](#)
- [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.



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 ingresar información adicional o una descripción útil para el proceso de identificación del archivo sospechoso.



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 el proceso de identificación de las 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.
- **Phishing** – suele usarse para obtener el acceso a datos confidenciales, como números de cuentas bancarias, códigos de identificación personal, 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 ingresar información adicional o una descripción útil para el análisis del 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.

## Cuarentena

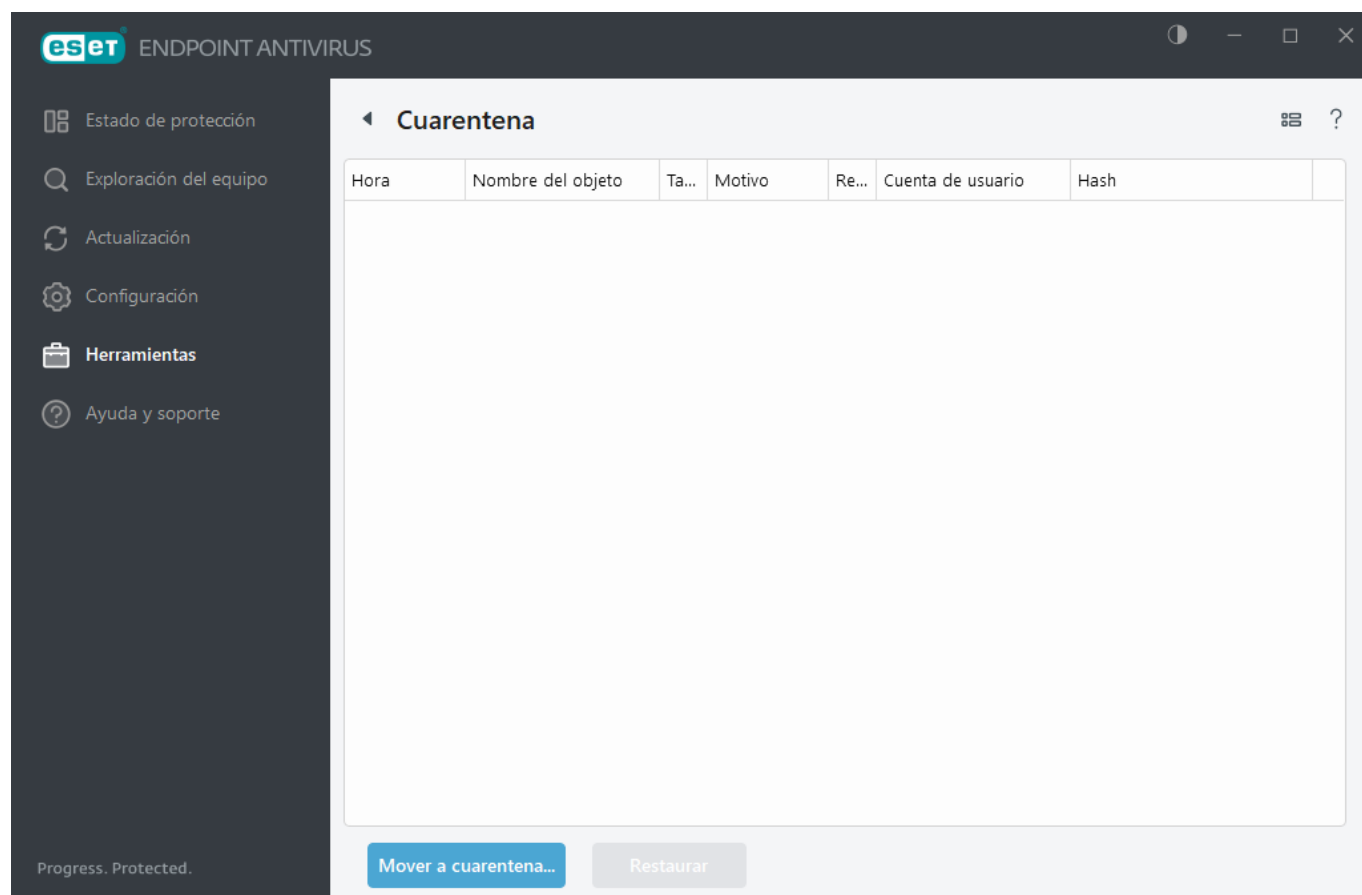
La principal función de la cuarentena es almacenar de forma segura los objetos informados (como malware, archivos infectados o aplicaciones potencialmente no deseadas).

Para acceder a la cuarentena, diríjase a la ventana principal del programa ESET Endpoint 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).

[Administro la cuarentena en las estaciones de trabajo de cliente de manera remota](#)



## Envío de archivos a cuarentena

ESET Endpoint 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:

- no pueden limpiarse,
- no es seguro o recomendable eliminarlos,
- ESET Endpoint Antivirus los detecta de manera falsa,
- un archivo presenta un comportamiento sospechoso pero el [escáner](#) no lo detecta.

Para poner un archivo en cuarentena, cuenta con varias opciones:

- 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.
- Haga clic en **Mover a cuarentena** en la ventana principal del programa.
- 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.



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

- [Administrar la cuarentena en ESET PROTECT](#)
- [Mi producto ESET me envió una notificación sobre una detección. ¿Qué debo hacer?](#)

## Ayuda y soporte

Haga clic en **Ayuda y soporte** en la [ventana del programa principal](#) para mostrar información de soporte y herramientas de solución de problemas que le permitirán resolver los problemas que pueda encontrar.



### Producto instalado

- [Acerca de ESET Endpoint Antivirus](#) – muestra información acerca de una copia de ESET Endpoint Antivirus.
- [Resolución de problemas del producto](#): haga clic en este enlace para buscar soluciones a los problemas más frecuentes.
- [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.



**Página de ayuda** – haga clic en este vínculo para abrir las páginas de ayuda de ESET Endpoint Antivirus.



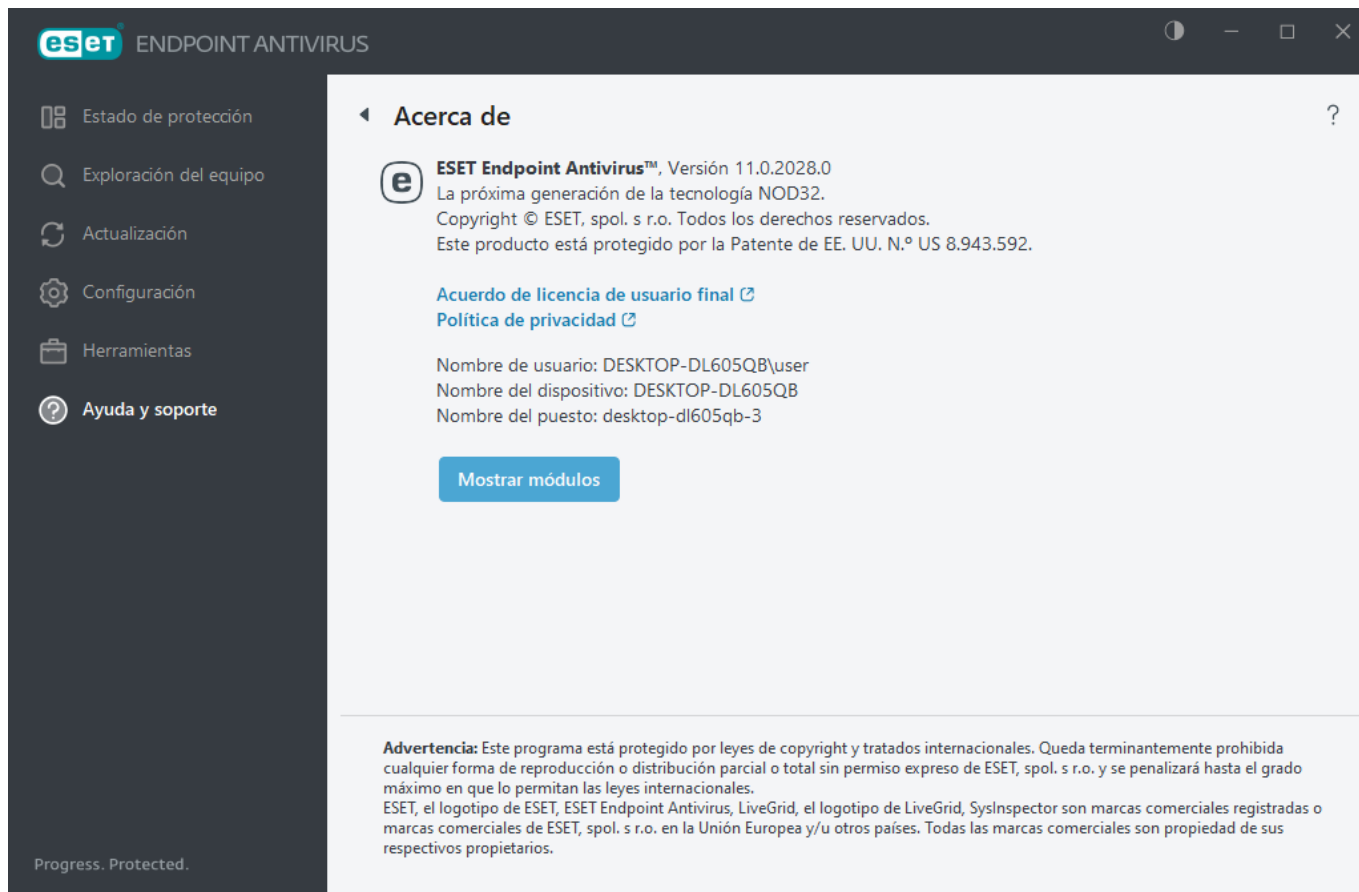
### [Soporte técnico](#)



**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 Endpoint Antivirus

Esta ventana brinda detalles sobre la versión instalada de ESET Endpoint 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.

## 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 Endpoint 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.

Después de 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. Al enviar el [formulario web](#) sin enviar ningún dato, haga clic en **No enviar datos** y continúe.

Puede configurar el envío de los datos de configuración del sistema en Soporte [Configuración avanzada](#) > **Herramientas** > **Diagnóstico** > [Soporte técnico](#).



Si ha decidido enviar los datos de configuración del sistema, es necesario completar y enviar el formulario web. De lo contrario, no se creará su ticket y se perderán los datos de configuración del sistema. Si no se pueden enviar los datos de configuración del sistema, complete el formulario web y espere las instrucciones del Soporte técnico.

# 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.

## Configuración avanzada

La configuración avanzada le permite configurar ESET Endpoint Antivirus ajustes detallados según sus necesidades.

Para abrir la Configuración avanzada, abra la [ventana principal del programa](#) y presione la tecla **F5** del teclado o haga clic en **Configuración** > **Configuración avanzada**.



Cuando cree una política desde la Consola Web de ESET PROTECT, puede seleccionar el indicador para cada configuración. Las configuraciones con el indicador Forzar tienen prioridad y no se pueden sobrescribir por una política posterior (incluso si la política posterior tiene un indicador Forzar). Esto garantiza que no se modificarán las configuraciones (por ejemplo, por el usuario o por políticas posteriores durante una fusión). Para obtener más información, consulte [Indicadores en la Ayuda en línea de ESET PROTECT](#).

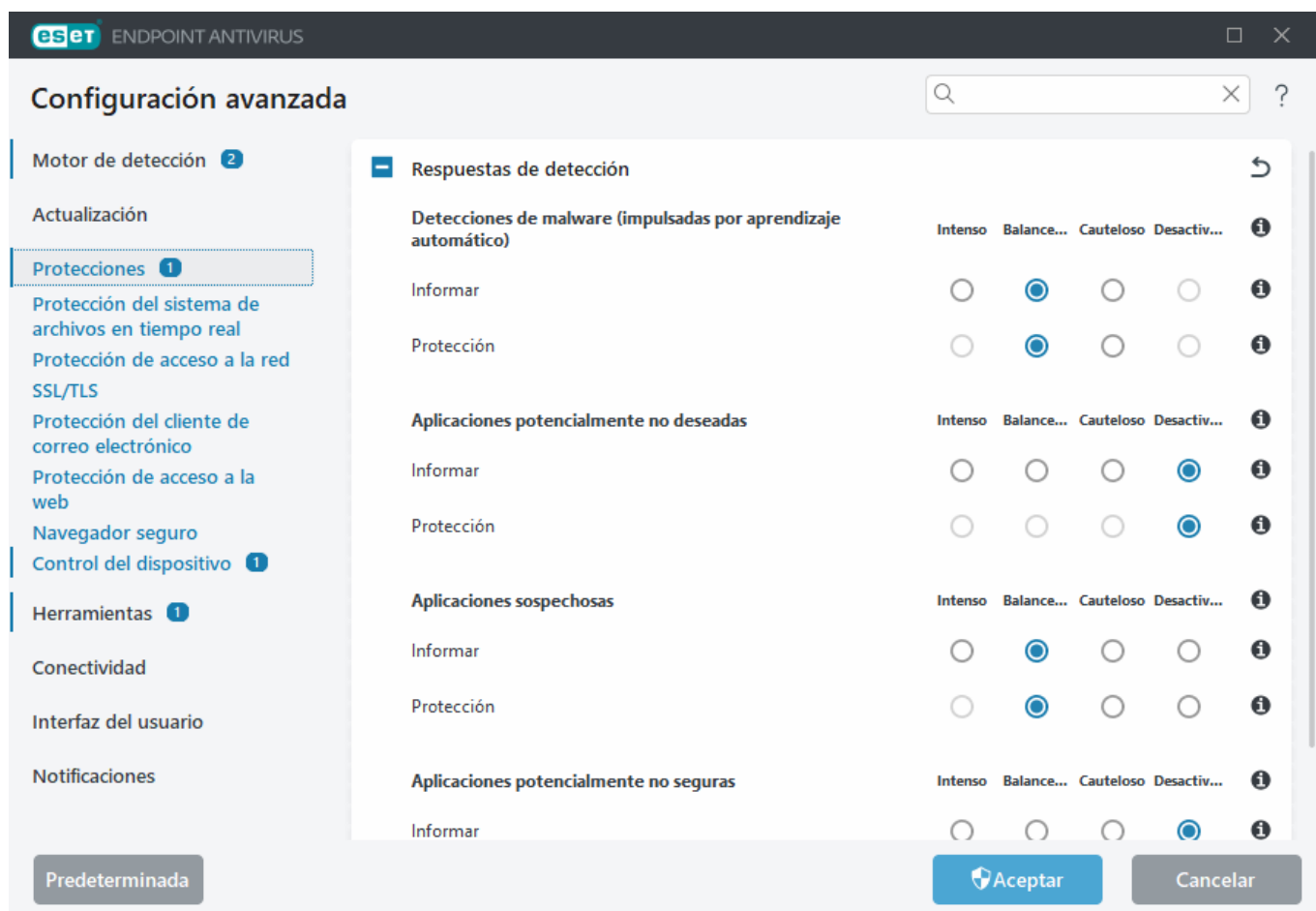


Según su [Configuración de acceso](#), es posible que se le solicite que escriba una contraseña para abrir la Configuración avanzada.

En la configuración avanzada, puede realizar los siguientes ajustes:

- [Motor de detección](#)
- [Actualización](#)

- [Protecciones](#)
- [Herramientas](#)
- [Conectividad](#)
- [Interfaz del usuario](#)
- [Notificaciones](#)



## Motor de detección

[Configuración avanzada](#) > **Motor de detección** le permite configurar las siguientes opciones:

- [Exclusiones](#)
- Opciones avanzadas
- [Explorador del tráfico de red](#)

## 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 desinfección 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 en [Configuración avanzada](#) > **Motor de detección** > **Exclusiones** > **Exclusiones de rendimiento** > **Editar**.

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.

The screenshot shows the 'Exclusiones de rendimiento' (Performance Exclusions) window in ESET Endpoint Antivirus. The window has a title bar with the ESET logo and 'ENDPOINT ANTIVIRUS'. Below the title bar is a header 'Exclusiones de rendimiento' with a help icon. The main area is a table with two columns: 'Excluir ruta' and 'Comentario'. Below the table are buttons: 'Agregar', 'Editar', 'Eliminar', 'Importar', and 'Exportar'. At the bottom right are 'Aceptar' and 'Cancelar' buttons.

**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

- **Añadir:** le permite añadir una nueva entrada para excluir objetos de la exploración.
- **Editar** – le permite editar las entradas seleccionadas.
- **Eliminar:** quita las entradas seleccionadas (CTRL + clic para seleccionar múltiples entradas).
- **Importar/Exportar:** la importación y exportación de las exclusiones de desempeño es útil si necesita hacer una copia de seguridad de las exclusiones actuales para usarlas más adelante. La opción para exportar la configuración también es conveniente para usuarios en entornos no administrados que desean usar su configuración preferida en varios sistemas, ya que pueden importar fácilmente un archivo .txt para transferir estas configuraciones.

 [Mostrar ejemplo del formato de archivo de importación/exportación](#)

```
# {"product":"endpoint","version":"10.0.2034","path":"Settings.ExclusionsManagement.PerformanceExclusions","columns":["Path","Description"]}
```

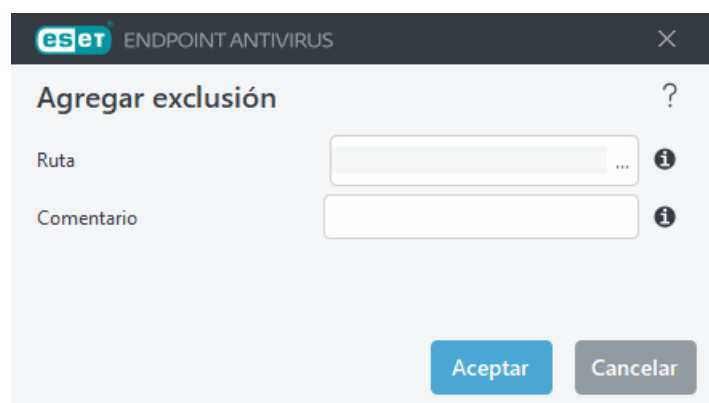
```
C:\Backup\*,custom comment
```

```
C:\pagefile.sys
```

## Agregar o editar exclusión de rendimiento

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

**i** Para elegir una ruta que corresponda, haga clic en ... en el campo **Ruta**. Si introduce la ruta 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.



- 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.

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%**).

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. Consulte el siguiente [artículo de la base de conocimiento](#) para obtener más información.

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 con los botones 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.

- 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.

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%

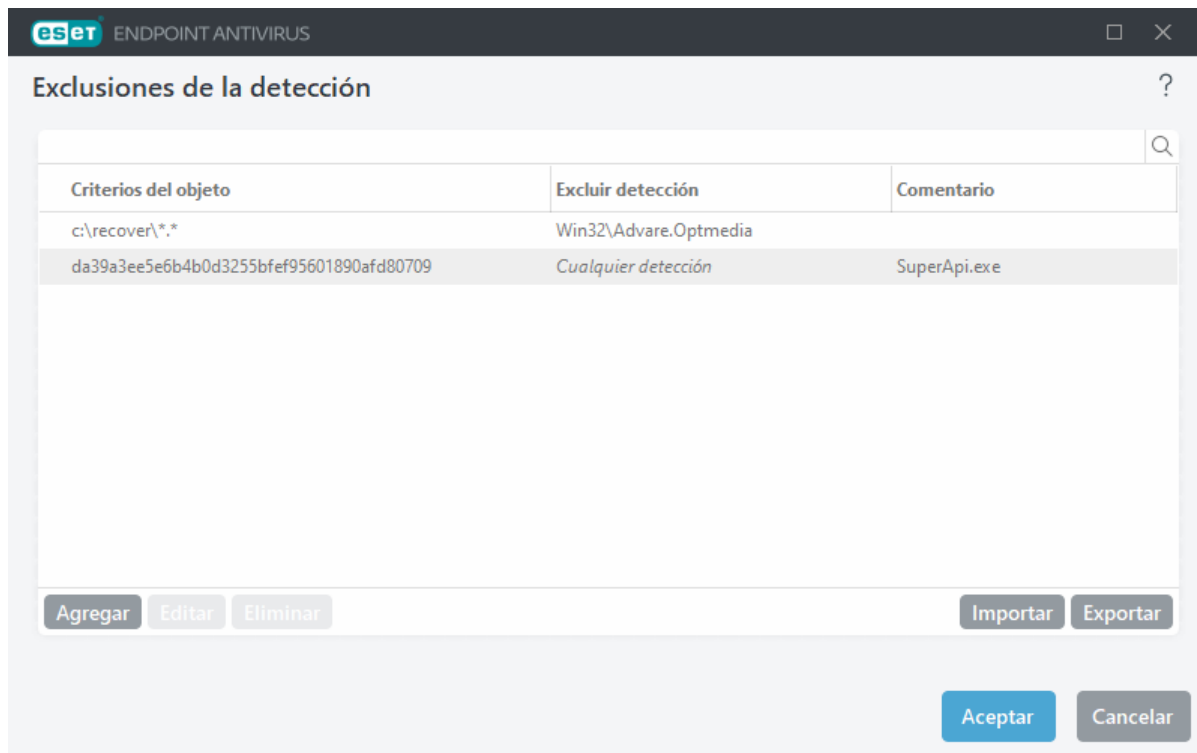
No se admiten las variables del sistema específicas del usuario (p. ej., %TEMP% o %USERPROFILE%) ni las variables de entorno (p. ej., %PATH%).

## Exclusiones de la detección

Las exclusiones de la detección permiten excluir objetos de la [desinfección](#) mediante el filtro del nombre de la detección, la ruta del objeto o su hash.

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.



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

Para añadir archivos y carpetas a la lista de exclusiones, abra [Configuración avanzada](#) > **Motor de detección** > **Exclusiones** > **Exclusiones de la detección** > **Editar**.

Para [excluir un objeto \(por su nombre de detección o hash\)](#) de la desinfección, 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.

## Elementos de control

- **Añadir:** le permite añadir una nueva entrada para excluir objetos de la desinfección.
- **Editar** – le permite editar las entradas seleccionadas.
- **Eliminar:** quita las entradas seleccionadas (CTRL + clic para seleccionar múltiples entradas).
- **Importar/Exportar:** la importación y exportación de las exclusiones de detección es útil si necesita hacer una copia de seguridad de las exclusiones actuales para usarlas más adelante. La opción para exportar la configuración también es conveniente para usuarios en entornos no administrados que desean usar su configuración preferida en varios sistemas, ya que pueden importar fácilmente un archivo .txt para transferir estas configuraciones.

 [Mostrar ejemplo del formato de archivo de importación/exportación](#)

```
# {"product":"endpoint","version":"10.0.2034","path":"Settings.ExclusionsManagement.DetectionExclusions","columns":["Id","Path","ThreatName","Description","File Hash"]}
```

```
4c59cd02-357c-4b20-a0ac-ca8400000001,,,SuperApi.exe,00117F70C86ADB0F979021391A8AEAA497C2C8DF
```

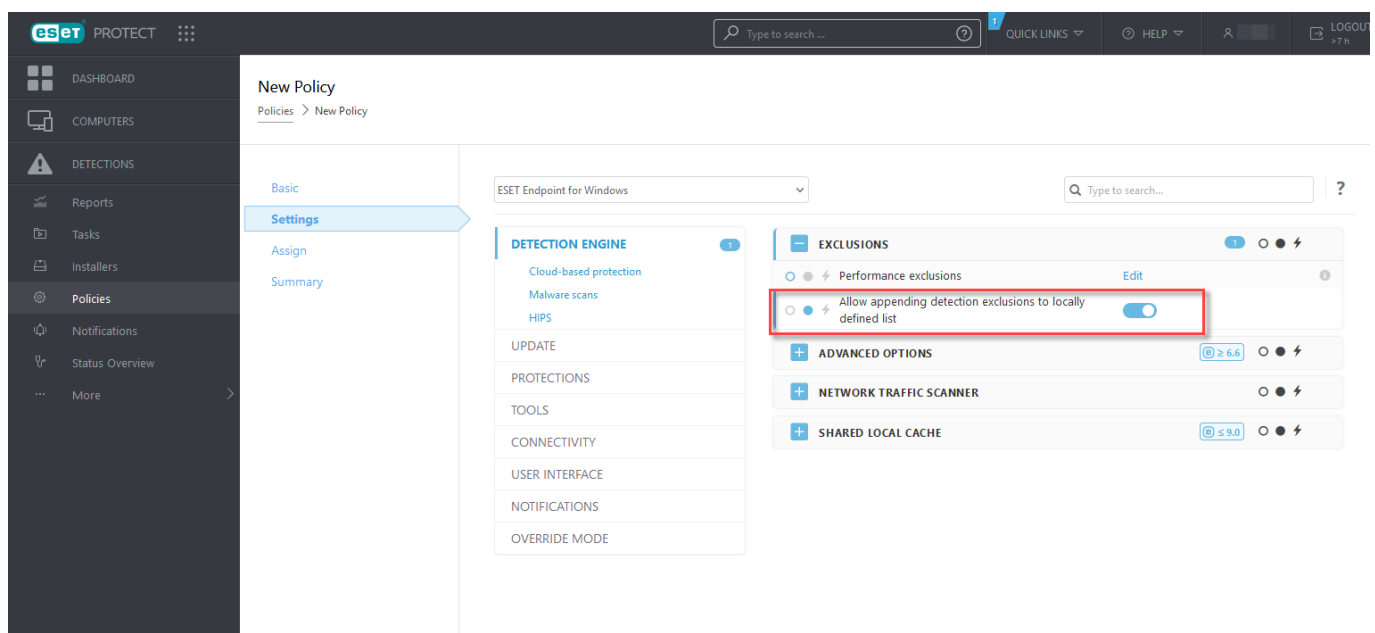
```
2c362ac8-a630-496e-9665-c76d00000001,C:\Recovery\*.*,Win32/Adware.Optmedia,
```

## Configuración de exclusiones de la detección en ESET PROTECT

[Asistente para la administración de exclusiones de la detección](#) de ESET PROTECT: cree una exclusión de la detección y aplíquela en más equipos/grupos.

### Las exclusiones de detección potenciales se anulan desde ESET PROTECT

Cuando ya existe una lista local de exclusiones de la detección, el administrador debe aplicar una política con **Permitir adjuntar exclusiones de la detección a una lista definida localmente**. Luego, la tarea de adjuntar exclusiones de la detección desde ESET PROTECT se ejecutará según lo previsto.

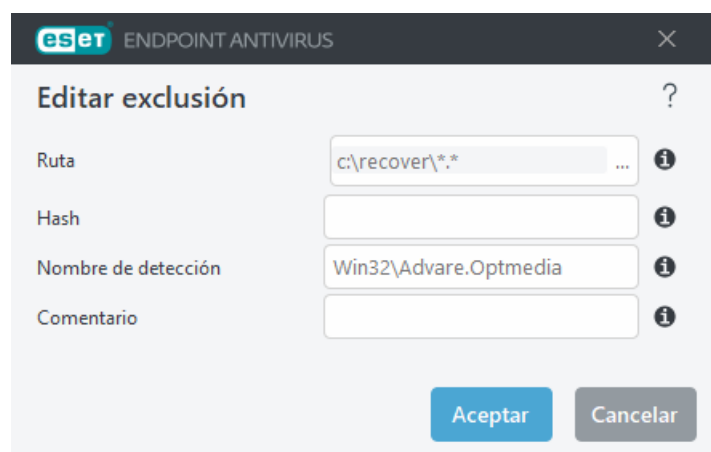


# Agregar o editar exclusiones de la detección

## 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 Endpoint 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](#).

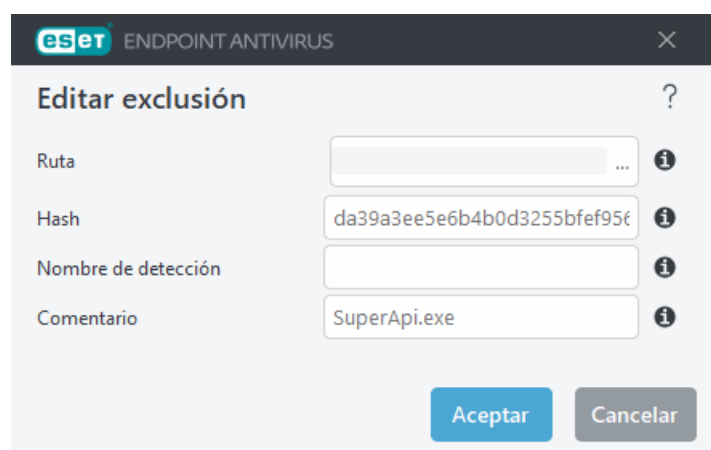


The screenshot shows the 'Editar exclusión' (Edit exclusion) window in ESET Endpoint Antivirus. It has a title bar with the ESET logo and 'ENDPOINT ANTIVIRUS'. The window contains four input fields: 'Ruta' (Path) with the value 'c:\recover\\*.\*\*\*', 'Hash', 'Nombre de detección' (Detection name) with the value 'Win32\Advare.Optmedia', and 'Comentario' (Comment). Each field has an information icon (i) to its right. At the bottom, there are two buttons: 'Aceptar' (Accept) and 'Cancelar' (Cancel).

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.



The screenshot shows the 'Editar exclusión' (Edit exclusion) window in ESET Endpoint Antivirus. It has a title bar with the ESET logo and 'ENDPOINT ANTIVIRUS'. The window contains four input fields: 'Ruta' (Path), 'Hash' with the value 'da39a3ee5e6b4b0d3255bfef956...', 'Nombre de detección' (Detection name), and 'Comentario' (Comment) with the value 'SuperApi.exe'. Each field has an information icon (i) to its right. At the bottom, there are two buttons: 'Aceptar' (Accept) and 'Cancelar' (Cancel).

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

✓ Endpoint 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**.

## 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.

## Explorador del tráfico de red

El explorador de tráfico de red proporciona protección contra malware para protocolos de aplicación, que integra múltiples técnicas avanzadas de exploración de malware. El explorador de tráfico de red explora los protocolos HTTP(S), POP3(S) e IMAP(S) automáticamente, independientemente del navegador de Internet o del cliente de correo electrónico. Puede habilitar/deshabilitar el explorador de tráfico de red en [Configuración avanzada](#) >

**Habilitar explorador de tráfico de red:** si desactiva esta opción, no se explorarán los protocolos HTTP(S), POP3(S) e IMAP(S). Tenga en cuenta que las siguientes funciones ESET Endpoint Antivirus requieren que el explorador de tráfico de red esté habilitado:

- [Protección del acceso a la Web](#)
- [SSL/TLS](#)
- [Protección antiphishing](#)
- [Protección del cliente de correo electrónico](#)

## 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 from the wild, 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:

### Opción 1: habilitar el sistema de reputación de ESET LiveGrid®

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

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®.

### Opción 2: 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 el equipo en relación con las nuevas amenazas detectadas. Esa información puede incluir una muestra o una copia del archivo donde apareció la amenaza, la ruta a ese archivo, el nombre del archivo, la fecha y la hora, el proceso por el que apareció la amenaza y la información sobre el sistema operativo del equipo.

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

### Opción 3: optar por no habilitar ESET LiveGrid®

No perderá funcionalidad alguna en el software pero, en algunos casos, ESET Endpoint Antivirus puede responder más rápido a las nuevas amenazas que una actualización del motor de detección cuando ESET LiveGrid® está habilitado.

Lea más sobre ESET LiveGrid® en el [glosario](#).



Consulte nuestras [instrucciones ilustradas](#) disponibles in inglés y otros idiomas sobre cómo habilitar o deshabilitar ESET LiveGrid® en ESET Endpoint Antivirus.

---

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

Para acceder a la configuración avanzada de ESET LiveGrid®, abra la [Configuración avanzada](#) > **Motor de detección** > **Protección basada 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 **Envío de muestras** a continuación) junto con informes de falla y estadísticas al laboratorio de investigación de ESET para un mayor análisis.

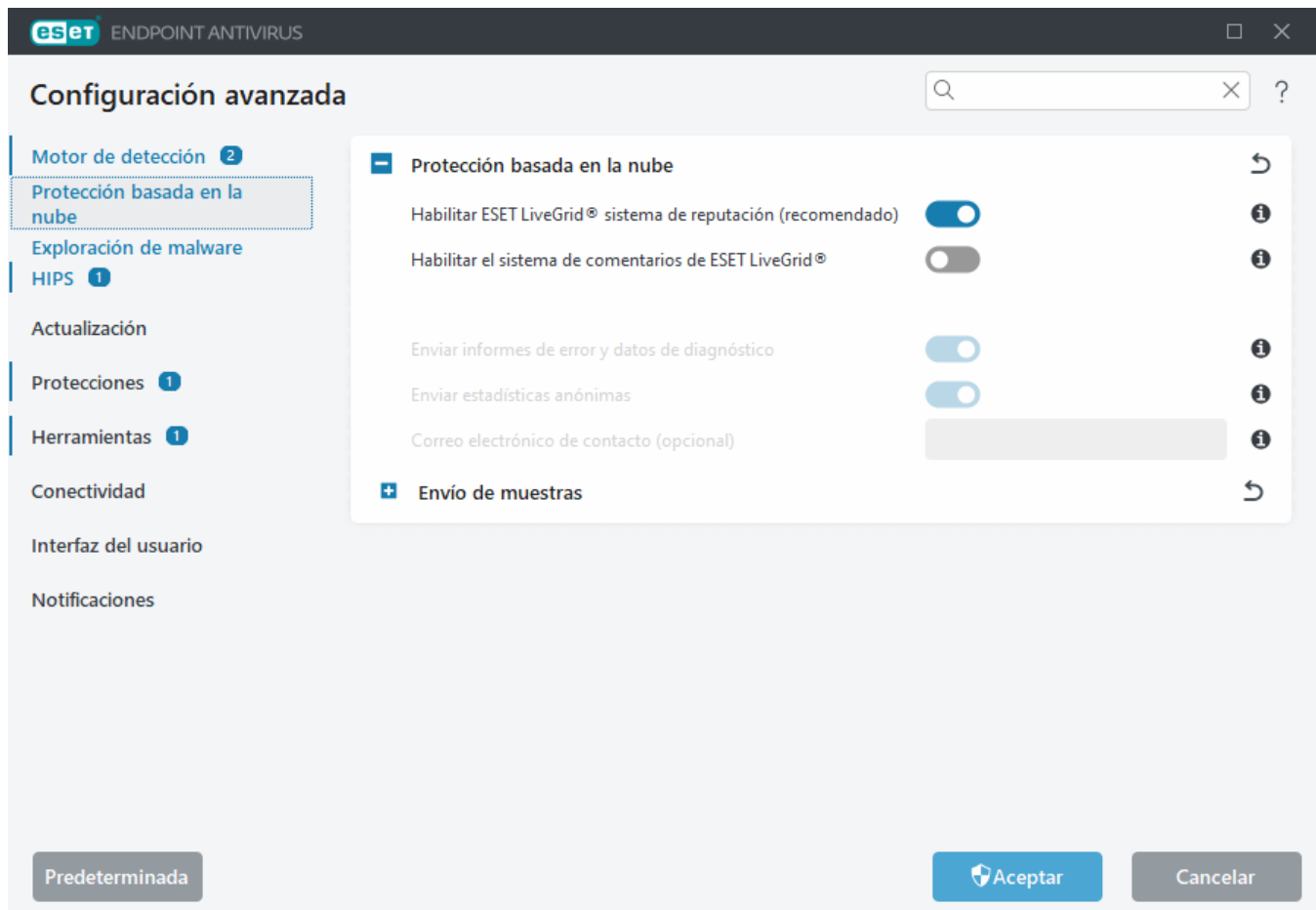
**Habilitar ESET LiveGuard** ([ESET LiveGuard](#) es una funcionalidad adicional vendida por ESET y no está disponible de forma predeterminada): ESET LiveGuard es un servicio pago proporcionado por ESET. Tiene por finalidad agregar una capa de protección diseñada de manera específica para atenuar las amenazas que son nuevas y se encuentran en actividad. Los archivos sospechosos se envían automáticamente a la nube de ESET. Allí, nuestros [motores de detección de malware avanzados](#) los analizan. El usuario que proporcionó la muestra recibirá un informe sobre comportamiento con un resumen del comportamiento de la muestra observada.

**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. 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 los ajustes 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, las muestras que casi no se detectan o alguno de los [módulos de protección](#) de ESET Endpoint Antivirus consideran estas muestras sospechosas o con un comportamiento poco claro.

- **Ejecutables** – Incluye archivos 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 como .bat, .cmd, .hta, .js, .vbs, .ps1.
- **Otros** – Incluye tipos de archivos como .jar, .reg, .msi, .sfw, .lnk.

- **Posibles correos electrónicos spam** – Esto permitirá 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 la lista de todos los tipos de archivos de documento incluidos](#)

ACCD, ACCDB, ACCDT, DOC, DOC\_OLD, DOC\_XML, DOCX, DCM, 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](#) > **Protección basada en la nube** > **Envío de muestras** > **Exclusiones** y agregue la exclusión \*download.domain.com\*.

**Tamaño máximo de muestras (MB):** define el tamaño máximo de las muestras que se envían automáticamente (1-64 MB).


## ESET LiveGuard


Para habilitar el servicio de ESET LiveGuard en una máquina de cliente que usa la consola web ESET PROTECT, consulte [Configuración de ESET LiveGuard para ESET Endpoint Antivirus](#).

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.

# 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, abra la [Configuración avanzada](#) > **Motor de detección** > **Protección en la nube** > **Envío de muestras** > **Exclusiones** y agregue la exclusión \*download.domain.com\*.

# Exploración de malware

Se puede acceder a la sección **Exploración de malware** desde [Configuración avanzada](#) > **Motor de detección** > **Exploración de malware** y le permite configurar los parámetros de exploración para los perfiles de exploración.

## Exploración a pedido

**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.

Después de seleccionar el perfil de exploración, puede configurar las siguientes opciones:

**Destinos de exploración:** si desea explorar un objeto específico o un grupo de objetos, haga clic en **Editar** junto a **Destinos de exploración** y elija una opción desde la estructura (de árbol) de la carpeta. Consulte [Destinos de exploración](#) para obtener información detallada.

**Respuestas de detección y análisis bajo demanda:** puede configurar los niveles de informes y protección para cada perfil de análisis. De forma predeterminada, los perfiles de exploración utilizan la misma configuración definida en la [protección del sistema de archivos en tiempo real](#). Desactive el interruptor junto a **Usar configuración de protección en tiempo real** para configurar niveles de protección e informes personalizados. Consulte [Protecciones](#) para obtener una explicación detallada de los niveles de informes y protección.

**ThreatSense:** opciones de configuración avanzada, como las extensiones de archivo que desea controlar y los métodos de detección utilizados. Consulte [ThreatSense](#) para obtener más información.

## Perfiles de exploración

Hay cuatro perfiles de exploración predefinidos en ESET Endpoint 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 [Configuración avanzada](#) > **Motor de detección** > **Exploración de malware** > **Exploración a demanda** > **Lista de perfiles** > **Editar**. 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

[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.

## Exploración en estado inactivo

Puede habilitar la exploración en estado inactivo en [Configuración avanzada](#) > **Motor de detección** > **Exploración de malware** > **Exploración en estado inactivo**.

### Exploración en estado inactivo

Habilite el interruptor junto a **Habilitar 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 el interruptor junto a **Ejecutar incluso si el equipo recibe alimentación de la batería** en la Configuración avanzada.

Encienda el interruptor junto a **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.

**ThreatSense:** opciones de configuración avanzada, como las extensiones de archivo que desea controlar y los métodos de detección utilizados. Consulte [ThreatSense](#) para obtener más información.

## Detección en estado inactivo

La configuración de la detección en estado inactivo puede establecerse desde [Configuración avanzada](#) > **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 el interruptor de cada estado correspondiente para habilitar o deshabilitar los desencadenantes de la detección en estado inactivo.

## 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](#). Para obtener instrucciones detalladas sobre la creación y administración de tareas programadas, consulte la [Creación de tareas nuevas](#).

**ThreatSense:** opciones de configuración avanzada, como las extensiones de archivo que desea controlar y los métodos de detección utilizados. Consulte [ThreatSense](#) para obtener más información.

## 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.

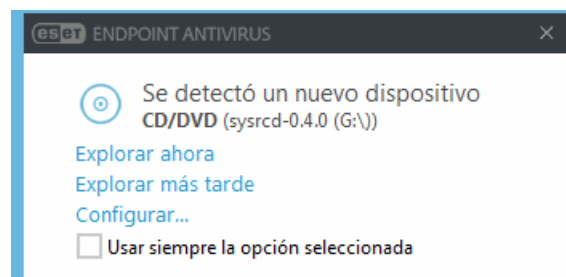
**Prioridad de exploración:** el nivel de prioridad usado para determinar cuándo se iniciará una exploración:

- **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.

