

ESET Endpoint Security

Guía para el usuario

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



Copyright ©2023 de ESET, spol. s r.o.

ESET Endpoint Security 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. 19/03/2023

1 ESET Endpoint Security 8	1
1.1 Novedades de esta versión?	2
1.2 Requisitos del sistema	3
1.2 Idiomas compatibles	4
1.3 Prevención	5
1.4 Páginas de ayuda	6
2 Documentación para puntos de conexión administrados de forma remota	8
2.1 Introducción a ESET PROTECT	8
2.2 Introducción a ESET PROTECT Cloud	10
2.3 Configuración protegida por contraseña	10
2.4 ¿Qué son las políticas?	11
2.4 Combinar políticas	12
2.5 Cómo funcionan los indicadores	12
3 Uso de ESET Endpoint Security por sí solo	14
3.1 Método de instalación	14
3.1 Instalación con ESET AV Remover	14
3.1 ESET AV Remover	15
3.1 La desinstalación con ESET AV Remover finalizó con un error	17
3.1 Instalación (.exe)	18
3.1 Cambiar la carpeta de instalación (.exe)	20
3.1 Instalación (.msi)	21
3.1 Instalación avanzada (.msi)	23
3.1 Instalación de línea de comando	25
3.1 Implementación a través de GPO o SCCM	30
3.1 Reemplazo a una versión más reciente	30
3.1 Actualización automática del producto de legado	31
3.1 Actualizaciones de seguridad y estabilidad	32
3.1 Problemas comunes de instalación	32
3.1 Falló la activación	32
3.2 Activación del producto	33
3.3 Exploración del equipo	33
3.4 Guía para principiantes	33
3.4 La interfaz del usuario	33
3.4 Configuración de la actualización	37
3.4 Configuración de zonas	39
3.4 Herramientas de control Web	40
4 Trabajar con ESET Endpoint Security	40
4.1 Equipo	43
4.1 Motor de detección	44
4.1 Opciones avanzadas del motor de detección	50
4.1 Infiltración detectada	50
4.1 Caché local compartido	52
4.1 Protección del sistema de archivos en tiempo real	53
4.1 Verificación de la protección en tiempo real	54
4.1 Cuándo modificar la configuración de la protección en tiempo real	55
4.1 Qué hacer si la protección en tiempo real no funciona	55
4.1 Exploración del equipo	55
4.1 Iniciador de la exploración personalizada	58
4.1 Progreso de la exploración	59
4.1 Registro de exploración del equipo	61

4.1 Exploración de malware	61
4.1 Exploración en estado inactivo	62
4.1 Perfiles de exploración	62
4.1 Objetos para explorar	63
4.1 Opciones avanzadas de exploración	64
4.1 Control del dispositivo	64
4.1 Editor de reglas del control del dispositivo	65
4.1 Dispositivos detectados	66
4.1 Grupos de dispositivos	67
4.1 Agregado de reglas del control del dispositivo	68
4.1 Sistema de prevención de intrusiones basado en el host (HIPS)	70
4.1 Ventana interactiva de HIPS	73
4.1 Se detectó un comportamiento ransomware potencial	74
4.1 Administración de reglas del HIPS	74
4.1 Configuración de reglas HIPS	75
4.1 Configuración avanzada de HIPS	78
4.1 Controladores siempre permitidos para cargar	78
4.1 Modo de presentación	78
4.1 Exploración en el inicio	79
4.1 Verificación de archivos de inicio automático	79
4.1 Protección de documentos	80
4.1 Exclusiones	80
4.1 Exclusiones de rendimiento	81
4.1 Agregar o editar exclusión de rendimiento	82
4.1 Formato de las exclusiones de ruta	84
4.1 Exclusiones de la detección	85
4.1 Agregar o editar exclusiones de la detección	88
4.1 Asistente para crear exclusiones de la detección	89
4.1 Exclusiones (versión 7.1 y anteriores)	89
4.1 Exclusiones de procesos	90
4.1 Agregado o edición de exclusiones de procesos	91
4.1 Exclusiones de HIPS	91
4.1 ThreatSense parámetros	92
4.1 Niveles de desinfección	96
4.1 Extensiones de archivos que no se analizarán	97
4.1 Parámetros adicionales de ThreatSense	98
4.2 Red	98
4.2 Firewall	99
4.2 Modo de aprendizaje	101
4.2 Protección contra ataques de red	103
4.2 Opciones avanzadas de filtrado	103
4.2 Reglas IDS	106
4.2 Amenaza sospechosa bloqueada	107
4.2 Solución de problemas de firewall	107
4.2 Redes conectadas	108
4.2 Redes conocidas	109
4.2 Editor de redes conocidas	109
4.2 Autenticación de red: configuración del servidor	112
4.2 Perfiles de firewall	113
4.2 Perfiles asignados a los adaptadores de red	113
4.2 Detección de modificaciones de la aplicación	114

4.2 Aplicaciones excluidas de la detección de modificaciones	114
4.2 Configuración y uso de reglas	115
4.2 Lista de reglas del firewall	115
4.2 Agregar o editar reglas del firewall	116
4.2 Regla de firewall: local	118
4.2 Regla de firewall: remota	119
4.2 Lista negra temporal de direcciones IP	120
4.2 Zona de confianza	120
4.2 Configuración de zonas	121
4.2 Zonas de firewall	121
4.2 Registro del Firewall	122
4.2 Establecimiento de una conexión: detección	122
4.2 Resolución de problemas con el Firewall de ESET	123
4.2 Asistente para la resolución de problemas	124
4.2 Registro y creación de reglas o excepciones desde el registro	124
4.2 Crear regla a partir del registro	124
4.2 Crear excepciones desde las notificaciones del firewall	125
4.2 Registro avanzado de protección de red	125
4.2 Resolución de problemas con el filtrado de protocolos	125
4.3 Internet y correo electrónico	126
4.3 Filtrado de protocolos	128
4.3 Aplicaciones excluidas	128
4.3 Direcciones IP excluidas	129
4.3 SSL/TLS	130
4.3 Certificados	132
4.3 Tráfico de red cifrada	132
4.3 Lista de certificados conocidos	133
4.3 Lista de aplicaciones SSL/TLS filtradas	133
4.3 Protección del cliente de correo electrónico	134
4.3 Protocolos de correo electrónico	136
4.3 Alertas y notificaciones por correo electrónico	137
4.3 Integración con los clientes de correo electrónico	138
4.3 Barra de herramientas de Microsoft Outlook	138
4.3 Barra de herramientas de Outlook Express y Windows Mail	139
4.3 Cuadro de diálogo de confirmación	140
4.3 Volver a explorar los mensajes	140
4.3 Protección antispam	140
4.3 Libretas de direcciones antispam	142
4.3 Lista negra/Lista blanca/Lista de excepciones	143
4.3 Agregar/Editar lista negra/Lista blanca/Dirección de excepciones	144
4.3 Protección del acceso a la Web	144
4.3 Configuración avanzada de la protección de acceso a la web	147
4.3 Protocolos Web	147
4.3 Administración de direcciones URL	148
4.3 Lista de direcciones URL	149
4.3 Crear nueva lista de direcciones URL	150
4.3 Cómo agregar una máscara URL	151
4.3 Protección antiphishing	151
4.3 Configuración avanzada de navegador seguro	153
4.3 Sitios Web protegidos	153
4.4 Control Web	154