## Medios extraíbles

ESET Endpoint 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 [Configuración avanzada](#) > **Motor de detección** > **Exploración de malware** > **medios extraíbles**, 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 [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 Endpoint 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 la [Configuración avanzada](#) > **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.
- **Análisis forzado de dispositivo:** se llevará a cabo un análisis del dispositivo de los medios extraíbles insertado y no se podrá cancelar.
- **Mostrar las opciones de exploración** – abre la sección de configuración de **medios extraíbles**.

## 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](#) > **Motor de detección** > **Exploración de malware** > **Protección de documentos** y haga clic en el interruptor junto a **Habilitar la protección de documentos**.

**ThreatSense:** opciones de configuración avanzada, como las extensiones de archivo que desea controlar y los métodos de detección utilizados. Consulte [ThreatSense](#) para obtener más información.



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).

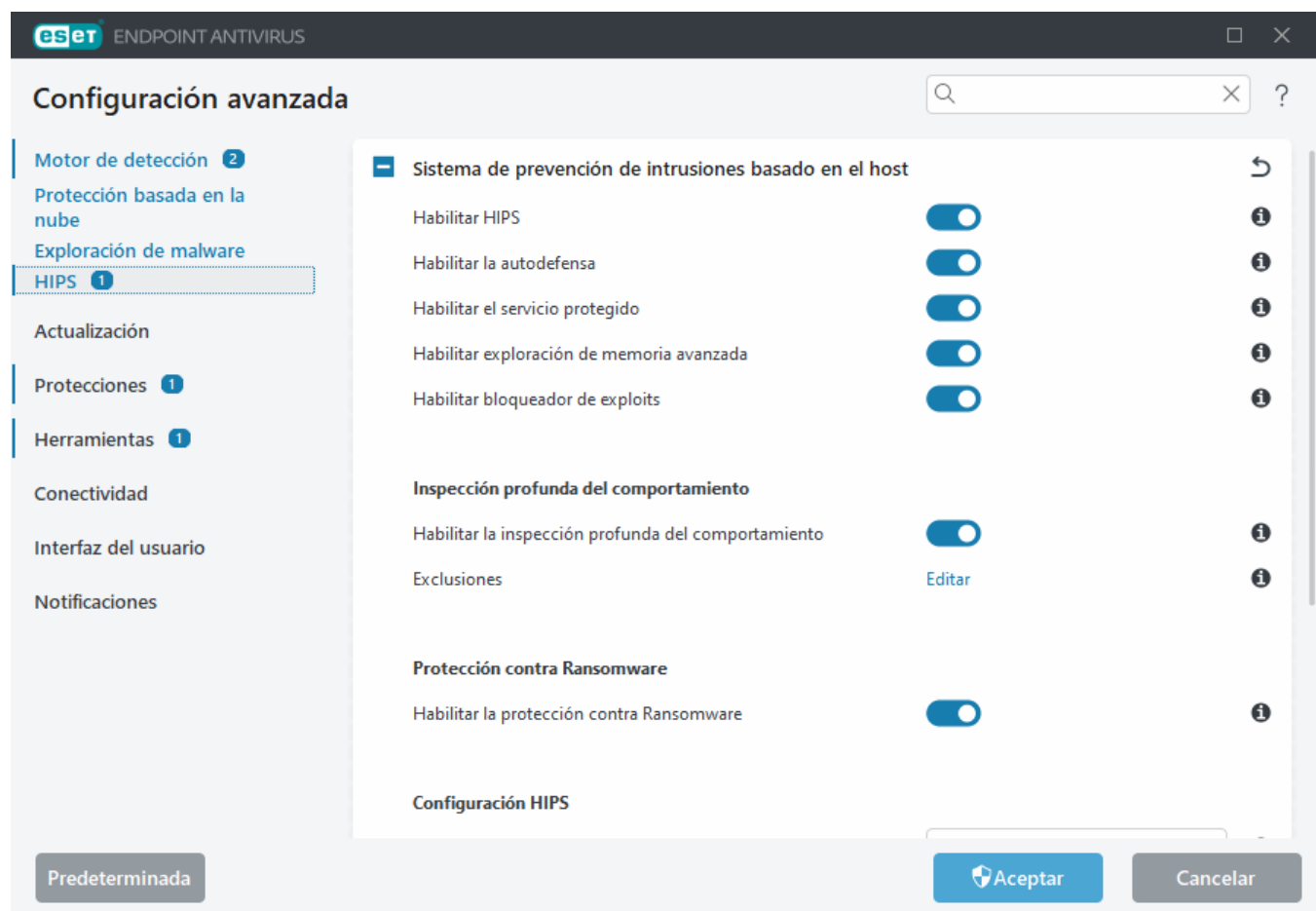
## HIPS: Sistema de prevención de intrusiones basado en el host)



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.

Puede configurar los ajustes de HIPS en [Configuración avanzada](#) > **Motor de detección** > **HIPS** > **Sistema de prevención de intrusiones basado en el host**. El estado de HIPS (habilitado/deshabilitado) se muestra en [la ventana principal del programa](#) de ESET Endpoint Antivirus > **Configuración** > **Equipo**.



## Sistema de prevención de intrusiones basado en el host

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

**Habilitar la autodefensa:** ESET Endpoint 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. El agente ESET Management se protege también cuando se instala.

**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. Esta opción está disponible en Windows 8.1 y Windows 10.

**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](#).

**Habilitar el modo de auditoría:** todo lo que detecta la protección contra Ransomware no se bloquea automáticamente, sino que [se registra con una advertencia de severidad](#) y se envía a la consola de administración con el indicador "MODO DE AUDITORÍA". El administrador puede decidir excluir dicha detección para evitar una posterior detección, o mantenerla activa, lo que significa que una vez que finalice el modo de auditoría, esta se bloqueará o eliminará. La habilitación/deshabilitación del modo de auditoría también se registrará en ESET Endpoint Antivirus. Esta opción está disponible solo en el editor de configuración de la política de ESET PROTECT.

## Configuración HIPS

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

Modo de filtrado	Descripción
<b>Modo automático</b>	Las operaciones están habilitadas, excepto las que se encuentran bloqueadas por las reglas predefinidas que protegen su sistema.
<b>Modo inteligente</b>	Se notificará al usuario solo en caso de eventos muy sospechosos.
<b>Modo interactivo</b>	El programa le solicitará al usuario que confirme las operaciones.
<b>Modo basado en políticas</b>	Bloquea todas las operaciones que no están definidas por una regla específica que las permite.

Modo de filtrado	Descripción
<b>Modo de aprendizaje</b>	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 <b>reglas HIPS</b> , pero su prioridad es inferior a la de las reglas creadas manualmente o en el modo automático. Cuando selecciona el <b>Modo de aprendizaje</b> en el menú desplegable <b>Modo de filtrado</b> , la <b>configuración del modo de aprendizaje finalizará</b> 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](#).

## Exclusiones de HIPS

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

Para editar exclusiones de HIPS, abra [Configuración avanzada](#) > **Motor de detección** > **HIPS** > **Sistema de prevención de intrusiones basado en el host** > **Exclusiones** > **Editar**.

**i** 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.

## 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.

**Eliminar** – 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 Endpoint Antivirus rellena la lista automáticamente con el correr del tiempo.

**i** Los controladores que siempre se pueden cargar son específicos para cada dispositivo y no se pueden editar mediante la política de ESET PROTECT. Tras la instalación, la lista de controladores está vacía. ESET Endpoint Antivirus rellena la lista automáticamente con el correr del tiempo.

## 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**:

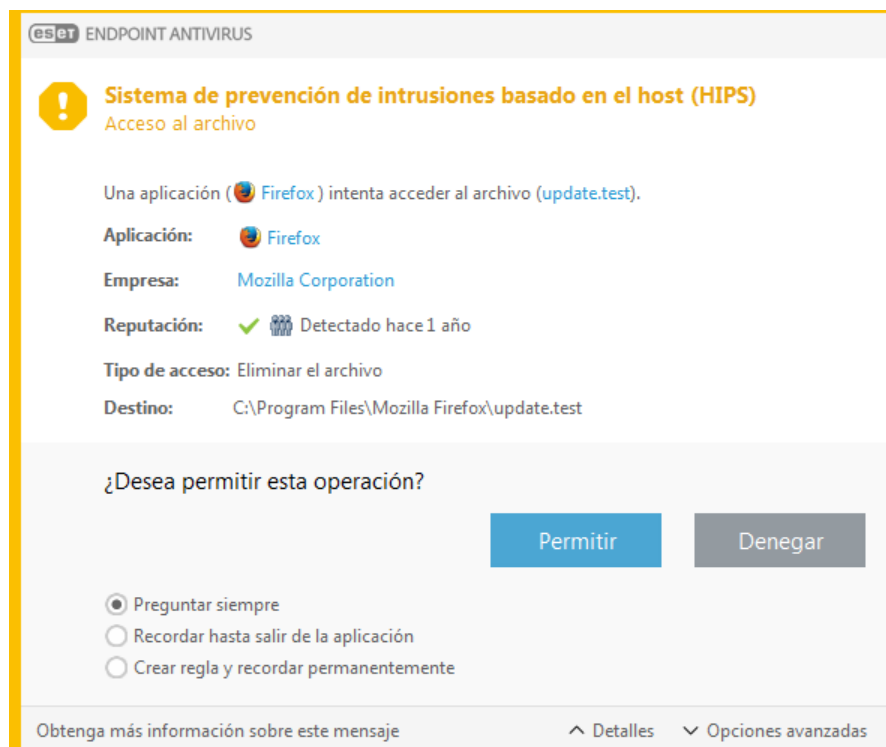
- **Crear una regla válida solo para esta aplicación:** si quita la marca de verificación de esta casilla, se creará

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.



Para evitar que aparezcan las notificaciones, cambie el modo de filtrado a **Modo automático** en [Configuración avanzada](#) > **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

Esta es 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 esta opción 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 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)

## Configuración de reglas HIPS

Vea primero [Administración de reglas del 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 alternar 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 desencadena un evento, aparece una notificación 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 agregar carpetas o archivos nuevos, o puede seleccionar **Todas las entradas** en el menú desplegable para agregar todas las aplicaciones.

**i** 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.

**i** Al especificar una ruta, C:\example afecta las acciones con la propia carpeta y C:\example\\*. \* afecta los archivos en la carpeta.

## 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.

### Uso de comodines en las reglas

Un asterisco en las reglas sólo se puede utilizar para sustituir una determinada clave, por ejemplo, "HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\\*\Start". No se admiten otras formas de utilizar comodines.

### **i** Crear reglas dirigidas a la clave HKEY\_CURRENT\_USER

Esta clave es sólo un enlace a la subclave apropiada de HKEY\_USERS específica para el usuario identificado por SID (identificador seguro). Para crear una regla sólo para el usuario actual, en lugar de utilizar una ruta a HKEY\_CURRENT\_USER, utilice una ruta que dirija a HKEY\_USERS\%SID%. Como un SID puede utilizar un asterisco para que la regla sea aplicable a todos los usuarios.

**!** 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 el interruptor **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.

The screenshot shows the 'Configuraciones de reglas HIPS' window in ESET Endpoint Antivirus. The window has a title bar with the ESET logo and 'ENDPOINT ANTIVIRUS'. The main area contains several settings:

- Nombre de regla:** A text box containing 'Sin título'.
- Acción:** A dropdown menu set to 'Permitir'.
- Operaciones que afectan:** A section with three toggle switches: 'Archivos de destino' (off), 'Aplicaciones' (off), and 'Entradas de registro' (off).
- Habilitado:** A toggle switch that is turned on (blue).
- Severidad de registro:** A dropdown menu set to 'Ninguno'.
- Notificar al usuario:** A toggle switch that is turned off (grey).

At the bottom of the window are three buttons: 'Atrás' (disabled), 'Siguiente' (active/highlighted), and 'Cancelar' (disabled).

# 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*

## Actualización

Las opciones de configuración de la actualización están disponibles en [Configuración avanzada](#) > **Actualizar**. 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.



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 HTTPS).

### Actualización

El perfil de actualización que está actualmente en uso se muestra en el menú desplegable **Seleccionar perfil de actualización predeterminado**.

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

**Configurar notificaciones de actualización:** haga clic en Editar para seleccionar qué [notificaciones de la aplicación](#) se muestran. Puede elegir si las notificaciones se Muestran en el escritorio y/o Se envían por correo electrónico.

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

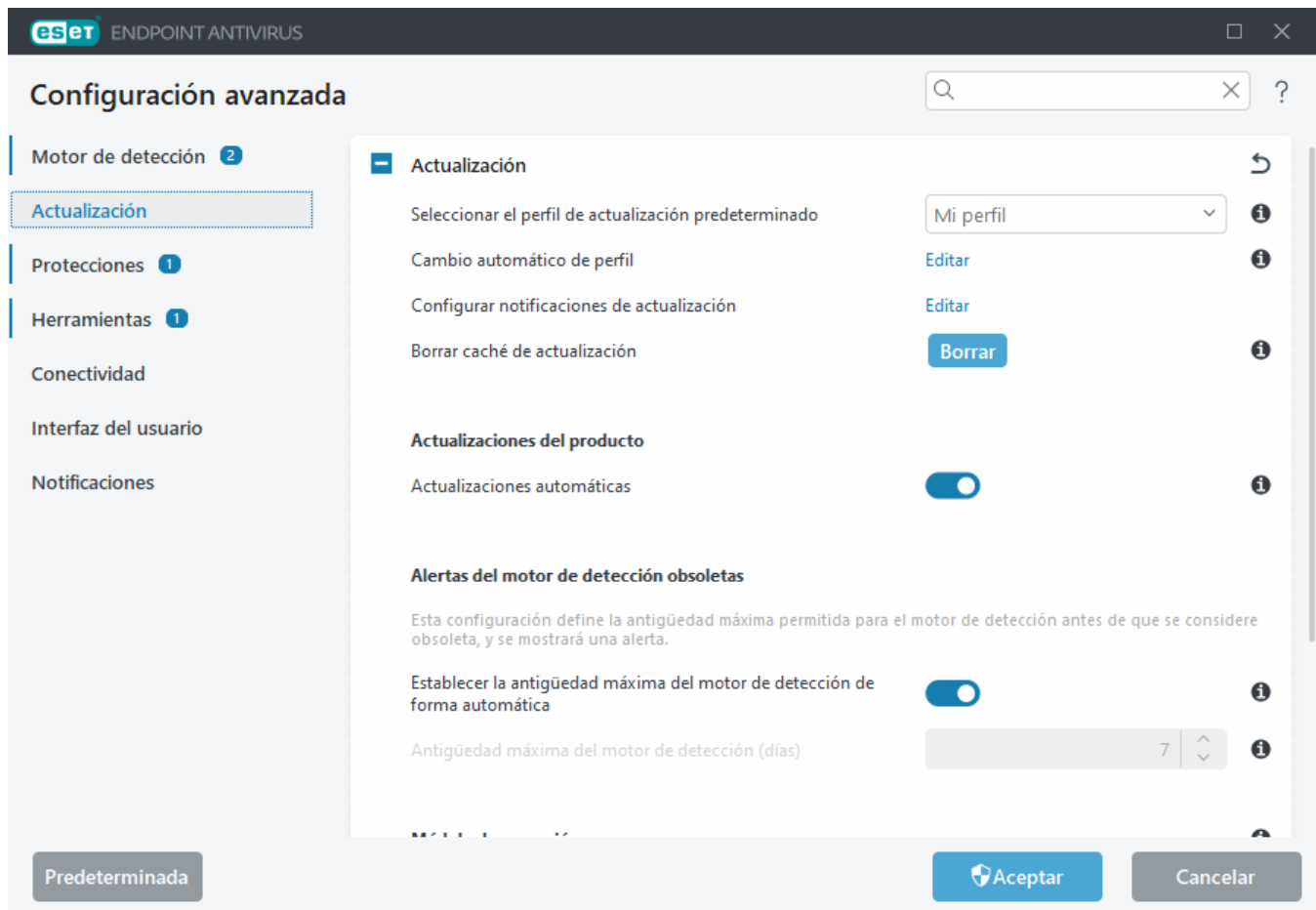
## Alertas del motor de detección obsoletas

**Establecer automáticamente una edad máxima para el motor de detección** :permite establecer el tiempo máximo (en días) luego del cual se informará que el motor de detección está obsoleto. El valor predeterminado de la **edad máxima del motor de detección** es 7.

## Módulo de reversión

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.





## 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**.

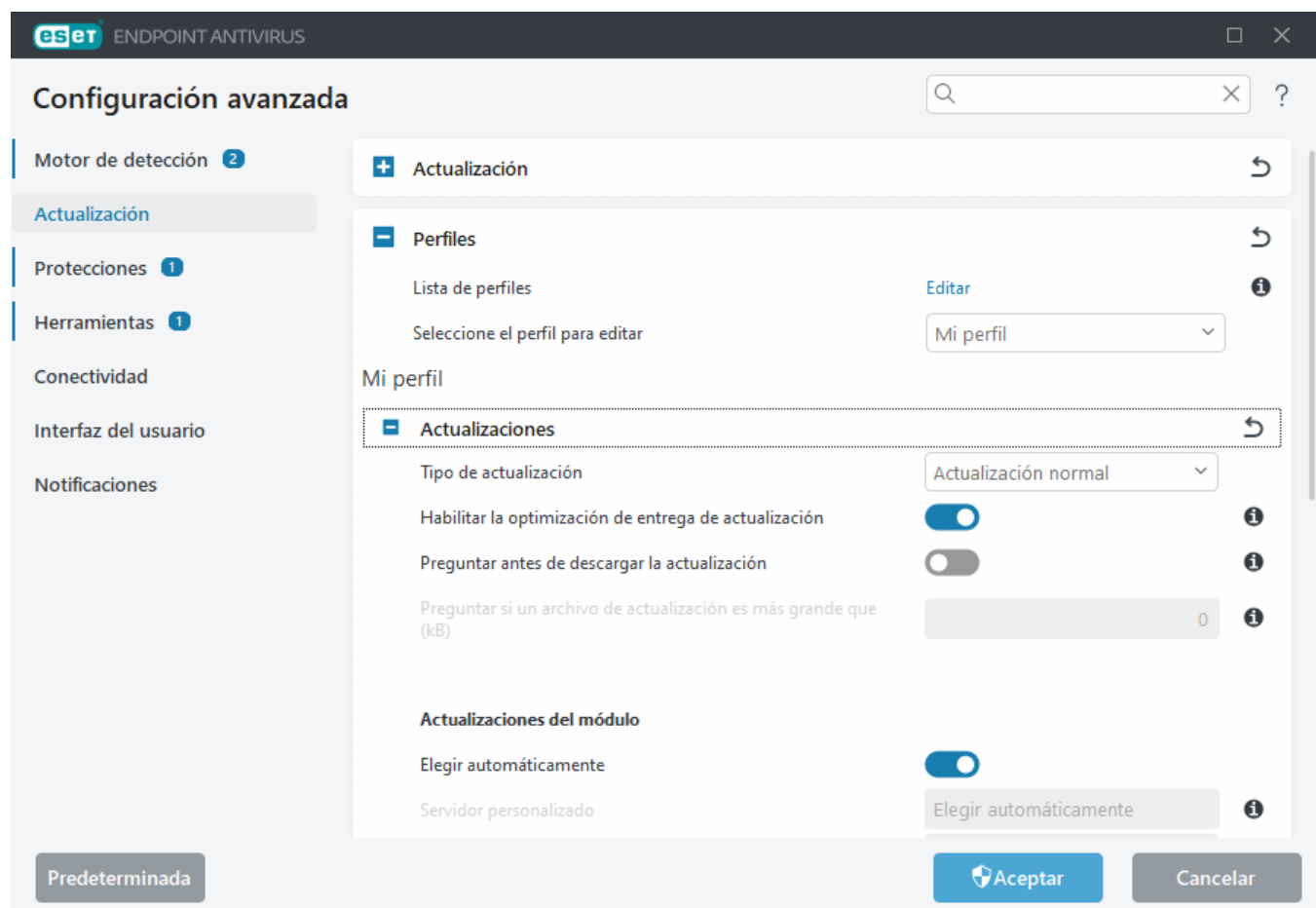
Para crear un perfil nuevo, haga clic en **Editar** junto a la **Lista de perfiles**, ingrese su propio **Nombre de perfil** y luego haga clic en **Agregar**.

## 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. Actualización demorada: permite hacer la actualización desde los servidores de actualización especial que proporcionan nuevas versiones de bases de datos de virus con un retraso de por lo menos X horas (es decir, bases de datos revisadas en un entorno real y por lo tanto consideradas como estables).

**Habilitar la optimización de entrega de actualización** – Cuando está habilitado, los archivos de actualización se pueden descargar desde CDN (red de entrega de contenido). Deshabilitar esta configuración puede interrumpir o ralentizar las descargas cuando los servidores de actualización dedicados de ESET están sobrecargados. Deshabilite esta opción cuando un firewall solo puede acceder a [direcciones de IP del servidor de actualizaciones de ESET](#) o cuando una conexión a los servicios de CDN no funciona.

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



## Actualizaciones de módulo

La opción **Elegir automáticamente** está habilitada de manera predeterminada. La opción **Servidor personalizado** es la ubicación donde se almacenan las actualizaciones. Si usa un servidor de actualización de ESET, recomendamos que deje seleccionada la opción predeterminada.

**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.

**Permitir actualizaciones del módulo desde medios extraíbles:** le permite actualizar desde medios extraíbles si contiene un mirror creado. Cuando se selecciona Automático, la actualización no se ejecutará en el fondo. Si desea mostrar diálogos de actualización, seleccione Preguntar siempre.

Cuando use un servidor HTTP local (también conocido como Mirror), el servidor de actualización debe ingresarse de la siguiente manera:

*[http://nombre\\_computadora\\_o\\_su\\_direccion\\_IP:2221](http://nombre_computadora_o_su_direccion_IP:2221)*

Cuando use un servidor HTTP local con SSL, el servidor de actualización debe ingresarse de la siguiente manera:  
*https://nombre\_computadora\_o\_su\_direccion\_IP:2221*

Cuando use una carpeta compartida local, el servidor de actualización debe configurarse de la siguiente manera:

*\\nombre\_computadora\_o\_su\_direccion\_IP\carpeta\_compartida*



El número de puerto del servidor de HTTP especificado en los ejemplos de arriba depende de qué puerto escuche su servidor de HTTP/HTTPS.

## Actualizaciones del producto

Consulte las [Actualizaciones del producto](#).

## Opciones de conexión

Vea [Opciones de conexión](#).

## Mirror de actualización

Vea [Mirror de actualización](#).

# Actualizar reversión

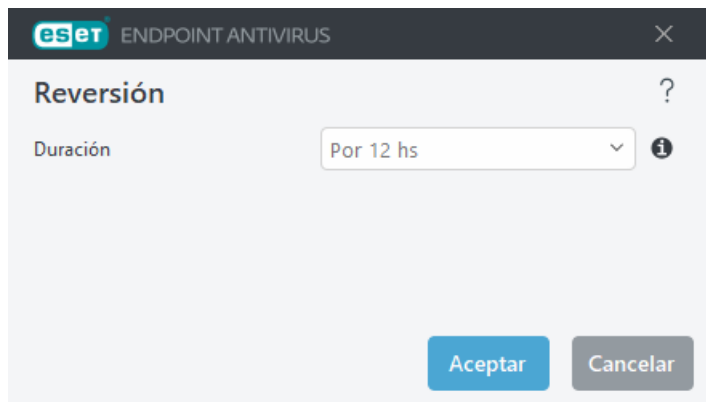
Si sospecha que la nueva actualización del motor de detección o los módulos de programas pueden ser inestables o estar corruptos, puede hacer una reversión a la versión anterior y deshabilitar cualquier actualización de manera temporal. O bien puede habilitar las actualizaciones que se deshabilitaron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

ESET Endpoint 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.



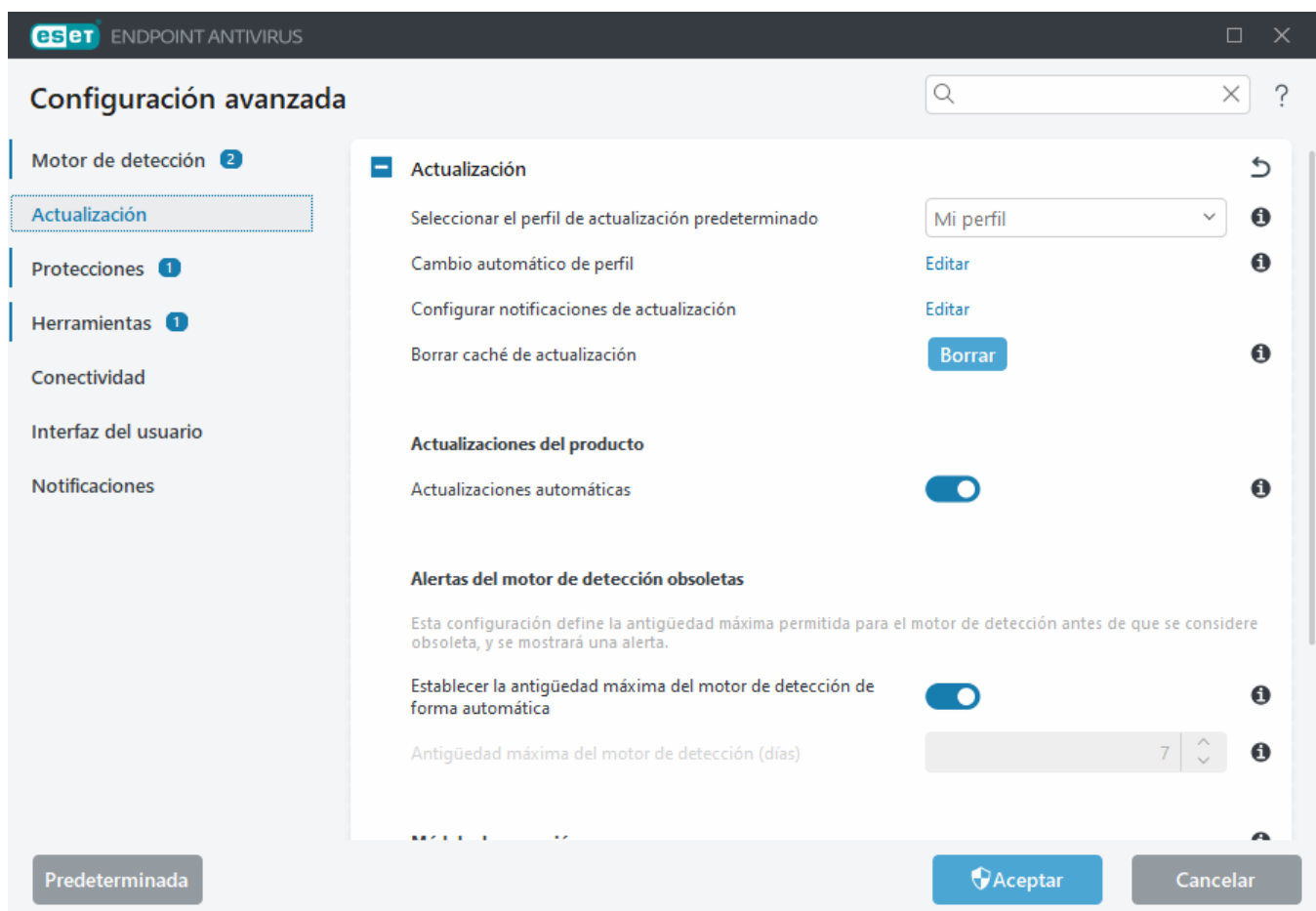
Cuando se alcanza la cantidad máxima de instantáneas (por ejemplo, tres), la instantánea más antigua se reemplaza con una nueva cada 48 horas. ESET Endpoint Antivirus revierte las versiones de actualización del motor de detección y del módulo del programa a la instantánea más antigua.

Abra [Configuración avanzada](#) > **Actualización** > **Actualización** > **Reversión de módulo** > **Reversión** para seleccionar un intervalo de tiempo en el menú desplegable **Duración**.



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

Si se realiza una reversión, el botón **Revertir** cambia a **Permitir actualizaciones**. No se 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](#).

## Actualizaciones del producto

La sección **Actualizaciones del producto** contiene las opciones relacionadas con las actualizaciones del producto. El programa le permite predefinir su conducta cuando esté disponible una nueva actualización del producto.


Las actualizaciones del producto incorporan nuevas características o incluyen modificaciones a las ya existentes en versiones anteriores. Puede realizarse automáticamente sin la intervención del usuario, pero también puede elegir recibir una notificación. Luego de instalar las actualizaciones del producto, es posible que se requiera reiniciar el equipo.

**Actualizaciones automáticas:** al pausar las actualizaciones automáticas para perfiles de actualización específicos, se desactivan temporalmente las actualizaciones automáticas del producto mientras está conectado a Internet mediante otras redes o conexiones en pantalla. Mantenga este ajuste activado para tener acceso constante a las funciones más recientes y a la máxima protección posible. Para obtener más información sobre las actualizaciones automáticas, consulte las [Preguntas frecuentes sobre actualizaciones automáticas](#).

De manera predeterminada, se descargan las actualizaciones del producto desde los servidores del repositorio de ESET. En entornos grandes o sin conexión, el tráfico puede distribuirse para permitir el caché interno de los archivos del producto.

### [Definir el servidor personalizado para las actualizaciones de los componentes del programa](#)

1. Defina la ruta para las actualizaciones del producto en el campo **Servidor personalizado**. Puede ser un enlace de HTTP(S), una ruta de uso compartido de red SMB, una unidad de disco local o una ruta de medios extraíbles. Para las unidades de red, utilice la ruta UNC en lugar de una carta de unidad controlada.
2. Deje los campos **Nombre de usuario** y **Contraseña** en blanco, si no son obligatorios. De ser necesario, defina las credenciales correspondientes aquí para la autenticación de HTTP en el servidor web personalizado.
3. Confirme los cambios y pruebe la presencia de una actualización del producto usando una actualización estándar de ESET Endpoint Antivirus.

 La selección de la opción más apropiada depende de la estación de trabajo donde se aplicará la configuración. Tenga en cuenta que existen diferencias entre las estaciones de trabajo y los servidores; por ejemplo, el reinicio automático de un servidor después de la actualización de un producto podría provocar serios daños a su empresa.

## Opciones de conexión

Para acceder a las opciones de configuración del servidor proxy para un perfil de actualización específico, abra [Configuración avanzada](#) > **Actualización** > **Perfiles** > **Actualizaciones** > **Opciones de conexión**.

## Servidor proxy

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

Seleccione la opción **Usar la configuración global del servidor proxy**, para usar la configuración del servidor proxy ya especificada en [Configuración avanzada](#) > **Conectividad** > **Servidor proxy**.

Seleccione **No usar servidor proxy** para indicar que no se usará ningún servidor proxy para actualizar ESET Endpoint 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 **Herramientas** > **Servidor proxy** para actualizar ESET Endpoint 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 Endpoint 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 navegador, 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.

## Compartir de Windows

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

Para configurar dicha cuenta, seleccione en el menú desplegable **Conectarse a LAN como**:


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

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

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

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


Las configuraciones de **Nombre de usuario y contraseña** son opcionales.


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

Seleccione **Desconectar** del servidor después de la actualización para forzar una desconexión si la conexión al servidor permanece activa aunque las actualizaciones se hayan terminado de descargar.

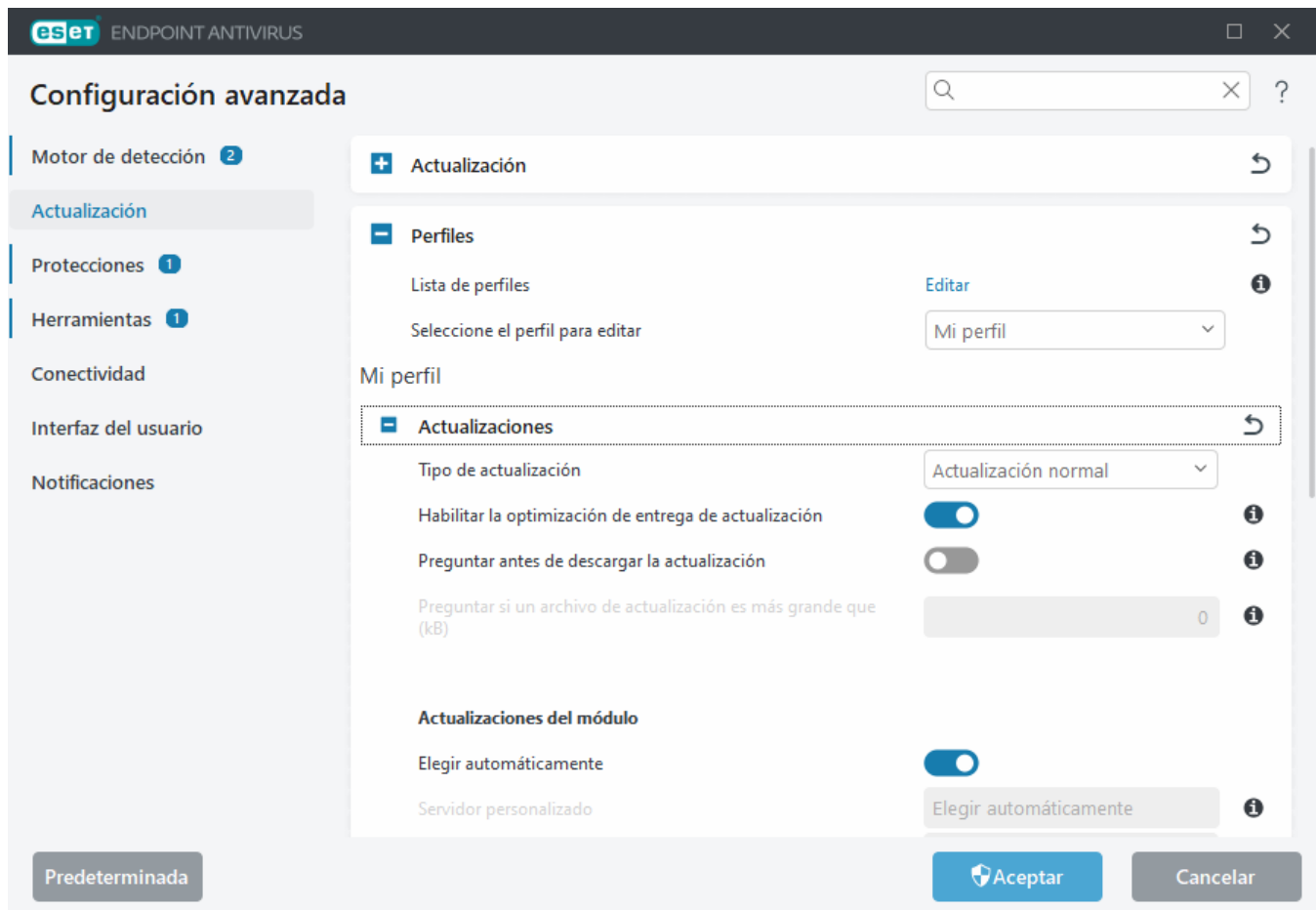
## Actualizar reflejo

ESET Endpoint Antivirus le permite crear copias de archivos de actualización que se pueden utilizar para actualizar otras estaciones de trabajo en la red. El uso de un “servidor reflejado” – es conveniente tener una copia de los archivos de actualización en el entorno de la LAN debido a que las estaciones de trabajo no necesitan descargar los archivos de actualización desde el servidor de actualización del proveedor reiteradamente. Las actualizaciones se descargan al servidor mirror local y, desde allí, se distribuyen a todas las estaciones de trabajo para evitar el riesgo de generar una sobrecarga en el tráfico de red. La actualización de las estaciones de trabajo cliente desde un mirror optimiza el equilibrio de carga de la red y preserva el ancho de banda de la conexión a Internet.

 El mirror de actualización crea copias de los archivos de actualización que se pueden usar para actualizar estaciones de trabajo que ejecutan la misma generación de ESET Endpoint Antivirus para Windows. (Por ejemplo, ESET Endpoint Antivirus para Windows versión 10.x solo crea archivos de actualización para la versión 10.x de ESET Endpoint Antivirus para Windows y ESET Endpoint Security para Windows)

 Para minimizar el tráfico de Internet en redes donde se usa ESET PROTECT para administrar una gran cantidad de clientes, recomendamos que use ESET Bridge en lugar de configurar un cliente como servidor mirror. ESET Bridge se puede instalar con ESET PROTECT mediante el instalador todo en uno o como un componente independiente. Para obtener más información y conocer las diferencias entre ESET Bridge, Apache HTTP Proxy, la herramienta de replicación y la conectividad directa, consulte nuestra [página de ayuda en línea de ESET PROTECT](#).

Las opciones de configuración del servidor Mirror local se encuentran en [Configuración avanzada](#) > **Actualización** > **Perfiles** > **Mirror de actualización**.



Para crear un servidor reflejado en la estación de trabajo de un cliente, habilite **Crear mirror de actualización**. Al habilitar esta opción, se activan otras opciones de configuración del Mirror, tales como la forma de acceder a los archivos de actualización y la ruta de actualización a los archivos replicados.

## Acceder a los archivos de actualización

**Habilitar servidor HTTP interno:** si esta opción se encuentra habilitada, se puede acceder a los archivos de [actualización a través de HTTP](#), sin necesidad de ingresar credenciales.

Los métodos para acceder al servidor Mirror se describen en detalle en [Actualizar desde el Mirror](#). Existen dos métodos básicos para acceder al Mirror – la carpeta con los archivos de actualización puede presentarse como una carpeta compartida de red, o los clientes pueden acceder al servidor reflejado ubicado en un servidor HTTP.


La carpeta destinada a almacenar los archivos de actualización para el Mirror se define en **Carpeta para almacenar los archivos replicados**. Para elegir una carpeta diferente, haga clic en **Eliminar** para borrar la carpeta predefinida `C:\ProgramData\ESET\ESET Endpoint Antivirus\mirror` y haga clic en **Editar** para buscar una carpeta en la computadora local o en la carpeta de red compartida. Si la carpeta especificada requiere una autorización, deberá ingresar los datos de autenticación en los campos **Nombre de usuario** y **Contraseña**. Si la carpeta de destino seleccionada está en un disco de la red cuyo sistema operativo es Windows NT, 2000 o XP, el nombre de usuario y la contraseña especificados deben contar con privilegios de escritura para la carpeta seleccionada. El nombre de usuario se deben ingresar con el formato *Dominio/Usuario* o *Grupo de trabajo/Usuario*. Recuerde que debe proporcionar las contraseñas correspondientes.



# Servidor HTTP y SSL para Mirror


En la sección **Servidor HTTP** de la pestaña **Mirror**, puede especificar el **Puerto del servidor** donde escuchará el servidor HTTP, así como el tipo de **Autenticación** que usa el servidor HTTP. En forma predeterminada, el puerto del servidor está establecido en **2221**.

**Autenticación** – define el método de autenticación utilizado para acceder a los archivos de actualización. Se encuentran disponibles las siguientes opciones: **Ninguna**, **Básica** y **NTLM**. Seleccione la opción **Básica** para usar la codificación de Base64 con la autenticación básica del nombre de usuario y la contraseña. La opción **NTLM** proporciona una codificación obtenida mediante un método seguro. Para la autenticación, se utiliza el usuario creado en la estación de trabajo que comparte los archivos de actualización. La configuración predeterminada es **Ninguna**, que otorga acceso a los archivos de actualización sin necesidad de autenticar.

 Los datos de autenticación, como el **Nombre de usuario** y la **Contraseña** sirven solo para acceder al servidor HTTP Mirror. Complete estos campos solo si el nombre de usuario y la contraseña son necesarios.


Añada su **Archivo de cadena de certificados** o genere un certificado de firma automática si desea ejecutar el servidor HTTP con el soporte de HTTPS (SSL). Se encuentran disponibles los siguientes **tipos de certificado**: ASN, PEM y PFX. Para obtener una seguridad adicional, puede usar el protocolo HTTPS para descargar los archivos de actualización. Es casi imposible realizar un seguimiento de las transferencias de datos y credenciales de registro con este protocolo. La opción **Tipo de clave privada** está configurada en **Integrada** de forma predeterminada (y por lo tanto, la opción **Archivo de clave privada** está deshabilitada de forma predeterminada). Esto significa que la clave privada es parte del archivo de cadena de certificados seleccionado.

## Certificados firmados automáticamente para HTTPS Mirror

 Si usa un servidor HTTPS Mirror, debe importar su certificado al almacén de raíz confiable en las máquinas de todos los clientes. Consulte [Instalación del certificado de raíz confiable](#) en Windows.

# Actualización desde el Mirror

Existen dos métodos básicos para configurar un Mirror, que es esencialmente un repositorio desde donde los clientes pueden descargar archivos de actualización. La carpeta con los archivos de actualización se puede presentar como una carpeta compartida de red o como un servidor HTTP.

 El mirror de actualización crea copias de los archivos de actualización que se pueden usar para actualizar estaciones de trabajo que ejecutan la misma generación de ESET Endpoint Antivirus para Windows. (Por ejemplo, ESET Endpoint Antivirus para Windows versión 10.x solo crea archivos de actualización para la versión 10.x de ESET Endpoint Antivirus para Windows y ESET Endpoint Security para Windows)

## Acceso al Mirror mediante un servidor HTTP interno

Esta es la configuración predeterminada que se especifica en la configuración predefinida del programa. Para permitir acceso al Mirror mediante el servidor HTTP, vaya hasta [Configuración avanzada](#) > **Actualizar** > **Perfiles** > **Mirror de actualización** y seleccione **Crear Mirror de actualización**.

En la sección **Servidor HTTP** de la pestaña **Mirror**, puede especificar el **Puerto del servidor** donde escuchará el servidor HTTP, así como el tipo de **Autenticación** que usa el servidor HTTP. En forma predeterminada, el puerto del servidor está establecido en **2221**.

**Autenticación** – define el método de autenticación utilizado para acceder a los archivos de actualización. Se encuentran disponibles las siguientes opciones: **Ninguna**, **Básica** y **NTLM**. Seleccione la opción **Básica** para usar la codificación de Base64 con la autenticación básica del nombre de usuario y la contraseña. La opción **NTLM** proporciona una codificación obtenida mediante un método seguro. Para la autenticación, se utiliza el usuario creado en la estación de trabajo que comparte los archivos de actualización. La configuración predeterminada es **Ninguna**, que otorga acceso a los archivos de actualización sin necesidad de autenticar.



Si desea permitir el acceso a los archivos de actualización a través del servidor HTTP, la carpeta del Mirror debe estar ubicada en el mismo equipo que la instancia de ESET Endpoint Antivirus que la crea.



El error **Nombre de usuario y/o contraseña no válidos** aparecerá en el panel de actualización del menú principal luego de varios intentos fallidos de actualizar desde Mirror. Le recomendamos que navegue hasta [Configuración avanzada](#) > **Actualización** > **Perfiles** > **Mirror de actualización** y verifique el nombre de usuario y la contraseña. El motivo más común de este error es el ingreso incorrecto de los datos de autenticación.

Después de configurar su servidor Mirror, debe agregar el nuevo servidor de actualización en las estaciones de trabajo cliente. Para hacerlo, siga estos pasos:

- Abra [Configuración avanzada](#) y haga clic en **Actualizar** > **Perfiles** > **Actualizaciones** > **Actualizaciones de módulo**.
- Deshabilitar **Elegir automáticamente** y agregue un nuevo servidor al **campo** Servidor de actualización mediante uno de los siguientes formatos:  
*http://IP\_address\_of\_your\_server:2221*  
*https://IP\_address\_of\_your\_server:2221* (si se utiliza SSL)

## Acceder al Mirror mediante el uso compartido del sistema

En primer lugar, se debe crear una carpeta compartida en un dispositivo local o de red. Cuando se crea la carpeta para el Mirror, se deberá proporcionar el acceso de “escritura” para el usuario que guardará los archivos de actualización en la carpeta y el acceso de “lectura” para todos los usuarios que actualizarán ESET Endpoint Antivirus desde la carpeta del Mirror.

Luego, configure el acceso al Espejo en la pestaña [Configuración avanzada](#) > **Actualizar** > **Perfiles** > **Mirror de actualización** mediante la deshabilitación de **Habilitar servidor HTTP**. Esta opción está habilitada en forma predeterminada en el paquete de instalación del programa.


Si la carpeta compartida se ubica en otro equipo de la red, es necesario ingresar los datos de autenticación para acceder al otro equipo. Para ingresar datos de autenticación, abra [Configuración avanzada](#) y haga clic en **Actualizar** > **Perfiles** > **Actualizaciones** > **Opciones de conexión** > **Compartir de Windows** > **Conectar a LAN como**. Esta configuración es la misma que se usa para la actualización, como se describe en la sección [Conectarse a la LAN como](#).

Para acceder a la carpeta del Mirror, esto se debe hacer bajo la misma cuenta que la que se utiliza para iniciar sesión en el equipo en el que se ha creado la réplica. En caso de que el equipo se encuentre en un dominio, se debe utilizar el nombre de usuario "dominio\usuario". En caso de que el equipo no se encuentre en un dominio, se debe utilizar "Dirección\_IP\_de\_su\_servidor\usuario" o "nombre de host del servidor\usuario".


Cuando la configuración del Mirror esté completa, en las estaciones de trabajo cliente establezca `\\UNC\RUTA` como el servidor de actualización siguiendo los pasos que figuran a continuación:

1. Abra [Configuración avanzada](#) y haga clic en **Actualizar** > **Perfiles** > **Actualizaciones**.

2. Deshabilitar **Elija automáticamente** junto a **Actualizaciones del módulo** y un nuevo servidor para el campo **Actualizar servidor** mediante el uso del formato `\\UNC\PATH`.

 Para un funcionamiento correcto de las actualizaciones, deberá especificar la ruta a la carpeta del Mirror como una ruta UNC. Es posible que no funcionen las actualizaciones de las unidades asignadas.

### Creación de la replicación con la herramienta de replicación

 La herramienta de replicación crea una estructura de carpetas diferente de la que crea la replicación de Endpoint. Cada carpeta contiene archivos de actualización para un grupo de productos. Debe especificar la ruta completa a la carpeta correcta en la configuración de actualización del producto con la replicación. Por ejemplo, para actualizar ESET PROTECT desde la replicación, establezca el [servidor de actualización](#) en (según la ubicación raíz de su servidor HTTP):  
`http://your_server_address/mirror/eset_upd/ep10`

La última sección controla los componentes del programa (PCU). De forma predeterminada, los componentes del programa descargados están preparados para copiarse en el servidor reflejado local. Si se activan las **Actualizaciones del producto**, no es necesario hacer clic en **Actualización**, ya que los archivos se copian en el servidor reflejado local automáticamente cuando están disponibles. Consulte el [Modo de actualización](#) para obtener más información sobre las actualizaciones del producto.

## Resolución de problemas de actualización desde el Mirror

En la mayoría de los casos, los problemas que surgen durante una actualización desde un servidor Mirror se provocan por uno o más de los siguientes motivos: especificación incorrecta de las opciones de la carpeta del Mirror, datos de autenticación incorrectos para acceder a la carpeta del Mirror, configuración incorrecta en las estaciones de trabajo locales que intentan descargar archivos de actualización desde el Mirror, o una combinación de las razones mencionadas. A continuación, se muestra información general sobre los problemas más frecuentes que pueden surgir durante una actualización desde el Mirror:

**ESET Endpoint Antivirus informa que se produjo un error al conectarse con el servidor Mirror:** probablemente causado por la especificación incorrecta del servidor de actualización (la ruta de red a la carpeta del Mirror) desde donde las estaciones de trabajo locales descargan las actualizaciones. Para verificar la carpeta, haga clic en el menú **Inicio** de Windows, haga clic en **Ejecutar**, ingrese el nombre de la carpeta y haga clic en **Aceptar**. Debería aparecer el contenido de la carpeta.

**ESET Endpoint Antivirus requiere un nombre de usuario y una contraseña:** probablemente causado por datos de autenticación incorrectos (nombre de usuario y contraseña) en la sección de actualización. El nombre de usuario y la contraseña se usan para otorgar acceso al servidor de actualización, desde donde se actualizará el programa. Asegúrese de que los datos de autenticación sean correctos y que se hayan ingresado en el formato requerido. Por ejemplo, Dominio/Nombre de usuario o Grupo de trabajo/Nombre de usuario, con sus contraseñas correspondientes. Si “cualquier persona” puede acceder al servidor Mirror, esté al tanto que esto no significa que cualquier usuario tiene acceso. “Cualquier persona” no significa cualquier usuario no autorizado, solo significa que todos los usuarios del dominio pueden acceder a la carpeta. Como resultado, si “Cualquier persona” puede acceder a la carpeta, el nombre de usuario y la contraseña del dominio deberá ingresarse en la sección de configuración de la actualización.

**ESET Endpoint Antivirus informa que se produjo un error al conectarse con el servidor Mirror:** la comunicación en el puerto definido para acceder a la versión HTTP del Mirror está bloqueada.

**ESET Endpoint Antivirus informa que se produjo un error al descargar archivos de actualización:** probablemente causado por la especificación incorrecta del servidor de actualización (la ruta de red a la carpeta del Mirror) desde donde las estaciones de trabajo locales descargan las actualizaciones.

## Protecciones

Las protecciones defienden el sistema ante ataques maliciosos mediante el control de archivos, correos electrónicos y comunicaciones por Internet. Por ejemplo, la corrección comienza si se detecta un objeto clasificado como malware. Protecciones puede eliminarlo bloqueándolo y luego realizar la limpieza, eliminación o la colocación en cuarentena.

Para configurar las protecciones en detalle, abra [Configuración avanzada](#) > **Protecciones**.



Las modificaciones de las protecciones deben realizarse únicamente por un usuario experimentado. La configuración incorrecta de los ajustes puede reducir el nivel de protección.

En esta sección:

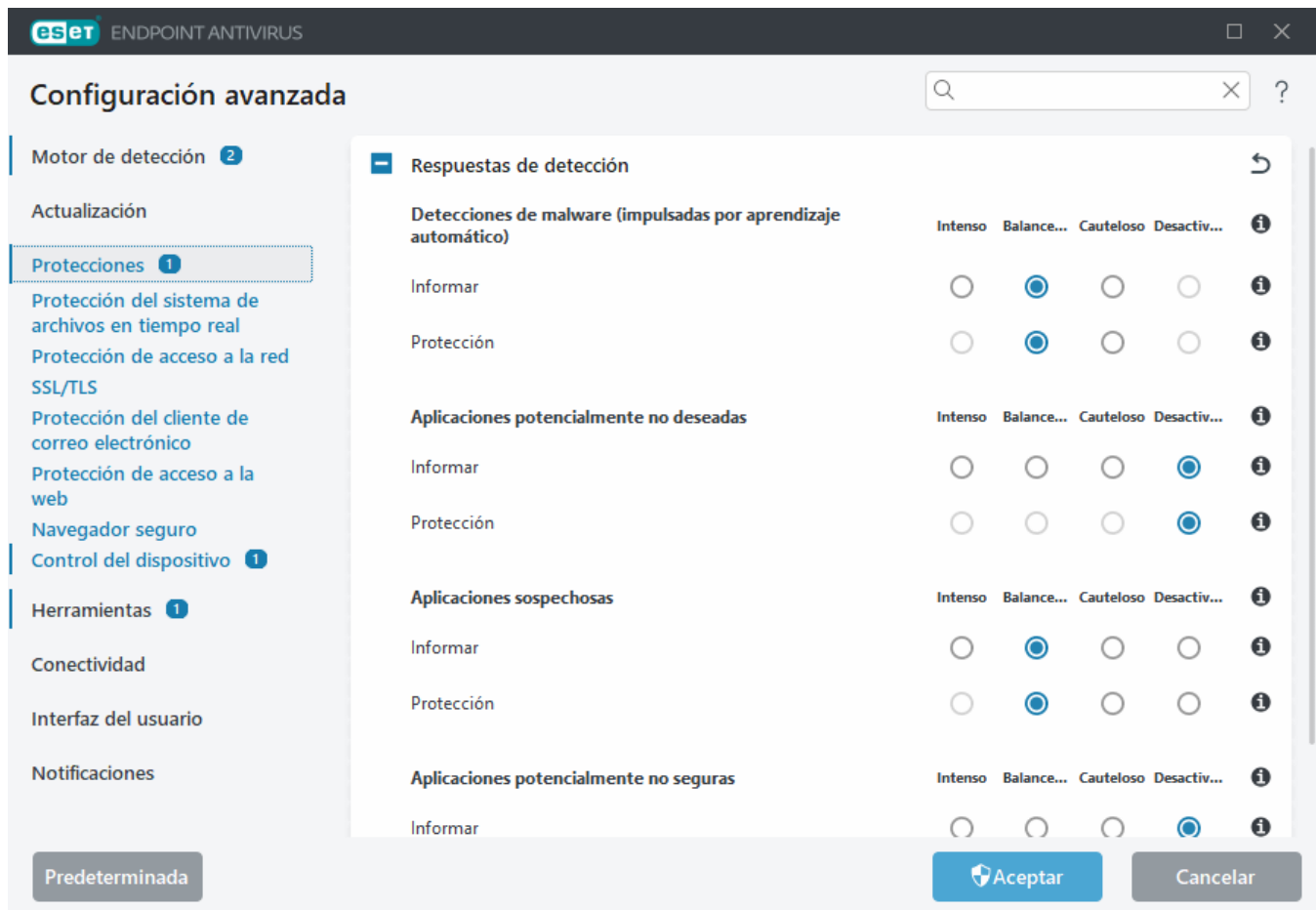
- [Respuestas de detección](#)
- [Configuración de informes](#)
- [Configuración de protección](#)

---

## Respuestas de detección

Las respuestas de detección permiten configurar niveles de informes y protección para las siguientes categorías:

- **Detecciones de malware (impulsadas por aprendizaje automático)** – Un virus del equipo es un programa con códigos maliciosos que está adjunto o añadido a archivos existentes de su equipo. 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

**i** El aprendizaje automático avanzado ahora es parte de las protecciones 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](#).

## 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 Endpoint Antivirus.

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

1. Detecciones de 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
<b>Intenso</b>	Configuración de máxima sensibilidad para informes de CATEGORÍA. Se informan más amenazas. La configuración como <b>"Intenso"</b> puede identificar erróneamente objetos como CATEGORÍA.
<b>Balanceado</b>	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.
<b>Cauteloso</b>	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.
<b>Desactivado</b>	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 Endpoint 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

\* 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 Endpoint 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** 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 Endpoint 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
<b>Intenso</b>	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.
<b>Balanceado</b>	Las amenazas reportadas de nivel balanceado (o más bajo) se bloquean, y se inicia la corrección automática (por ejemplo, la desinfección).
<b>Cauteloso</b>	Las detecciones reportadas de nivel cauteloso se bloquean, y se inicia la corrección automática (por ejemplo, la desinfección).
<b>Desactivado</b>	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.

## Prácticas recomendadas

### NO ADMINISTRADO (Estación de trabajo de cliente individual)

Mantener los valores recomendados predeterminados.

### ENTORNO ADMINISTRADO

Por lo general, esta configuración se aplica en estaciones de trabajo a través de una [política](#).

#### 1. Etapa inicial

Esta etapa puede tomar hasta una semana.

- Configurar todos los umbrales de **Informes** en el nivel **Balanceado**.  
NOTA: de ser necesario, configure como **Intenso**.
- Configurar o mantener la **Protección** contra malware en el nivel **Balanceado**.
- Configurar la **Protección** para otras CATEGORÍAS en el nivel **Cauteloso**.  
**NOTA:** No es recomendable configurar el umbral de **Protección** como **Intenso** en esta etapa porque todas las amenazas se corregirán, incluidos las que se identificaron en forma errónea.
- Encuentre los objetos identificados en forma errónea en el [Registro de detección](#) y primero agréguelos a [Exclusiones de la detección](#).

#### 2. Etapa de transición

- Implementar la “Etapa de producción” en algunas estaciones de trabajo a modo de prueba (no hacerlo en todas las estaciones de trabajo de la red).

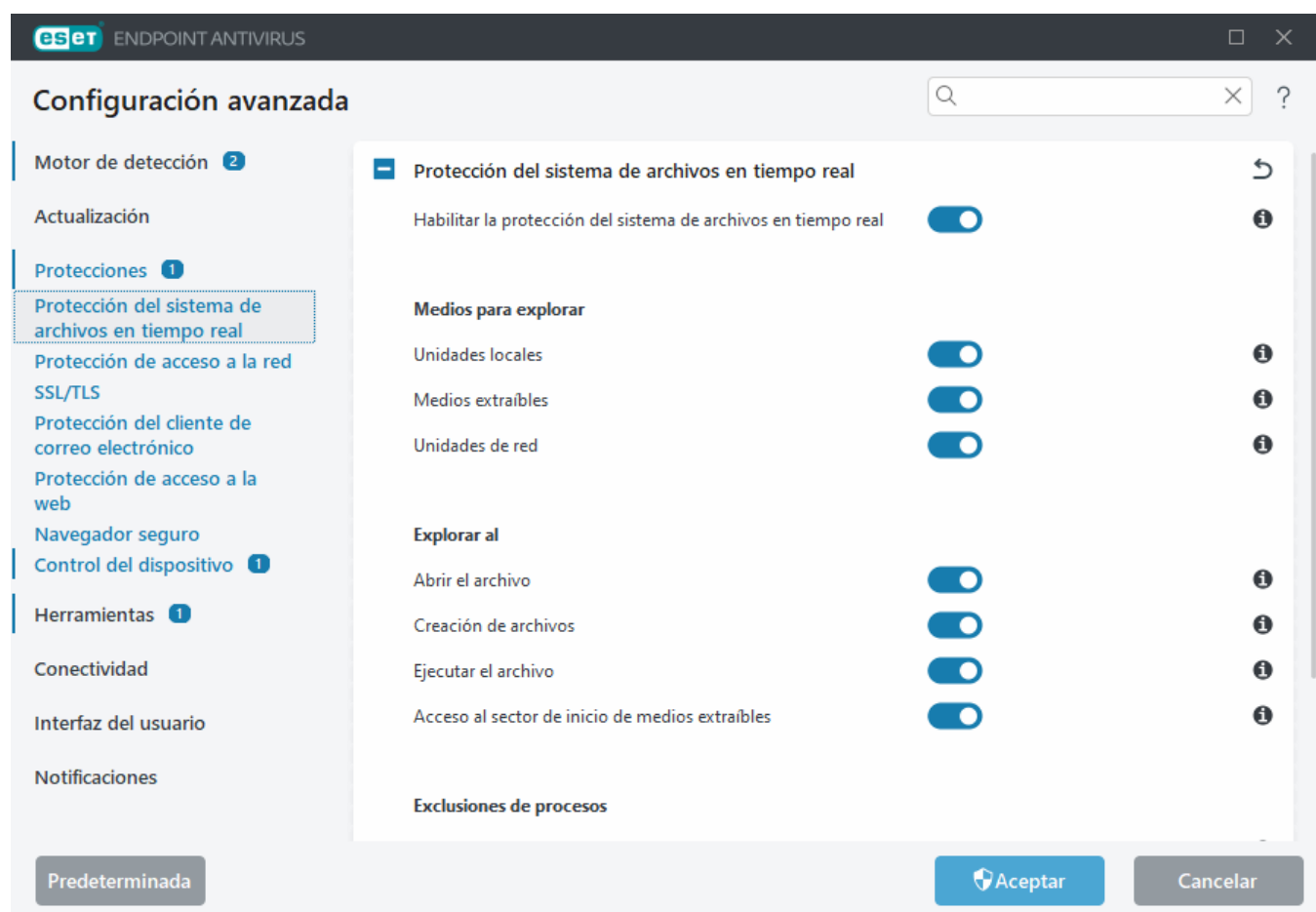


### 3. Etapa de producción

- Configurar todos los umbrales de **Protección** en el nivel **Balanceado**.
- Cuando se administra de forma remota, usar la [política predefinida](#) pertinente del antivirus para ESET Endpoint Antivirus.
- El umbral de protección de nivel **Intenso** puede configurarse si se requieren las tasas de detección más altas y se aceptan los objetos identificados en forma errónea.
- Revisar el [Registro de detección](#) o los informes de ESET PROTECT para encontrar posibles amenazas faltantes.

## 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](#) > **Protecciones** > **Protección del sistema de archivos en tiempo real** > **Protección del sistema de archivos en tiempo real**.



## 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 ThreatSense.

## Exclusiones de procesos

Consulte [Exclusiones de procesos](#).

## 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 [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, abra [Configuración avanzada](#) > **Protecciones** > **Protección del sistema de archivos en tiempo real**. Haga clic en **ThreatSense** > **Otros** y seleccione o anule la selección de **Habilitar la optimización inteligente**.

La protección del sistema de archivos en tiempo real también le permite configurar [Parámetros ThreatSense adicionales](#).

# 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 agregar archivos ejecutables a la lista de procesos excluidos en [Configuración avanzada](#) > **Protecciones** > **Protección del sistema de archivos en tiempo real** > **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 Endpoint 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 Endpoint 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.

## 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 Endpoint 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 en ↶ junto a [Configuración avanzada](#) > **Protecciones** > **Respuestas de detección**.

## Verificación de la protección en tiempo real

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

El archivo está disponible para su descarga desde <http://www.eicar.org/download/eicar.com>.

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 **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, abra [Configuración avanzada](#) > **Protecciones > Protección del sistema de archivos en tiempo real**.

## Si la protección en tiempo real no detecta ni desinfecta infiltraciones

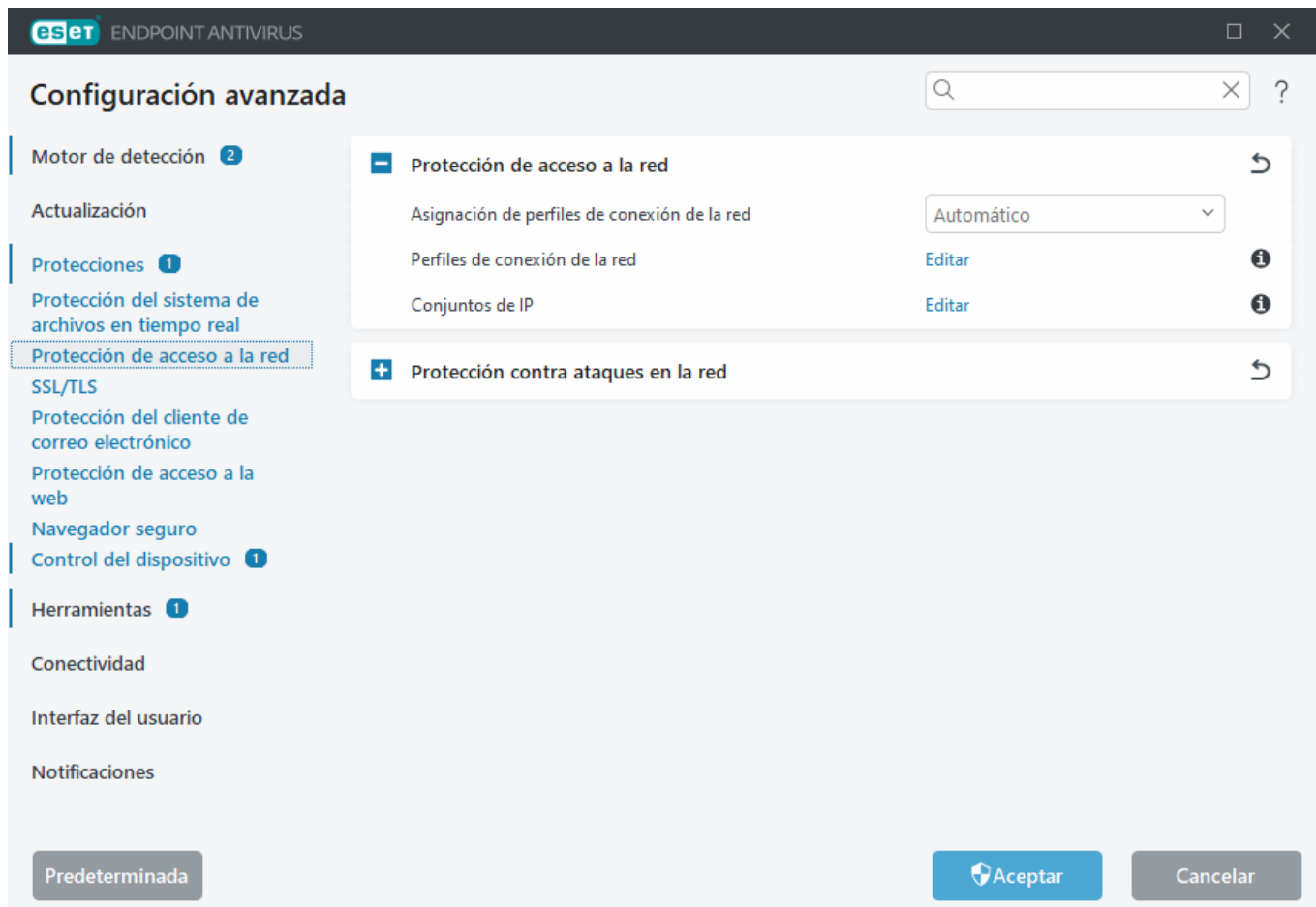
Asegúrese de que no haya otros programas antivirus instalados en el equipo. Si hay dos programas antivirus instalados a la vez, es posible que tengan conflictos entre ellos. Es recomendable desinstalar cualquier otro programa antivirus que haya en el sistema antes de instalar ESET.

## 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](#).

## Protección de acceso a la red

La protección de acceso a la red le permite configurar todas las conexiones de red. De forma predeterminada, ESET Endpoint Antivirus tiene protección de acceso a la red preconfigurada para una máxima seguridad. Sin embargo, es posible que determinados entornos necesiten una configuración personalizada. El cambio de la configuración predeterminada solo debe ser realizado por un usuario experimentado.



Puede configurar los siguientes ajustes en [Configuración avanzada](#) > **Protecciones** > **Protección de acceso a la red** (haga clic en los vínculos siguientes para obtener una descripción detallada de cada opción de protección de acceso a la red):

## Protección de acceso a la red

[Perfiles de conexión de red](#): los perfiles se pueden usar para controlar la protección de acceso a la red para conexiones de red específicas.

[Conjuntos de direcciones IP](#): puede definir colecciones de direcciones IP que creen un grupo de direcciones IP lógico, que luego se puede agregar como zona de confianza o excluirse de la [protección contra ataques a la red \(IDS\)](#).


[Protección contra ataques de red](#)

## Perfiles de conexión de la red

Los perfiles se pueden usar para controlar el comportamiento de la protección de acceso a la red de ESET Endpoint Antivirus para una conexión de red específica. Al crear o editar [reglas IDS](#), reglas de [protección contra ataque por fuerza bruta](#), puede asignarlas a un perfil específico o aplicarlas a todos los perfiles. Cuando un perfil esté activo en una conexión de red, solo se aplicarán las reglas globales (reglas sin ningún perfil especificado) y las reglas asignadas a dicho perfil.

Puede configurar los perfiles y las asignaciones de conexión de red en [Configuración avanzada](#) > **Protecciones** > **Protección de acceso a la red** > **Protección de acceso a la red**.

**Asignación de perfiles de conexión de la red:** permite elegir si a las conexiones de red recién descubiertas se les asigna automáticamente (seleccione **Automático** en el menú desplegable) un perfil predefinido o personalizado basado en [Activadores](#) configurados en perfiles de conexión de red o si desea que se le solicite (seleccione **Solicitar** en el menú desplegable) [Configurar la protección de red](#) y se asigne un perfil manualmente cada vez que se detecte una nueva conexión de red.

También puede asignar manualmente un perfil de conexión de red específico en la [ventana principal del programa](#) > **Configuración** > **Red** > **Conexiones de red**. Desplácese sobre una conexión de red específica y haga clic en el icono de menú  > **Editar** para abrir la ventana [Configurar protección de red](#) y seleccione un perfil.

**Perfiles de conexión de la red:** haga clic en **Editar** para [Agregar o editar perfiles de conexión de red](#).

Los siguientes perfiles están predefinidos y no se pueden editar/eliminar:

**Privado:** para redes confiables (red doméstica o de oficina). Su equipo y los archivos compartidos almacenados en su equipo están visibles para otros usuarios en la red y estos pueden acceder a los recursos del equipo (el acceso a archivos e impresoras compartidos está habilitado, la comunicación entrante RPC está habilitada y el uso compartido de escritorio remoto está disponible). Recomendamos el uso de esta configuración al acceder a una red local segura. Este perfil se asigna automáticamente a una conexión de red si está configurado como Dominio o Red privada en Windows.

**Público:** para redes no confiables (red pública). Los archivos y las carpetas en su equipo no se comparten con otros usuarios en la red o no están visibles para ellos, y el uso compartido de recursos del equipo está desactivado. Recomendamos el uso de esta configuración al acceder a redes inalámbricas. Este perfil se asigna automáticamente a cualquier conexión de red que no esté configurada como Dominio o Red privada en Windows.

Cuando la conexión de red cambie a otro perfil, aparecerá una notificación en la esquina inferior derecha de la pantalla.

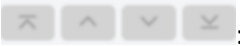
## Agregar o editar perfiles de conexión de red

Puede agregar o editar [perfiles de conexión de red](#) en [Configuración avanzada](#) > **Protecciones** > **Protección de acceso a la red** > **Protección de acceso a la red** > **Perfiles de conexión de red** > **Editar**. Para editar un perfil, debe seleccionarse en la ventana lista de **perfiles de conexión de red**.

Los siguientes perfiles están predefinidos y no se pueden editar/eliminar:

**Privado:** para redes confiables (red doméstica o de oficina). Su equipo y los archivos compartidos almacenados en su equipo están visibles para otros usuarios en la red y estos pueden acceder a los recursos del equipo (el acceso a archivos e impresoras compartidos está habilitado, la comunicación entrante RPC está habilitada y el uso compartido de escritorio remoto está disponible). Recomendamos el uso de esta configuración al acceder a una red local segura. Este perfil se asigna automáticamente a una conexión de red si está configurado como Dominio o Red privada en Windows.

**Público:** para redes no confiables (red pública). Los archivos y las carpetas en su equipo no se comparten con otros usuarios en la red o no están visibles para ellos, y el uso compartido de recursos del equipo está desactivado. Recomendamos el uso de esta configuración al acceder a redes inalámbricas. Este perfil se asigna automáticamente a cualquier conexión de red que no esté configurada como Dominio o Red privada en Windows.

**Arriba/Superior/Abajo/Inferior**  : permite ajustar el nivel de prioridad de los perfiles de

conexión de red (los perfiles de conexión de red se evalúan y aplican según su prioridad. Siempre se aplica el primer perfil coincidente).

## Agregar o editar un perfil

El perfil de conexión de red personalizado permite aplicar reglas de [protección contra ataque por fuerza bruta](#) y definir configuraciones adicionales para conexiones de red específicas. Especificará a qué conexiones de red se asignará el perfil personalizado en la sección [Activadores](#).

Para abrir el editor de perfiles, en la ventana **Perfiles de conexión de red**:

- Haga clic en **Agregar**.
- Seleccione uno de los perfiles existentes y haga clic en **Editar**.
- Seleccione uno de los perfiles existentes y haga clic en **Copiar**.

**Nombre:** nombre personalizado para su perfil.

**Descripción:** descripción del perfil para identificarlo con mayor facilidad.

**Direcciones de confianza adicionales:** las direcciones definidas aquí se agregan a la zona de confianza de la conexión de red a la que se aplica este perfil (independientemente del tipo de protección de la red).

**Conexión de confianza:** su equipo y los archivos compartidos almacenados en su equipo están visibles para otros usuarios en la red y estos pueden acceder a los recursos del equipo (el acceso a archivos e impresoras compartidos está habilitado, la comunicación entrante RPC está habilitada y el uso compartido de escritorio remoto está disponible). Se recomienda usar esta configuración al crear un perfil para una conexión de red local segura. Todas las subredes de red conectadas directamente también se consideran de confianza. Por ejemplo, si un adaptador de red está conectado a esta red con la dirección IP 192.168.1.5 y la máscara de subred es 255.255.255.0, la subred 192.168.1.0/24 se agregará a la zona de confianza de dicha conexión de red. Si el adaptador tiene más direcciones/subredes, todas serán de confianza.

**Informar sobre cifrado Wi-Fi débil:** ESET Endpoint Antivirus mostrará una [notificación de escritorio](#) cuando se conecte a una red inalámbrica desprotegida o a una red con protección débil.

**Activadores:** condiciones personalizadas que deben cumplirse para asignar este perfil de conexión de red a una conexión de red. Consulte [Activadores](#) para obtener una explicación detallada.

## Activadores

Los activadores son condiciones personalizadas que deben cumplirse para asignar un [perfil de conexión de red](#) a una conexión de red. Si la red conectada tiene los mismos atributos definidos en activadores para un perfil de red conectado, el perfil se aplicará a la red. Un perfil de conexión de red puede tener uno o varios activadores. Si hay varios activadores, se aplica la lógica OR (se debe cumplir al menos una condición). Puede definir activadores en el [editor de perfiles de conexión de red](#). Un usuario experimentado debe llevar a cabo la creación de perfiles de conexión de red personalizados.

Los siguientes activadores están disponibles:

 [Adaptador](#)

**Tipo de adaptador:** aplica el perfil si la conexión de red se establece en el tipo de adaptador seleccionado.  
**Nombre del adaptador:** aplica el perfil si el nombre del adaptador de red coincide.  
**IP del adaptador:** aplica el perfil si la dirección IP del adaptador de red coincide.

#### [DNS](#)

**Sufijo DNS:** aplica el perfil si el nombre de dominio coincide.  
**IP DNS:** aplica el perfil si la dirección IP del servidor DNS coincide.

#### [WINS](#)

Aplica el perfil si la Windows Internet Name Service (WINS) dirección IP asignada coincide.

#### [DHCP](#)

**IP DHCP:** coincide con la dirección IP del servidor DHCP.

#### [Puerta de enlace predeterminada](#)

**IP:** aplica el perfil si la dirección IP de la puerta de enlace predeterminada coincide.  
**Dirección MAC:** aplica el perfil si la dirección MAC de la puerta de enlace predeterminada coincide.

#### [Wi-Fi](#)

**SSID:** aplica el perfil si el SSID (nombre de la red Wi-Fi) coincide.  
**Nombre del perfil:** aplica el perfil si el nombre del perfil de Wi-Fi coincide.  
**Tipo de seguridad:** aplica el perfil si el tipo de seguridad coincide con el seleccionado en el menú desplegable. Si quiere hacer coincidir más de uno, cree otro activador.  
**Tipo de cifrado:** aplica el perfil si el tipo de cifrado coincide con el seleccionado en el menú desplegable. (Si quiere hacer coincidir más de uno, cree otro activador).  
**Seguridad de red:** aplica el perfil si la red está **abierta/protegida**.

#### [Perfil de Windows](#)

Aplica el perfil si la red está configurada en Windows como **Dominio/Privado/Público**.

#### [Autenticación](#)



La autenticación de red busca un servidor específico en la red y usa cifrado asimétrico (RSA) para autenticar dicho servidor. El nombre de la red que se autentica debe coincidir con el nombre establecido en la configuración del servidor de autenticación. El nombre distingue entre mayúsculas y minúsculas. El nombre del servidor se puede escribir como una dirección IP, DNS o nombre NetBios.

[Descargue ESET Authentication Server.](#)

La clave pública se puede importar mediante alguno de los siguientes tipos de archivos:

- Clave pública cifrada PEM (.pem); puede generar esta clave con ESET Authentication Server
- Clave pública cifrada
- Certificado de clave pública (.crt)

Haga clic en **Probar** para probar su configuración. Si la autenticación es correcta, se mostrará Autenticación del servidor correcta. Si la autenticación no está configurada correctamente, se mostrará uno de los siguientes mensajes de error:

Falló la autenticación del servidor. Firma no válida o que no coincide.

La firma del servidor no coincide con la clave pública ingresada.

Falló la autenticación del servidor. El nombre de la red no coincide.

El nombre de la red configurada no corresponde al nombre de la red del servidor de autenticación. Revise los dos nombres y asegúrese de que sean iguales.

Falló la autenticación del servidor. No válido o sin respuesta desde el servidor.

No se recibe respuesta alguna si el servidor no está en funcionamiento o no se puede acceder al mismo. Se puede recibir una respuesta no válida si otro servidor HTTP se ejecuta en la dirección especificada.

Se ingresó una clave pública no válida.

Verifique que el archivo de la clave pública que ha ingresado no esté dañado.

## Conjuntos de IP

Un conjunto de direcciones IP es una colección de direcciones IP que crean un grupo lógico de direcciones IP, útil cuando se reutiliza el mismo conjunto de direcciones en varias reglas de [protección contra ataques de fuerza bruta](#). ESET Endpoint Antivirus también contiene conjuntos de IP predefinidos para los que se aplican reglas internas. Un ejemplo de este tipo de grupo es la **zona de confianza**. La zona de confianza representa un grupo de direcciones de red donde su equipo y los archivos compartidos almacenados en su equipo están visibles para otros usuarios en la red y estos pueden acceder a los recursos del equipo.

Para agregar un conjunto de IP:

1. Abra [Configuración avanzada](#) > **Protecciones** > **Protección de acceso a la red** > **Conjuntos de IP** > **Editar**
2. Haga clic en **Agregar**, escriba un **Nombre** y una **Descripción** para la zona y escriba una dirección IP remota en **Dirección del equipo remoto (IPv4/IPv6, intervalo, máscara)**.
3. Haga clic en **Aceptar**.

Para obtener más información, consulte [Editar conjuntos de IP](#).

## Editar conjuntos de IP

Para obtener más información acerca de los conjuntos de IP, consulte [Conjuntos de IP](#).

### Columnas

**Nombre** – nombre de un grupo de equipos remotos.

**Descripción:** descripción general del grupo.

**Direcciones IP:** direcciones de IP remotas que pertenecen a un conjunto de IP.

## Elementos de control

Cuando **agrega** o **edita** un conjunto de IP, los siguientes campos se encuentran disponibles:

**Nombre** – nombre de un grupo de equipos remotos.

**Descripción:** descripción general del grupo.

**Dirección del equipo remoto (IPv4, IPv6, rango, máscara)** – le permite agregar una dirección remota, un rango de direcciones o una subred.

**Eliminar:** elimina una zona de la lista.

 Los conjuntos de IP predefinidos no se pueden eliminar.

### Ejemplos de direcciones IP

Agregar dirección IPv4:

**Dirección única:** agrega una dirección IP de un equipo individual (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 (por ejemplo, *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 la subred 192.168.1.0. Para excluir todo el tipo de subred en *192.168.1.0/24*.

Agregar dirección IPv6:

**Dirección única:** agrega la dirección IP de un equipo individual (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*).

## Protección contra ataques en la red (IDS)

La protección contra ataques de red (IDS) mejora la detección de exploits para vulnerabilidades conocidas. Lea más sobre la protección contra ataques de red en el [Glosario](#). Para configurar la protección contra ataques a la red, abra [Configuración avanzada](#) > **Protecciones** > **Protección de acceso a la red** > **Protección contra ataques a la red**.

**Habilitar la Protección contra ataques en la red (IDS)** – Analiza el contenido del tráfico de la red y protege de ataques en la red. Todo tráfico que se considere perjudicial será bloqueado.

**Habilitar protección contra botnets:** detecta y bloquea la comunicación con los servidores maliciosos de comando y control según patrones típicos cuando el equipo está infectado y un bot está tratando de comunicarse. Lea más sobre la protección contra botnets en el glosario [\\*\\*\\*](#).

**Reglas IDS** – Esta opción le permite configurar opciones avanzadas de filtrado para detectar diversos tipos de ataques y exploits que se pueden utilizar para dañar su equipo.

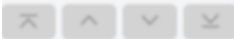
Todos los eventos importantes detectados por la protección de red se guardan en un archivo de registro. Consulte [registro de protección de red](#) para obtener más información.