4.4 Reglas del control Web	155
4.4 Agregado de reglas de control Web	156
4.4 Grupos de categoría	158
4.4 Grupos de URL	159
4.4 Personalización de mensajes de la página web bloqueada	160
4.5 Actualización del programa	163
4.5 Configuración de la actualización	166
4.5 Actualizar reversión	169
4.5 Actualización de componentes del programa	171
4.5 Opciones de conexión	172
4.5 Mirror de actualización	173
4.5 Servidor HTTP y SSL para Mirror	175
4.5 Actualización desde el Mirror	175
4.5 Resolución de problemas de actualización desde el Mirror	177
4.5 Cómo crear tareas de actualización	178
4.6 Herramientas	178
4.6 Archivos de registro	179
4.6 Filtrado de registros	182
4.6 Configuración de registro	183
4.6 Registros de auditorías	184
4.6 Tareas programadas	186
4.6 Observar la actividad	188
4.6 ESET SysInspector	189
4.6 Protección basada en la nube	190
4.6 Filtro de exclusión para la protección basada en la nube	194
4.6 Procesos en ejecución	194
4.6 Informe de seguridad	196
4.6 Conexiones de red	197
4.6 ESET SysRescue Live	199
4.6 Envío de muestras para su análisis	199
4.6 Seleccionar muestra para su análisis: archivo sospechoso	200
4.6 Seleccionar muestra para su análisis: sitio sospechoso	201
4.6 Seleccionar muestra para su análisis: archivo con falso positivo	201
4.6 Seleccionar muestra para su análisis: sitio de falso positivo	201
4.6 Seleccionar muestra para su análisis: otros	202
4.6 Notificaciones	202
4.6 Notificaciones de la aplicación	203
4.6 Notificaciones en el escritorio	204
4.6 Notificaciones por correo electrónico	205
4.6 Personalización de las notificaciones	207
4.6 Cuarentena	208
4.6 Configuración del servidor proxy	210
4.6 Intervalos de tiempo	211
4.6 Actualización de Microsoft Windows	212
4.6 Verificación de intervalo de licencia	213
4.7 Interfaz del usuario	213
4.7 Elementos de la interfaz del usuario	214
4.7 Estados de la aplicación	215
4.7 Configuración del acceso	216
4.7 Contraseña para configuración avanzada	217
4.7 Alertas y cuadros de mensajes	217

4.7 Alertas interactivas	219
4.7 Mensajes de confirmación	220
4.7 Error de conflicto de configuraciones avanzadas	222
4.7 Medios extraíbles	222
4.7 Se requiere el reinicio	223
4.7 Se recomienda el reinicio	225
4.7 Ícono de la bandeja del sistema	226
4.7 Menú contextual	227
4.7 Ayuda y soporte	228
4.7 Acerca de ESET Endpoint Security	229
4.7 Enviar datos de configuración del sistema	229
4.7 Soporte técnico	230
4.7 Administrador de perfiles	230
4.7 Accesos directos desde el teclado	231
4.7 Diagnósticos	232
4.7 Exploración de la línea de comandos.	233
4.7 ESET CMD	236
4.7 Detección en estado inactivo	238
4.7 Importar y exportar configuración	238
4.7 Restauración de todas las configuraciones a las predeterminadas	239
4.7 Restauración de todas las configuraciones en la sección actual	239
4.7 Error al guardar la configuración	240
4.7 Monitoreo y administración remotos	240
4.7 Línea de comandos de ERMM	241
4.7 Lista de los comandos ERMM JSON	243
4.7 Obtener estado de protección	244
4.7 Obtener información de la aplicación	244
4.7 Obtener información de licencia	247
4.7 Obtener registros	247
4.7 Obtener estado de activación	248
4.7 Obtener información de la exploración	249
4.7 Obtener configuración	250
4.7 Obtener estado de actualización	251
4.7 Comenzar exploración	252
4.7 Comenzar activación	252
4.7 Comenzar desactivación	253
4.7 Comenzar actualización	254
4.7 Establecer configuración	254
5 Preguntas habituales	255
5.1 Cómo actualizar ESET Endpoint Security	256
5.2 Cómo activar ESET Endpoint Security	256
5.2 Ingreso de su clave de licencia durante la activación	257
5.2 Inicie sesión en ESET Business Account	257
5.2 Procedimiento para usar credenciales de la licencia para activar un producto de punto de conexión de ESET más reciente.	258
5.3 Cómo quitar un virus del equipo	258
5.4 Cómo permitir la comunicación para una aplicación específica	258
5.5 Cómo crear una nueva tarea en Tareas programadas	259
5.5 Cómo programar una exploración semanal del equipo	260
5.6 Cómo conectar ESET Endpoint Security al ESET PROTECT	261
5.6 Cómo utilizar el modo anulación	261

5.6 Procedimiento para aplicar una política recomendada para ESET Endpoint Security	263
5.7 Cómo configurar un servidor reflejado	265
5.8 Cómo actualizo a Windows 10 con ESET Endpoint Security	266
5.9 Cómo activar el monitoreo y la administración remotos	266
5.10 Cómo bloquear la descarga de tipos específicos de archivos desde Internet	269
5.11 Cómo minimizar la interfaz del usuario de ESET Endpoint Security	270
5.12 Cómo resolver el mensaje de error	270
6 Acuerdo de licencia de usuario final	272
7 Política de privacidad	279

ESET Endpoint Security 8

ESET Endpoint Security 8 representa un nuevo enfoque para la seguridad del equipo plenamente integrada. La versión más reciente del motor de exploración ThreatSense®, combinado con el Firewall hecho a medida y el módulo antispam, utiliza velocidad y precisión para mantener el equipo seguro. El resultado es un sistema inteligente constantemente alerta frente a los ataques y el software malicioso que pongan en peligro su equipo.

ESET Endpoint Security 8 es una solución de seguridad completa, producto de nuestro esfuerzo a largo plazo para combinar la máxima protección con el mínimo impacto 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 Security 8 está diseñado principalmente para usar en estaciones de trabajo de un entorno de empresas pequeñas.

En la sección [Uso de ESET Endpoint Security por sí solo](#), 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 Security 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

Interfaz del usuario rediseñada	La interfaz del usuario en esta versión se ha rediseñado y simplificado considerablemente con base en los resultados de las pruebas de usabilidad. Todas las etiquetas y notificaciones de la interfaz gráfica del usuario se han revisado cuidadosamente. Ahora, la interfaz es compatible con idiomas de derecha a izquierda, como hebreo y árabe. La ayuda en línea se encuentra integrada en ESET Endpoint Security y ofrece contenido de soporte actualizado en forma dinámica.
Antivirus y antispymware	Detecta en forma proactiva y desinfecta más cantidad de amenazas conocidas y desconocidas, tales como virus, gusanos , troyanos y rootkits . La Heurística avanzada identifica hasta al malware nunca antes visto. Lo protege de amenazas desconocidas, a las que neutraliza antes de que lleguen a causar daño. La Protección del acceso a la web y Anti-Phishing funciona mediante el monitoreo de la comunicación entre navegadores Web y servidores remotos (incluido SSL). La Protección del cliente de correo electrónico proporciona el control de las comunicaciones por correo electrónico recibidas a través de los protocolos POP3(S) e IMAP(S).
Actualizaciones de rutina	La actualización frecuente del motor de detección (anteriormente conocido como “base de datos de firmas de virus”) y de los módulos de programa es el mejor método para asegurar el máximo nivel de seguridad en su equipo.
ESET LiveGrid® (Reputación basada en la nube)	Usted podrá verificar la reputación de los procesos en ejecución y de los archivos directamente desde ESET Endpoint Security.

Gestión remota	ESET PROTECT o ESET Security Management Center le permiten administrar los productos de ESET en estaciones de trabajo, servidores y dispositivos móviles en un entorno de red desde una ubicación central. A través de la consola web de ESET Security Management Center (Consola web de ESMC), 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.
Protección contra ataques de red	Analiza el contenido del tráfico de la red y protege de ataques en la red. Todo tráfico considerado perjudicial será bloqueado.
Control web (ESET Endpoint Security únicamente)	El Control Web permite bloquear 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 de esta versión?

ESET Endpoint Security 8 ya se lanzó y está [disponible para descarga](#).

Navegador seguro

- protege un navegador web de otros procesos que se ejecutan en el equipo
- enfoque de confianza cero y supone que el equipo o sus capacidades de protección se ven afectados o son insuficientes y no permite manipular el espacio de memoria del navegador, y, en consecuencia, el contenido de la ventana del navegador
- no está activa de forma predeterminada para que los administradores tengan tiempo suficiente para sacar provecho del potencial de sus políticas de seguridad

Exploración de VMI y del registro completo

- mejorando la exploración del registro que puede descubrir y eliminar referencias maliciosas o contenido peligroso en cualquier parte del repositorio del registro o de VMI
- la inspección puede llevar cierto tiempo. Se deben seleccionar estos objetivos de exploración para todas las exploraciones a pedido, incluso para el perfil de exploración “exhaustiva”.