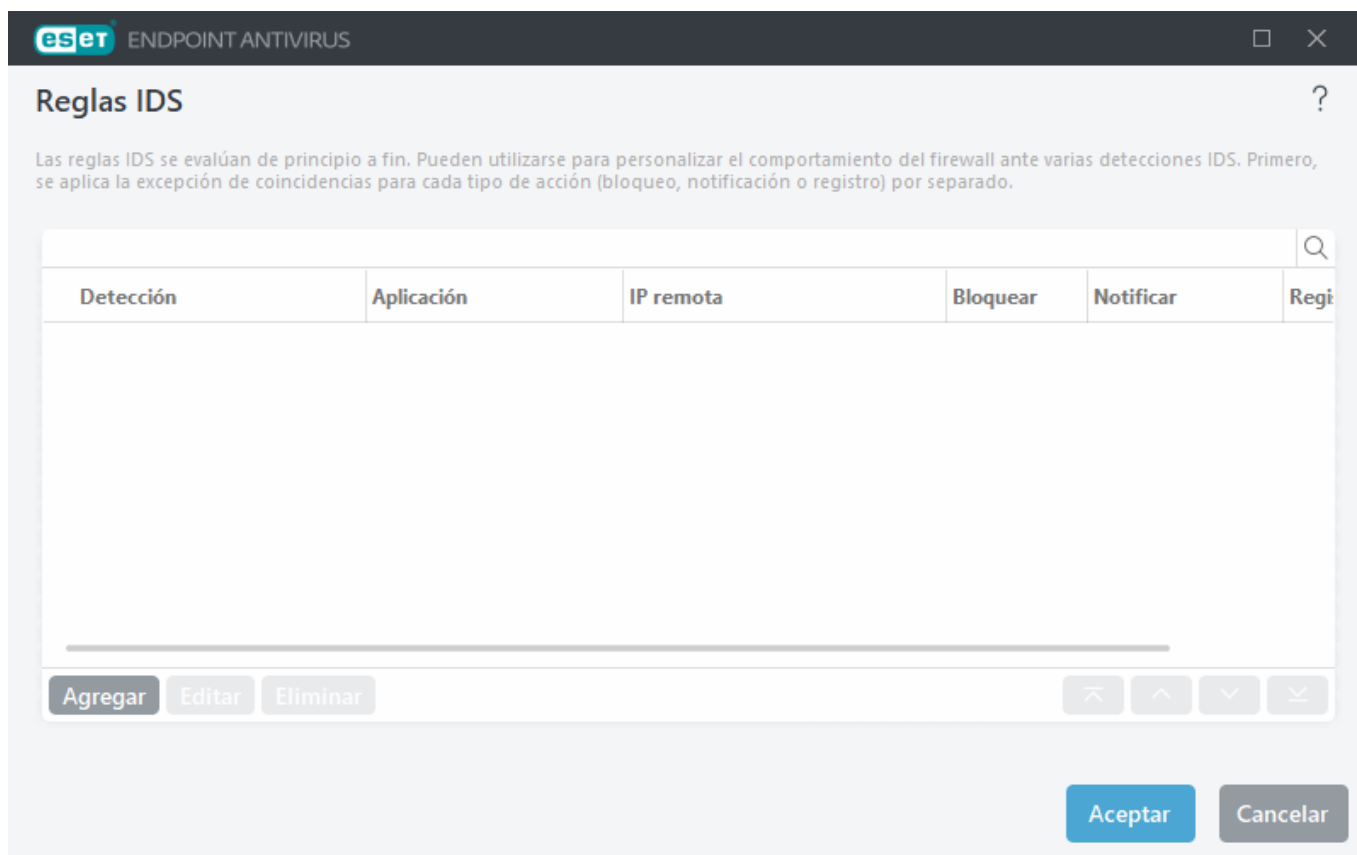
# Reglas IDS

En algunas situaciones, el [servicio de detección de intrusiones \(IDS\)](#) puede detectar la comunicación entre routers u otros dispositivos de red internos como un posible ataque. Por ejemplo, puede agregar la dirección segura conocida a las direcciones excluidas de la zona del IDS para que evada el IDS.

- i** Los siguientes artículos de la base de conocimiento de ESET pueden estar disponibles solo en inglés:
- [Cree reglas IDS en las estaciones de trabajo de cliente en ESET Endpoint Antivirus](#)
  - [Cree reglas IDS en las estaciones de trabajo de cliente en ESET PROTECT](#)

## Administrar reglas IDS

- **Agregar:** haga clic para crear una nueva regla IDS.
- **Editar:** haga clic para editar una regla IDS existente.
- **Quitar:** seleccione y haga clic si desea quitar una regla existente de la lista de reglas IDS.
-  **Superior/Arriba/Abajo/Inferior:** le permite ajustar el nivel de prioridad de las reglas (las excepciones se evalúan desde arriba hacia abajo).



Detección	Aplicación	IP remota	Bloquear	Notificar	Regi
-----------	------------	-----------	----------	-----------	------

Se mostrarán **exclusiones** de fichas si el administrador [crea exclusiones de IDS en la consola web de ESET PROTECT](#). Las exclusiones de IDS solo pueden contener reglas permitidas y se evalúan antes que las reglas IDS.

## Editor de reglas

**Detección:** tipo de detección

**Nombre de amenaza:** puede especificar un nombre de amenaza para algunas de las detecciones disponibles.

**Aplicación** : 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.

**Dirección IP remota** : una lista de direcciones/rangos/subredes IPv4 o IPv6 remotas. Si incluye varias direcciones, deben estar separadas por una coma.


**Perfil**: puede elegir un [perfil de conexión de red](#) al que se aplicará esta regla.

## Acción

**Bloquear** : cada proceso de sistema tiene su propia conducta predeterminada y acción asignada (bloquear o permitir). Para anular la conducta predeterminada de ESET Endpoint Antivirus, puede seleccionar si bloquearla o permitirla mediante el uso del menú desplegable.

**Notificar** : seleccione **Sí** para mostrar las [notificaciones de escritorio](#) en su equipo. Seleccione **No** si no quiere recibir notificaciones de escritorio. Los valores disponibles son Predeterminado/Sí/No.

**Registro**: Seleccione **Sí** para registrar eventos en archivos de registro de [ESET Endpoint Antivirus](#). Seleccione **No** si no quiere recibir eventos de registro. Los valores disponibles son **Predeterminado/Sí/No**.


ENDPOINT ANTIVIRUS
✕

## Agregar regla IDS ?

Detección

Cualquier detección ▼

Nombre de amenaza

Dirección

Ambos ▼

Aplicación

...

Dirección IP remota

i

Perfil

i

Agregar

Eliminar

Acción

Bloquear

Predeterminado ▼

Notificar

Predeterminado ▼

Registrar

Predeterminado ▼

Aceptar

Cancelar

Quiere recopilar una notificación y obtener un registro cada vez que ocurre el evento:

1. Haga clic en **Agregar** para agregar una nueva regla IDS.
2. Seleccione la alerta específica del menú desplegable **Detección**.
3. Haga clic en **...** y seleccione la ruta del archivo de la aplicación respecto de la cual quiere aplicar la notificación.
4. Deje la opción **Predeterminado** en el menú desplegable **Boquear**. De esta manera, se heredaré la acción predeterminada aplicada por ESET Endpoint Antivirus.
5. Seleccione ambos menús desplegables **Notificar** y **Registrar** en la opción **Sí**.
6. Haga clic en **Aceptar** para guardar esta notificación.

Quiere eliminar notificaciones recurrentes para un tipo de detección que no considera una amenaza:

1. Haga clic en **Agregar** para agregar una nueva excepción de IDS.
2. Seleccione la alerta específica del menú desplegable **Detección**, por ejemplo, **Sesión de SMB sin extensiones de seguridad**.
3. Seleccione **En** del menú desplegable de dirección en caso de que se trate de una comunicación entrante.
- ✓ 4. Configure el menú desplegable de la opción **Notificar** en **No**.
5. Configure el menú desplegable de la opción **Registrar** en **Sí**.
6. Deje la opción **Aplicación** en blanco.
7. Si la comunicación no procede de una dirección IP específica, deje la opción **Direcciones IP remotas** en blanco.
8. Haga clic en **Aceptar** para guardar esta notificación.

## Protección contra ataques de fuerza bruta

La protección contra ataques por fuerza bruta bloquea los ataques de adivinar contraseñas para los servicios RDP y SMB. Un ataque por fuerza bruta es un método para descubrir una contraseña de destino intentando de forma sistemática todas las letras, números y símbolos que se pueden intentar de forma sistemática. Para configurar la protección contra ataques por fuerza bruta, abra [Configuración avanzada](#) > **Protecciones** > **Protección de acceso a la red** > **Protección contra ataques a la red** > **Protección contra ataques por fuerza bruta**.

**Activar la protección contra ataques por fuerza bruta:** ESET Endpoint Antivirus inspecciona el contenido del tráfico de red y bloquea los intentos de ataques para adivinar contraseñas.

**Reglas:** le permiten crear, editar y ver reglas para las conexiones de red entrantes y salientes. Para obtener más información, consulte [Reglas](#).

**Exclusiones:** lista de detecciones excluidas definidas por una dirección IP o una ruta de la aplicación. Puede crear y editar exclusiones en su ESET PROTECT. Para obtener más información, consulte [Exclusiones](#).

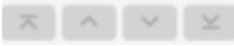


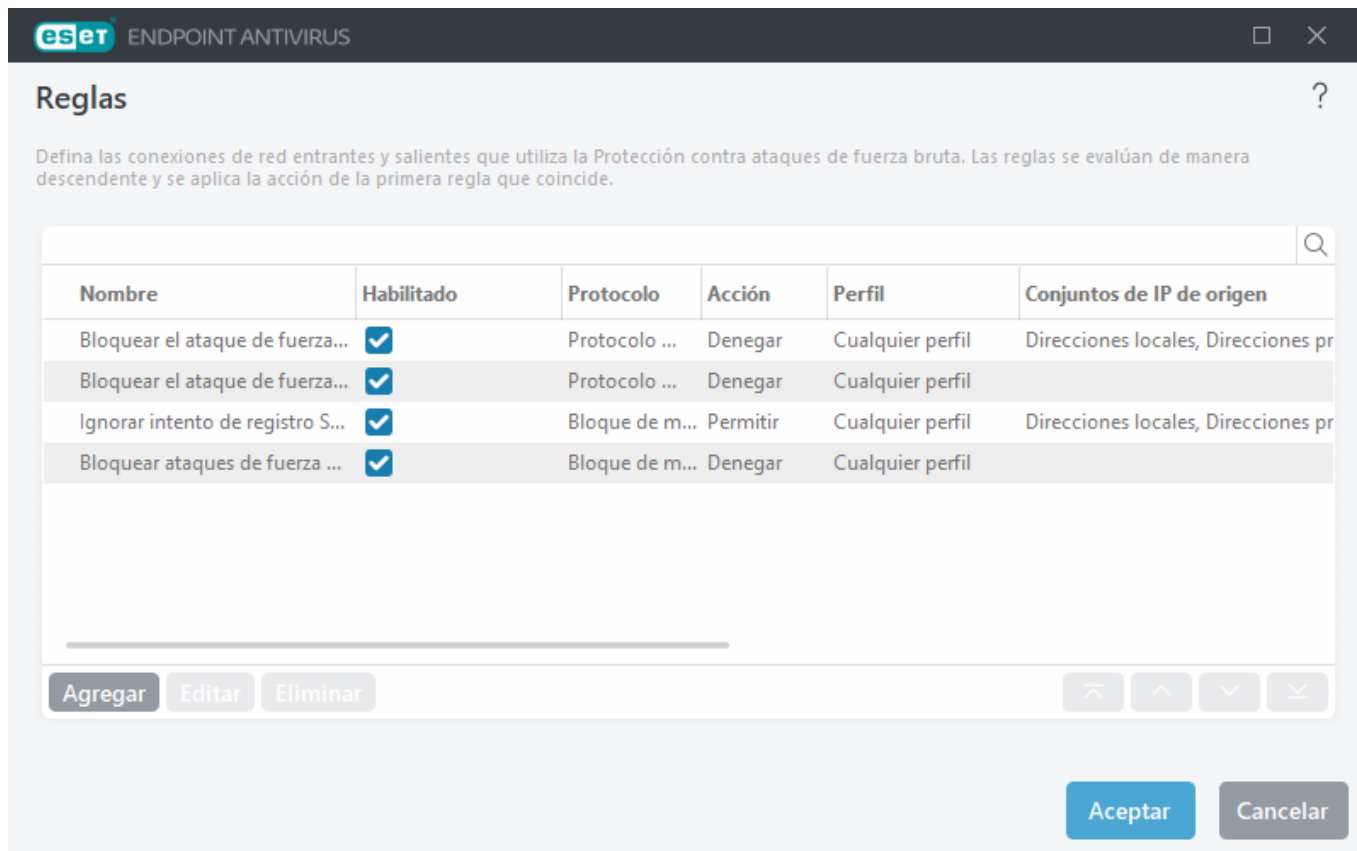
Para obtener más información sobre la protección contra ataques de fuerza bruta, consulte el artículo de la [Guía de seguridad digital de ESET](#).

## Reglas

Las reglas de protección contra ataques por fuerza bruta le permiten crear, modificar y ver reglas para las conexiones de red entrantes y salientes. Las reglas predefinidas no se pueden editar ni eliminar.

### Administrar las reglas de protección contra ataques de fuerza bruta

- **Agregar:** haga clic para crear una nueva regla de protección contra ataques de fuerza bruta.
- **Editar:** haga clic para editar un regla de protección contra ataques de fuerza bruta existente.
- **Quitar:** seleccione y haga clic si desea quitar una excepción existente de la lista de reglas IDS.
-  **Superior/Arriba/Abajo/Inferior:** permite ajustar el nivel de prioridad de las reglas.



Para garantizar la máxima protección posible, se aplica la regla de bloqueo con el valor de **Cantidad máxima de intentos** más bajo, aun si la regla se encuentra en una posición más baja en la lista de Reglas cuando varias reglas de bloqueo cumplen las condiciones de detección.

## Editor de reglas

**Nombre:** nombre de la regla.

**Habilitada** – deshabilite la alternar si desea conservar la regla en la lista pero no quiere aplicarla.

**Acción:** elija si desea **denegar** o **permitir** la conexión si se cumple la configuración de la regla.

**Protocolo:** el protocolo de comunicación que inspeccionará esta regla.


**Perfil:** puede elegir un [perfil de conexión de red](#) al que se aplicará esta regla.

**Cantidad máxima de intentos** - La cantidad máxima de intentos permitidos de repetición de ataques hasta que la dirección IP se bloquea y se agrega a la lista negra.

**Periodo de retención de la lista negra (min):** establece el tiempo en el cual la dirección caduca de la lista negra.

**IP de origen:** una lista de subredes, rangos o direcciones IP. Si incluye varias direcciones, deben estar separadas por una coma.

**Conjuntos de IP de origen:** conjunto de direcciones IP que ya ha definido en [conjuntos de IP](#).


ENDPOINT ANTIVIRUS
✕

## Agregar regla ?

Nombre

Sin título

Habilitado

☒

Acción

Denegar

Protocolo

Protocolo de escritorio remoto (RDP)

Perfil

Agregar

Eliminar

Cantidad máxima de intentos

10

i

Periodo de retención de la lista negra (min.)

30

i

IP de origen

Agregar

Eliminar

Conjuntos de IP de origen

Agregar

Eliminar

Aceptar

Cancelar

## Exclusiones

Las exclusiones de fuerza bruta pueden utilizarse para suprimir las detecciones de fuerza bruta para criterios específicos. Esas exclusiones se crean desde ESET PROTECT en función de las detecciones de fuerza bruta.

## Columnas

- **Detección:** tipo de detección
- **Aplicación :** 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.
- **IP remota :** una lista de direcciones/rangos/subredes IPv4 o IPv6 remotas. Si incluye varias direcciones, deben estar separadas por una coma.

152



## Administrar exclusiones

Se mostrarán exclusiones si un administrador [crea exclusiones de fuerza bruta en la consola web de ESET PROTECT](#). Las exclusiones solo pueden contener reglas permitidas y se evalúan antes que las reglas IDS.

## Opciones avanzadas

En [Configuración avanzada](#) > **Protecciones** > **Protección de acceso a la red** > **Protección contra ataques a la red** > **Opciones avanzadas**, puede habilitar o deshabilitar la detección de varios tipos de ataques y vulnerabilidades que pueden dañar su equipo.



En algunos casos no recibirá una notificación de amenaza sobre las comunicaciones bloqueadas. Consulte la sección [Registrar y crear reglas o excepciones desde el registro](#) para obtener instrucciones para ver todas las comunicaciones bloqueadas en el registro del Firewall.



La disponibilidad de las opciones determinadas en esta ventana pueden variar dependiendo del tipo o versión de su producto de ESET y el módulo de firewall, como así también de la versión de su sistema operativo.

### Detección de intrusiones

- **Protocolo SMB** – detecta y bloquea distintos problemas de seguridad en el protocolo SMB, a saber:
  - **Detección de autenticación de ataque de desafío del servidor ficticio** – esta opción lo protege contra un ataque que utiliza un desafío ficticio durante la autenticación para obtener credenciales de usuario.
  - **Evasión de IDS durante la detección de abertura de tubería nombrada** – detección de técnicas de evasión utilizadas para abrir tuberías denominadas MSRPC en el protocolo SMB.
  - **Detecciones de CVE** (Exposiciones y vulnerabilidades comunes) – métodos de detección implementados de varios ataques, formas, agujeros de seguridad y explotaciones sobre el protocolo SMB. Consulte el [Sitio Web de CVE en cve.mitre.org](#) para buscar y obtener información más detallada sobre los identificadores de CVE (CVE).
- **Protocolo RPC** – detecta y bloquea distintos CVE en el sistema remoto de llamadas de procedimientos desarrollado para el Entorno de Computación Distribuida (DCE).
- **Protocolo RDP** – detecta y bloquea varios CVE en el protocolo RDP (consulte arriba).
- **Bloquear la dirección no segura una vez detectado el ataque** – las direcciones IP detectadas como fuentes de ataques se agregan a la Lista negra para prevenir la conexión durante un cierto periodo. Puede definir el **período de retención de la lista negra**, que establece el tiempo durante el cual se bloqueará la dirección después de la detección del ataque.
- **Notificar sobre la detección de ataques** – activa el área de notificación de Windows en la esquina inferior derecha de la pantalla.
- **Mostrar notificaciones también para ataques entrantes frente a agujeros de seguridad** – le proporciona alertas si se detectan ataques frente a agujeros de seguridad, o si una amenaza intenta ingresar al sistema de esta forma.

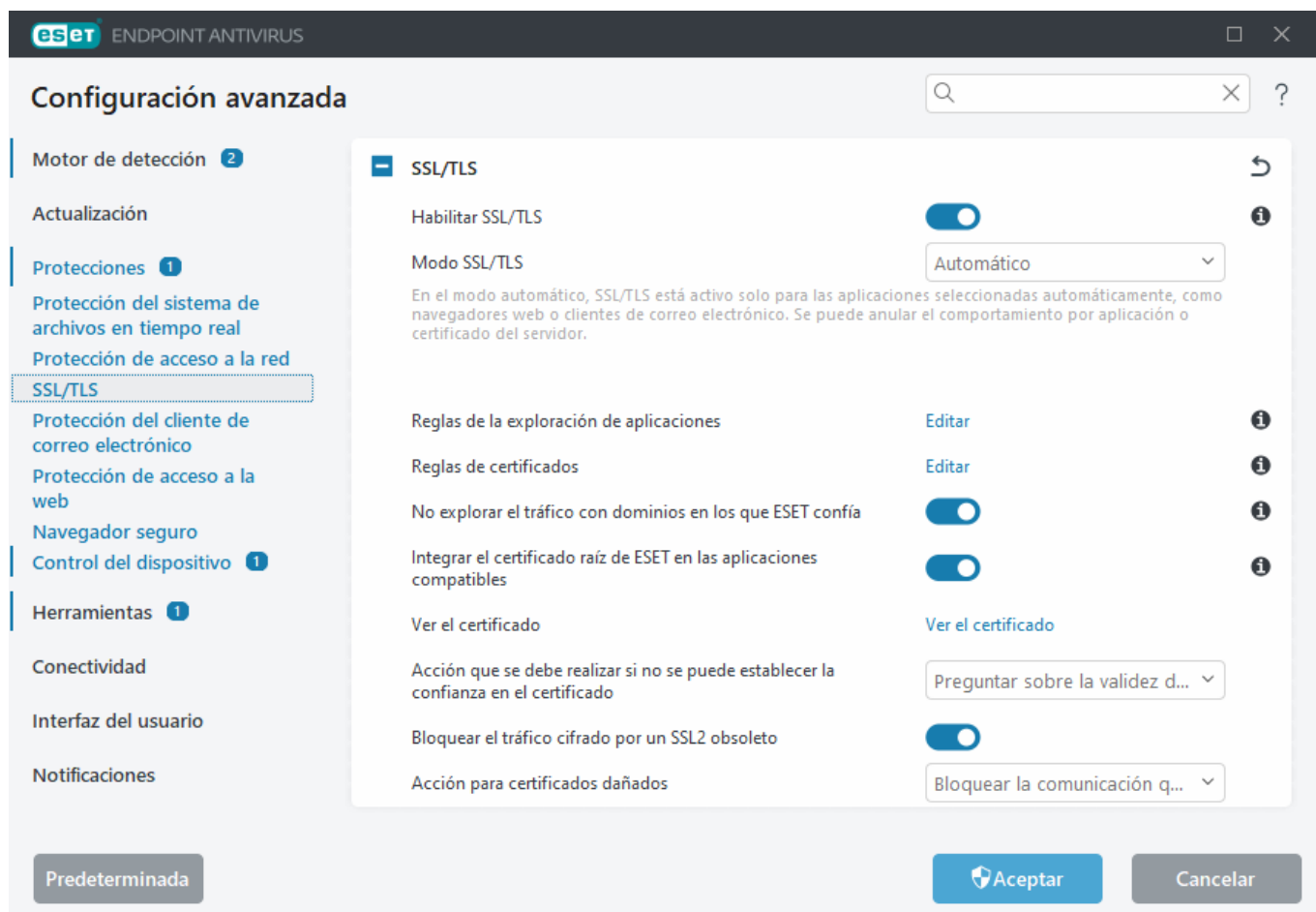
## Inspección de paquetes

- **Permitir una conexión entrante para intercambios admin. en el protocolo de SMB:** los intercambios administrativos (intercambios admin.) son los intercambios de red predeterminados que intercambian particiones del disco duro (*C\$, D\$, ...*) en el sistema junto con la carpeta del sistema (*ADMIN\$*). Deshabilitar la conexión a intercambios de admin. debería mitigar cualquier riesgo de seguridad. Por ejemplo, el gusano Conficker realiza ataques por diccionario para conectarse a intercambios de admin.
- **Denegar dialectos SMB anteriores (no compatibles)** – denegar sesiones SMB que usan un dialecto SMB anterior que no es compatible con IDS. Los sistemas operativos modernos de Windows son compatibles con los dialectos SMB anteriores debido a la retrocompatibilidad con sistemas operativos anteriores, como Windows 95. El atacante puede usar un dialecto anterior en una sesión SMB para evadir la inspección de tráfico. Denegar dialectos SMB anteriores si su equipo no necesita intercambiar archivos (o usar la comunicación SMB en general) con un equipo que posee una versión anterior de Windows.
- **Denegar sesiones SMB sin extensiones de seguridad** – se puede utilizar la seguridad extendida durante la negociación de la sesión SMB para proporcionar un mecanismo de autenticación más seguro que la autenticación Desafío/respuesta del administrador LAN (LM). El esquema LM es considerado débil y no se recomienda su uso.
- **Permitir la comunicación con el servicio Security Account Manager** – para obtener más información acerca de este servicio, consulte [\[MS-SAMR\]](#).
- **Permitir la comunicación con el servicio Local Security Authority** – para obtener más información acerca de este servicio, consulte [\[MS-LSAD\]](#) y [\[MS-LSAT\]](#).
- **Permitir la comunicación con el servicio Remote Registry** – para obtener más información acerca de este servicio, consulte [\[MS-RRP\]](#).
- **Permitir la comunicación con el servicio Service Control Manager** – para obtener más información acerca de este servicio, consulte [\[MS-SCMR\]](#).
- **Permitir la comunicación con el servicio Server** – para obtener más información acerca de este servicio, consulte [\[MS-SRVS\]](#).
- **Permitir la comunicación con los otros servicios** – otros servicios MSRPC. MSRPC es la implementación de Microsoft del mecanismo DCE RPC. Además, MSRPC puede usar tuberías denominadas dentro del protocolo SMB (compartir archivo de red) para su transporte (transporte ncacn-np). Los servicios MSRPC proporcionan interfaces para el acceso y administración de los sistemas de Windows de modo remoto. Se han descubierto y explotado varias vulnerabilidades de seguridad bajo condiciones normales de operación en el sistema MSRPC de Windows (gusano Conficker, gusano Sasser...). Deshabilite la comunicación con los servicios MSRPC que no necesite proporcionar para mitigar muchos riesgos de seguridad (como la ejecución remota de códigos o ataques por fallas del servicio).

## SSL/TLS

ESET Endpoint Antivirus puede comprobar si hay amenazas de comunicación que utilizan 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. Para editar la configuración de SSL/TLS, abra **Configuración avanzada > Protecciones > [SSL/TLS](#)**.





**Habilitar SSL/TLS:** si está desactivado, ESET Endpoint Antivirus no explorará la comunicación a través de SSL/TLS.

el modo **SSL/TLS** está disponible en las siguientes opciones:

Modo de filtrado	Descripción
<b>Automático</b>	El modo predeterminado solo explorará las aplicaciones correspondientes, como los navegadores web y los clientes de correo electrónico. Seleccione las aplicaciones donde se explora la comunicación para anularlo.
<b>Interactivo</b>	Si ingresa un nuevo sitio protegido por SSL (con un certificado desconocido), se mostrará un <a href="#">cuadro de diálogo para la selección de acción</a> . Este modo le permite crear una lista de certificados/aplicaciones SSL que se excluirán de la exploración.
<b>Basado en políticas</b>	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.

**Reglas de exploración de aplicaciones:** le permite personalizar el comportamiento de ESET Endpoint Antivirus de aplicaciones específicas.

**Reglas de certificados:** le permite personalizar el comportamiento de ESET Endpoint Antivirus de certificados SSL específicos.

**No explorar el tráfico con dominios en los que ESET confía:** cuando esté habilitada esta opción, la comunicación

con dominios de confianza se excluirá de la exploración. Una lista blanca integrada administrada por ESET determina la confiabilidad de un dominio.

**Integrar el certificado raíz de ESET en las aplicaciones compatibles** – 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 Endpoint 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.


**Acción que se debe realizar si no se puede establecer la confianza en el certificado:** en algunos casos, un certificado de sitio web no se puede comprobar mediante el almacén de Autoridades de Certificación de Raíz de Confianza (TRCA), (por ejemplo, certificado caducado, certificado que no es de confianza, certificado no válido para el dominio específico o la firma que se puede analizar pero no firma el certificado correctamente). Los sitios web legítimos siempre utilizarán certificados de confianza. Si no lo proporcionan, podría significar que un atacante está descifrando su comunicación o que el sitio web está experimentando dificultades técnicas.

Si se selecciona **Preguntar sobre la validez del certificado** (predeterminado), se le solicitará que seleccione la acción a realizar cuando se establezca una comunicación cifrada. Se mostrará un cuadro de diálogo para la selección de la acción donde puede 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 a un sitio que use el certificado no confiable.

**Bloquear tráfico cifrado por SSL2 obsoleto:** la comunicación que utiliza la versión anterior del protocolo SSL se bloqueará automáticamente.

**Acción para certificados dañados:** un certificado dañado significa que el certificado utiliza un formato no reconocido por ESET Endpoint Antivirus o que se ha recibido dañado (por ejemplo, sobrescrito por datos aleatorios). 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 elija una acción cuando se establezca la comunicación cifrada.

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

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

## Reglas de la exploración de aplicaciones

Las **reglas de exploración de aplicaciones** se puede usar para personalizar la conducta de ESET Endpoint Antivirus para aplicaciones específicas y para recordar las acciones elegidas cuando el **modo SSL/TLS** está en el **Modo interactivo**. La lista se puede ver y editar en [Configuración avanzada](#) > **Protecciones** > **SSL/TLS** > **Reglas de la exploración de aplicaciones** > **Editar**.

La ventana **Reglas de exploración de aplicaciones** consta de:

## 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.

## Reglas de certificados

Las reglas del certificado se pueden usar para personalizar el comportamiento de ESET Endpoint Antivirus de certificados SSL específicos y para recordar las acciones elegidas cuando el modo SSL/TLS está en modo interactivo. La lista se puede ver y editar en [Configuración avanzada](#) > **Protecciones** > **SSL/TLS** > **Reglas de certificados** > **Editar**.

La ventana **Reglas de certificado** 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.

## Tráfico de red cifrada

Si su sistema está configurado para usar una exploración SSL/TLS, 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 Endpoint 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 **SSL/TLS** 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 Endpoint 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 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 las [reglas de certificado](#).

## Protección del cliente de correo electrónico

Para configurar la protección del cliente de correo electrónico, abra **Configuración avanzada > Protecciones > Protección del cliente de correo electrónico** y elija entre las siguientes opciones de configuración:

- [Protección del transporte de correo electrónico](#)
- [Protección de la casilla de correo](#)
- [ThreatSense](#)

## Protección del transporte de correo electrónico

IMAP(S) y POP3(S) 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 Endpoint 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 MAPI 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.

**i** ESET Endpoint 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 Endpoint Antivirus verifica la comunicación mediante el SSL (protocolo de capa de conexión segura) y la TLS (seguridad de la capa de transporte). La comunicación cifrada se explorará de forma predeterminada. Para ver la configuración del explorador, abra [Configuración avanzada](#) > **Protecciones** > [SSL/TLS](#).

Para configurar la Protección del transporte de correo electrónico, abra [Configuración avanzada](#) > **Protecciones** > **protección del cliente de correo electrónico** > **protección del transporte de correo electrónico**.

**Habilitar Protección del transporte de correo electrónico:** cuando está activada, la comunicación del transporte de correo electrónico se explorará mediante ESET Endpoint Antivirus.

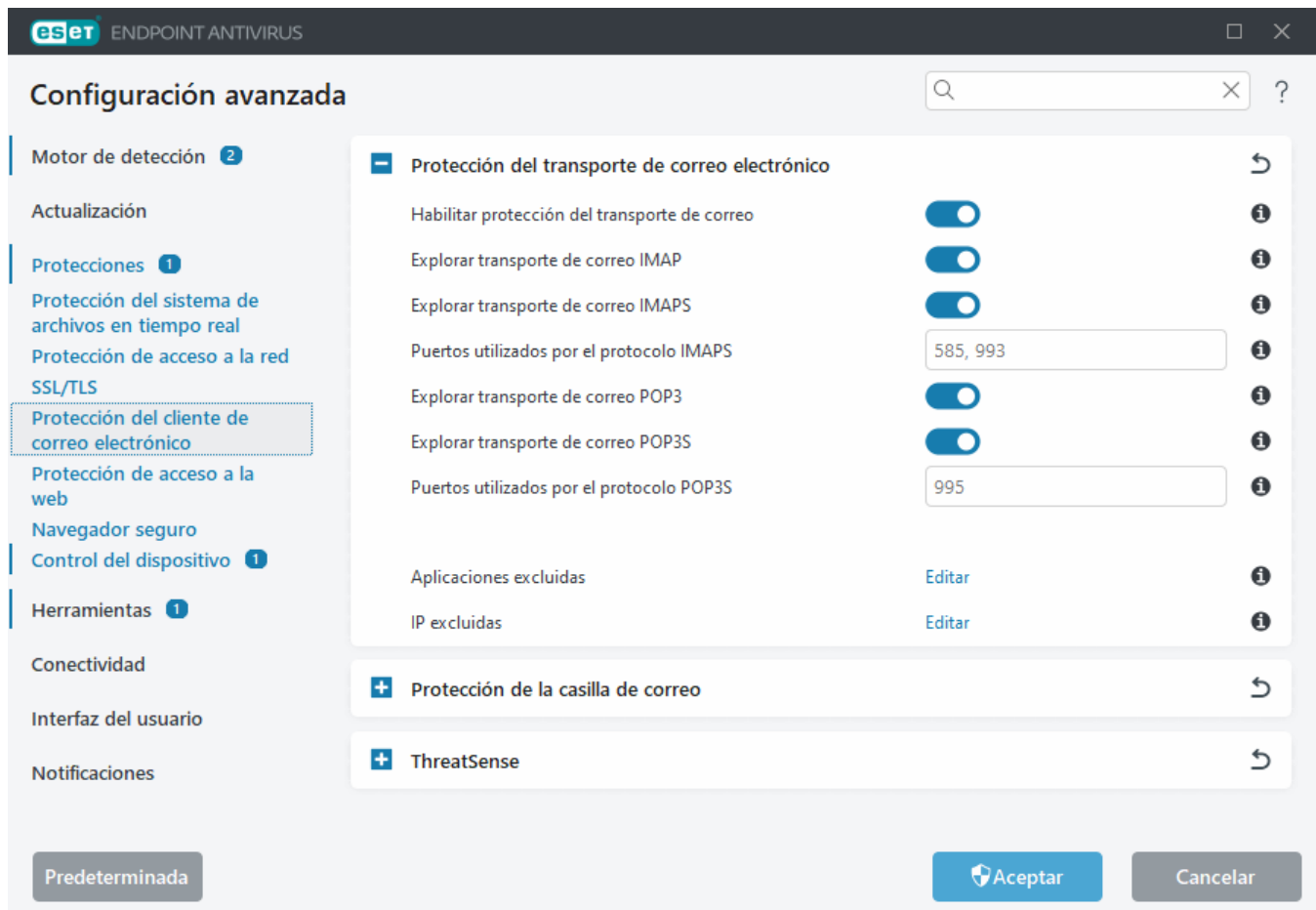
Puede elegir qué protocolos de transporte de correo se explorarán con un clic en el interruptor situado junto a las siguientes opciones (de forma predeterminada, está habilitada la exploración de todos los protocolos):

- **Explorar transporte de correo IMAP**
- **Explorar transporte de correo IMAPS**
- **Explorar transporte de correo POP3**
- **Explorar transporte de correo POP3S**

De forma predeterminada, ESET Endpoint Antivirus explorará la comunicación IMAPS y POP3S en los puertos estándar. Para agregar puertos personalizados para los protocolos IMAPS y POP3S, agréguelos al campo de texto junto a los **Puertos utilizados por el protocolo IMAPS** o **Puertos utilizados por el protocolo POP3S**. Los números de puerto múltiples deben delimitarse con una coma.

[Aplicaciones excluidas:](#) permite excluir aplicaciones específicas de la protección del transporte de correo electrónico. Útil cuando la protección de acceso a la Web causa problemas de compatibilidad.

[IP excluidas:](#) permite excluir direcciones remotas específicas de la exploración de la protección del transporte de correo electrónico. Útil cuando la protección de acceso a la Web causa problemas de compatibilidad.



## Aplicaciones excluidas

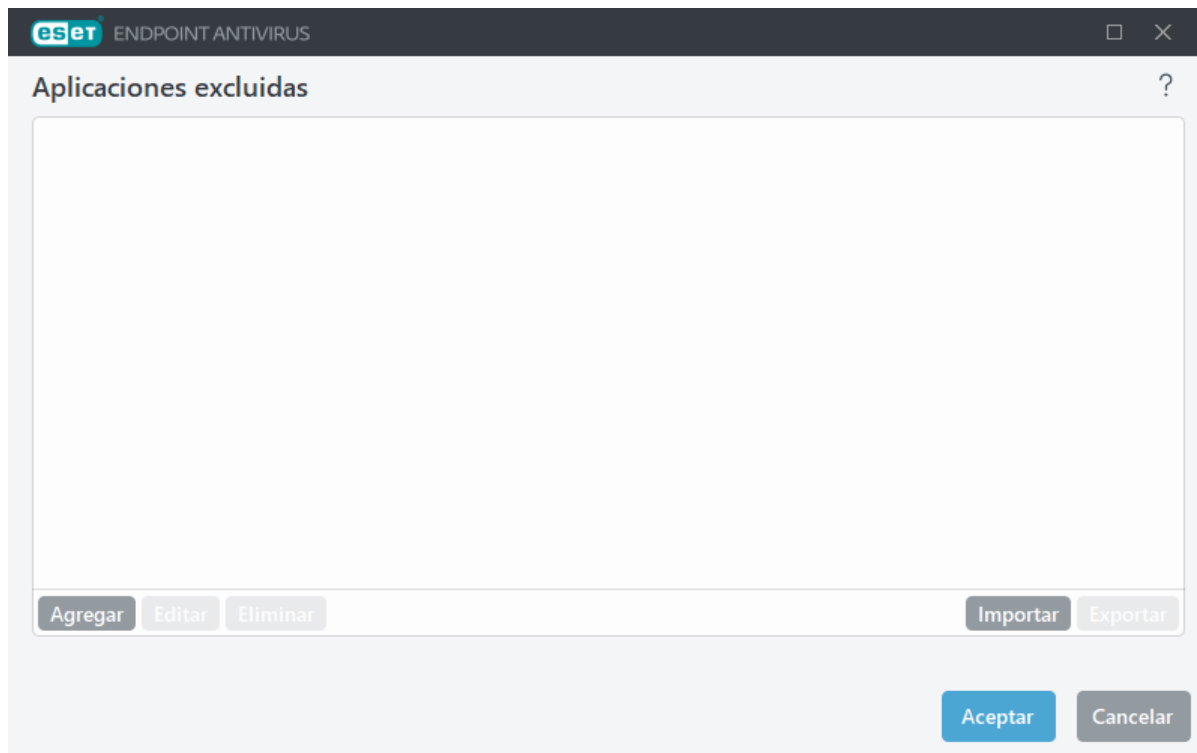
Para excluir la exploración de la comunicación para aplicaciones específicas, agréguelas a la lista. La comunicación HTTP(S)/POP3(S)/IMAP(S) de las aplicaciones seleccionadas no se verificará en busca de amenazas. Es recomendable usar esta opción solamente para las aplicaciones que no funcionen correctamente cuando se explora su comunicación.

Las aplicaciones y los servicios activos se mostrarán automáticamente en esta ventana al hacer clic en **Agregar**. Haga clic en ... y navegue hasta una aplicación para agregar la exclusión manualmente.

**Editar** – edite las entradas seleccionadas de la lista.

**Quitar** – elimine las entradas seleccionadas de la lista.





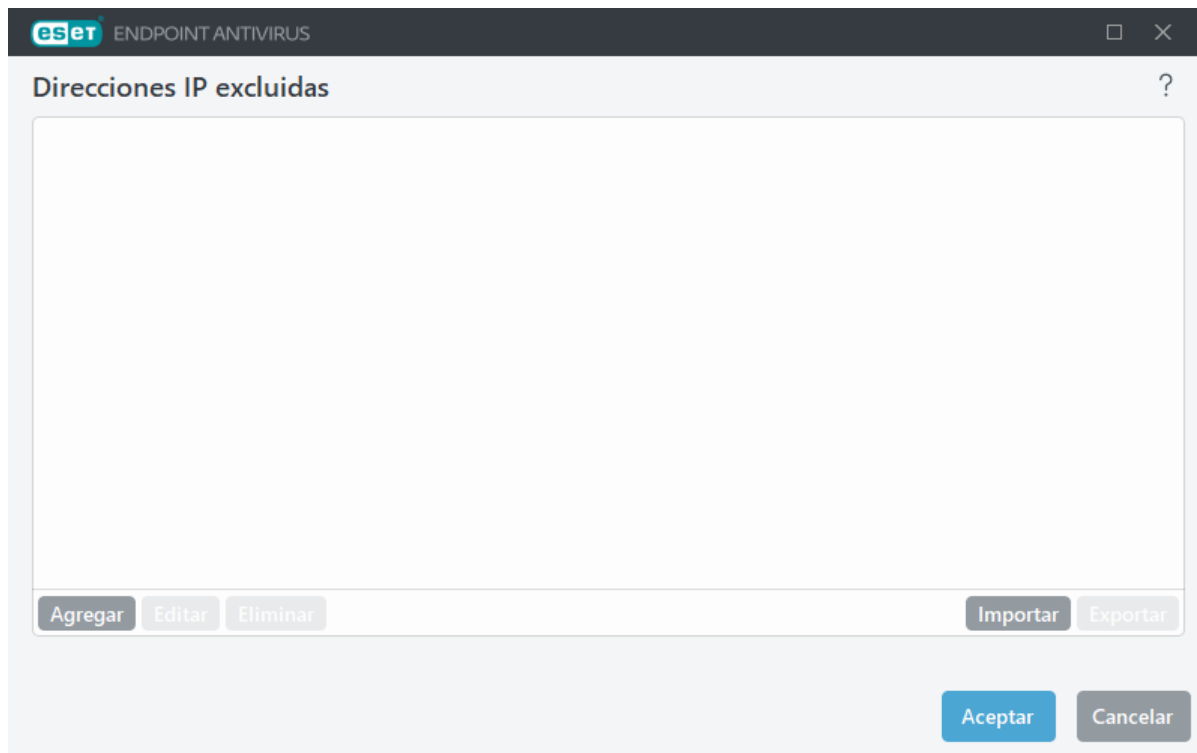
## IP excluidas

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

**Agregar**— haga clic para agregar una dirección IP, un rango de direcciones o una subred de un punto remoto, al que se debe aplicar la regla.

**Editar** — edite las entradas seleccionadas de la lista.

**Quitar** — elimine las entradas seleccionadas de la lista.



### Ejemplos de direcciones IP

Agregar dirección IPv4:

**Dirección única:** agrega una dirección IP de un equipo individual (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 (por ejemplo, *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 la subred 192.168.1.0. Para excluir todo el tipo de subred en *192.168.1.0/24*.

Agregar dirección IPv6:

**Dirección única:** agrega la dirección IP de un equipo individual (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*).

## Protección de la casilla de correo

La integración de ESET Endpoint Antivirus con su buzón de correo aumenta el nivel de protección activa frente a código malicioso en los mensajes de correo electrónico.

Para configurar la protección del buzón de correo, abra **Configuración avanzada** > [Protecciones](#) > **Protección del cliente de correo electrónico** > **Protección del buzón**.

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

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 la [Protección del transporte de correo electrónico](#) (IMAP/IMAPS y POP3/POP3S).

**Integraciones:** le permite integrar la protección del buzón de correo en su cliente de correo electrónico. Consulte [Integraciones](#) para obtener más información.

**Respuesta:** le permite personalizar la gestión de los mensajes de spam. Consulte [Respuesta](#) para obtener más información.

## Integraciones

La integración de ESET Endpoint 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 Endpoint Antivirus. Cuando se integra a su cliente de correo electrónico, la barra de herramientas de ESET Endpoint Antivirus se inserta directamente en el cliente de correo electrónico, lo que permite una protección de correo electrónico más eficaz. Para editar la configuración de integración, abra [Configuración avanzada](#) > **Protecciones** > **Protección del cliente de correo electrónico** > **Protección del buzón de correo** > **Integración**.

**Integrar con Microsoft Outlook** – [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.

**Procesamiento avanzado del cliente de correo electrónico:** procesa eventos extra [Outlook Messaging API \(MAPI\)\\*\\*\\*](#): Objeto modificado (fnevObjectModified) y objeto creado (fnevObjectCreated). Si experimenta lentitud en el sistema al trabajar con su cliente de correo electrónico, habilite esta opción.

## Barra de herramientas de Microsoft Outlook

La protección de Microsoft Outlook funciona como un módulo de complemento. Después de instalar ESET Endpoint Antivirus, esta barra de herramientas que contiene las opciones de protección antivirus se agrega a Microsoft Outlook:

**ESET Endpoint Antivirus:** haga doble clic en el ícono para abrir la ventana principal de ESET Endpoint 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 [Protección del buzón de correo](#).

**Configuración del explorador:** muestra las opciones de configuración de la [Protección del buzón de correo](#).

# Cuadro de diálogo de confirmación

Esta notificación sirve para corroborar que el usuario realmente desea realizar la acción seleccionada para, así, 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 Endpoint 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.

## Respuesta

Según los resultados de la exploración de mensajes, ESET Endpoint Antivirus puede mover los mensajes explorados o agregar texto personalizado al asunto. Puede configurar estas opciones en [Configuración avanzada](#) > **Protecciones** > del **cliente de correo electrónico** > **Protección del buzón de correo electrónico** > **Respuesta**.

Si hay un mensaje que contiene detección, de forma predeterminada, ESET Endpoint Antivirus intenta aclarar el mensaje. Si el mensaje no se puede aclarar, puede elegir una **Acción a realizar si la limpieza no es posible**:

- **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.

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.

**Actualizar el asunto de los correos electrónicos recibidos leídos / Actualizar asunto del correo electrónico:** habilite esta opción para agregar al mensaje texto personalizado especificado a continuación.

**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.

## ThreatSense

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** ubicado en [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 Endpoint Antivirus durante la desinfección de objetos.

## 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 ThreatSense permite definir los tipos de archivos que

se van a explorar.

## Otros

Cuando se configuran los valores 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.

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

## Protección del acceso a la Web

La protección de acceso a la web permite configurar opciones avanzadas del módulo de [protección de Internet](#). Las siguientes opciones están disponibles en [Configuración avanzada](#) > **Protecciones** > **Protección de acceso a la Web** > **Protección de acceso a la web**:

**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](#).

**i** Le recomendamos encarecidamente que deje habilitada la protección de acceso a la web y no excluya ninguna aplicación o dirección IP de forma predeterminada.

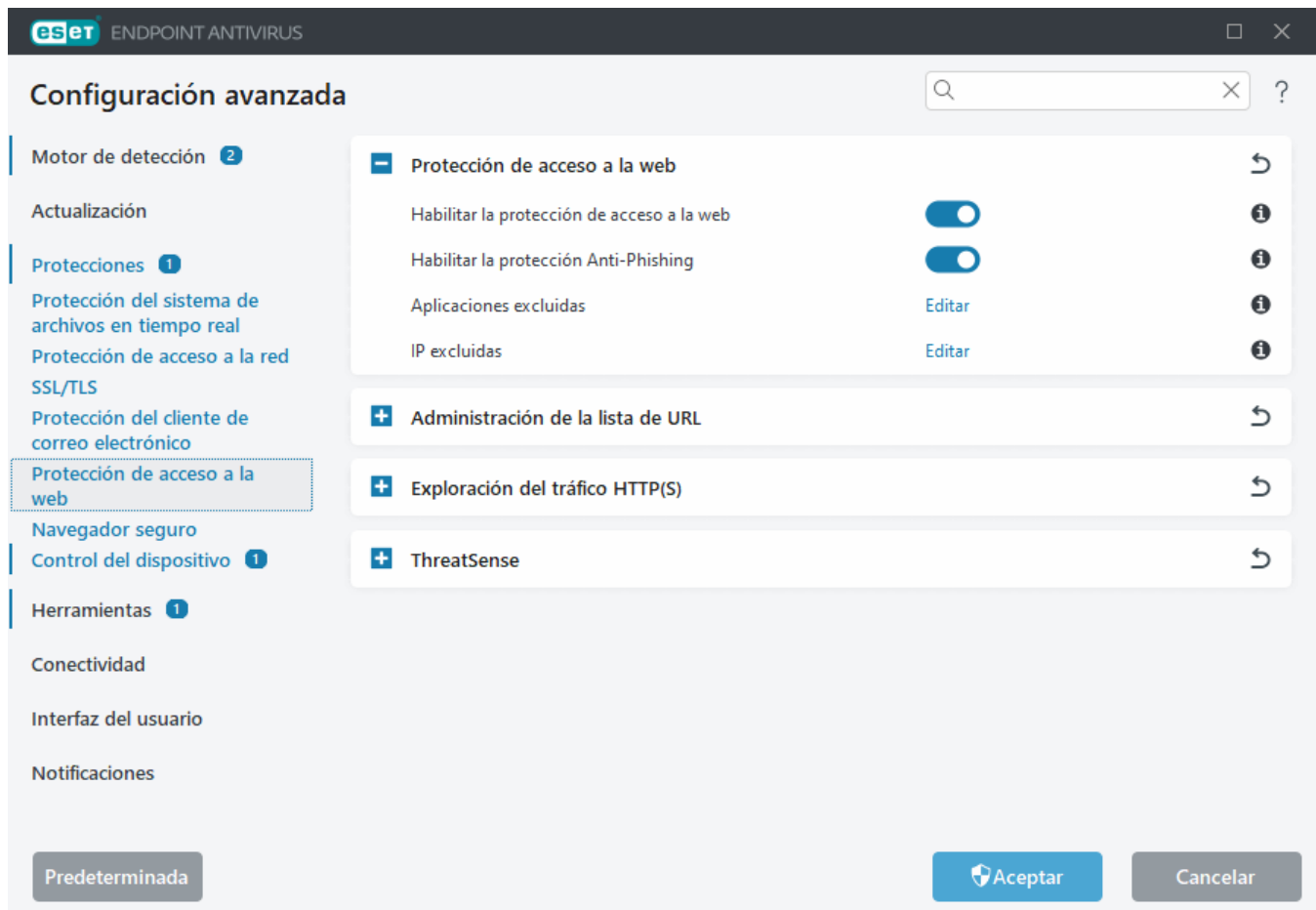
**Explorar scripts del navegador**: cuando está activado, el motor de detección comprueba todos los programas JavaScript ejecutados por los navegadores web.

**Habilitar protección antiphishing**: cuando está habilitada, las páginas web de phishing se bloquean. Consulte [Protección antiphishing](#) para obtener más información.

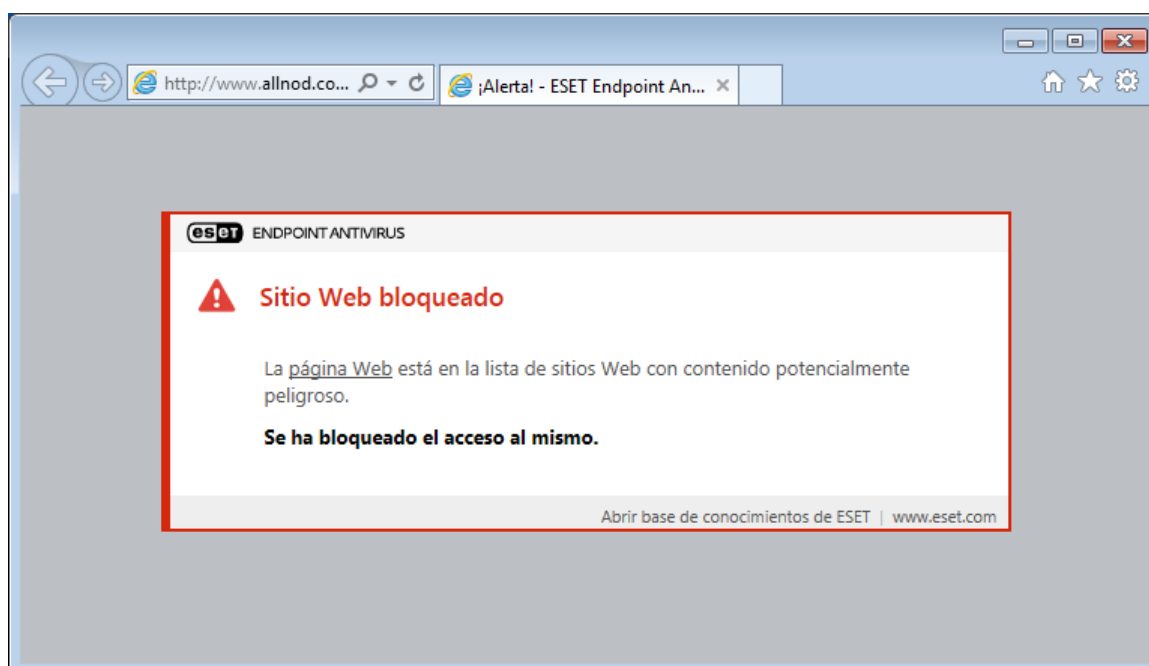
[Aplicaciones excluidas](#): permite excluir aplicaciones específicas de la exploración mediante la Protección de acceso a la Web. Útil cuando la protección de acceso a la Web causa problemas de compatibilidad.

[IP excluidas](#): permite excluir direcciones remotas específicas de la exploración mediante la Protección de acceso a la Web. Útil cuando la protección de acceso a la Web causa problemas de compatibilidad.





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



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

- [Desbloquear un sitio web seguro en una estación de trabajo individual en ESET Endpoint Antivirus](#)

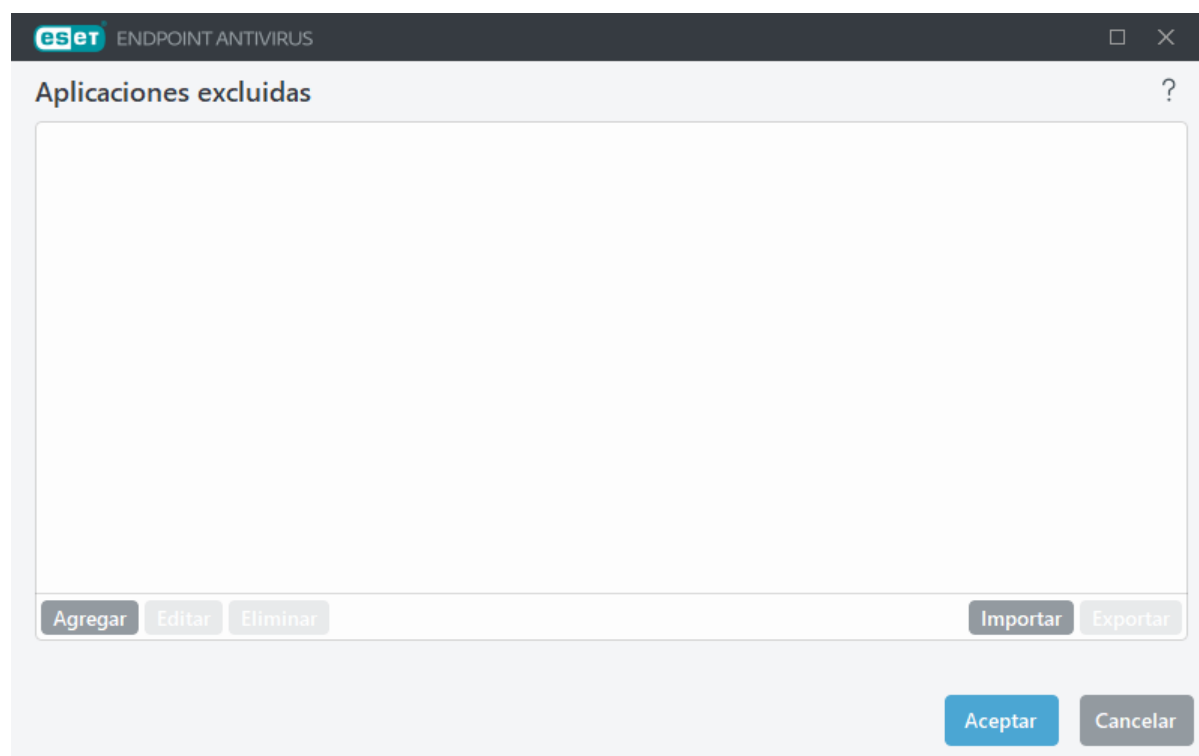
## Aplicaciones excluidas

Para excluir la exploración de la comunicación para aplicaciones específicas, agréguelas a la lista. La comunicación HTTP(S)/POP3(S)/IMAP(S) 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 explora su comunicación.

Las aplicaciones y los servicios activos se mostrarán automáticamente en esta ventana al hacer clic en **Agregar**. Haga clic en ... y navegue hasta una aplicación para agregar la exclusión manualmente.

**Editar** – edite las entradas seleccionadas de la lista.

**Quitar** – elimine las entradas seleccionadas de la lista.



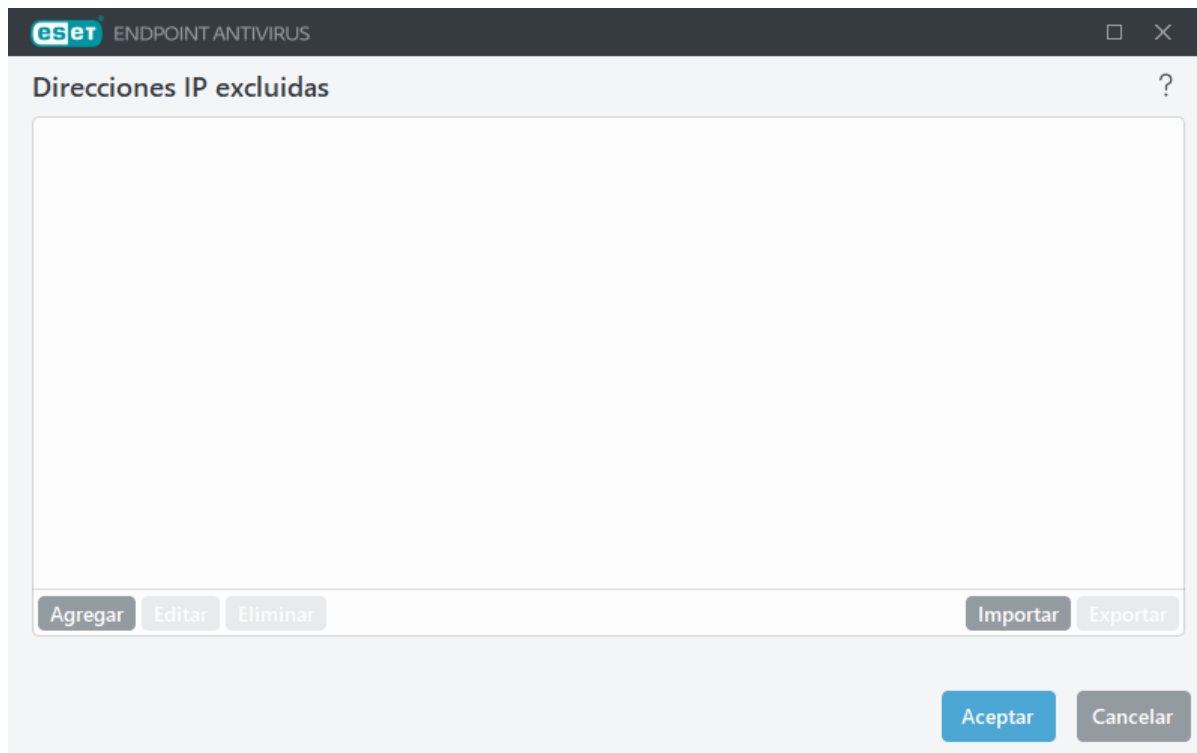
## IP excluidas

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

**Agregar**– haga clic para agregar una dirección IP, un rango de direcciones o una subred de un punto remoto, al que se debe aplicar la regla.

**Editar** – edite las entradas seleccionadas de la lista.

**Quitar** – elimine las entradas seleccionadas de la lista.



### Ejemplos de direcciones IP

Agregar dirección IPv4:

**Dirección única:** agrega una dirección IP de un equipo individual (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 (por ejemplo, *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 la subred 192.168.1.0. Para excluir todo el tipo de subred en *192.168.1.0/24*.

Agregar dirección IPv6:

**Dirección única:** agrega la dirección IP de un equipo individual (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*).

## Administración de la lista de URL

La **administración de la lista URL** en [Configuración avanzada](#) > **Protecciones** > **Protección de acceso a la Web** le permite especificar HTTP direcciones para bloquear, permitir o excluir de la exploración de contenido.

[SSL/TLS](#) debe estar habilitado si desea filtrar direcciones HTTPS además de 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.

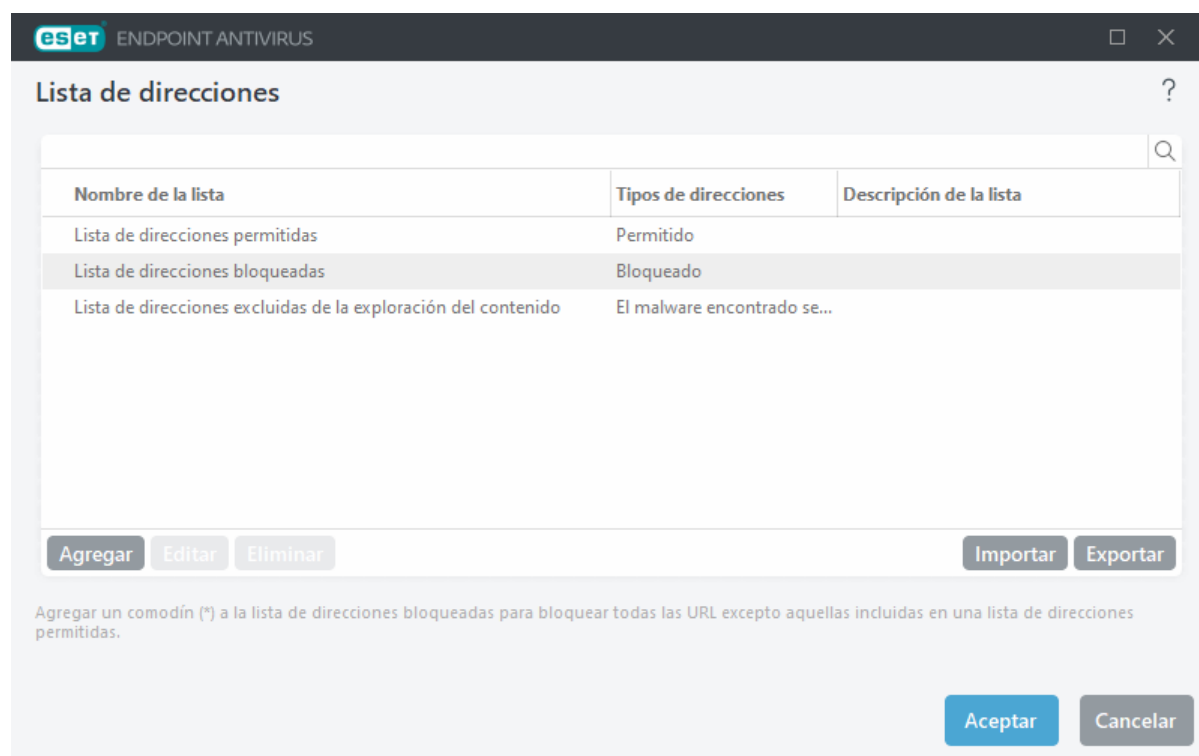
Si desea bloquear todas las direcciones HTTP excepto las direcciones presentes en la **Lista de direcciones permitidas** activa, agregue un \* a la **Lista de direcciones bloqueadas** activa.

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**.

### Direcciones en las que confía ESET

**i** Si **No explorar el tráfico con dominios en los que ESET confía** está habilitado es [SSL/TLS](#), los dominios en la lista blanca administrados por ESET no se verán afectados por la configuración de administración de la lista de URL.



## 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.

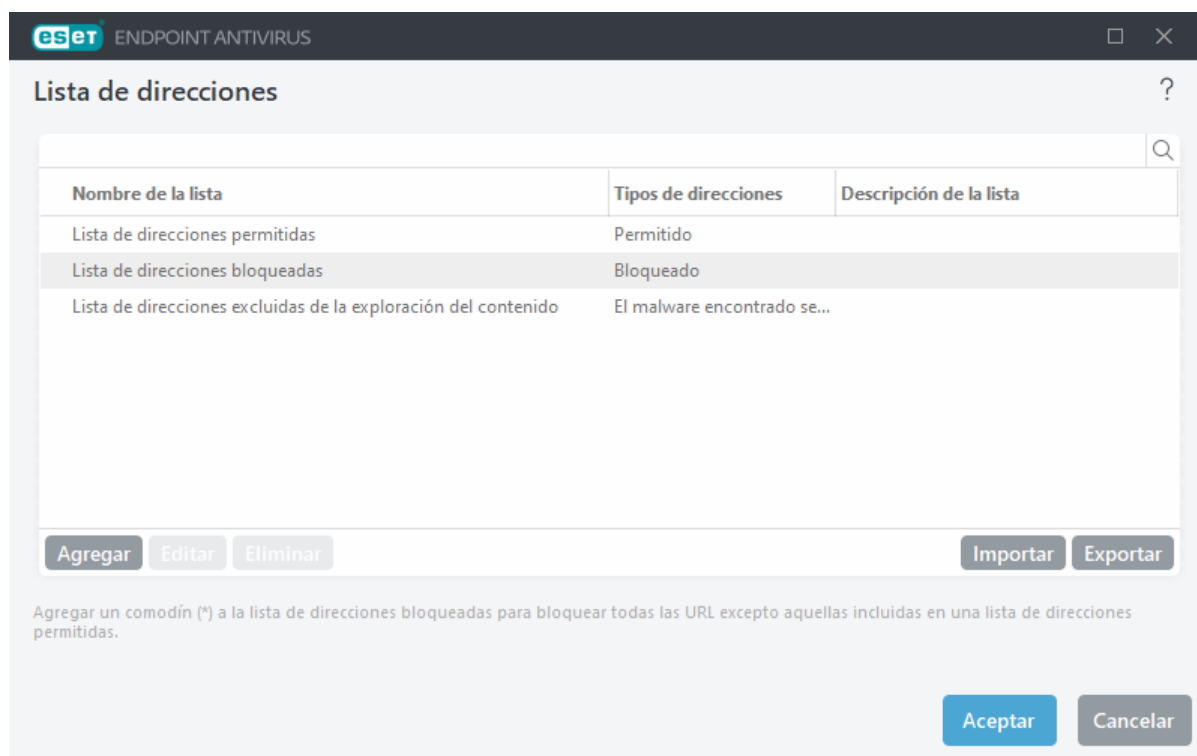
## Lista de direcciones

En esta sección, puede especificar las listas de direcciones HTTP(S) 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**.



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

- [Desbloquear un sitio web seguro en una estación de trabajo individual en ESET Endpoint Antivirus](#)

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

## Crear nueva lista de direcciones

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** – seleccione la severidad de registro del menú desplegable. ESET PROTECT puede recopilar los registros con el nivel de detalle de Advertencia.



El nivel de detalle de registro de información y advertencia solo está disponible para las reglas que contienen al menos dos componentes sin comodines dentro del dominio. Por ejemplo:

- \*.domain.com/\*
- \*www.domain.com/\*

## 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).



Para obtener más información, consulte el capítulo [Cómo agregar una máscara URL](#).

## Cómo agregar una máscara URL

Consulte las instrucciones de este cuadro de diálogo antes de escribir la dirección/máscara de dominio que desee.

ESET Endpoint Antivirus les permite a los usuarios bloquear el acceso a determinados sitios Web para evitar que el navegador de Internet muestre su contenido. También puede especificar las direcciones que no se deben comprobar. 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.).

Por ejemplo: la máscara \*x? incluye todas las direcciones que contengan el carácter "x" en el anteúltimo carácter. Para hacer coincidir el dominio completo, escríbalo en la forma \*.domain.com/\*. La especificación del prefijo del protocolo http://, https:// en la máscara es opcional. Si se omite, la máscara coincidirá con cualquier protocolo.

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>.



El nivel de detalle de registro de información y advertencia solo está disponible para las reglas que contienen al menos dos componentes sin comodines dentro del dominio. Por ejemplo:

- \*.domain.com/\*
- \*www.domain.com/\*

## Exploración del tráfico HTTP(S)

De forma predeterminada, ESET Endpoint Antivirus está configurado para explorar el tráfico HTTP y HTTPS que utilizan los navegadores de Internet y otras aplicaciones. Debe deshabilitar la exploración de tráfico únicamente si tiene problemas con un software de terceros y desea saber si el problema es causado por ESET Endpoint Antivirus.

**Activar exploración del tráfico HTTP:** el tráfico de HTTP se supervisa siempre en todos los puertos para todas las aplicaciones.

**Habilitar la exploración del tráfico HTTPS:** el tráfico HTTPS utiliza un canal cifrado para transferir información entre el servidor y el cliente. ESET Endpoint 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 definidos en **Puertos utilizados por el protocolo HTTPS**, independientemente de la versión del sistema operativo (puede agregar puertos a los predefinidos 443 y 0-65535).

## ThreatSense

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** ubicado en [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 Endpoint Antivirus durante la desinfección de objetos.

## 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 ThreatSense permite definir los tipos de archivos que se van a explorar.

## Otros

Cuando se configuran los valores 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.

## Control de dispositivos

ESET Endpoint Antivirus proporciona control de dispositivo (CD/DVD//USBetc.) automático. 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 (dispositivos con batería, como medios de comunicación, smartphones, dispositivos plug-and-play, etc.)
- Todos los tipos de dispositivos

Las opciones de configuración del control del dispositivo se pueden modificar en [Configuración avanzada](#) > **Protecciones** > **Control del dispositivo**.

Haga clic en el interruptor **Habilitar control del dispositivo** para habilitar la función Control del dispositivo en ESET Endpoint Antivirus; debe reiniciar el equipo para que este cambio surta efecto. Después de habilitar el Control del dispositivo, podrá definir las **Reglas** en la ventana [Editor de reglas](#).

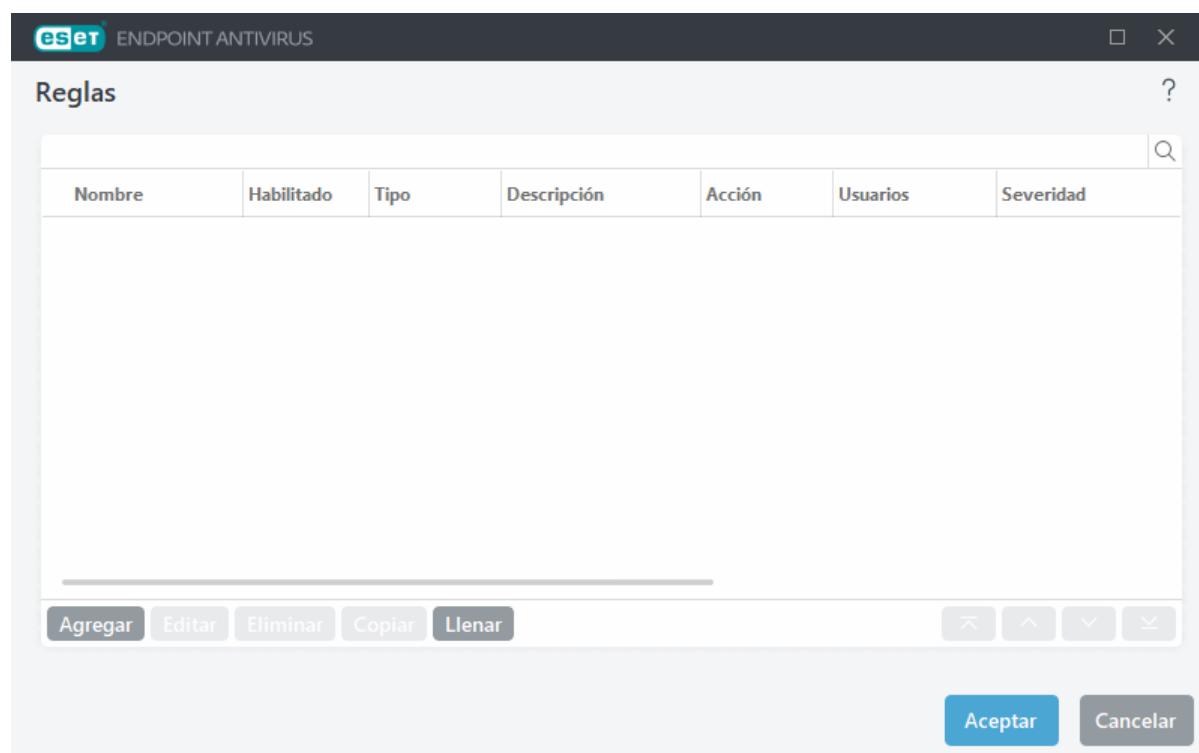
**i** Puede importar un grupo de control de dispositivos con reglas de un archivo xml mediante las tareas programadas. Para obtener más información y una guía paso a paso, consulte el artículo de nuestra [base de conocimiento de ESET](#).

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. También consulte [Agregar reglas de control del dispositivo](#).

**i** Los siguientes artículos de la base de conocimiento de ESET pueden estar disponibles solo en inglés: [Agregue y modifique las reglas del control del dispositivo mediante el uso de los productos de punto de conexión de ESET](#)







Los dispositivos específicos pueden ser permitidos o bloqueados para el usuario, el grupo de usuarios, o cualquiera de los varios parámetros adicionales que se pueden especificar en la configuración de reglas. La lista

de reglas contiene varias descripciones de una regla como nombre, tipo de dispositivo externo, acción a realizar después de conectar un dispositivo externo en su equipo y la severidad del registro.

Haga clic en **Agregar** o **Editar** para administrar una regla. Anule la selección de la casilla de verificación **Habilitada** que se encuentra junto a una regla para deshabilitarla hasta que desee usarla en el futuro. Seleccione una o más reglas, y haga clic en **Eliminar** para eliminar las reglas de forma permanente.

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

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


Las reglas se incluyen en la lista por orden de prioridad, con las reglas de prioridad más alta más cerca de la parte superior. Las reglas se pueden mover al hacer clic en     **Superior/Arriba/Abajo/Inferior**, y se pueden mover individualmente o en grupos.

El [Registro del control de dispositivos](#) registra todas las instancias en las que se activa el Control de dispositivos. Las entradas de registro se pueden ver desde la ventana principal del programa de ESET Endpoint Antivirus en **Herramientas** > [Archivos de registro](#).

## 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.

**Agregar regla** ?

Nombre: Sin título

Regla habilitada: ☒

Aplicar durante: Siempre

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 el interruptor junto a **Regla habilitada** para deshabilitar o habilitar esta regla; esto puede ser útil si no desea eliminar la regla permanentemente.

**Aplicar durante:** le permite aplicar la regla creada durante el tiempo especificado. En el menú desplegable, seleccione el intervalo de tiempo creado. Consulte más información sobre [Intervalos](#).

## 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.

**i** La funcionalidad de la lista del usuario no está disponible para el tipo de dispositivo módem. La regla se aplicará para todos los usuarios y se eliminará la lista actual del usuario.

## 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 aún se mostrará una notificación en 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

- **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 los mensajes de advertencia, y los envía a ERA Server.
- **Ninguno** – no se realizará registro alguno.

Las reglas se pueden limitar a ciertos usuarios o grupos de usuarios al agregarlos a la **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).



Puede importar un grupo de control de dispositivos con reglas de un archivo xml mediante las tareas programadas. Para obtener más información y una guía paso a paso, consulte el artículo de nuestra [base de conocimiento de ESET](#).

## 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.



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** si desea salir de la ventana **Grupos de dispositivos** sin guardar los cambios.



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. 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).

## ThreatSense

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** ubicado en [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 Endpoint Antivirus durante la desinfección de objetos.

## 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 ThreatSense permite definir los tipos de archivos que se van a explorar.

## Otros

Cuando se configuran los valores 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.

## Niveles de desinfección

Para cambiar la configuración del nivel de desinfección de un módulo de protección deseado, expanda **ThreatSense** (por ejemplo, **Protección del sistema de archivos en tiempo real**) y, a continuación, elija un **Nivel de desinfección** en el menú desplegable.

ThreatSense incluye los siguientes niveles de corrección (es decir, desinfección).

### Corrección ESET Endpoint Antivirus

Nivel de desinfección	Descripción
<b>Corregir siempre la detección</b>	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. <b>Corregir siempre la detección</b> es la configuración predeterminada que se recomienda en un <a href="#">entorno administrado</a> .
<b>Corregir la detección si es seguro, de lo contrario conservar</b>	Intento de corregir la detección al desinfectar <a href="#">objetos</a> 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.
<b>Corregir la detección si es seguro, de lo contrario preguntar</b>	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.
<b>Preguntar siempre al usuario final</b>	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.

## Extensiones de archivos que no se analizarán

Las extensiones de archivo que no se analizarán forman parte de [ThreatSense](#). Para configurar las extensiones de archivo excluidas, haga clic en **ThreatSense** de la [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 ThreatSense permite definir los tipos de archivos que se van a explorar.

**i** 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`).

**i** 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 adicionales de ThreatSense

Para editar esta configuración, abra [Configuración avanzada](#) > **Protecciones** > **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 Endpoint 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.

# Herramientas

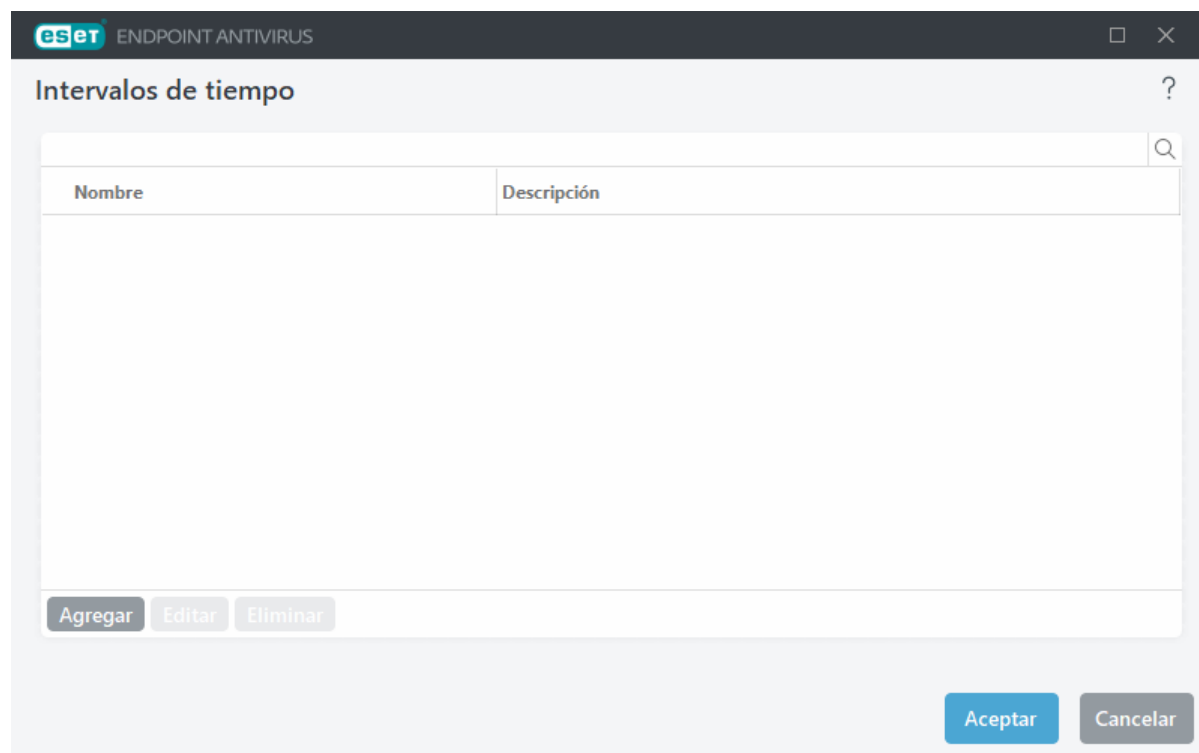
Puede configurar opciones avanzadas para funciones que ofrecen seguridad adicional y ayudan a simplificar la administración de ESET Endpoint Antivirus en [Configuración avanzada](#) > **Herramientas**.

- [Intervalos de tiempo](#)
- [Actualización de Microsoft Windows](#)
- [ESET CMD](#)
- [Monitoreo y administración remotos](#)
- [Verificación de intervalo de licencia](#)
- [Archivos de registro](#)
- [Modo de presentación](#)
- [Diagnósticos](#)

## Intervalos de tiempo

Se pueden crear intervalos de tiempo y luego asignarlos a reglas para el **Control de dispositivos**. La configuración de los **intervalos de tiempo** se encuentra en [Configuración avanzada](#) > **Herramientas**. Esto le permite definir los intervalos de tiempo de uso común (por ejemplo, tiempo de trabajo, fin de semana, etc.) y reutilizarlas fácilmente

sin tener que redefinir los intervalos de tiempo para cada regla. El intervalo de tiempo es aplicable a cualquier tipo de regla relevante que sea compatible con el control basado en el tiempo.



Para crear un intervalo de tiempo, complete lo siguiente:

1. Haga clic en **Editar** > **Agregar**.
2. Ingrese el nombre y la **descripción** del intervalo de tiempo y haga clic en **Agregar**.
3. Especifique el día y la hora de inicio/fin para el intervalo de tiempo o seleccione **Todo el día**.
4. Haga clic en **Aceptar** para confirmar.

Se puede definir un único intervalo de tiempo con uno o más intervalos de tiempo basados en días y horas. Cuando se crea el intervalo de tiempo, este se mostrará en el menú desplegable **Aplicar durante** en la [ventana del editor de reglas de control del dispositivo](#).

## 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 Endpoint 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.

## Ventana de diálogo: actualizaciones del sistema operativo

Si hay algunas actualizaciones disponibles para su sistema operativo, la ESET Endpoint Antivirus ventana Inicio muestra la notificación. 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.

## 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 Endpoint 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 cual 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 Endpoint 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.

Los comandos `ecmd` avanzados solo pueden ejecutarse de forma local. Solo se pueden pausar los comandos `ecmd` mediante la tarea del cliente **Ejecutar comando** con ESET PROTECT.