Actualización de componentes del programa Micro (actualización de funciones)

- una [solución inteligente](#) para reducir el mantenimiento de ESET Endpoint Security al mínimo indispensable
- MicroPCU puede esperar un reinicio por semanas
- no reinstala el producto con todas las desventajas, como la cancelación del registro del sistema durante el proceso, incluida la transferencia de la configuración
- descarga menos datos (actualización diferencial)

- incluye un recordatorio simple o completamente suprimible para el usuario y es compatible con las redes administradas

Actualizaciones de seguridad y estabilidad

- Las [actualizaciones de seguridad y estabilidad](#) se distribuirán automáticamente a versiones compatibles (7.x y posteriores), que contienen solo modificaciones esenciales que se documentarán con total transparencia en registros de cambio considerables

Este lanzamiento viene con varias soluciones de errores y mejoras en el desempeño.

Para obtener información adicional e instantáneas sobre las nuevas características de ESET Endpoint Security, lea el siguiente artículo de la base de conocimiento de ESET:

- [Novedades de la versión 8 de ESET Endpoint Security](#)

Requisitos del sistema

Para un funcionamiento óptimo de ESET Endpoint Security, 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

Sistemas operativos

Microsoft® Windows® 10
Microsoft® Windows® 8.1
Microsoft® Windows® 8

Microsoft® Windows® 7 SP1 con las actualizaciones de Windows más recientes (al menos [KB4474419](#) y [KB4490628](#))

Windows XP y Windows Vista ya no son [compatibles](#).



Siempre intente mantener su sistema operativo actualizado.

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 mínima del monitor 1024x768
- 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 podría ser posible instalar y ejecutar el producto en sistemas que no cumplen con esos requisitos, recomendamos realizar una prueba de uso previa en base a los requisitos de rendimiento.

- i**
- (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 necesario para descargar el instalador, instalar el producto y guardar una copia del paquete de instalación en los datos del programa y copias de seguridad de las actualizaciones del producto para que sea compatible con la función de reversión. El producto podría usar más espacio en disco en diferentes entornos (por ejemplo, cuando se almacenan más versiones de copias de seguridad de actualización del producto, volcados de memoria o cuando se mantienen grandes cantidades de registros) o en un equipo infectado (por ejemplo, debido a la función de cuarentena). Recomendamos tener suficiente espacio libre en disco para admitir las actualizaciones del sistema operativo y para las actualizaciones de productos ESET.
 - (3):** Aunque no es recomendado, el producto se podría actualizar manualmente desde un medio extraíble.

Idiomas compatibles

ESET Endpoint Security 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

Idioma	Código de idioma	LCID
Kazajo	kk-KZ	1087
Coreano	ko-KR	1042
* Letón	lv-LV	1062
Lituano	lt-LT	1063
Nederlands	nl-NL	1043
Noruego	nn-NO	1044
Polaco	pl-PL	1045
Portuguese	pt-BR	1046
Rumano	ro-RO	1048
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 Security 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 el extremo superior derecho).

Prevención

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

Actualizaciones habituales

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

Descargas de revisiones de seguridad

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

Copia de seguridad de datos importantes

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

Exploración habitual del equipo en busca de virus

El módulo de protección del sistema de archivos en tiempo real maneja la detección de virus, gusanos, troyanos y rootkits más conocidos y desconocidos. Esto significa que, cada vez que accede a un archivo o lo abre, se lo explora para evitar actividades de malware. Se recomienda realizar una exploración completa del equipo al menos una vez por mes, ya que las firmas de malware varía y el motor de detección se actualiza todos los días.

Seguimiento de reglas de seguridad básicas

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

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

Páginas de ayuda

Bienvenido a los archivos de ayuda de ESET Endpoint Security. La información aquí incluida sirve para que se familiarice con el producto y ayudarlo a hacer que su equipo sea más seguro.

Introducción

Antes de comenzar a utilizar ESET Endpoint Security, tenga en cuenta que nuestro producto puede ser utilizado

por [usuarios conectados mediante ESET Security Management Center](#) o [por si solo](#). 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 Security. También preparamos una guía para ayudarlo a configurar y personalizar las opciones básicas de ESET Endpoint Security.

Cómo usar las páginas de ayuda de ESET Endpoint Security

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 Security. 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
En negrita	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.
Hiperínculo	Proporciona un acceso fácil y rápido a temas con referencias cruzadas o una ubicación web externa. Los hiperínculos están resaltados en azul y pueden estar subrayados.
<code>%ProgramFiles%</code>	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 Security 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 Security puede administrarse de forma remota mediante ESET Security Management Center o ESET Cloud Administrator.

- [Introducción a ESET PROTECT](#)
- [Introducción a ESET PROTECT Cloud](#)

Herramientas de administración remota de terceros

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

Prácticas recomendadas

- [Conectar todos los puntos de conexión con ESET Endpoint Security 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 Security

Guías de procedimientos

- [Cómo utilizar el modo anulación](#)
- [Procedimiento para implementar ESET Endpoint Security 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.

Al usar la 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 detecciones 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](#): el servidor de ESET PROTECT se puede instalar tanto en Windows como en Linux y también viene como un Dispositivo virtual. 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](#): La consola web de ESET PROTECT es la interfaz principal que le permite administrar los equipos cliente en su entorno. Muestra una visión general del estado de los clientes en su red y le permite implementar las soluciones de ESET en equipos no administrados en forma remota. 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](#): el 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.
- [Sensor de Rogue Detection](#): El Sensor de Rogue Detection (RD) de ESET PROTECT detecta equipos no administrados en su red y envía la información de dichos equipos al Servidor ESET PROTECT. Esto le permite agregar fácilmente nuevos equipos cliente a su red segura. El sensor RD recuerda los equipos que han sido detectados y no enviará la misma información dos veces.
- [Proxy HTTP Apache](#): 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.
- [Conector de dispositivo móvil](#): 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](#): La VA ESET PROTECT está destinada para los usuarios que desean ejecutar ESET PROTECT en un ambiente virtualizado.
- [Host del agente virtual ESET PROTECT](#): Un componente del ESET PROTECT que virtualiza las entidades del agente para permitir la administración de máquinas virtuales sin agentes. 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](#): La 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](#): Esta herramienta le 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.
- [ESET Business Account](#): El nuevo portal de licencias para los productos comerciales de ESET le permite administrar las licencias. Consulte la sección de [ESET Business Account](#) este documento para obtener instrucciones sobre cómo activar su producto o consulte la Guía del usuario de ESET Business Account*** para obtener más información sobre cómo usar 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](#).
- [ESET Enterprise Inspector](#): 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.

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.

i Para obtener más información, consulte la [Guía para el usuario en línea de ESET PROTECT](#).

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 ESMC. 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.

- [Lea más al respecto en la Guía para el usuario en línea de ESET PROTECT Cloud](#).

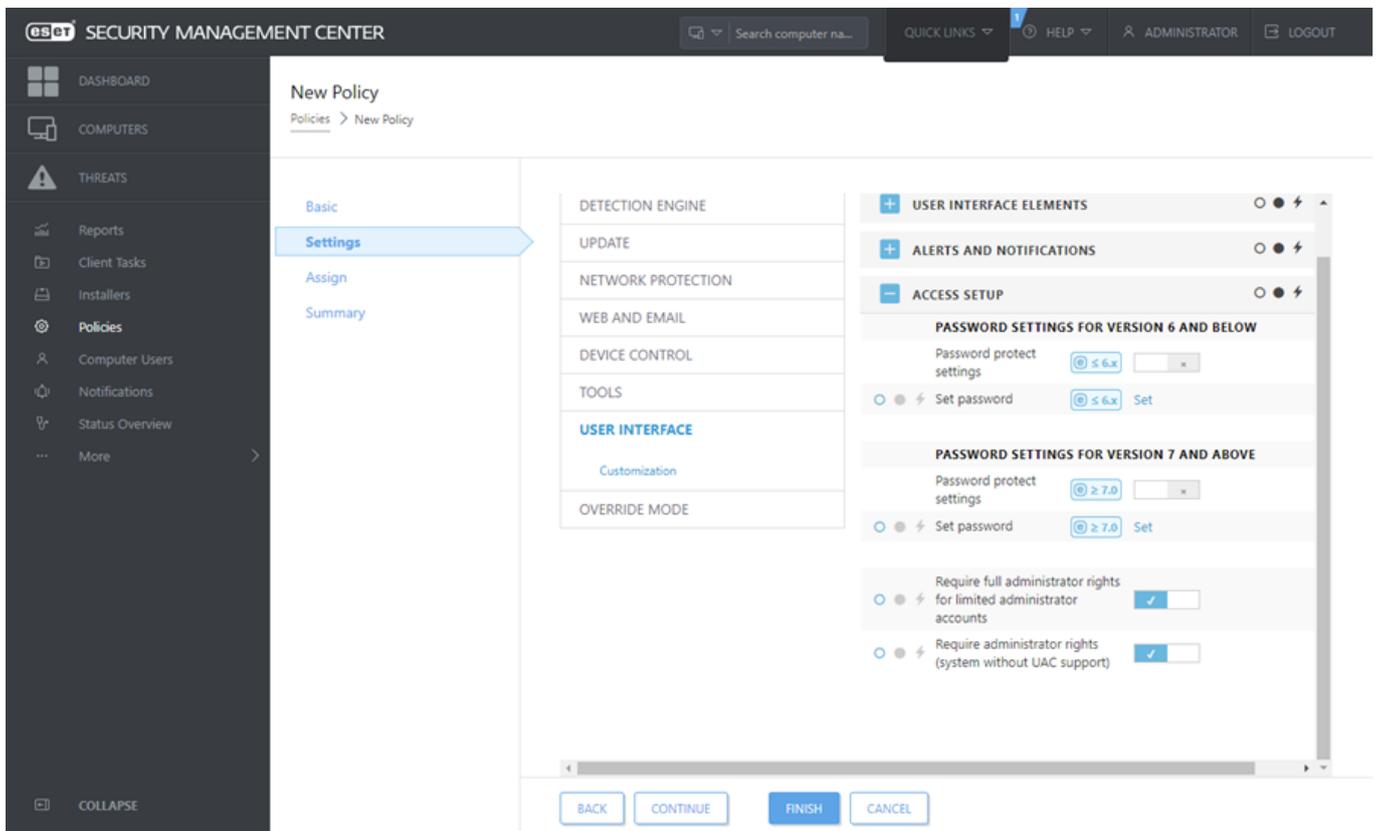
Configuración protegida por contraseña

Para proporcionar la máxima seguridad para su sistema, ESET Endpoint Security 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 Security en los equipos de cliente conectados. Para crear una nueva política:

1. En la consola web de ESET PROTECT o en la consola web de ESMC, 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 Security, haga clic en la barra deslizante 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 emergente, 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 o Consola web de ESMC. Las políticas se pueden aplicar directamente a equipos individuales o 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 en que se organizan los Grupos estáticos. Esto no es cierto en el caso de los Grupos dinámicos, donde las políticas se aplican primero a los Grupos dinámicos más recientes. Esto le permite aplicar políticas con mayor impacto en la parte superior del árbol de grupos y aplicar políticas más específicas a los subgrupos. Al usar [indicadores](#) un usuario de ESET Endpoint Security 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 los grupos que se ubiquen en la parte superior del 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 Security 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:

 No corresponde	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.
 Aplicar	La configuración con el indicador Aplicar 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.
 Forzar	Las configuraciones con el indicador Forzar tienen prioridad y no se pueden sobrescribir con ninguna política aplicada posteriormente (incluso si también tiene un indicador de Forzar). 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**.

Uso de ESET Endpoint Security por sí solo

Esta sección y la sección [Trabajar con ESET Endpoint Security](#) de esta Guía para el usuario está dedicada a los usuarios que utilizan ESET Endpoint Security sin ESET PROTECT, ESET Security Management Center o ESET PROTECT Cloud. Todas las características y funcionalidades de ESET Endpoint Security son completamente accesibles, dependiendo de los derechos de la cuenta del usuario.

Método de instalación

Hay varios métodos de instalación de la versión 8.x de ESET Endpoint Security en una estación de trabajo de cliente, a menos que [implemente ESET Endpoint Security de forma remota en estaciones de trabajo de cliente a través de ESET PROTECT, ESET Security Management Center o ESET PROTECT Cloud](#).

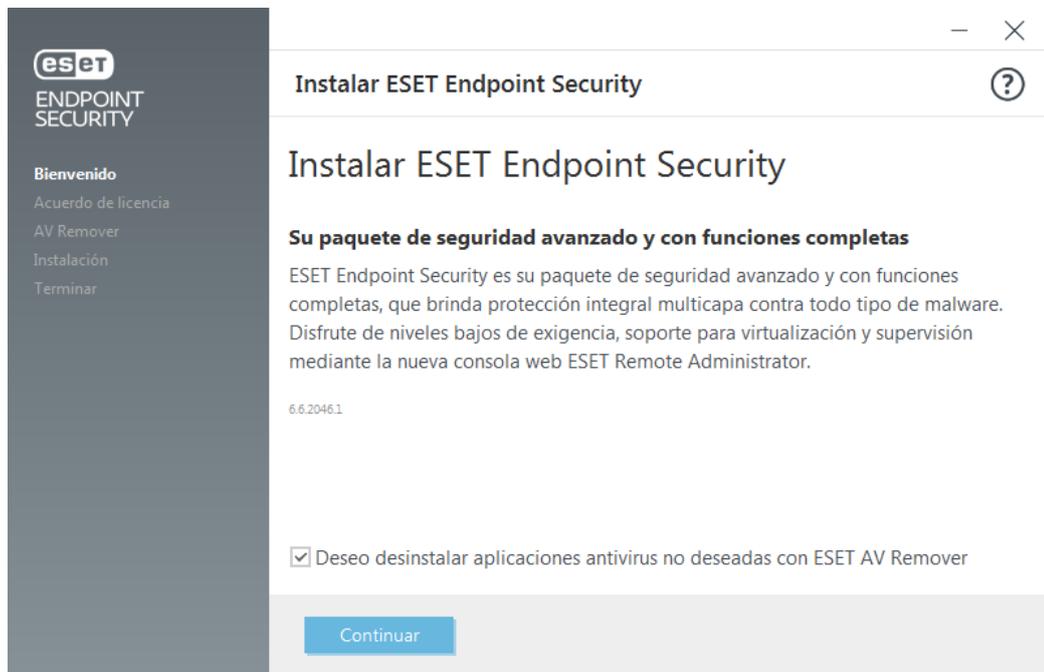
- [Instalar o actualizar ESET Endpoint Security a la versión 6.6.x](#)

Métodos	Finalidad	Enlace de descarga
Instalación con ESET AV Remove	La herramienta ESET AV Remove le ayudará a eliminar casi cualquier software antivirus que se haya instalado previamente en su sistema antes de seguir adelante con la instalación.	Descargar 64 bits Descargar 32 bits
*** Instalación (.exe)	Proceso de instalación sin ESET AV Remove.	N/A
Instalación (.msi)	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 Security Management Center.	Descargar 64 bits Descargar 32 bits
Instalación de línea de comando	ESET Endpoint Security puede instalarse a nivel local utilizando la línea de comando o de manera remota utilizando una tarea de cliente desde ESET PROTECT o ESET Security Management Center.	N/A
Implementación a través de GPO o SCCM	Use administración herramientas como GPO o SCCM para implementar ESET Management Agent y las estaciones de trabajo de cliente de ESET Endpoint Security.	N/A
Implementación con herramientas de RMM	Los complementos de ESET DEM para la herramienta Remote Management and Monitoring (RMM) le permiten implementar ESET Endpoint Security en las estaciones de trabajo de cliente.	N/A