Exportar comando de configuración:  
`ecmd /getcfg c:\config\settings.xml`  
Importar comando de configuración:  
`ecmd /setcfg c:\config\settings.xml`

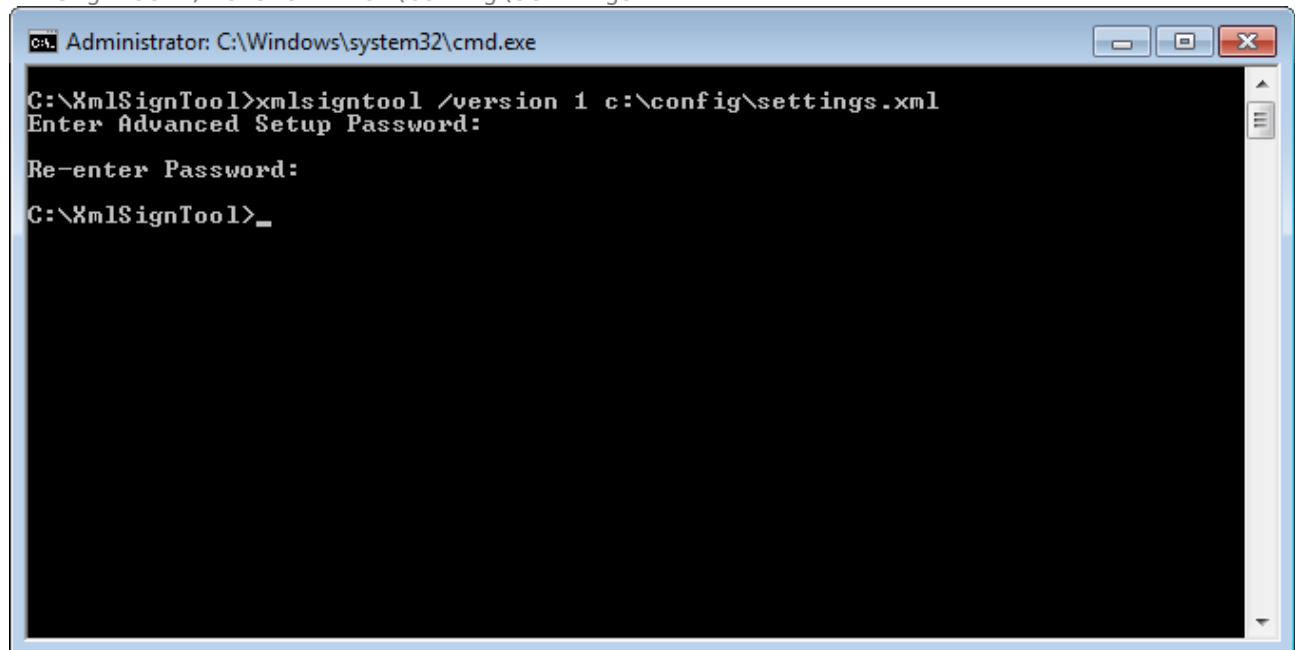
Firmar un archivo de configuración `.xml`:

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 parámetro `/version` depende de la versión que tenga instalada de ESET Endpoint Antivirus. Use `/version 2` para la versión 7 y posteriores.

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 Endpoint 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`







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 Endpoint 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.

## Lista de comandos ecmd

Las características de seguridad individuales pueden habilitarse y deshabilitarse temporalmente con el comando Ejecución de tareas de cliente ESET PROTECT. Los comandos no sobrescriben las configuraciones de la política y las configuraciones pausadas regresarán a su estado original luego de que se haya ejecutado el comando o se haya reiniciado el dispositivo. Para utilizar esta característica, especifique la línea de comandos para ejecutar en el campo con el mismo nombre.

Revise la lista de comandos para cada característica de seguridad abajo:

Característica de seguridad	Comando de pausa temporal	Habilitar comando
Protección del sistema de archivos en tiempo real	ecmd /setfeature onaccess pause	ecmd /setfeature onaccess enable
Protección de documentos	ecmd /setfeature document pause	ecmd /setfeature document enable
Control del dispositivo	ecmd /setfeature devcontrol pause	ecmd /setfeature devcontrol enable
Modo de presentación	ecmd /setfeature presentation pause	ecmd /setfeature presentation enable
Firewall personal	ecmd /setfeature firewall pause	ecmd /setfeature firewall enable
Protección contra ataques en la red (IDS)	ecmd /setfeature ids pause	ecmd /setfeature ids enable
protección contra botnets	ecmd /setfeature botnet pause	ecmd /setfeature botnet enable
Control Web	ecmd /setfeature webcontrol pause	ecmd /setfeature webcontrol enable
Protección del acceso a la Web	ecmd /setfeature webaccess pause	ecmd /setfeature webaccess enable
Protección del cliente de correo electrónico	ecmd /setfeature email pause	ecmd /setfeature email enable
Antispam del cliente de correo electrónico	ecmd /setfeature antispam pause	ecmd /setfeature antispam enable
Protección antiphishing	ecmd /setfeature antiphishing pause	ecmd /setfeature antiphishing habilitar

## Monitoreo y administración remotos

El Monitoreo y la Administración Remotos (RMM) es el proceso de supervisión y control de sistemas de software mediante el uso de un agente instalado localmente al que se puede acceder a través de un proveedor de servicios de administración.

## ERMM: complemento de ESET para RMM

- La instalación predeterminada de ESET Endpoint Antivirus contiene el archivo `ermm.exe` ubicado en la aplicación Endpoint dentro del directorio:  
*C:\Program Files\ESET\ESET Security\ermm.exe*
- `ermm.exe` es una utilidad de la línea de comandos diseñada para facilitar la administración de productos de punto de conexión y comunicaciones con cualquier complemento de RMM.
- `ermm.exe` intercambia datos con el complemento de RMM, que se comunica con el agente de RMM vinculado a un servidor de RMM. De manera predeterminada, la herramienta ESET RMM está deshabilitada.

### Recursos adicionales

- [Línea de comandos de ERMM](#)
- [Lista de los comandos ERMM JSON](#)
- [Cómo activar el monitoreo y la administración remotosESET Endpoint Antivirus](#)

## Complementos de ESET Direct Endpoint Management para soluciones de RMM de terceros

El servidor de RMM se está ejecutando como un servicio en un servidor de terceros. Para obtener más información, consulte las siguientes guías de usuario en línea de ESET Direct Endpoint Management:

- Complemento de [ESET Direct Endpoint Management para ConnectWise Automate](#)
- Complemento de [ESET Direct Endpoint Management para DattoRMM](#)
- [ESET Direct Endpoint Management para Solarwinds N-Central](#)
- [ESET Direct Endpoint Management para NinjaRMM](#)

## Línea de comandos de ERMM

La administración del monitoreo remoto se ejecuta mediante la interfaz de línea de comandos. La instalación predeterminada de ESET Endpoint Antivirus contiene el archivo `ermm.exe` ubicado en la aplicación Endpoint dentro del directorio: *C:\Program Files\ESET\ESET Security*.

Ejecute el símbolo de comando (`cmd.exe`) como administrador y vaya a la ruta mencionada (para abrir el símbolo de comando, presione el botón de Windows + R en el teclado, escriba `cmd` en la ventana de ejecución y presione Entrar).

La sintaxis del comando es: `ermm context command [options]`

Los parámetros del registro distinguen entre mayúsculas y minúsculas.

```

C:\WINDOWS\system32\cmd.exe
C:\Program Files\ESET\ESET Security>ermm
Invalid arguments.

Usage: eRmm context command [options]

Contexts: get, start, set

Commands for specified contexts with options:
get: get information about products
  application-info: get information about application
  license-info: get information about license
  protection-status: get protection status
  logs: get logs: all, virlog, warnlog, scanlog ...
    -N [--name] arg=all (retrieve all logs) name of log to retrieve
    -S [--start-date] arg start time from which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])
    -E [--end-date] arg end time until which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])
  scan-info: get information about scan
    -I [--id] arg id of scan to retrieve
  configuration: get product configuration
    -F [--file] arg path where configuration file will be saved
    -O [--format] arg=json format of configuration: json, xml
  update-status: get information about update
  activation-status: get information about last activation

start: start task
  scan: Start on demand scan
    -P [--profile] arg scanning profile
    -T [--target] arg scan target
  activation: Start activation
    -K [--key] arg activation key
    -O [--offline] arg path to offline file
    -T [--token] arg activation token
  deactivation: start deactivation of product
  update: start update of product

set: set configuration to product
  configuration: set product configuration
    -V [--value] arg configuration data (encoded in base64)
    -F [--file] arg path to configuration xml file
    -P [--password] arg password for configuration

Application parameters:
  -H [--help] help
  -L [--log] log application
--debug display input json

Example: eRmm start scan --target C:\ -p "@Smart scan"

C:\Program Files\ESET\ESET Security>_

```

ermm.exe usa tres contextos básicos: Get, Start y Set. En la siguiente tabla puede encontrar ejemplos de sintaxis de los comandos. Haga clic en el enlace de la columna Comando para ver más opciones, parámetros y ejemplos de uso. Tras la ejecución correcta del comando, se mostrará la parte de salida (resultado). Para ver una parte de entrada, agregue un parámetro `--debug` al comando.

Contexto	Comando	Descripción
get		<b>Obtener información sobre los productos</b>
	<a href="#">application-info</a>	Obtener información sobre el producto
	<a href="#">license-info</a>	Obtener información sobre la licencia
	<a href="#">protection-status</a>	Obtener estado de protección
	<a href="#">logs</a>	Obtener registros
	<a href="#">scan-info</a>	Obtener información sobre la ejecución de una exploración
	<a href="#">configuration</a>	Obtener configuración producto
	<a href="#">update-status</a>	Obtener información sobre la actualización
	<a href="#">activation-status</a>	Obtener información sobre la última activación
start		<b>Iniciar tarea</b>
	<a href="#">scan</a>	Iniciar exploración a petición

Contexto	Comando	Descripción
	<a href="#">activation</a>	Iniciar activación del producto
	<a href="#">deactivation</a>	Iniciar desactivación del producto
	<a href="#">update</a>	Iniciar actualización del producto
<b>set</b>		<b>Definir las opciones del producto</b>
	<a href="#">configuration</a>	Definir la configuración del producto

En el resultado de salida de cada comando, la primera información que se muestra es el identificador del resultado. Para comprender mejor la información del resultado, consulte la tabla de ID que aparece a continuación.

ID de error	Error	Descripción
<b>0</b>	Success	
<b>1</b>	Command node not present	El nodo "Command" no está presente en el json de entrada
<b>2</b>	Command not supported	El comando no es compatible
<b>3</b>	General error executing the command	Error durante la ejecución del comando
<b>4</b>	Task already running	La tarea solicitada ya se está ejecutando y no se ha iniciado
<b>5</b>	Invalid parameter for command	Entrada de usuario defectuosa
<b>6</b>	Command not executed because it's disabled	RMM no está habilitado en configuración avanzada ni se inicia como administrador

## Lista de los comandos ERMM JSON

- [get protection-status](#)
- [get application-info](#)
- [get license-info](#)
- [get logs](#)
- [get activation-status](#)
- [get scan-info](#)
- [get configuration](#)
- [get update-status](#)
- [start scan](#)
- [start activation](#)
- [start deactivation](#)
- [start update](#)
- [set configuration](#)

## get protection-status

Get the list of application statuses and the global application status

### Línea de comandos

```
ermm.exe get protection-status
```

## Parámetros

None

## Ejemplo

call
<pre>{   "command": "get_protection_status",   "id": 1,   "version": "1" }</pre>
result
<pre>{   "id": 1,   "result": {     "statuses": [{       "id": "EkrrnNotActivated",       "status": 2,       "priority": 768,       "description": "Product not activated"     }],     "status": 2,     "description": "Security alert"   },   "error": null }</pre>

## get application-info

Get information about the installed application

## Línea de comandos

```
ermm.exe get application-info
```

## Parámetros

None

## Ejemplo

call
<pre>{   "command": "get_application_info",   "id": 1,   "version": "1" }</pre>
result

```

{
  "id":1,
  "result":{
    "description":"ESET Endpoint Antivirus",
    "version":"6.6.2018.0",
    "product":"eea",
    "lang_id":1033,
    "modules":[{
      "id":"SCANNER32",
      "description":"Detection engine",
      "version":"15117",
      "date":"2017-03-20"
    },{
      "id":"PEGASUS32",
      "description":"Rapid Response module",
      "version":"9734",
      "date":"2017-03-20"
    },{
      "id":"LOADER32",
      "description":"Update module",
      "version":"1009",
      "date":"2016-12-05"
    },{
      "id":"PERSEUS32",
      "description":"Antivirus and antispyware scanner module",
      "version":"1513",
      "date":"2017-03-06"
    },{
      "id":"ADVHEUR32",
      "description":"Advanced heuristics module",
      "version":"1176",
      "date":"2017-01-16"
    },{
      "id":"ARCHIVER32",
      "description":"Archive support module",
      "version":"1261",
      "date":"2017-02-22"
    },{
      "id":"CLEANER32",
      "description":"Cleaner module",
      "version":"1132",
      "date":"2017-03-15"
    },{
      "id":"SYSTEMSTATUS32",
      "description":"ESET SysInspector module",
      "version":"1266",
      "date":"2016-12-22"
    },{
      "id":"TRANSLATOR32",
      "description":"Translation support module",
      "version":"1588B",
      "date":"2017-03-01"
    },{
      "id":"HIPS32",
      "description":"HIPS support module",
      "version":"1267",
      "date":"2017-02-16"
    },{
      "id":"PROTOSCAN32",
      "description":"Internet protection module",
      "version":"1300",
      "date":"2017-03-03"
    },{
      "id":"DBLITE32",
      "description":"Database module",
      "version":"1088",
      "date":"2017-01-05"
    },{
      "id":"CONFENG32",
      "description":"Configuration module (33)",
      "version":"1496B",
      "date":"2017-03-17"
    },{
      "id":"IRIS32",
      "description":"LiveGrid communication module",
      "version":"1022",
      "date":"2016-04-01"
    },{
      "id":"SAURON32",
      "description":"Rootkit detection and cleaning module",
      "version":"1006",
      "date":"2016-07-15"
    },{
      "id":"SSL32",
      "description":"Cryptographic protocol support module",
      "version":"1009",
      "date":"2016-12-02"
    }
  ],
  "error":null
}

```

## get license-info

Get information about the license of the product

### Línea de comandos

```
ermm.exe get license-info
```

### Parámetros

None

### Ejemplo

#### call

```
{
  "command": "get_license_info",
  "id": 1,
  "version": "1"
}
```

#### result

```
{
  "id": 1,
  "result": {
    "type": "NFR",
    "expiration_date": "2020-12-31",
    "expiration_state": "ok",
    "public_id": "3XX-7ED-7XF",
    "seat_id": "6f726793-ae95-4e04-8ac3-e6a20bc620bf",
    "seat_name": "M"
  },
  "error": null
}
```

## get logs

Get logs of the product

### Línea de comandos

```
ermm.exe get logs --name warnlog --start-date "2017-04-04 06-00-00" --end-date "2017-04-04 12-00-00"
```

### Parámetros

Name	Value
name	{ all, virlog, warnlog, scanlog, blocked, hipslog, urllog, devctrllog } : log to retrieve
start-date	start date from which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])

end-date	end time until which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])
----------	---

## Ejemplo

### call

```
{
  "command": "get_logs",
  "id": 1,
  "version": "1",
  "params": {
    "name": "warnlog",
    "start_date": "2017-04-04 06-00-00",
    "end_date": "2017-04-04 12-00-00"
  }
}
```

### result

```
{
  "id": 1,
  "result": {
    "warnlog": {
      "display_name": "Events",
      "logs": [
        {
          "Time": "2017-04-04 06-05-59",
          "Severity": "Info",
          "PluginId": "ESET Kernel",
          "Code": "Malware database was successfully updated to version 15198 (20170404).",
          "UserData": ""
        },
        {
          "Time": "2017-04-04 11-12-59",
          "Severity": "Info",
          "PluginId": "ESET Kernel",
          "Code": "Malware database was successfully updated to version 15199 (20170404).",
          "UserData": ""
        }
      ]
    }
  },
  "error": null
}
```

## get activation-status

Get information about the last activation. Result of status can be { success, running, failure }

### Línea de comandos

```
ermm.exe get activation-status
```

### Parámetros

None



## Ejemplo

### call

```
{
  "command": "get_activation_status",
  "id": 1,
  "version": "1"
}
```

### result

```
{
  "id": 1,
  "result": {
    "status": "success"
  },
  "error": null
}
```

## get scan-info

Obtenga información sobre la ejecución de una exploración.

## Línea de comandos

```
ermm.exe get scan-info
```

## Parámetros

Ninguno

## Ejemplo

### llamar

```
{
  "command": "get_scan_info",
  "id": 1,
  "version": "1"
}
```

### result

```
{
  "id":1,
  "result":{
    "scan-info":{
      "scans":[{
        "scan_id":65536,
        "timestamp":272,
        "state":"finished",
        "pause_scheduled_allowed":false,
        "pause_time_remain":0,
        "start_time":"2017-06-20T12:20:33Z",
        "elapsed_tickcount":328,
        "exit_code":0,
        "progress_filename":"Operating memory",
        "progress_arch_filename":"",
        "total_object_count":268,
        "infected_object_count":0,
        "cleaned_object_count":0,
        "log_timestamp":268,
        "log_count":0,
        "log_path":"C:\\ProgramData\\ESET\\ESET Security\\Logs\\eScan\\ndl31494.dat",
        "username":"test-PC\\test",
        "process_id":3616,
        "thread_id":3992,
        "task_type":2
      }],
      "pause_scheduled_active":false
    }
  },
  "error":null
}
```

## get configuration

Get the product configuration. Result of status may be { success, error }

### Línea de comandos

```
ermm.exe get configuration --file C:\\tmp\\conf.xml --format xml
```

### Parámetros

Name	Value
file	the path where the configuration file will be saved
format	format of configuration: json, xml. Default format is xml

### Ejemplo

```
call
```

```
{
  "command": "get_configuration",
  "id": 1,
  "version": "1",
  "params": {
    "format": "xml",
    "file": "C:\\tmp\\conf.xml"
  }
}
```

#### result

```
{
  "id": 1,
  "result": {
    "configuration": "PD94bWgdmVyc2lvbj0iMS4w=="
  },
  "error": null
}
```

## get update-status

Get information about the update. Result of status may be { success, error }

### Línea de comandos

ermm.exe get update-status

### Parámetros

None

### Ejemplo

#### call

```
{
  "command": "get_update_status",
  "id": 1,
  "version": "1"
}
```

#### result

```
{
  "id": 1,
  "result": {
    "last_update_time": "2017-06-20 13-21-37",
    "last_update_result": "error",
    "last_successful_update_time": "2017-06-20 11-21-45"
  },
  "error": null
}
```

## start scan

Start scan with the product

### Línea de comandos

```
ermm.exe start scan --profile "profile name" --target "path"
```

### Parámetros

Name	Value
profile	Profile name of On-demand computer scan defined in product
target	Path to be scanned

### Ejemplo

```
call
{
  "command": "start_scan",
  "id": 1,
  "version": "1",
  "params": {
    "profile": "Smart scan",
    "target": "c:\\\"
  }
}
```

```
result
{
  "id": 1,
  "result": {
    "task_id": 458752
  },
  "error": null
}
```

## start activation

Start activation of product

### Línea de comandos

```
ermm.exe start activation --key "activation key" | --offline "path to offline file"
```

### Parámetros

Name	Value
key	Activation key

offline	Path to offline file
---------	----------------------

## Ejemplo

### call

```
{
  "command": "start_activation"
  "id": 1,
  "version": "1",
  "params": {
    "key": "XXXX-XXXX-XXXX-XXXX-XXXX"
  }
}
```

### result

```
{
  "id": 1,
  "result": {
  },
  "error": null
}
```

## start deactivation

Start deactivation of the product

## Línea de comandos

ermm.exe start deactivation

## Parámetros

None

## Ejemplo

### call

```
{
  "command": "start_deactivation",
  "id": 1,
  "version": "1"
}
```

### result

```
{
  "id": 1,
  "result": {
  },
  "error": null
}
```

## start update

Start update of the product. Only one update may be running in the product so in case the update is already running, "Task already running" error code is returned

### Línea de comandos

```
ermm.exe start update
```

### Parámetros

None

### Ejemplo

#### call

```
{
  "command": "start_update",
  "id": 1,
  "version": "1"
}
```

#### result

```
{
  "id": 1,
  "result": {
  },
  "error": {
    "id": 4,
    "text": "Task already running."
  }
}
```

## set configuration

Set configuration to the product. Result of status may be { success, error }

### Línea de comandos

```
ermm.exe set configuration --file C:\tmp\conf.xml --format xml --password pass
```

### Parámetros

Name	Value
file	the path where the configuration file will be saved
password	password for configuration
value	configuration data from the argument (encoded in base64)

## Ejemplo

### call

```
{
  "command": "set_configuration",
  "id": 1,
  "version": "1",
  "params": {
    "format": "xml",
    "file": "C:\\tmp\\conf.xml",
    "password": "pass"
  }
}
```

### result

```
{
  "id": 1,
  "result": {
  },
  "error": null
}
```

## Verificación de intervalo de licencia

ESET Endpoint Antivirus debe conectarse a los servidores de licencias de ESET de manera automática. Puede limitar el número de conexiones al servidor de licencias de ESET en [Configuración avanzada](#) > **Herramientas** > **Licencia**. De forma predeterminada, la **comprobación de intervalo** se establece en **Automática** y la conexión se establece varias veces cada hora. En caso de que haya mayor tráfico de red, cambie la **comprobación de intervalo** a **Limitada** para disminuir la sobrecarga. Cuando la opción **Limitada** está seleccionada, ESET Endpoint Antivirus se conecta al servidor de la licencia una sola vez por día, o bien, cuando se reinicia el equipo.



Si la configuración **Verificación del intervalo** está configurada en **Limitada**, todos los cambios relacionados con la licencia y aplicados a través de ESET HUB/ESET MSP Administrator pueden demorar hasta un día en aplicar las configuraciones de ESET Endpoint Antivirus.

## Archivos de registro

Se puede acceder a la configuración de registro de ESET Endpoint Antivirus en [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 está activada, se desfragmentarán automáticamente los archivos de registro si el porcentaje de fragmentación es mayor al valor especificado en el campo **Si la cantidad de historiales no utilizados excede (%)**.

Haga clic en **Optimizar** para comenzar la desfragmentación de los archivos de registro. Se quitan todas las entradas vacías del registro para mejorar el rendimiento y aumentar la velocidad del procesamiento de registros. Esta mejora puede observarse cuando los registros contienen una gran cantidad de entradas.

**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** – seleccione el directorio donde se almacenarán los archivos de registro (solo se aplica a texto/CSV). Puede copiar la ruta de acceso o seleccionar otro directorio haciendo clic en **Borrar**. 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 **Amenazas detectadas**, 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.

**Habilitar el seguimiento de los cambios en la configuración en el registro de auditoría:** le informa sobre cada uno de los cambios en la configuración. Consulte [Registros de auditorías](#) para obtener más información.



**i** 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, consulte nuestro [artículo de la Base de conocimiento de ESET](#).

## Modo de presentación

El Modo de presentación 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 presentación 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 presentación en la [ventana principal del programa](#) en **Configuración** >



**Equipo** con un clic en  o  junto a **Modo de presentación**. Habilitar el modo de presentación constituye un riesgo potencial para la seguridad; por ese motivo, el ícono de estado de protección ubicado en la barra de tareas se pondrá naranja y mostrará una advertencia. Esta advertencia también aparecerá en la [ventana principal del programa](#), donde el **Modo de presentación activo** aparecerá en naranja.

Active **modo de presentación al ejecutar aplicaciones en modo de pantalla completa automáticamente** en [Configuración avanzada](#) > **Herramientas** > **Modo de presentación** 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 presentación automáticamente después de** para definir la cantidad de tiempo luego de la cual el modo de presentación se deshabilitará automáticamente.

## Diagnósticos

Los diagnósticos proporcionan el volcado de memoria de los procesos de ESET (por ejemplo, ekrn). Si una aplicación se bloquea, se generará un volcado. Esto puede ayudar a los desarrolladores a depurar y reparar distintos problemas ESET Endpoint 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

**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 o la protección del sistema de archivos en tiempo real.

**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** - Registrar toda la comunicación del producto entre el producto y los servidores de Direct Cloud.

**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.

**Habilitar el registro avanzado de núcleo:** registre todos los eventos que tienen lugar en el servicio de núcleo de ESET (ekrn) para poder diagnosticar y resolver problemas.

**Habilitar el registro avanzado de licencias:** registra todas las comunicaciones del producto con la activación de ESET y los servidores de licencias.

**Habilitar seguimiento de memoria:** Registre todos los eventos que ayudarán a los desarrolladores a diagnosticar pérdidas de memoria.

**Habilitar el registro avanzado del Firewall:** registra todos los datos de red que pasan a través del firewall en formato PCAP para ayudar a que los desarrolladores diagnostiquen y corrijan problemas relacionados con el firewall.

**Activar registro avanzado del explorador del tráfico de red:** registra todos los datos que pasan a través del explorador del tráfico de red en el formato PCAP para ayudar a los desarrolladores a diagnosticar y solucionar problemas relacionados con el explorador del tráfico de red.

**Habilitar el registro avanzado de sistemas operativos:** se recopilará 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.

**Permitir el registro avanzado de envío de mensajes push** - Registrar todos los sucesos que ocurran durante el envío de mensajes push para permitir el diagnóstico y la solución de problemas.

**Habilitar el registro avanzado de la Protección del sistema de archivos en tiempo real:** graba todos los eventos que ocurren en la Protección del sistema de archivos en tiempo real para permitir el diagnóstico y la resolución de problemas.

**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.

**Habilitar el registro avanzado de Gestión de parches y vulnerabilidades:** registre todos los eventos en [Gestión de parches y vulnerabilidades](#). Esta configuración solo se muestra si la Gestión de parches y vulnerabilidades está habilitada en su entorno (habilitada en ESET PROTECT Cloud).

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 Endpoint 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.

## Conectividad

En redes específicas, la comunicación entre su equipo e Internet puede tener como intermediario un servidor proxy. Si está utilizando un servidor proxy, debe definir la siguiente configuración. De lo contrario, ESET Endpoint Antivirus y sus módulos no se pueden actualizar automáticamente. En ESET Endpoint Antivirus, la configuración del servidor proxy está disponible en dos secciones diferentes de la [Configuración avanzada](#).

La configuración global del servidor proxy puede establecerse en [Configuración avanzada](#) > **Conectividad** > **Servidor proxy**. La especificación del servidor proxy en esta etapa define la configuración global del servidor proxy para todo ESET Endpoint Antivirus. Todos los módulos que requieran una conexión a Internet utilizarán los parámetros aquí ingresados.

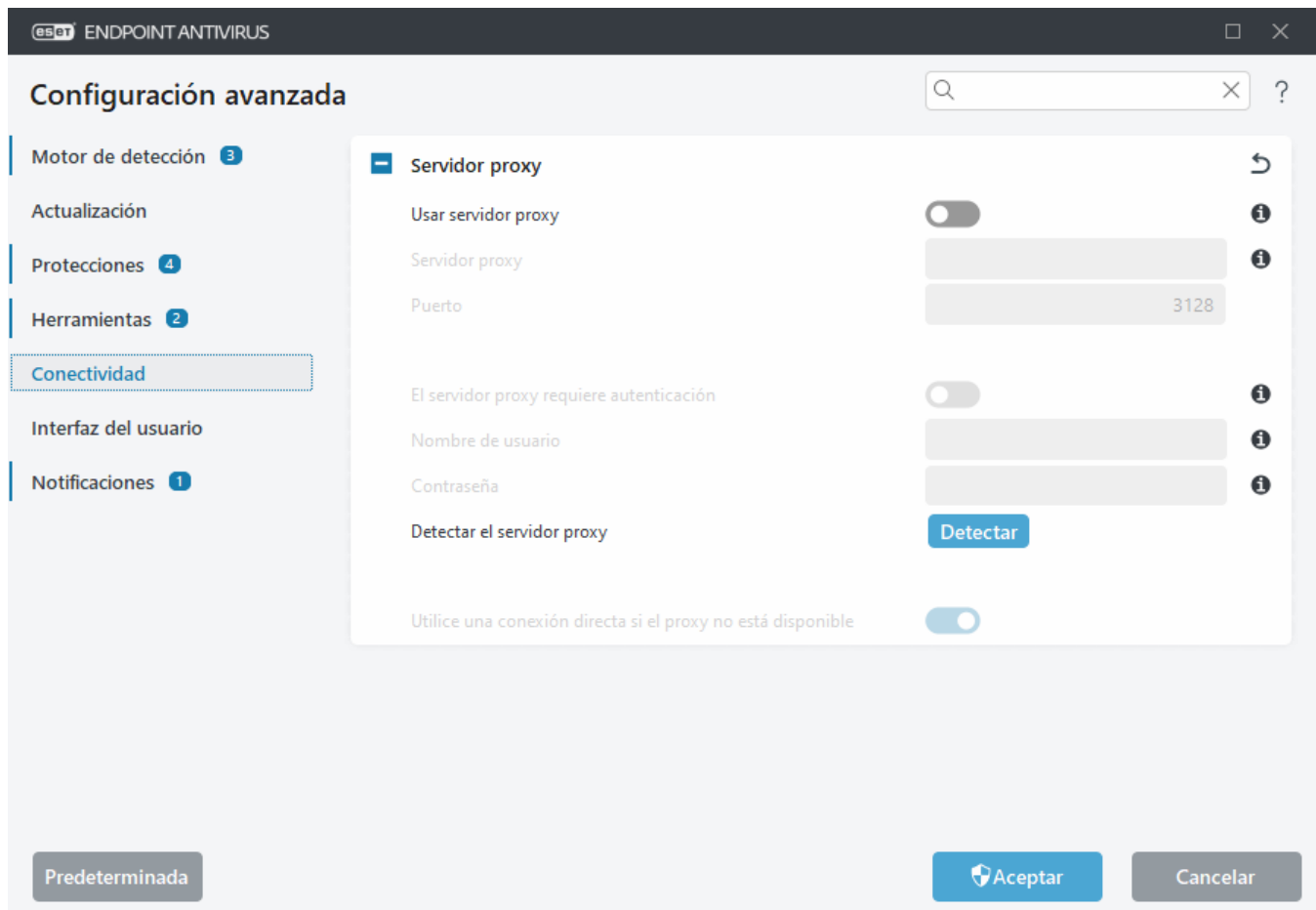
Para especificar la configuración global del servidor proxy, habilite **Usar servidor proxy** y escriba la dirección del **servidor proxy** junto con el número de **puerto** del servidor proxy.

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 correspondientes. Haga clic en **Detectar servidor proxy** para detectar y llenar la configuración del servidor proxy en forma automática. Para buscar la configuración de proxy en su sistema operativo, presione las teclas de acceso directo de **Windows + I** y haga clic en **Red e Internet** > **Proxy**. ESET Endpoint Antivirus copiará los parámetros especificados en las opciones de Internet para 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 Endpoint Antivirus está configurado para usar proxy y no puede llegar al proxy, ESET Endpoint Antivirus evadirá el proxy y se comunicará directamente con los servidores ESET.

La configuración del servidor proxy también puede configurarse en [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 solo para actualizaciones y se recomienda para equipos portátiles que reciben actualizaciones de módulos desde ubicaciones remotas. Para obtener más información, consulte [Configuración avanzada de actualizaciones](#).



## Interfaz del usuario

Para configurar el comportamiento de la interfaz gráfica de usuario (GUI) del programa, abra [Configuración avanzada](#) > **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](#).

El [Modo de presentación](#) es útil para los usuarios que deseen trabajar con una aplicación sin que las ventanas emergentes, las tareas programadas o cualquier componente que pueda sobrecargar el procesador y la memoria RAM provoquen interrupciones.

También consulte [Cómo minimizar la interfaz del usuario de ESET Endpoint Antivirus](#) (útil para entornos administrados).

# Elementos de la interfaz del usuario

Las opciones de configuración de la interfaz del usuario en ESET Endpoint Antivirus permiten ajustar el entorno de trabajo conforme a sus necesidades. Estas opciones de configuración son accesibles en **Configuración avanzada** (F5) > **Interfaz de usuario** > **Elementos de la interfaz de usuario**.


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

**Completo** – se mostrará la GUI completa.

**Mínimo**: la GUI está en ejecución, pero solo se muestran las notificaciones al usuario.


**Manual**: la GUI no inició automáticamente en el inicio de sesión. Cualquier usuario puede iniciarla de forma manual.

**Silencioso**: no se mostrarán notificaciones ni alertas. Solo el administrador puede iniciar la GUI. Este modo puede ser útil en entornos administrados o en situaciones en las que necesita preservar los recursos del sistema.

 Una vez que se selecciona el modo de inicio de GUI Mínimo y su equipo se reinicia, se mostrarán las notificaciones, pero la interfaz gráfica no. Para volver al modo de interfaz de usuario gráfica completo, ejecute la GUI desde el menú Inicio en **Todos los programas** > **ESET** > ESET Endpoint Antivirus como administrador, o puede hacerlo mediante ESET PROTECT con una [política](#).

**Modo de color**— seleccione el esquema de colores de la GUI de ESET Endpoint Antivirus en el menú desplegable:

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

 También puede seleccionar el esquema de colores de la interfaz gráfica de usuario de ESET Endpoint Antivirus en la esquina superior derecha de la [ventana principal del programa](#).

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

Para que ESET Endpoint Antivirus reproduzca un sonido cuando ocurren sucesos importantes durante una exploración como, por ejemplo, cuando se descubre una amenaza o cuando finaliza la exploración, seleccione **Usar señal sonora**.

**Integrar en el menú contextual** – integrar los elementos de control de ESET Endpoint Antivirus al menú contextual.

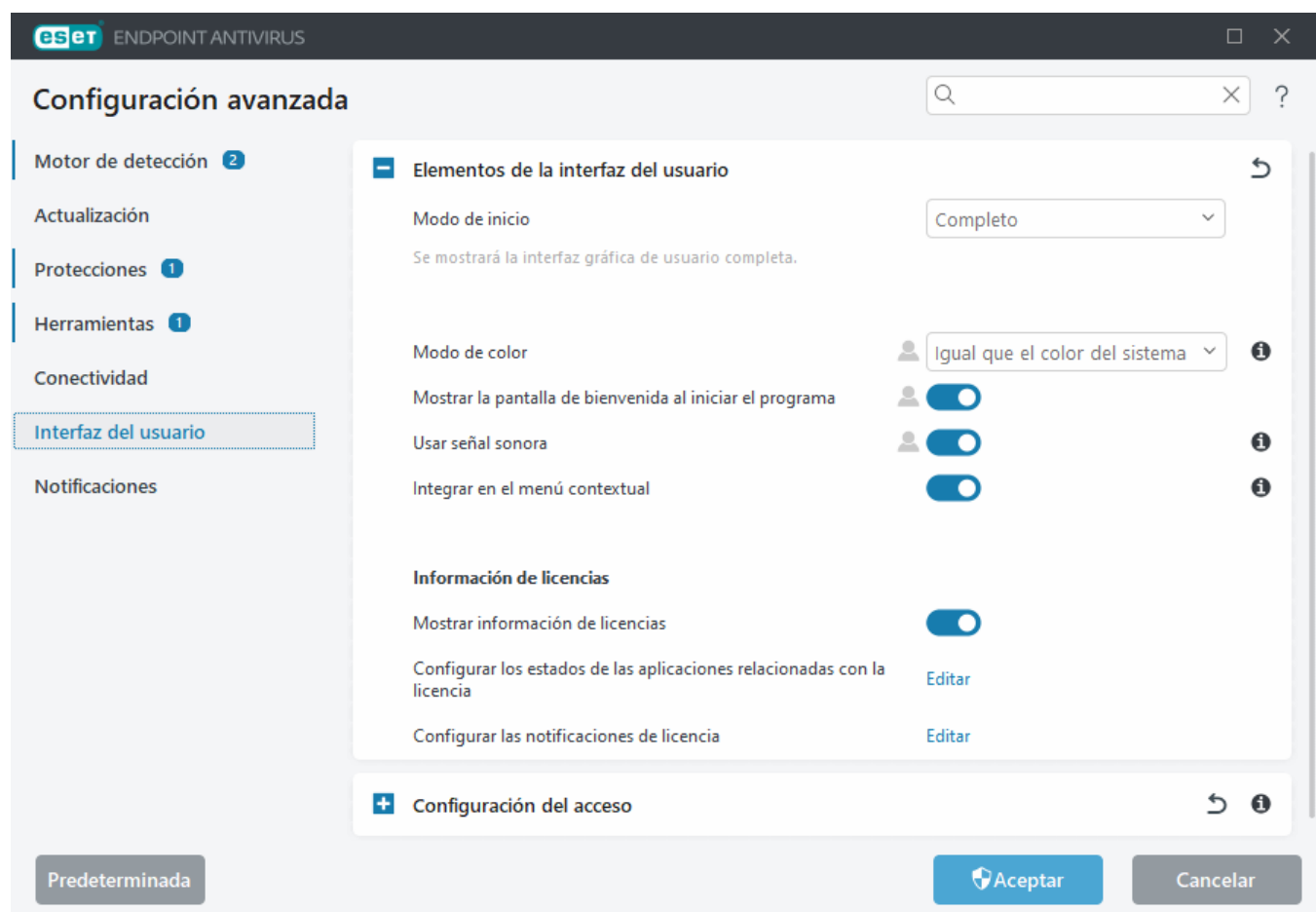
## Información de licencias

**Mostrar información de licencias**: cuando está deshabilitada, no se mostrará la fecha de vencimiento de la licencia en **Estado de protección** ni la pantalla **Ayuda y soporte**.

**Configurar estados de la aplicación relacionados con las licencias**: abre la lista de [estados de la aplicación](#) relacionados con la licencia.

**Configurar notificaciones de licencia:** abre la lista de notificaciones relacionadas con la licencia.

**i** La configuración de información de licencia se aplica pero no está accesible para ESET Endpoint Antivirus activado con licencia MSP.



## Configuración del acceso

Las configuraciones ESET Endpoint 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 Endpoint Antivirus pueden protegerse con una contraseña. La configuración de acceso se puede configurar en [Configuración avanzada](#) > **Interfaz del usuario** > **Configuración de acceso**.

Para establecer una contraseña para proteger los parámetros de configuración y desinstalación de ESET Endpoint Antivirus, haga clic en **Establecer** junto a **Proteger la configuración con una contraseña**.

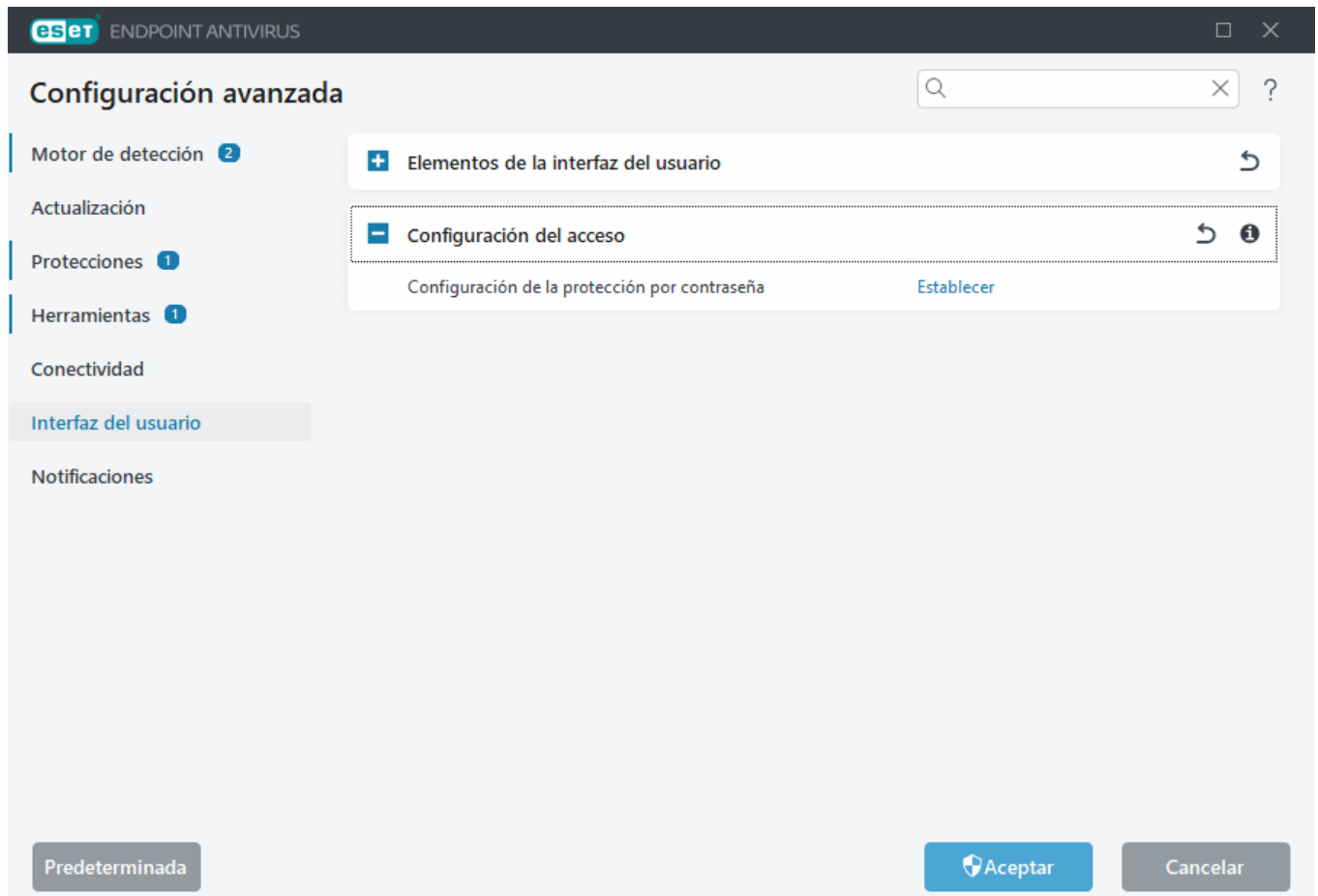
Para cambiar la contraseña, haga clic en **Cambiar contraseña** junto a **Proteger la configuración con una contraseña**.

Para quitar la contraseña, haga clic en **Quitar** junto a **Proteger la configuración con una contraseña**.

## Entornos administrados

El administrador puede crear una política para proteger con contraseña la configuración de ESET Endpoint Antivirus en los equipos cliente conectados. Para crear una nueva política, consulte [Configuraciones protegidas de](#)

[las contraseñas.](#)



## Contraseña para configuración avanzada

Para proteger la Configuración avanzada de ESET Endpoint Antivirus y evitar modificaciones no autorizadas, ingrese su nueva contraseña en los campos **Nueva contraseña** y **Confirmar contraseña**. Haga clic en **Aceptar**.

### Entornos administrados

El administrador puede crear una política para proteger con contraseña la configuración de ESET Endpoint Antivirus en los equipos cliente conectados. Para crear una nueva política, consulte [Configuraciones protegidas de las contraseñas](#).

### Sin administración

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 futuras modificaciones de ESET Endpoint Antivirus.

Si ha olvidado su contraseña, consulte [Desbloquear la contraseña de configuración en los productos ESET Endpoint](#).

Para recuperar la clave de licencia de ESET perdida, la fecha de caducidad de su licencia u otra información sobre la licencia de ESET Endpoint Antivirus, consulte [Perdí mi Nombre de usuario y Contraseña/Clave de licencia](#).

## Contraseña

Para evitar la modificación no autorizada, los parámetros de configuración de ESET Endpoint Antivirus pueden protegerse con una contraseña.

## Modo seguro

Si la interfaz gráfica de ESET Endpoint Antivirus se ejecuta en modo seguro, aparecerá una ventana de diálogo con la indicación de que la aplicación se debe ejecutar en modo seguro. Debido a que en este modo el funcionamiento de todos los programas es limitado, no es posible abrir la interfaz gráfica de ESET Endpoint Antivirus como en el modo estándar.

La ventana que se muestra le permitirá ejecutar una exploración del equipo. Si desea verificar el equipo en busca de códigos maliciosos, seleccione la opción **Sí**.

De esta forma, la exploración se ejecutará en una ventana separada con los mismos parámetros que el perfil predeterminado de exploración del equipo después de la instalación de ESET Endpoint Antivirus.

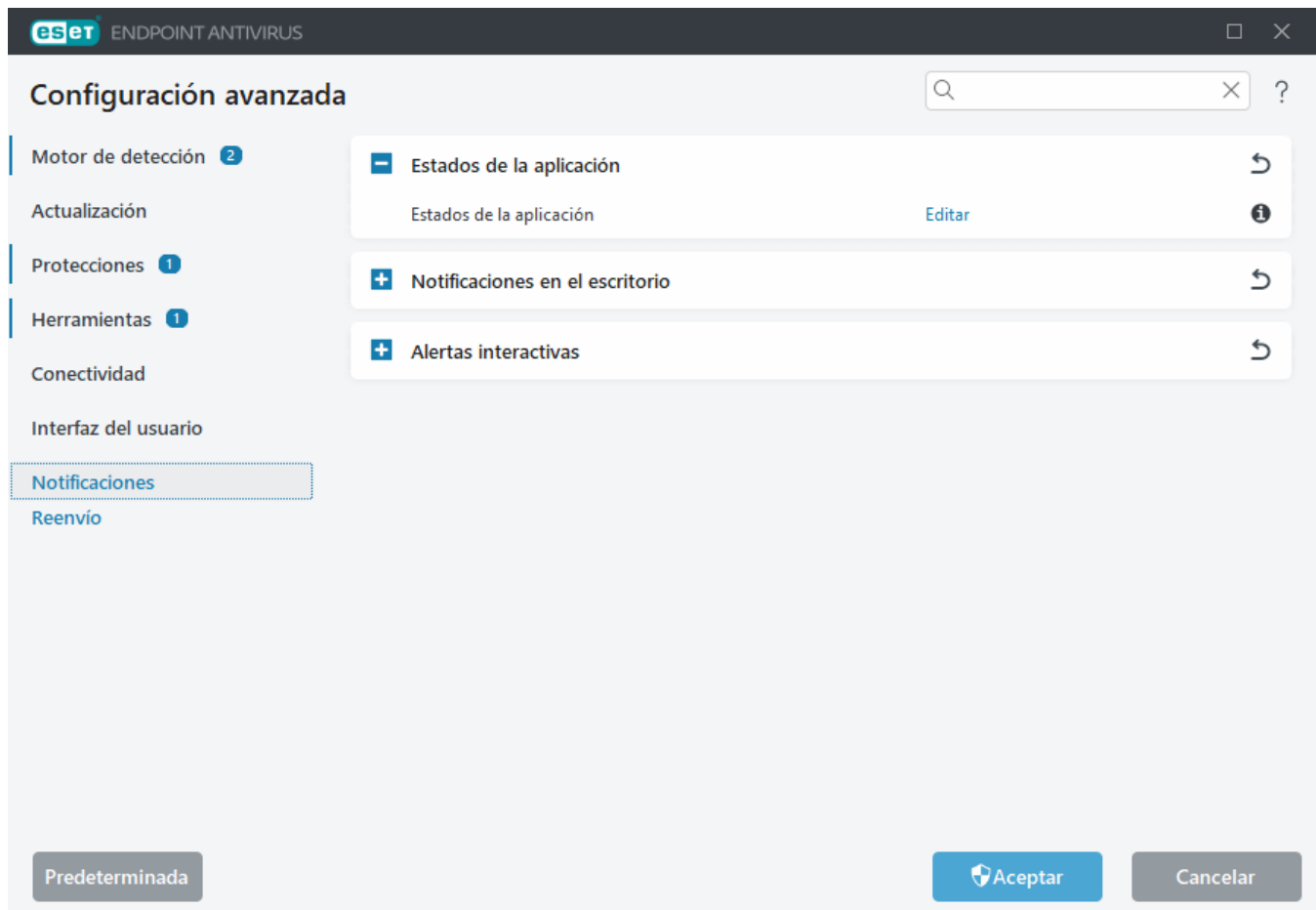
Seleccione la opción **No** para cerrar la ventana de diálogo; ESET Endpoint Antivirus no realizará ninguna acción.

## Notificaciones

Para administrar las notificaciones de ESET Endpoint Antivirus, abra [Configuración avanzada](#) > **Notificaciones**. Puede configurar los siguientes tipos de notificaciones:

- Estados de la aplicación: notificaciones que se muestran en la sección de inicio de la [ventana principal del programa](#).
- [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.
- [Personalización de las notificaciones](#) : se agrega un mensaje personalizado a una notificación de escritorio, por ejemplo.





## 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.

## Estados de la aplicación

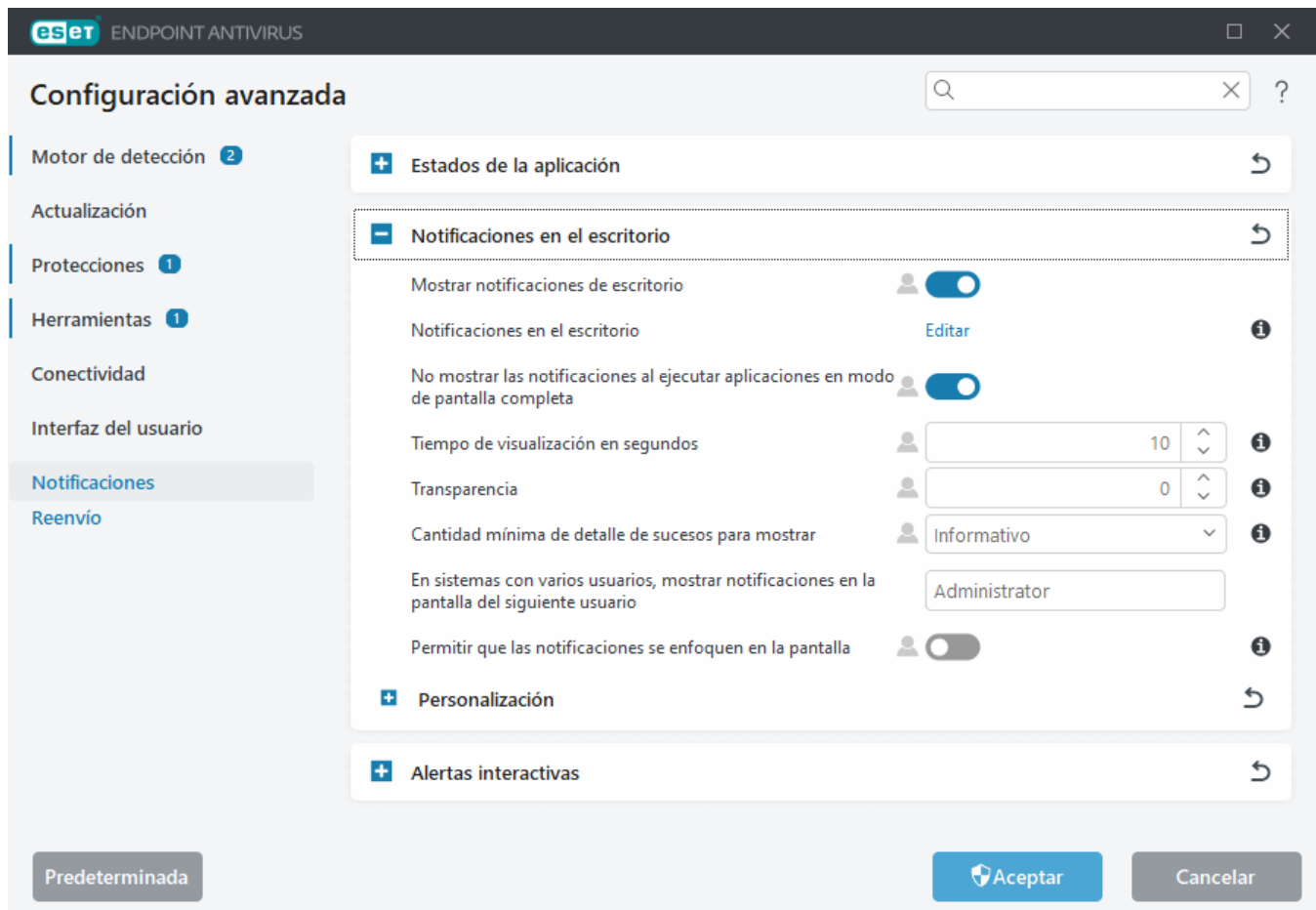
Para configurar los estados de la aplicación que se mostrarán (por ejemplo, al pausar la protección antivirus y antispyware o activar el modo de presentación), abra [Configuración avanzada](#) > **Notificaciones** y haga clic en **Editar** junto a **Estados de la aplicación**.

El estado de la aplicación también se mostrará si su producto no está activado o si la licencia ha vencido. Esta configuración puede cambiarse mediante las políticas de [ESET PROTECT](#).



## Notificaciones en el escritorio

La notificación de escritorio está representada por una pequeña ventana de notificación ubicada junto a la barra de tareas del sistema. De manera predeterminada, se configura para mostrarse durante 10 segundos y, luego, desaparece lentamente. Esta es la manera principal en que ESET Endpoint Antivirus se comunica con el usuario y envía notificaciones sobre actualizaciones correctas del producto, nuevos dispositivos conectados, compleción de tareas de detección de virus o nuevas amenazas detectadas.



**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:

- **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 solo los errores críticos, como error al iniciar la protección antivirus o sistema infectado.

**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:** las notificaciones tendrán enfoque en la pantalla y podrá accederse con Alt+Tab.

## Personalización de las notificaciones

En esta ventana puede personalizar la mensajería que se usa en las notificaciones.

**Mensaje de notificación predeterminado** – un mensaje predeterminado que será mostrado en el pie de página de las notificaciones.

### Detecciones

Habilite **No cerrar las notificaciones sobre malware automáticamente** para que las notificaciones de malware permanezcan en la pantalla hasta que se cierren manualmente.

Deshabilite **Usar mensaje predeterminado** e introduzca su propio mensaje en el campo **Mensaje de notificación de detección** para usar mensajería de notificación personalizada.

## Cuadro de diálogo: notificaciones en el escritorio

Para ajustar la visibilidad de las notificaciones en el escritorio (mostradas en la parte inferior derecha de la pantalla), abra la [Configuración avanzada](#) > **Notificaciones** > **Notificaciones en el escritorio**. Haga clic en **Editar** junto a **Notificaciones en el escritorio** y marque la casilla de verificación **Mostrar en el escritorio** correspondiente.

Nombre	Mostrar en escritorio
<b>ACTUALIZACIÓN</b>	
El motor de detección se actualizó correctamente	<input type="checkbox"/>
Error de actualización de la aplicación	<input type="checkbox"/>
Error de actualización de red	<input type="checkbox"/>
Error de actualización de réplica	<input type="checkbox"/>
Error de actualización del módulo	<input checked="" type="checkbox"/>
Hay una nueva actualización de la aplicación disponible	<input checked="" type="checkbox"/>
La actualización de la aplicación está preparada	<input checked="" type="checkbox"/>
Los módulos se actualizaron correctamente	<input type="checkbox"/>
<b>ANTIVIRUS</b>	
Comenzó la exploración inicial	<input checked="" type="checkbox"/>

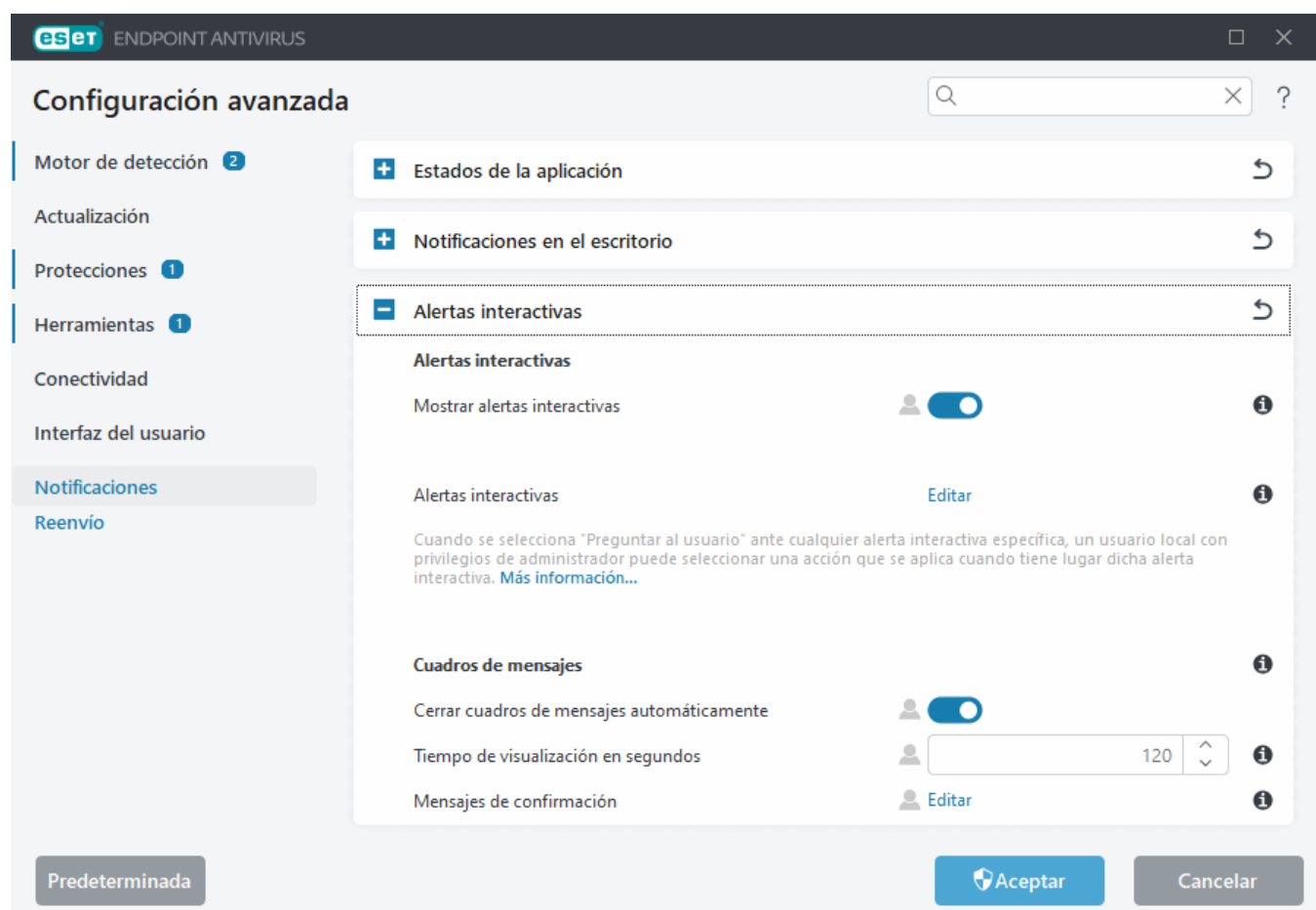
**i** Si desea configurar notificaciones de **Archivo analizado** y **Archivo no analizado** mientras usa ESET LiveGuard, se debe configurar la [protección proactiva](#) en **Bloquear ejecución hasta recibir el resultado del análisis**.

## Alertas interactivas

### ¿Necesita información sobre alertas y notificaciones comunes?

- [Amenaza detectada](#)
- [La dirección se ha bloqueado](#)
- [Producto no activado](#)
- [Está disponible la actualización](#)
- **!** La información sobre la actualización no es consistente
- [Resolución de problemas para el mensaje «error de actualización de módulos»](#)
- ['Archivo corrupto' o 'Ocurrió un error al asignar un nuevo nombre al archivo'](#)
- [Certificado de sitio web revocado](#)
- [Se bloqueó una amenaza de red](#)
- [Archivo bloqueado debido al análisis](#)

La sección **Alertas interactivas** de [Configuración avanzada](#) > **Notificaciones** le permite configurar cómo gestiona ESET Endpoint 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.

- Para los usuarios no administrados, recomendamos dejar esta opción en su configuración predeterminada (habilitada).
- Para los usuarios administrados, deje esta configuración habilitada y seleccione una acción predefinida para los usuarios en la [Lista de alertas interactivas](#).

**Alertas interactivas:** haga clic en **Editar** para seleccionar qué [alertas interactivas](#) se mostrarán.

## 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.

## Lista de alertas interactivas

Esta sección describe distintas ventanas de alerta interactivas que ESET Endpoint Antivirus muestra antes de realizar una acción.

Para ajustar el comportamiento de las alertas interactivas configurables, abra [Configuración avanzada](#) > **Notificaciones** > **Alertas interactivas** y haga clic en **Editar** junto a **Alertas interactivas**.



Útil para entornos administrados en los que el administrador puede anular la selección de **Solicitar al usuario** en cualquier lugar y seleccionar una acción predefinida que se aplica cuando se muestran ventanas de alerta interactivas.



Consulte otras secciones de ayuda para obtener referencias para una ventana de alerta interactiva específica:

## Medios extraíbles

- [Se detectó un nuevo dispositivo](#)

## Protección de la red

- [Acceso a la red bloqueado](#) se muestra cuando se activa la tarea de cliente **Aislar equipo de la red** de esta estación de trabajo desde ESET PROTECT.
- [Se bloqueó la comunicación de red](#)
- [Se bloqueó una amenaza de red](#)

## Alertas del navegador web

- [Se encontró contenido potencialmente no deseado](#)
- [Sitio web bloqueado debido a phishing](#)

## Equipo

La presencia de estas alertas cambiará el color de la interfaz del usuario:

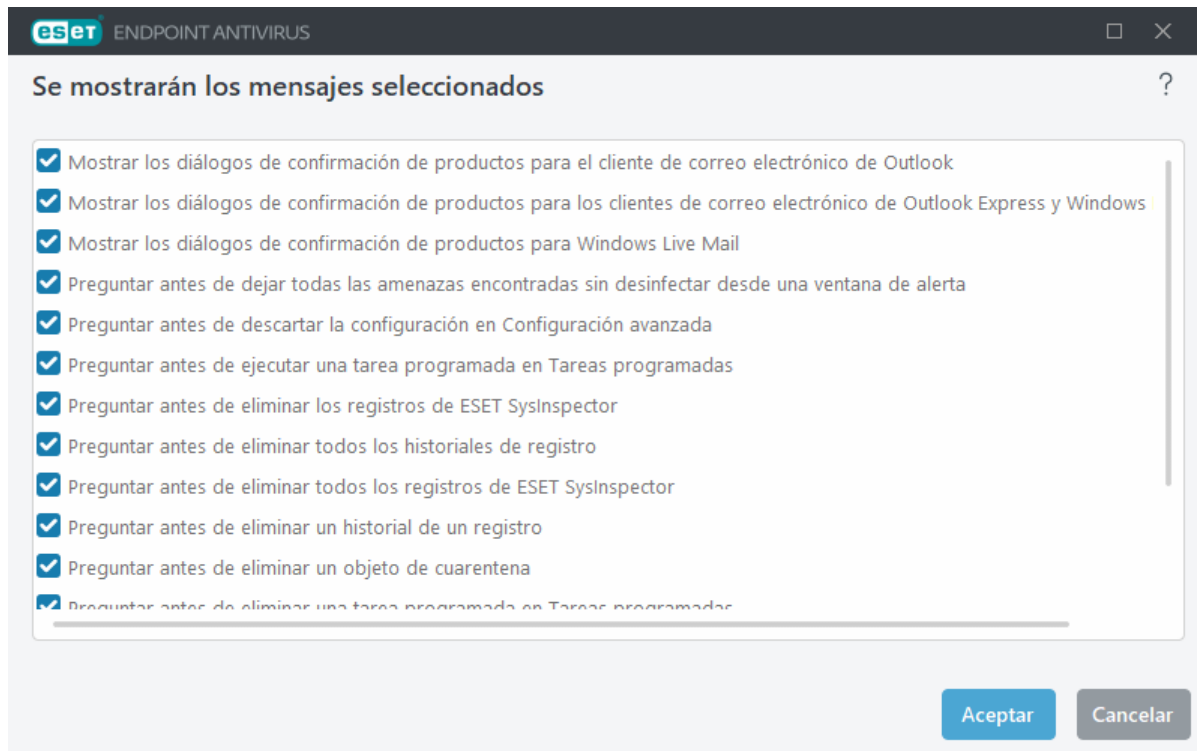
- [Reiniciar equipo \(requerido\)](#)
- [Reiniciar equipo \(recomendado\)](#)



Las alertas interactivas no incluyen ventanas interactivas del motor de detección, HIPS o Firewall ya que su comportamiento puede configurarse de forma individual en la función específica.

# Mensajes de confirmación

Para ajustar los mensajes de confirmación, vaya a [Configuración avanzada](#) > **Notificaciones** > **Alertas interactivas** y haga clic en **Modificar** junto a **Mensajes de confirmación**.



Esta ventana de diálogo muestra mensajes de confirmación que ESET Endpoint 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](#)



# Error de conflicto de configuraciones avanzadas

Este error puede ocurrir si algún componente (por ejemplo, HIPS) y el usuario crean las reglas en modo interactivo o de aprendizaje al mismo tiempo.



Recomendamos cambiar el modo de filtrado por el **Modo automático** predeterminado si desea crear sus propias reglas. Obtenga más información sobre [HIPS y los modos de filtrado de HIPS](#).

## Se requiere el reinicio

Se requiere un reinicio de equipo después de actualizar ESET Endpoint Antivirus a una nueva versión o aplicar parches a las aplicaciones a través de la [Administración de parches y vulnerabilidades](#). Las versiones nuevas de ESET Endpoint Antivirus se emiten para implementar mejoras o corregir problemas que las actualizaciones automáticas de los módulos del programa no pueden resolver.

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 **Estado de protección** de la ventana principal del programa.

Para deshabilitar la alerta “Se requiere el reinicio” o “Se recomienda el reinicio”, siga los pasos a continuación:

1. Abra **Configuración avanzada** (F5) > **Notificaciones** > **Alertas interactivas**.
2. Haga clic en **Editar** junto a **Alertas interactivas**. En la sección **Equipo**, anule la selección de las casillas de verificación junto a **Reiniciar equipo (requerido)** y **Reiniciar equipo (recomendado)**.
3. Haga clic en **Aceptar** para guardar los cambios en las dos ventanas abiertas.
4. Las alertas ya no se visualizarán en la máquina de punto de conexión.
5. (opcional) Para deshabilitar el estado de la aplicación en la ventana principal del programa ESET Endpoint Antivirus, en la [Ventana de estados de aplicación](#) anule la selección de las casillas de verificación para **Se requiere el reinicio del equipo** y **Se recomienda el reinicio del equipo**.

## Se recomienda el reinicio

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

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 **Estado de protección** de la ventana principal del programa.

Para deshabilitar la alerta “Se requiere el reinicio” o “Se recomienda el reinicio”, siga los pasos a continuación:

1. Abra **Configuración avanzada** (F5) > **Notificaciones** > **Alertas interactivas**.
2. Haga clic en **Editar** junto a **Alertas interactivas**. En la sección **Equipo**, anule la selección de las casillas de verificación junto a **Reiniciar equipo (requerido)** y **Reiniciar equipo (recomendado)**.
3. Haga clic en **Aceptar** para guardar los cambios en las dos ventanas abiertas.
4. Las alertas ya no se visualizarán en la máquina de punto de conexión.
5. (opcional) Para deshabilitar el estado de la aplicación en la ventana principal del programa ESET Endpoint

Antivirus, en la [Ventana de estados de aplicación](#) anule la selección de las casillas de verificación para **Se requiere el reinicio del equipo** y **Se recomienda el reinicio del equipo**.

## Reenvío

ESET Endpoint Antivirus puede enviar correos electrónicos de forma automática si se produce un suceso con el nivel de detalle seleccionado. En la sección [Configuración avanzada](#) > **Notificaciones** > **Reenvío** > **Reenviar al correo electrónico**, habilite la opción **Reenviar notificaciones al correo electrónico** para activar las notificaciones por correo electrónico.

**Notificaciones reenviadas:** seleccione las notificaciones de escritorio que se reenvían al 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

**Servidor SMTP** – el servidor SMTP utilizado para enviar notificaciones (por ej. *smtp.provider.com:587*, el puerto predeterminado es 25).

 Los servidores SMTP con cifrado TLS son admitidos por ESET Endpoint 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.

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

**Direcciones del destinatario** – este campo especifica la dirección del destinatario que se mostrará en el encabezado de los correos electrónicos de notificación. Use punto y coma “;” para separar varias direcciones de correo electrónico.

**Habilitar TLS** – habilita el envío de mensajes de alerta y notificación admitidos por el cifrado TLS.

## 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. No es recomendable modificar dicho formato. 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).

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

- **%TimeStamp%:** fecha y la hora del suceso
- **%Scanner%:** módulo pertinente
- **%ComputerName%:** nombre del equipo en el que se produjo la alerta
- **%ProgramName%:** programa que generó la alerta
- **%InfectedObject%:** nombre del archivo, mensaje, etc., infectado
- **%VirusName%:** identificación de la infección
- **%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.

## Restauración de todas las configuraciones a las predeterminadas

En **Configuración avanzada**, 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](#).

## 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](#).

## 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 Endpoint 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"> <li>• <b>none</b> (predeterminado): no se realizará desinfección automática alguna.</li> <li>• <b>standard</b>: ecls.exe intentará desinfectar o eliminar en forma automática los archivos infectados.</li> <li>• <b>estricta</b>: 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).</li> <li>• <b>rigurosa</b>: ecls.exe eliminará los archivos sin intentar desinfectarlos, independientemente de archivo sea.</li> <li>• <b>eliminar</b>: ecls.exe eliminará los archivos sin intentar desinfectarlos, pero se abstendrá de eliminar los archivos importantes, como los archivos del sistema de Windows.</li> </ul>
/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

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

## Preguntas habituales

Este capítulo abarca las preguntas más frecuentes y los problemas que se pueden encontrar. Haga clic en el título de un tema para obtener información sobre cómo solucionar el problema:

- [Cómo actualizar ESET Endpoint Antivirus](#)
- [Cómo activar ESET Endpoint Antivirus](#)
- [ESET Endpoint Antivirus ha detectado una amenaza](#)
- [Cómo quitar un virus del equipo](#)
- [Cómo crear una nueva tarea en Tareas programadas](#)
- [Cómo programar una exploración semanal del equipo](#)
- [Cómo administrar notificaciones y alertas interactivas](#)
- [Cómo conectar mi producto a ESET PROTECT](#)

- [Cómo utilizar el modo anulación](#)
- [Procedimiento para aplicar una política recomendada para ESET Endpoint Antivirus](#)
- [Cómo configurar un servidor reflejado](#)
- [Cómo actualizar a Windows 10 con ESET Endpoint Antivirus](#)
- [Cómo activar el monitoreo y la administración remotos](#)
- [Cómo bloquear la descarga de tipos específicos de archivos desde Internet](#)
- [Cómo minimizar la interfaz del usuario de ESET Endpoint Antivirus](#)

Si el problema no está contemplado en la lista de páginas de ayuda precedente, intente buscarlo en las Páginas de ayuda de ESET Endpoint Antivirus por palabra clave o mediante una frase que describa el problema.

Si no puede encontrar la solución a su problema o pregunta en las Páginas de ayuda, visite la [Base de conocimiento de ESET](#) donde se encuentran disponibles las respuestas a preguntas y problemas habituales.

- [Cómo instalar ESET Endpoint Antivirus](#)
- [Mejores prácticas para protegerse contra malware tipo Filecoder \(ransomware\)](#)
- [Preguntas frecuentes sobre ESET Endpoint Security y ESET Endpoint Antivirus](#)
- [¿Qué direcciones y puertos en mi firewall de terceros debería abrir para permitir la funcionalidad plena de mi producto de ESET?](#)

En caso de ser necesario, también puede ponerse en contacto con nuestro centro de soporte técnico en línea para consultar sus preguntas o problemas. El vínculo a nuestro formulario de contacto en línea se puede encontrar en el panel **Ayuda y soporte** de la ventana principal del programa.

## Preguntas frecuentes sobre actualizaciones automáticas



Para obtener más información sobre actualizaciones del producto en ESET Endpoint Antivirus, lea el siguiente artículo de la base de conocimiento de ESET:

- [¿Cuáles son los diferentes tipos de versiones y actualizaciones de productos ESET?](#)

### ¿Se actualizarán los equipos automáticamente? ¿Se descarga la actualización antes o después del reinicio?

La descarga tiene lugar antes del reinicio y, en esta etapa, también se prepararán los archivos actualizados. Tras el reinicio, los archivos actualizados solo están preparados para su uso y la versión instalada actualmente ofrece una protección sin interrupciones. Los cambios se aplican tras el siguiente inicio del producto ESET Endpoint Antivirus.

### Tengo, aproximadamente, 3000 equipos. ¿Todos los equipos descargarán las actualizaciones al mismo tiempo? ¿Puedo usar el proxy para las actualizaciones automáticas en tantos equipos?

ESET ofrece la herramienta de replicación y soluciones proxy para redes de gran tamaño, de modo que las actualizaciones se descargan solo una vez de Internet y, posteriormente, se distribuyen localmente. Las actualizaciones son más pequeñas, suelen tener entre 5 y 10 MB, y ESET limitará las actualizaciones durante las primeras semanas de disponibilidad. Por lo tanto, no todos los clientes iniciarán la descarga simultáneamente cuando se conecten directamente a los servidores de ESET.



**¿Puedo decidir cuántos equipos o cuáles se actualizarán automáticamente? No quiero descargar más de diez equipos por hora, o solo quiero actualizar diez equipos por ahora y otro equipo después de un par de días.**

Los entornos administrados tienen una política de actualización automática en la que puede especificar la versión más alta deseada. También se admiten comodines (por ejemplo, 9.0.2032.\*). Para obtener más información, consulte el capítulo Actualizaciones automáticas de la ayuda en línea de [ESET PROTECT](#) o [ESET PROTECT Cloud](#). Lamentablemente, en este momento no hay otras opciones disponibles para limitar las actualizaciones automáticas. Puede asignar varias políticas para varios grupos.

**¿Las actualizaciones automáticas solo se configuran a través de la política? ¿Puedo desactivar la política si no quiero actualizar un producto de ESET?**

Si existe una revisión de seguridad y estabilidad para el producto ESET Endpoint, el producto se actualizará incluso cuando las actualizaciones automáticas estén desactivadas, de acuerdo con los términos establecidos en el Acuerdo de licencia de usuario final aplicable. ESET usa [revisiones de seguridad y estabilidad](#) para resolver problemas críticos y garantizar la máxima seguridad y estabilidad para su producto de ESET.

Puede asignar una política de actualización automática a cualquier grupo de puntos de acceso, sea cual sea su configuración de actualización automática actual. En entornos no administrados, el usuario puede configurar las actualizaciones automáticas de forma local en la pantalla Configuración avanzada de un producto ESET Endpoint.

**¿Qué sucede si configuro una política para usar la versión más antigua disponible? Incluso entonces, ¿ESET actualizará mis productos?**

Las revisiones y revisiones críticas (actualizaciones de seguridad y estabilidad) son categorías de actualizaciones ligeramente distintas. Cuando se aceptan ajustes de usuario, se asignan correcciones periódicas a actualizaciones automáticas con una prioridad estándar. Las correcciones críticas se aplican con prioridad máxima, independientemente de la configuración del usuario.

**¿Cómo funcionan las actualizaciones en situaciones sin conexión?  
¿Cuándo usan los usuarios el repositorio sin conexión?**

El repositorio sin conexión también contiene archivos .dup y .fup. La sección del repositorio debe descargarse con la herramienta de replicación, no con la actualización del módulo. Para obtener más información, consulte el tema [Repositorio sin conexión](#) en la ayuda en línea para ESET PROTECT.

**¿Cómo saben los productos de ESET que es necesaria la actualización?  
¿Desde el repositorio? ¿Se envían datos a los servidores? Si ESET tiene previsto realizar una actualización un mes después del lanzamiento de**

## una versión, ¿los servidores de ESET estarán preparados para un lanzamiento mundial?

Los productos de ESET descargan actualizaciones automáticas del repositorio. Los servidores están preparados para eso, ya que las actualizaciones fundamentales son de solo unos kilobytes de tamaño. ESET no limitará las actualizaciones fundamentales en los servidores del repositorio. No obstante, existe la opción de limitar las actualizaciones del servidor si las actualizaciones automáticas son más grandes. En la siguiente tabla puede ver ejemplos de tamaños de revisiones en caso de una actualización automática diferencial:

Versión anterior	Nueva versión	Tamaño
9.0.2032.2	9.0.2032.6	420 KB
8.1.2037.2	9.0.2032.2	6.5 MB
8.0.2028.0	9.0.2032.2	11.5 MB

Si una actualización automática diferencial falla, existe la posibilidad de que su producto de ESET inicie una actualización completa. Sigue siendo una actualización automática con una garantía de funcionalidad, pero en lugar de un archivo .dup se descargará un .fup, que es un archivo de mayor tamaño. Para la versión 9.0.2032.2, es de 27 MB. No obstante, este caso es poco común.

## ¿Se activará la actualización de ESET Endpoint Antivirus con limitaciones? ¿Durante cuánto tiempo se limita la actualización tras su lanzamiento?

ESET limita las actualizaciones durante las primeras semanas tras el lanzamiento de una nueva versión con el fin de reducir la carga en nuestros servidores y distribuir la nueva versión de forma uniforme.

## Las actualizaciones automáticas se convertirán en uno de los métodos principales de actualización ¿Cómo funciona exactamente?

ESET apunta a tener tantos clientes actualizados a través de actualizaciones automáticas como sea posible. Es difícil brindar apoyo a tantas versiones anteriores. La característica de actualizaciones automáticas opera de forma sencilla. Hay archivos .dup que se descargan durante la primera comprobación de la actualización del módulo. Durante el procedimiento de actualización, el producto es totalmente funcional y protege el equipo. La nueva versión se activa tras el reinicio. En ESET PROTECT (lado del servidor), puede usar una política para especificar la versión más reciente a la que desea actualizar. Para obtener más información, consulte el capítulo Actualizaciones automáticas de la ayuda en línea de [ESET PROTECT](#) o [ESET PROTECT Cloud](#).

## ¿Es correcto que las actualizaciones automáticas funcionen en 1/10? Al usar ESET Endpoint Security 8.0.2028.1. Si se ejecutan las actualizaciones automáticas, ¿a qué versión se actualizará?

La actualización de los productos con actualizaciones automáticas puede retrasarse debido a los límites de los servidores de repositorio. Si se libera una actualización del producto con límites, es posible que las comprobaciones de actualización automáticas no la reciban inmediatamente. Si se considera que la actualización es segura y estable, la limitación posteriormente puede reducirse o quitarse por completo para que todos los clientes restantes reciban la actualización.

El procedimiento de limitación podría tardar un tiempo diferente en cada actualización. Varía en función de la

cantidad de clientes que soliciten la actualización, del tráfico de nuestros servidores y otros factores. Este procedimiento siempre evoluciona y los cambios se suceden en todo momento.

## Si inicio un equipo a las 8:45 a. m. y lo apago a las 5:00 p. m., ¿cuándo comenzarán las actualizaciones automáticas?

Las actualizaciones automáticas comenzarán con la siguiente actualización del módulo programada correctamente, como máximo una vez cada 24 horas.

## Si el equipo se apaga mientras se ejecutan las actualizaciones automáticas, ¿cuándo se ejecutará la siguiente actualización?

La actualización se ejecutará en la siguiente ventana de actualización programada. Hay un mecanismo a prueba de fallos sólido para el procedimiento de actualización automática (anteriormente uPCU). Tras descargar la actualización y reiniciar el equipo, los archivos actualizados siguen estando solo preparados para su uso, y la versión instalada actualmente ofrece protección sin interrupciones. Los cambios se aplican tras el siguiente inicio del producto ESET Endpoint.

## ¿Cómo puedo ejecutar las actualizaciones automáticas inmediatamente sin esperar una conexión regular cada 24 horas? ¿Existe alguna otra forma de hacer clic en Buscar actualizaciones?

Solo puede iniciar el procedimiento de actualización automática de forma manual al abrir la ventana principal del programa y hacer clic en **Actualizar > Buscar actualizaciones**. El resto de las maneras de iniciar las actualizaciones del módulo refleja la política de Tareas programadas de actualización automática durante 24 horas. En este momento, no es posible iniciar de forma remota una descarga de actualización automática. Agregaremos esta característica en el futuro.

## Cómo actualizar ESET Endpoint Antivirus

La actualización de ESET Endpoint 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. Para cambiar el 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 **Exploración inteligente** para comenzar a explorar el sistema.
3. Una vez finalizada la exploración, consulte el registro con la cantidad de archivos explorados, infectados y desinfectados.

4. Si solo desea explorar una parte determinada 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 tarea** 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**)

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](#) > **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 tarea** en la pantalla principal de Tareas programadas.
2. Seleccione **Exploración del equipo a pedido** en el menú desplegable.
3. Ingrese un nombre para la tarea y seleccione **Semanalmente para establecer su 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 conectar ESET Endpoint Antivirus al ESET PROTECT

Cuando haya instalado ESET Endpoint Antivirus en su equipo y desee conectarse a través de ESET PROTECT, asegúrese de haber instalado también el agente ESET Management en su estación de trabajo de cliente. Es una parte esencial de todas las soluciones de cliente que se comunica con el servidor ESET PROTECT.

- [Instalar o implementar el agente ESET Management en las estaciones de trabajo de cliente](#)

Vea también:

- [Documentación para puntos de conexión administrados de forma remota](#)
- [Cómo utilizar el modo anulación](#)
- [Procedimiento para aplicar una política recomendada para ESET Endpoint Antivirus](#)

## Cómo utilizar el modo anulación


Los usuarios con los productos ESET para Endpoint (versión 6.5 y superior) para Windows instalado en sus equipos pueden utilizar la característica de anulación. El modo anulación le permite a los usuarios en el nivel cliente-computadora cambiar la configuración en el producto ESET instalado, incluso si hubiera una política aplicada sobre esta configuración. El modo anulación puede habilitarse para ciertos usuarios AD, o puede estar protegida por contraseña. La función no puede habilitarse por más de cuatro horas de una sola vez.