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

Instalación con ESET AV Remove

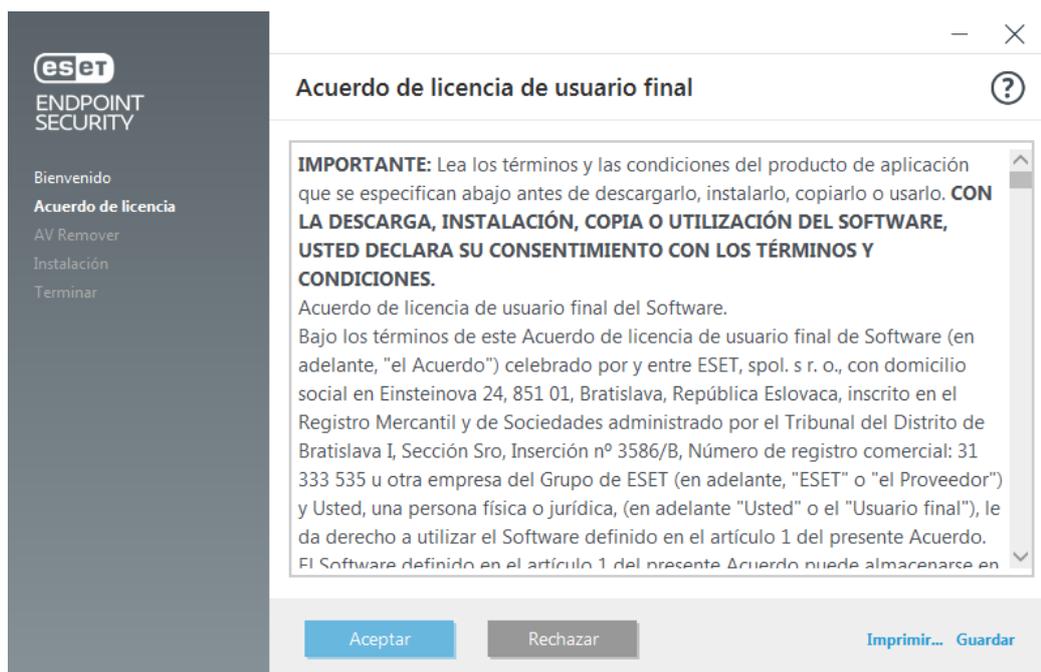
Antes de que continúe con el proceso de instalación, es importante que desinstale todas las aplicaciones de seguridad del equipo. Seleccione la casilla de verificación junto a **Desear desinstalar aplicaciones antivirus no deseadas con ESET AV Remove** para que ESET AV Remove explore el sistema y elimine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



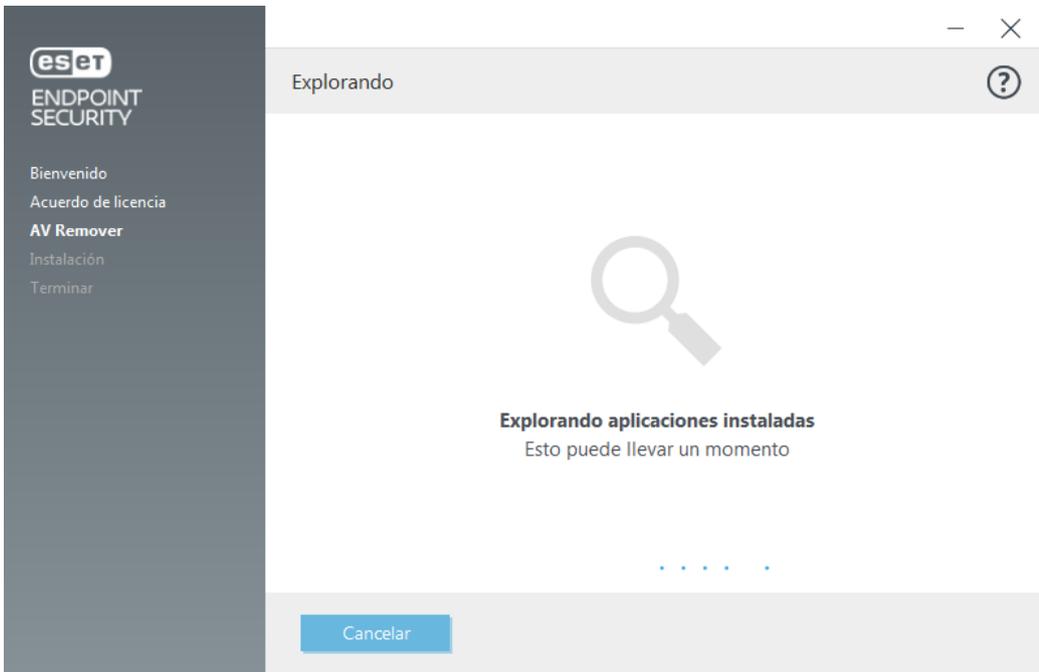
ESET AV Remover

La herramienta ESET AV Remover le ayudará a eliminar casi cualquier software antivirus que se haya instalado previamente en su sistema. Siga las instrucciones que se encuentran a continuación para eliminar un programa antivirus existente mediante ESET AV Remover:

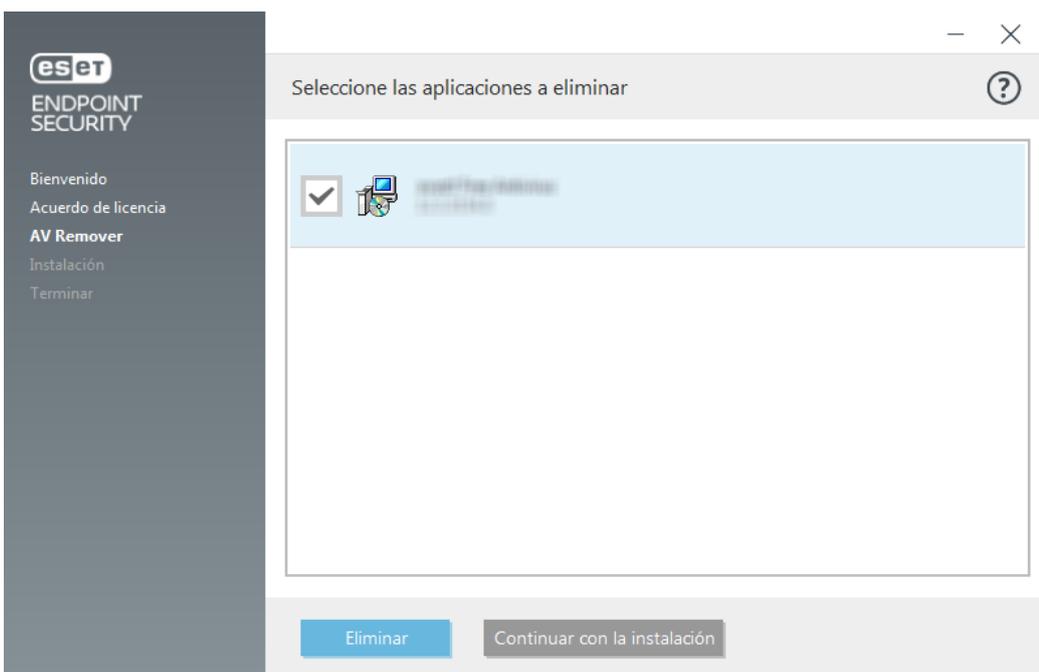
1. Para ver una lista de los software antivirus que ESET AV Remover puede eliminar, [visite el artículo de la base de conocimiento de ESET](#).
2. Lea el Contrato de licencia de usuario final y haga clic en **Aceptar** para dar su consentimiento. Si hace clic en **Rechazar**, procederá a la instalación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