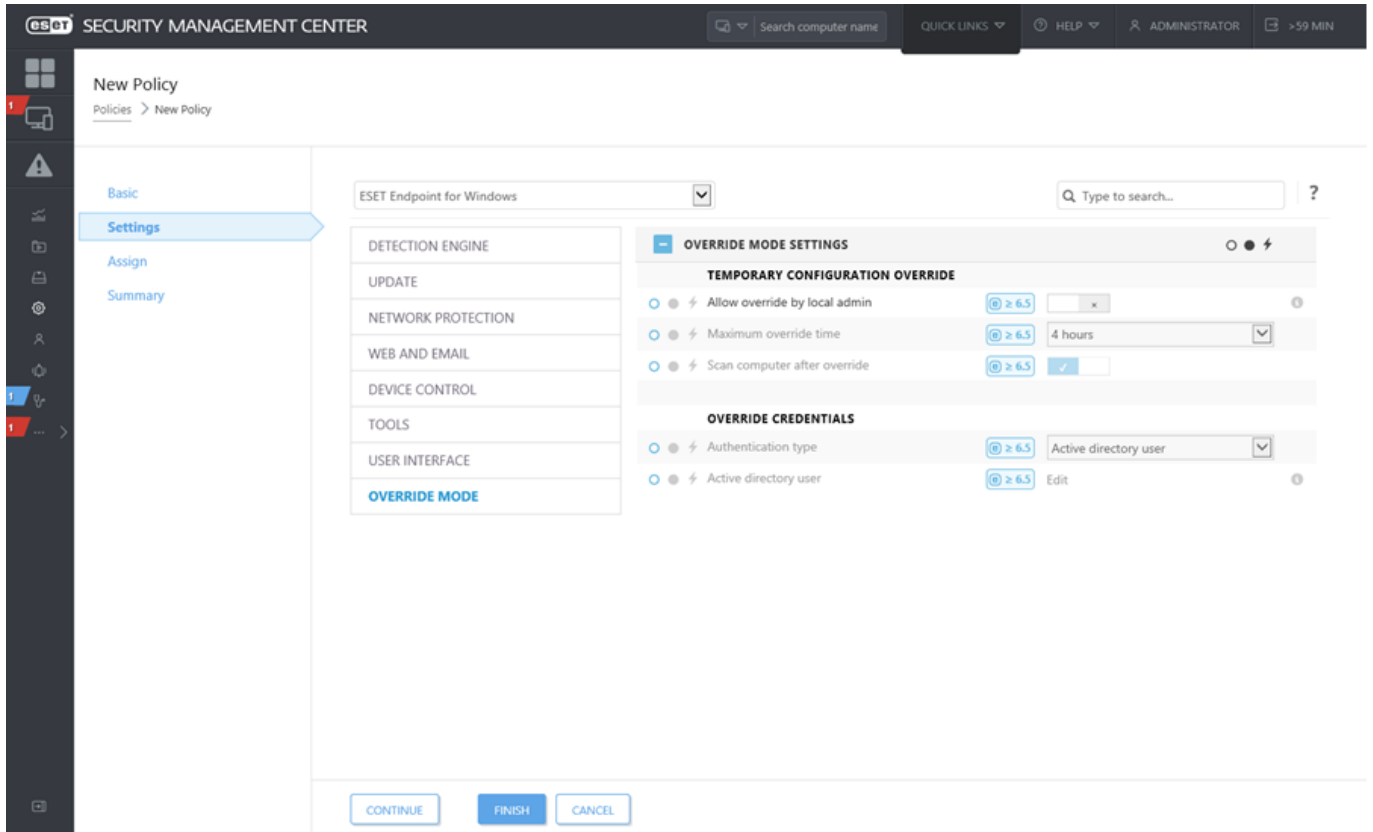


No puede detener el modo de anulación desde la consola web de ESET PROTECT una vez que se habilitó. El modo de anulación se deshabilitará automáticamente cuando venza el período de anulación. También puede desactivarse en el equipo de cliente.

El usuario que usa el modo de anulación también debe tener derechos de administrador de Windows. De lo contrario, el usuario no puede guardar los cambios en los ajustes de ESET Endpoint Antivirus. Se admite la autenticación de grupo de Active Directory.

Para establecer el **modo anulación**:

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



ESet SECURITY MANAGEMENT CENTER

Search computer name QUICK LINKS HELP ADMINISTRATOR >59 MIN

### New Policy

Policies > New Policy

Basic Settings Assign Summary

ESET Endpoint for Windows

Q Type to search...

DETECTION ENGINE

UPDATE

NETWORK PROTECTION

WEB AND EMAIL

DEVICE CONTROL

TOOLS

USER INTERFACE

**OVERRIDE MODE**

**OVERRIDE MODE SETTINGS**

**TEMPORARY CONFIGURATION OVERRIDE**

- Allow override by local admin
- Maximum override time
- Scan computer after override

**OVERRIDE CREDENTIALS**

- Authentication type
- Active directory user

CONTINUE FINISH CANCEL

Si *John* tiene un problema con la configuración de su endpoint porque bloquea alguna funcionalidad importante o el acceso a la web en su máquina, el Administrador puede permitir que *John* anule la política existente de su endpoint y que corrija los ajustes manualmente en su máquina. Luego, es posible que ESET PROTECT solicite estos ajustes para que el Administrador pueda crear una nueva política de ellos.

Para hacerlo, siga los siguientes pasos:

1. Vaya a **Políticas > Nueva política**.
2. Complete los campos **Nombre** y **Descripción**. En la sección **Configuración**, seleccione **ESET Endpoint para Windows**.
3. Haga clic en **Modo anulación**, habilite el modo anulación durante una hora y seleccione *John* como usuario AD.
4. Asigne la política a la *computadora de John* y haga clic en **Finalizar** para guardar la política.
5. *John* tiene que habilitar el **Modo anulación** en este endpoint de ESET y cambie los ajustes manualmente en su máquina.
6. En la consola web de ESET PROTECT, navegue a **Computadoras**, seleccione la *computadora de John* y haga clic en **Mostrar detalles**.
7. En la sección **Configuración**, haga clic en **Solicitar configuración** para programar una tarea de cliente para obtener la configuración de cliente ASAP.
8. Tras un corto período, aparecerá la nueva configuración. Haga clic en el producto de los ajustes que desea guardar y luego haga clic en **Abrir configuración**.
9. Puede repasar los ajustes y luego hacer clic en **Convertir a política**.
10. Complete los campos **Nombre** y **Descripción**.
11. En la sección **Configuración**, usted puede modificar los ajustes, de ser necesario.
12. En la sección **Asignar**, usted puede asignar esta política para la *computadora de John* (u otras).
13. Haga clic en **Finalizar** para guardar los ajustes.
14. No olvide quitar la política de anulación una vez que ya no la necesite.

## Procedimiento para aplicar una política recomendada para ESET Endpoint Antivirus

La práctica recomendada después de conectar ESET Endpoint Antivirus con ESET PROTECT es aplicar una [política recomendada](#) o una personalizada.


Hay varias políticas incorporadas para ESET Endpoint Antivirus:

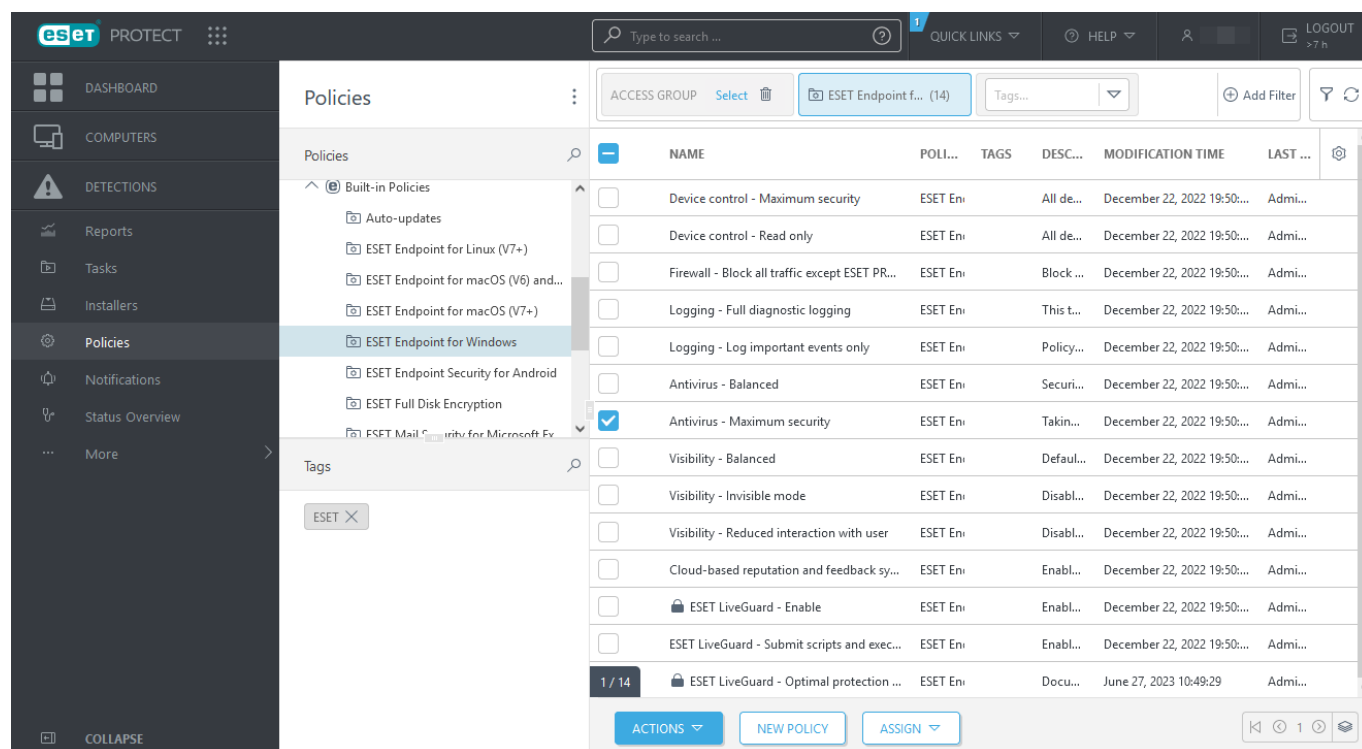
Política	Descripción
Antivirus - Balanceado	Configuración de seguridad recomendada para la mayoría de las configuraciones.
Antivirus: seguridad máxima	Sacando provecho del aprendizaje automático, de la inspección profunda del comportamiento y del filtrado de la SSL. La detección de aplicaciones potencialmente peligrosas, no deseadas y sospechosas no está afectada.
Sistema de comentarios y reputación basado en la nube	Habilita el sistema de comentarios y reputación basado en la nube <a href="#">ESET LiveGrid®</a> para mejorar la detección de las amenazas más recientes y ayudar a compartir posibles amenazas maliciosas o desconocidas para análisis futuros.
Control del dispositivo - seguridad máxima	Todos los dispositivos están bloqueados. Cuando cualquier dispositivo trate de conectarse, necesita ser permitido por un administrador.
Control del dispositivo: solo lectura	Todos los dispositivos son de solo lectura. No se permite la escritura.
Firewall: bloquear todo el tráfico, excepto ESET PROTECT y la conexión a ESET Inspect	Bloquear todo el tráfico, excepto la conexión con ESET PROTECT y <a href="#">el servidor de ESET Inspect</a> (ESET Endpoint Security únicamente).

Política	Descripción
Registros - Diagnóstico completo de registros	Esta plantilla garantizará que el administrador tenga todos los registros disponibles, cuando sea necesario. Se registrará todo con el detalle mínimo incluyendo los parámetros del HIPS y de <a href="#">ThreatSense</a> y el Firewall. Los registros se eliminan automáticamente luego de 90 días.
Registros - Registrar solo los eventos importantes	La política asegura que se registren las advertencias, los errores y los eventos críticos. Los registros se eliminan automáticamente luego de 90 días.
Visibilidad - Balanceada	Configuración predeterminada para visibilidad. Los estados y las notificaciones están habilitadas.
Visibilidad - Modo invisible	Las notificaciones, las alertas, la <a href="#">interfaz gráfica de usuario</a> y la integración con el menú contextual están deshabilitadas. No se ejecutará egui.exe. Adecuado únicamente para la administración desde el <a href="#">ESET PROTECT Cloud</a> .
Visibilidad - Interacción reducida con el usuario	Estatus deshabilitados, notificaciones deshabilitadas, interfaz gráfica de usuario presente.

Para establecer la política denominada **Antivirus - Seguridad máxima** que implementa más de 50 configuraciones recomendadas para ESET Endpoint Antivirus instalado en sus estaciones de trabajo, siga estos pasos:

**i** Los siguientes artículos de la base de conocimiento de ESET pueden estar disponibles solo en inglés:  
[Aplique una política recomendada o predefinida para ESET Endpoint Antivirus mediante ESET PROTECT](#)

1. Abra ESET PROTECT Web Console.
2. Vaya a  **Políticas** y expanda **Políticas incorporadas > ESET Endpoint para Windows**.
3. Haga clic en **Antivirus - Seguridad máxima - recomendado**.
4. En la ficha **Asignado a**, haga clic en **Asignar cliente(s)** o **Asignar grupo(s)** y seleccione los equipos correspondientes para los que desea aplicar esta política.

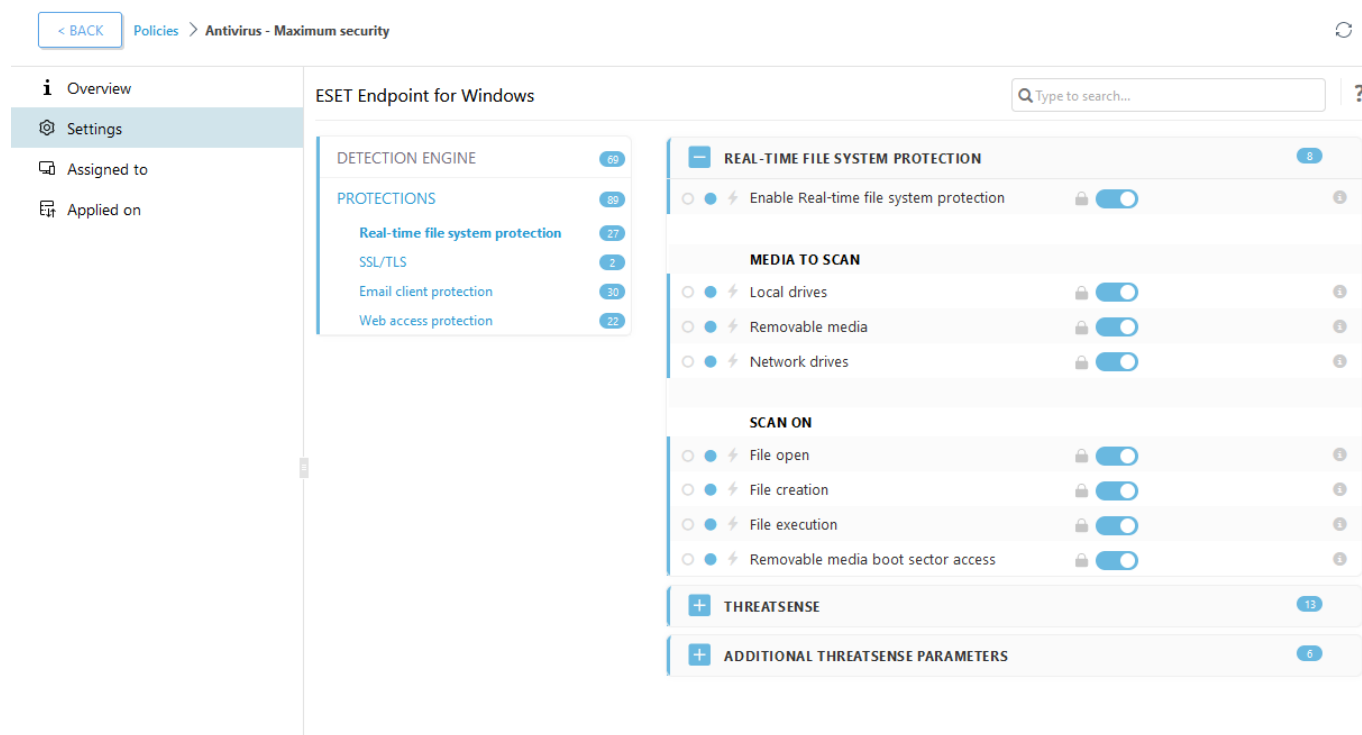


The screenshot displays the ESET PROTECT Web Console interface. On the left, a sidebar contains navigation options: DASHBOARD, COMPUTERS, DETECTIONS, Reports, Tasks, Installers, Policies (selected), Notifications, Status Overview, and More. The main content area is titled 'Policies' and shows a list of built-in policies. The 'Antivirus - Maximum security' policy is selected, indicated by a blue highlight and a checkmark in the selection column. The table lists various policies including Device control, Firewall, Logging, Antivirus, and Visibility. At the bottom, there are buttons for 'ACTIONS', 'NEW POLICY', and 'ASSIGN', along with a pagination indicator '1 / 14'.




Para ver la configuración que se aplica a esta política, haga clic en la ficha **Configuración** y expanda el árbol de Configuración avanzada.

- El punto azul representa una configuración modificada para esta política
- El número con el marco azul representa una cantidad de configuraciones modificadas por esta política
- [Obtener más información acerca de las políticas de ESET PROTECT](#)



## Cómo configurar un servidor reflejado

ESET Endpoint Antivirus se puede configurar para almacenar copias de los archivos de actualización del motor de detección y distribuir las actualizaciones a otras estaciones de trabajo que estén ejecutando ESET Endpoint Antivirus o ESET Endpoint Security.

 El mirror de actualización crea copias de los archivos de actualización que se pueden usar para actualizar estaciones de trabajo que ejecutan la misma generación de ESET Endpoint Antivirus para Windows. (Por ejemplo, ESET Endpoint Antivirus para Windows versión 10.x solo crea archivos de actualización para la versión 10.x de ESET Endpoint Antivirus para Windows y ESET Endpoint Security para Windows)

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

1. Presione **F5** para acceder a la Configuración avanzada y expanda **Actualizar > Perfiles > Actualizar reflejo**.
2. Expanda **Actualizaciones** y asegúrese de que la opción **Elegir automáticamente** debajo de **Actualizaciones de módulo** esté habilitada.
3. Expanda **Actualizar reflejo** y habilite **Crear reflejo de actualización** y **Habilitar servidor HTTP**.



Para obtener más información, consulte:

- [Mirror de actualización](#)
- [Actualización desde el Mirror](#)

## Configuración de un servidor Mirror para proporcionar actualizaciones mediante una carpeta compartida de red

1. Cree una carpeta compartida en un dispositivo local o de red. Esta carpeta debe ser legible para todos los usuarios que ejecuten soluciones de seguridad de ESET y se debe poder escribir desde la cuenta de SISTEMA local.
2. Active **Crear servidor reflejado de actualización** en **Configuración avanzada > Actualizar > Perfiles > Actualizar reflejo**.
3. Elija una **Carpeta de almacenamiento** adecuada. Para ello, haga clic en **Borrar** y, luego, en **Editar**. Examine y seleccione la carpeta compartida creada.



Si no desea proporcionar actualizaciones del módulo a través del servidor HTTP interno, deshabilite **Habilitar servidor HTTP**.

## Cómo actualizo a Windows 10 con ESET Endpoint Antivirus



Recomendamos que actualice a la última versión de su producto ESET, luego, descargue las últimas actualizaciones de los módulos, antes de actualizar a Windows 10. Esto le asegurará una máxima protección y preservará la configuración de su programa y la información de licencia durante la actualización a Windows 10.

### Versiones en otros idiomas:

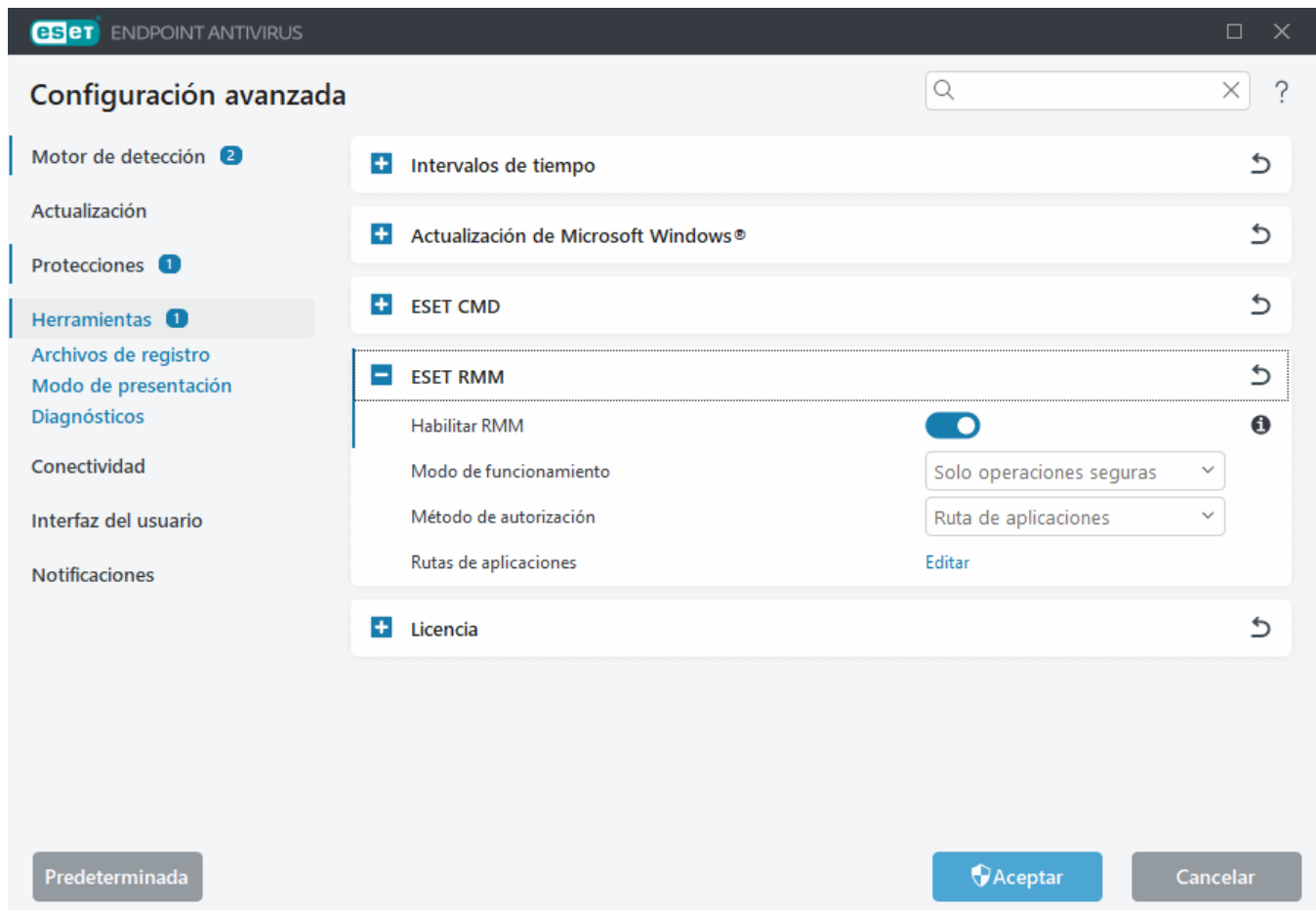
Si busca versiones en otros idiomas para su ESET endpoint product, visite nuestro [sitio de descarga](#).



[Más información acerca de la compatibilidad de los productos comerciales ESET con Windows 10.](#)

## Cómo activar el monitoreo y la administración remotos

Monitoreo y Administración Remotos (RMM) es el proceso de supervisión y control de sistemas de software (como aquellos presentes en equipos de escritorio, servidores y dispositivos móviles) mediante el uso de un agente instalado localmente al que se puede acceder a través de un proveedor de servicios de administración. ESET Endpoint Antivirus puede estar bajo la administración de RMM de la versión 6.6.2028.0.



De forma predeterminada, ESET RMM está deshabilitado. Para habilitar ESET RMM, abra [Configuración avanzada](#) > **Herramientas** > **ESET RMM** y habilite el interruptor junto a **Habilitar RMM**.

**Modo de trabajo:** seleccione **Solo operaciones seguras** si quiere habilitar la interfaz de RMM para operaciones seguras de solo lectura. Seleccione **Todas las operaciones** si quiere habilitar la interfaz de RMM para todas las operaciones.

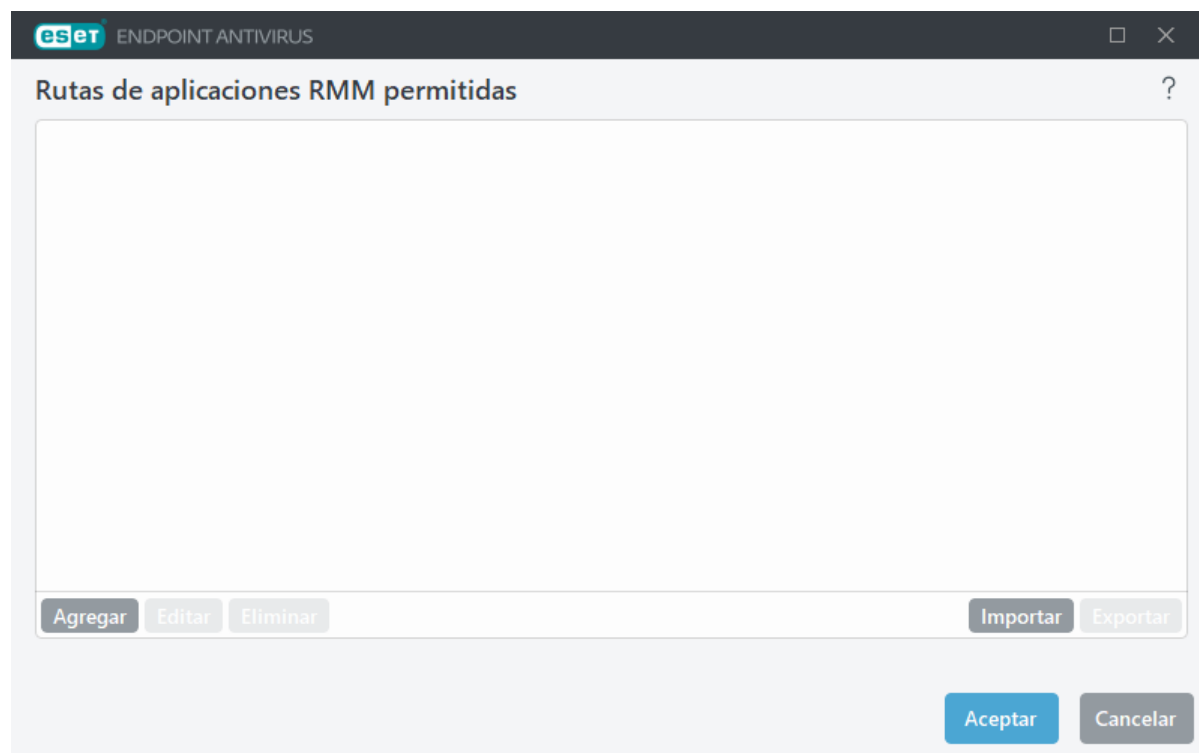
Operación	Modo Operaciones seguras únicamente	Modo Todas las operaciones
Obtener información de la aplicación	✓	✓
Obtener configuración	✓	✓
Obtener información de la licencia	✓	✓
Obtener registros	✓	✓
Obtener estado de protección	✓	✓
Obtener estado de actualización	✓	✓
Establecer configuración		✓
Comenzar activación		✓
Comenzar exploración	✓	✓
Comenzar actualización	✓	✓

**Método de autorización** – Configure el método de autorización de RMM. Para usar la autorización, seleccione **Ruta de aplicación** del menú desplegable; de lo contrario, seleccione **Ninguno**.



RMM siempre debe utilizar autorización para evitar que el software malicioso deshabilite o evada la protección de ESET Endpoint.

**Rutas de aplicaciones:** aplicación específica autorizada a ejecutar RMM. Si ha seleccionado **Ruta de aplicación** como método de autorización, haga clic en **Editar** para abrir la ventana de configuración **Rutas de aplicaciones de RMM habilitadas**.



**Agregar** – Cree una nueva ruta de aplicación de RMM habilitada. Ingrese la ruta o haga clic en el botón ... para seleccionar un ejecutable.

**Editar** – Modifica una ruta habilitada existente. Use **Editar** si la ubicación del ejecutable ha cambiado a otra carpeta.

**Eliminar** – Elimina una ruta habilitada existente.

En la instalación predeterminada de ESET Endpoint Antivirus, el archivo ermm.exe se encuentra en el directorio de la aplicación Endpoint (ruta predeterminada: *C:\Program Files\ESET\ESET Security*). Archivo ermm.exe intercambia información con el complemento RMM, que se comunica con el agente RMM, conectado a un servidor RMM.

- ermm.exe – utilidad de la línea de comandos desarrollada por ESET que permite la administración de los productos de Endpoint y la comunicación con cualquier complemento RMM.
- El complemento RMM es una aplicación de terceros que se ejecuta localmente en un sistema Endpoint para Windows. El complemento se diseñó para comunicarse con agentes RMM específicos (por ejemplo, exclusivamente con Kaseya) y con ermm.exe.
- El agente RMM es una aplicación de terceros (por ejemplo, de Kaseya) que se ejecuta localmente en un sistema Endpoint para Windows. El agente se comunica con el complemento RMM y con el servidor RMM.

# Cómo bloquear la descarga de tipos específicos de archivos desde Internet

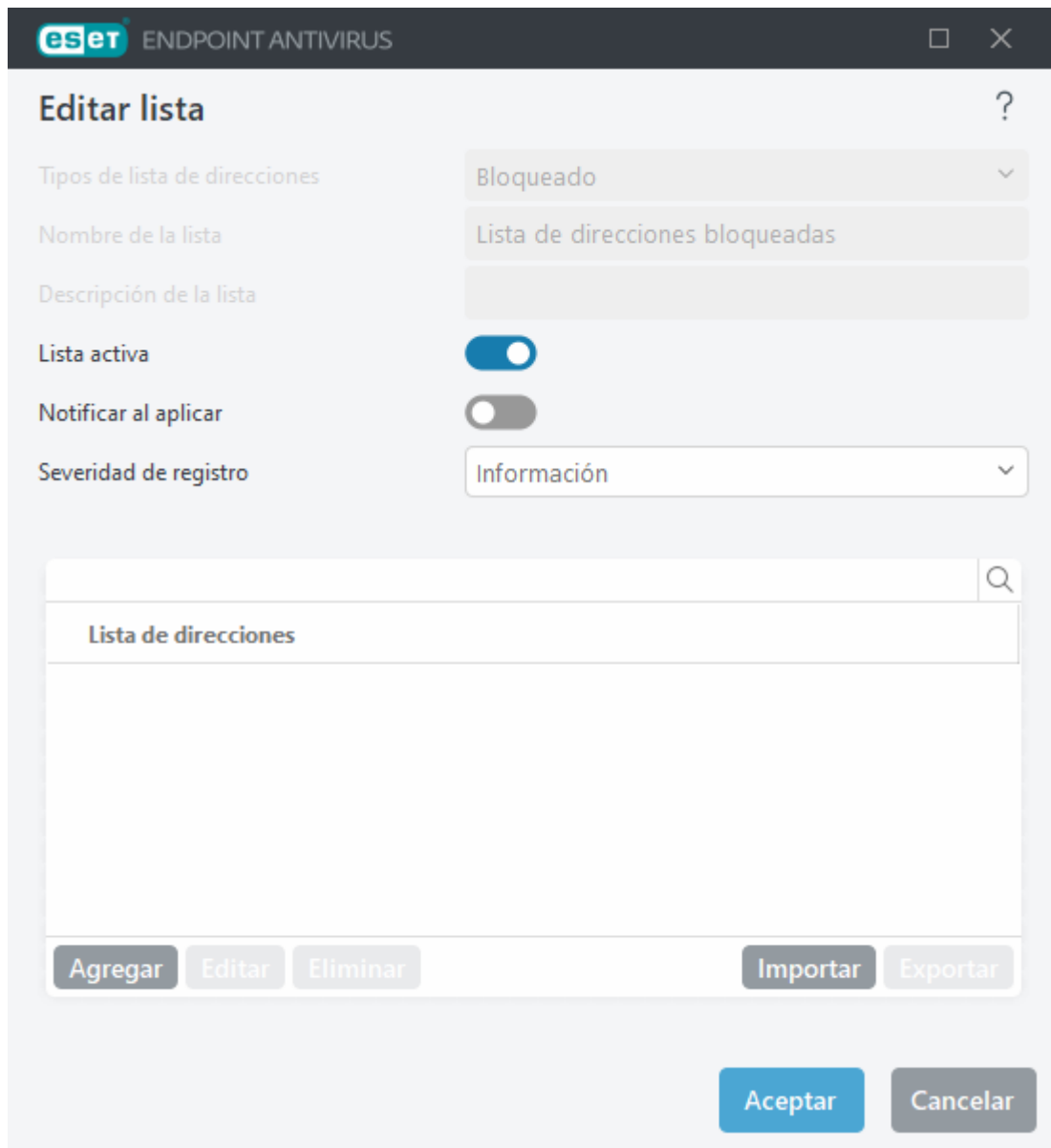
Si no desea permitir la descarga de tipos específicos de archivos (por ejemplo, exe, pdf o zip) desde Internet, utilice la [Administración de direcciones URL](#) con una combinación de comodines. Pulse la tecla F5 para acceder a **Configuración avanzada**. Haga clic en **Internet y Correo electrónico > Protección de acceso a la web** y expanda la **Administración de direcciones URL**. Haga clic en **Editar** junto a la **lista de direcciones**.

En la ventana **Lista de direcciones**, seleccione **Lista de direcciones bloqueadas** y haga clic en **Editar** o en **Agregar** para crear o editar una lista. Se abrirá una nueva ventana. Si está creando una nueva lista, seleccione **Bloqueado** en el menú desplegable de la lista del **tipo de direcciones** y asigne un nombre a la lista. Si desea que se le notifique cuando acceda a un tipo de archivo de la lista actual, active la opción **Notificar al activar** la barra deslizante. Seleccione la **severidad de registro** en el menú desplegable. ESET PROTECT puede recopilar registros con verbosidad **Advertencia**.



El nivel de detalle de registro de información y advertencia solo está disponible para las reglas que contienen al menos dos componentes sin comodines dentro del dominio. Por ejemplo:

- \*.domain.com/\*
- \*www.domain.com/\*



**eset** ENDPOINT ANTIVIRUS

## Editar lista

Tipos de lista de direcciones: Bloqueado

Nombre de la lista: Lista de direcciones bloqueadas

Descripción de la lista:

Lista activa: ☒

Notificar al aplicar: ☐

Severidad de registro: Información

Lista de direcciones

Agregar Editar Eliminar Importar Exportar

Aceptar Cancelar

Haga clic en **Agregar** para introducir una máscara que especifique los tipos de archivos que desea bloquear para que no se descarguen. Introduzca la URL completa si desea bloquear la descarga de un archivo específico desde un sitio web específico, por ejemplo, *http://example.com/file.exe*. Puede utilizar comodines para abarcar un grupo de archivos. Un signo de interrogación (?) representa un único carácter de variable mientras que un asterisco (\*) representa una cadena de variables de cero o más caracteres. Por ejemplo, la máscara *\*/\*.zip* bloquea la descarga de todos los archivos zip comprimidos.

Observe que solo puede bloquear la descarga de tipos de archivo específicos con este método cuando la extensión del archivo es parte de la URL del archivo. Si la página web usa URL de descarga de archivos, por ejemplo, *www.example.com/download.php?fileid=42*, se descargarán todos los archivos ubicados en este enlace aun si tienen una extensión que haya bloqueado.

## Cómo minimizar la interfaz del usuario de ESET Endpoint Antivirus

Cuando se administra de forma remota, puede aplicar una [política predefinida de "Visibilidad"](#).

De lo contrario, siga estos pasos manualmente:

1. Presione **F5** para acceder a Configuración avanzada y amplíe **Interfaz del usuario > Elementos de la interfaz del usuario**.
2. Defina **Modo de inicio** en el valor deseado. [Más información sobre los modos de inicio](#).
3. Deshabilite **Mostrar la pantalla de bienvenida al iniciar el programa** y **Usar señal sonora**.
4. Configure [Notificaciones](#).
5. Configure [Estados de la aplicación](#).
6. Configure [Mensajes de confirmación](#).
7. Configure [Alertas y cuadros de mensajes](#).

## 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\\_business](https://go.eset.com/eol_business). 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 LiveGrid 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 LICENCIARIOS, 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 LICENCIARIOS 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 JURISDICCIONES 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.

EULAID: EULA-PRODUCT-LG; 3537.0

## Política de privacidad

ESET, spol. s r. o., con domicilio social en Einsteinova 24, 851 01 Bratislava, República Eslovaca, inscrita en el Registro comercial del Tribunal de distrito de Bratislava I, Sección Sro, Registro No 3586/B, Número de registro de empresa: 31333532 como Controlador de datos (“ESET” o “Nosotros”) desea ser transparente con el procesamiento de datos personales y la privacidad de nuestros clientes. 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”) acerca de los siguientes temas:

- Procesamiento de datos personales,
- Confidencialidad de datos,
- Datos de la persona registrada.

## Procesamiento de datos personales

Los servicios prestados por ESET implementados en nuestro producto se prestan de acuerdo con los términos del Acuerdo de licencia de usuario final (“EULA”), pero algunos pueden requerir atención especial. Quisiéramos brindarle más detalles sobre la recolección de datos relacionada a la provisión de nuestros servicios. Prestamos distintos servicios descritos en el EULA y la documentación del producto, como el servicio de actualización, ESET LiveGrid®, la protección contra el mal uso de los datos, la asistencia, etc. Para hacer que todo funcione, necesitamos recolectar la siguiente información:

- Estadísticas sobre actualizaciones y de otro tipo con información relativa al proceso de instalación y a su ordenador, 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.
- Funciones hash unidireccionales relativas a infiltraciones como parte del sistema de reputación de ESET LiveGrid®, que mejora la eficiencia de nuestras soluciones de protección frente a programas malignos

comparando archivos analizados con una base de datos de elementos puestos en listas blancas y negras en la nube.

- 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 sobre dispositivos de la red local, como el tipo, el proveedor, el modelo o el nombre del dispositivo;

- 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.

- Para fines de facturación, verificación de autenticidad de la licencia y prestación de nuestros servicios, se requiere información de licencia como identificación de licencia y datos personales, como nombre, apellido, dirección y dirección de correo electrónico.
- Pueden ser necesarios datos de contacto y datos contenidos en sus solicitudes de soporte para el servicio técnico. 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 información adicional para facilitar la prestación del servicio de soporte.

## Confidencialidad de los datos

ESET es una compañía que opera globalmente a través de entidades o socios afiliados como parte de nuestra red de distribución, servicio y soporte. Los datos procesados por ESET pueden ser transferidos desde y hasta las entidades afiliadas o socios para ejecutar EULA, como por ejemplo la prestación de servicios o soporte o facturación. Según la ubicación y servicio que Usted decida utilizar, Nosotros podemos solicitarle que transfiera sus datos a un país sin una decisión adecuada de la Comisión Europea. Incluso en tal situación, cada transferencia de datos se encuentra sujeta a la regulación de la protección de datos y se realiza solo si es necesaria. Se deben establecer cláusulas contractuales estándar, normas corporativas vinculantes u otra forma de protección adecuada sin excepción.

Nosotros hacemos todo lo posible para evitar que los datos se almacenen más tiempo del necesario durante la prestación de servicios de acuerdo con el EULA. Nuestro período de retención puede ser mayor que la validez de su licencia para que tenga tiempo de renovarla de una forma sencilla y cómoda. Pueden continuar procesándose estadísticas y otros datos minimizados y seudonimizados de ESET LiveGrid® con fines estadísticos.

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 confiabilidad, integridad, disponibilidad y capacidad de recuperación de los sistemas operativos y servicios. Sin embargo, si ocurre una filtración de datos que resulta en un riesgo para sus derechos y libertades, Nosotros estamos preparados para notificar a la autoridad supervisora así como también a las personas registradas. Como persona registrada, Usted tiene el derecho de presentar una queja con una autoridad supervisora.

## Derechos de la persona registrada

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. De conformidad con las condiciones establecidas por las leyes aplicables de protección de los datos, usted tiene los siguientes derechos como sujeto de datos:

- derecho a que ESET le solicite acceso a sus datos personales,
- derecho a rectificación de datos personales de ser erróneos (Usted también tiene el derecho a completar los datos personales que estén incompletos),
- derecho a solicitar la eliminación de sus datos personales,
- derecho a solicitar una restricción al procesamiento de sus datos personales
- derecho a oponerse al procesamiento
- derecho a presentar un reclamo así como
- derecho a la portabilidad de datos.

Creemos que toda información procesada es valiosa y necesaria para nuestro fin legítimo, que es la provisión de productos y servicios a nuestros clientes.

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