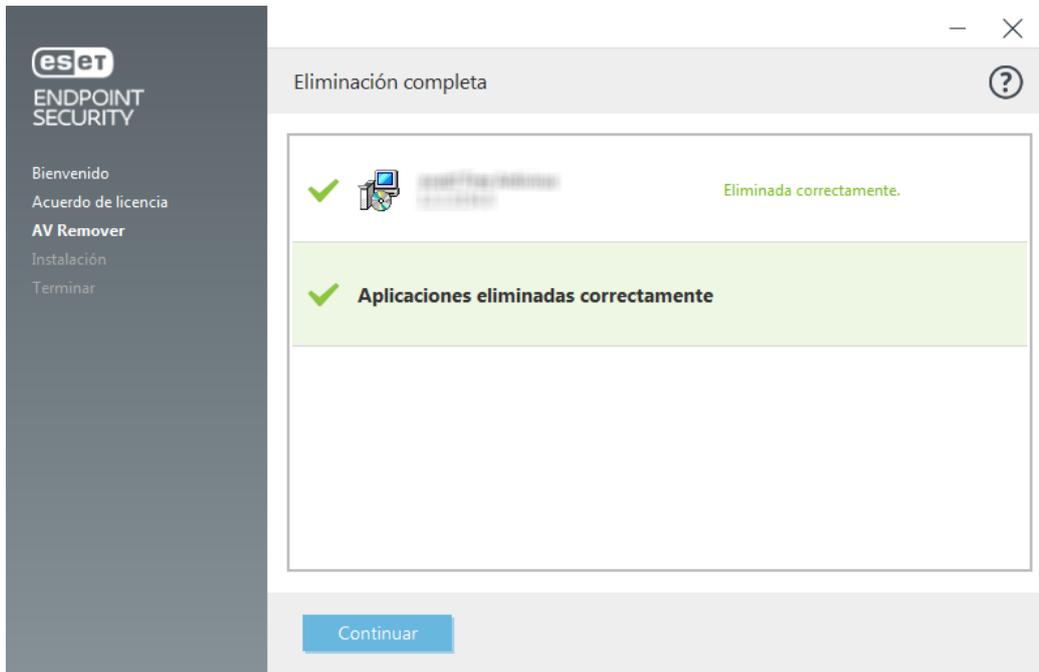
3. ESET AV Remover comenzará a buscar el software antivirus en el sistema.



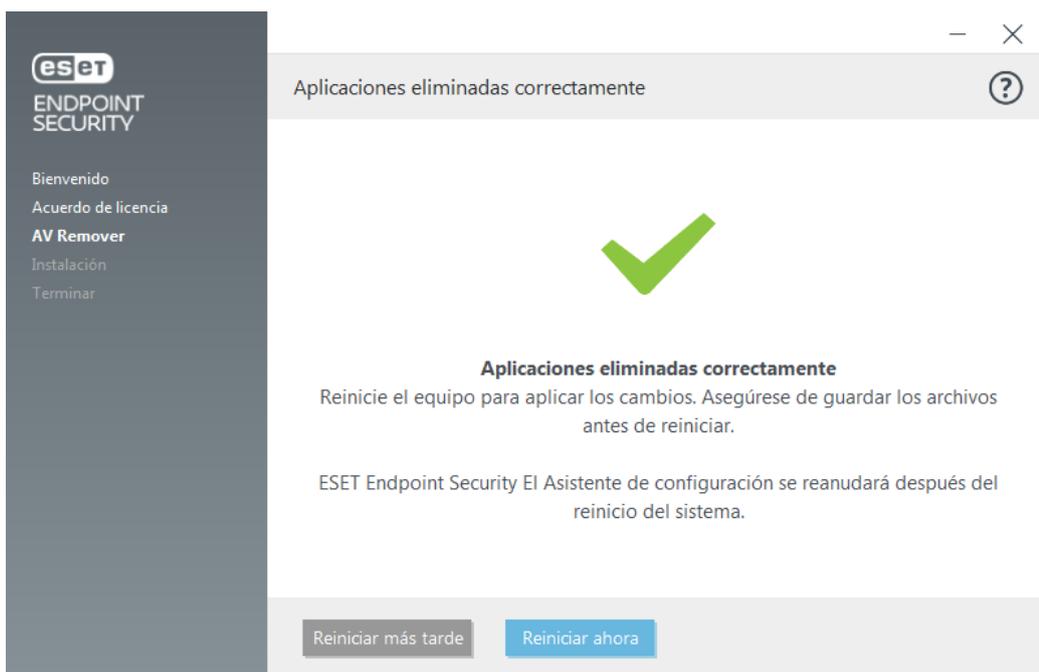
4. Seleccione cualquier aplicación de antivirus enumerada y haga clic en **Quitar**. La eliminación puede llevar unos minutos.



5. 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 Security. Si no es posible realizar la instalación, consulte la sección [La desinstalación con ESET AV Remover finalizó 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. Lea el Acuerdo de licencia de usuario final y haga clic en **Acepto** 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.



2. Elija si habilitar 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.

3. El paso siguiente en el proceso de instalación consiste en configurar la detección de aplicaciones potencialmente no deseadas. Vea el capítulo [Aplicaciones potencialmente no deseadas](#) para obtener más detalles.

4. El último paso es confirmar la instalación al hacer clic en **Instalar**. Puede instalar ESET Endpoint Security en una carpeta específica. Para ello, haga clic en [Cambiar la carpeta de instalación](#). Una vez que se completa la instalación, se lo direccionará a [activar ESET Endpoint Security](#).



Cambiar la carpeta de instalación (.exe)

Después de seleccionar su preferencia por la detección de aplicaciones potencialmente no deseadas y hacer clic en **Cambiar la carpeta de instalación**, se le solicitará que seleccione una ubicación para la carpeta de instalación del producto ESET Endpoint Security. De forma predeterminada, el programa se instala en el siguiente directorio:

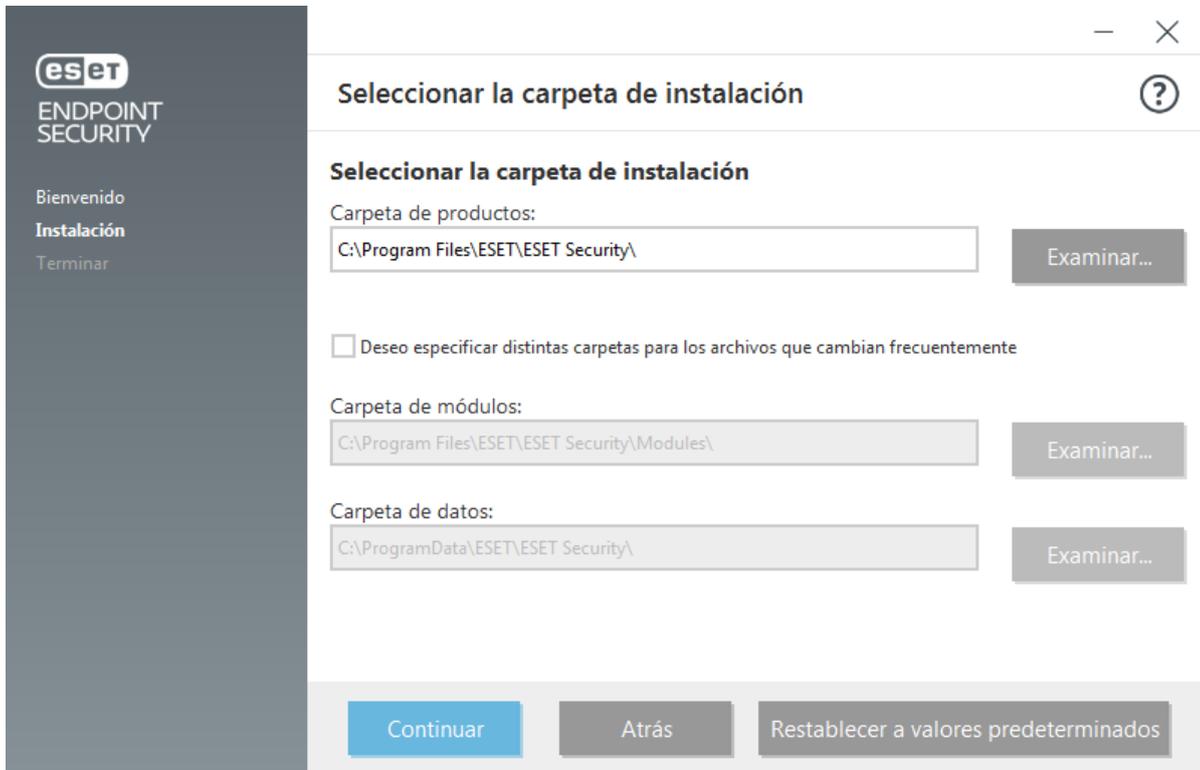
C:\Program Files\ESET\ESET Security

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

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 **Continuar** y luego en **Instalar** para comenzar la instalación.

Instalación (.msi)

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

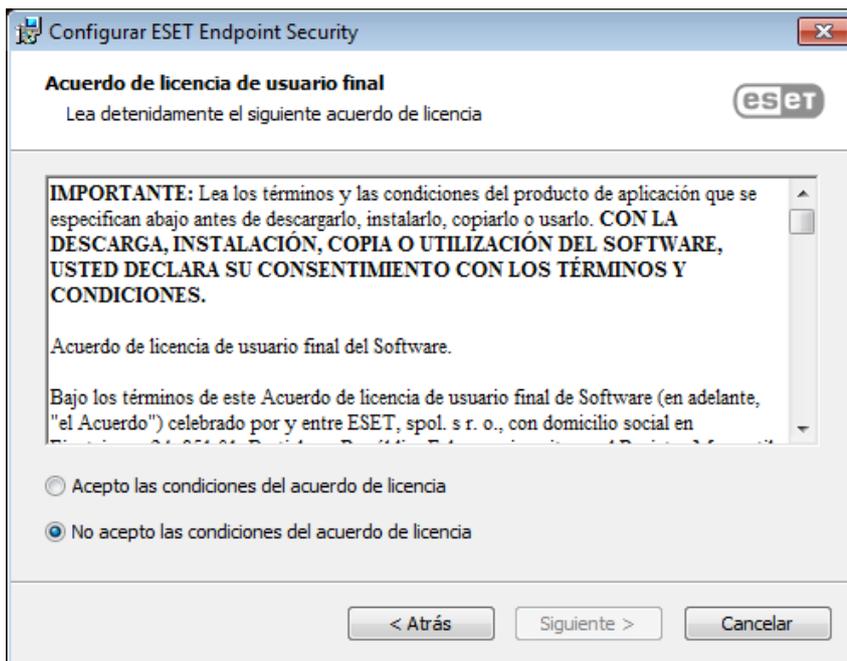
✓ En entornos comerciales, el instalador .msi es el paquete de instalación de preferencia. Esto se debe principalmente a las implementaciones sin conexión y remotas que utilizan varias herramientas, como ESET Security Management Center.

⚠ 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).

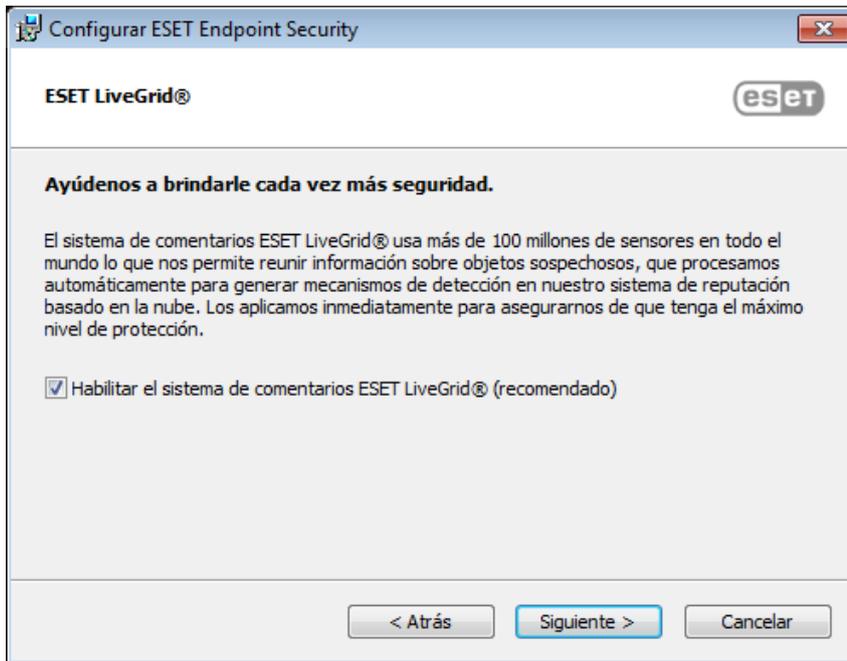
1. Seleccione un idioma deseado y haga clic en **Siguiente**.



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.



4. El paso siguiente en el proceso de instalación consiste en configurar la detección de aplicaciones potencialmente no deseadas. Vea el capítulo [Aplicaciones potencialmente no deseadas](#) para obtener más detalles.

Haga clic en **Configuración avanzada** si desea continuar con la [Instalación avanzada \(.msi\)](#).



5. 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 Security](#).

Instalación avanzada (.msi)

La instalación avanzada le permite personalizar un cierto número de parámetros de instalación no disponibles cuando se realiza una instalación típica.

5. Después de seleccionar su preferencia por la detección de [aplicaciones potencialmente no deseadas](#) y hacer

clic en **Configuración avanzada**, se le solicitará que seleccione una ubicación para la instalación de la Carpeta de productos ESET Endpoint Security. De forma predeterminada, el programa se instala en el siguiente directorio:

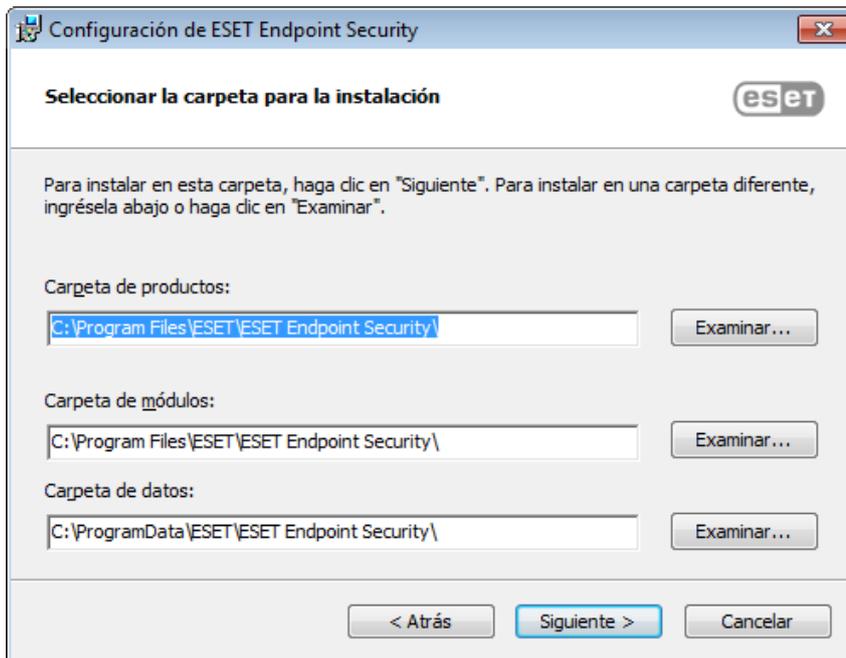
C:\Program Files\ESET\ESET Security

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

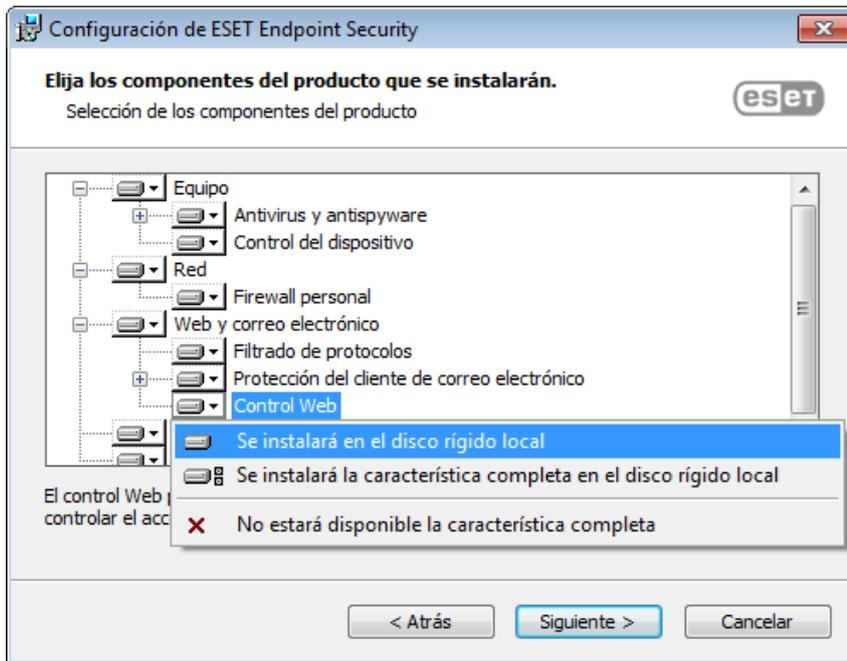
C:\Program Files\ESET\ESET Security\Modules

C:\ProgramData\ESET\ESET Security

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



6. Elija qué componentes del producto se instalarán. Los componentes del producto en la sección [Equipo](#) incluyen Protección del sistema de archivos en tiempo real, Exploración del equipo, Protección de documentos y Control del dispositivo. Tenga en cuenta que los primeros dos componentes son obligatorios para que su solución de seguridad funcione. La sección [Red](#) ofrece la opción de instalar el Firewall de ESET, que monitorea todo el tráfico de redes entrantes y salientes, y aplica reglas para las conexiones individuales de redes. El Firewall proporciona protección frente a ataques de equipos remotos. [La protección contra los ataques de red \(IDS\)](#) analiza el contenido del tráfico de red y ofrece protección contra los ataques de red. Los componentes en la sección [Internet y correo electrónico](#) son responsables de su protección mientras que navega en Internet y se comunica por medio de correo electrónico. 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.



7. El último paso es confirmar la instalación al hacer clic en **Instalar**.

Instalación de línea de comando

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

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 sub-funciones

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

Descripción	Nombre de característica	Característica principal	Presencia
Componentes básicos del programa	Computer		Marcador
Motor de detección	Antivirus	Computer	Obligatoria

Descripción	Nombre de característica	Característica principal	Presencia
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
Web y correo electrónico/Filtrado de protocolos	ProtocolFiltering	WebAndEmail	Invisible
Web y correo electrónico / Protección del acceso a la Web	WebAccessProtection	WebAndEmail	Opcional
Web y correo electrónico / Protección de cliente de correo electrónico	EmailClientProtection	WebAndEmail	Opcional
Web y correo electrónico/Protección de cliente de correo electrónico/Cientes de correo electrónico	MailPlugins	EmailClientProtection	Invisible
Web y correo electrónico / Protección de cliente de correo electrónico / Protección antispam	Antispam	EmailClientProtection	Opcional
Web y correo electrónico / Control Web	WebControl	WebAndEmail	Opcional
Herramientas/ESET RMM	Rmm		Opcional
Actualización/Perfiles/Replicación de actualización	UpdateMirror		Opcional
Complemento de ESET Enterprise Inspector	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 UPDTEMIRROR.

Lista de propiedades de configuración

Propiedad	Valor	Característica
CFG_POTENTIALLYUNWANTED_ENABLED=	0: Deshabilitado 1: Habilitado	Detección de aplicaciones potencialmente no deseadas (PUA)
CFG_LIVEGRID_ENABLED=	Ver a continuación	Consulte la propiedad LiveGrid a continuación
FIRSTSCAN_ENABLE=	0: Deshabilitado 1: Habilitado	Programe y ejecute una Exploración del equipo 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=	Ver a continuación	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 configuración XML exportada (valor predeterminado <i>cfg.xml</i>)

Propiedades de configuración solo en ESET Endpoint Security

CFG_EPFW_MODE=	0: Automático (predeterminado) 1: Interactivo 2: Basado en políticas 3: Aprendizaje	Modo de filtrado de firewall
CFG_EPFW_LEARNINGMODE_ENDTIME=	<timestamp>	Fecha de finalización del modo Aprendizaje como fecha y hora de Unix

Propiedad de [LiveGrid®](#)

Al instalar ESET Endpoint Security con CFG_LIVEGRID_ENABLED, el comportamiento del producto después de la instalación será el siguiente:

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

Propiedad ACTIVATION_DATA

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

Propiedades de idioma

Idioma de ESET Endpoint Security (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 lista de códigos de idioma .
PRODUCT_LANG_CODE=	Cadena LCID (Nombre cultural del idioma) en minúscula, por ejemplo en-us para inglés - Estados Unidos de América, consulte la lista de códigos de idioma .

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 Security se configure automáticamente después de la instalación, puede especificar parámetros de configuración básicos dentro del comando de instalación.
 Instale ESET Endpoint Security 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 Security 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 Security en una estación de trabajo del cliente](#) o [remota mediante una tarea del servidor en ESMC](#), 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 Security a través de ESET Security Management Center (ESMC). Debe tener ESMC 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 ESMC.
5. [Implemente y active ESET Endpoint Security 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 \(GPO\)](#)



Reemplazo a una versión más reciente

Las versiones nuevas de ESET Endpoint Security 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. Automáticamente, mediante el uso de ESET PROTECT, ESET Security Management Center (ESMC) o ESET PROTECT Cloud. ESET Endpoint Security versión 8 no puede administrarse con ESET Remote Administrator.
2. Automáticamente, [mediante el uso de GPO o SCCM](#).
3. Reemplazar automáticamente mediante una actualización del programa.
Como el reemplazo de componentes del programa por una versión posterior se distribuye a todos los usuarios y puede afectar ciertas configuraciones del sistema, se emite luego de un largo período de prueba para asegurar la funcionalidad en todas las configuraciones posibles de sistema. Si necesita reemplazar el programa por una versión posterior inmediatamente después de su lanzamiento, use uno de los siguientes métodos. Asegúrese de tener habilitada la opción **Modo de actualización** en **Configuración avanzada (F5) > Actualización > Perfiles > Actualización de componentes del programa**.
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, ESET PROTECT Cloud o ESMC.

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

De manera similar, no instale la versión 8 sobre una versión 4.x si tiene una versión 5.x o 6.x anterior o que no funciona de ESET Endpoint Security.

Si planea administrar actualizaciones en estaciones de trabajo de clientes individuales en forma manual:

1. Compruebe que su sistema operativo sea [compatible](#) Windows Vista y Windows XP no es compatible con la versión.
2. Descargue e [instale una versión más reciente](#) sobre la anterior.

Si desea maximizar las posibilidades de una actualización correcta a la versión [más reciente 8.x](#), actualice desde una de las siguientes versiones de ESET Endpoint Security:

- 5.0.2272.x
- 6.5.2132.x
- 7.3.2044.x

De lo contrario, desinstale ESET Endpoint Security primero. Para obtener información adicional sobre la actualización de ESET Endpoint Security en una estación de trabajo cliente, lea el siguiente [artículo de la base de conocimiento de ESET](#).

Actualización automática del producto de legado

Su versión del producto ESET ya no es compatible y se ha actualizado su producto a la versión 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 es posible regresar 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 Security es una parte fundamental para mantener una protección completa contra códigos maliciosos. Cada nueva versión de ESET Endpoint Security presenta nuevas mejoras y reparaciones de errores. Recomendamos realizar actualizaciones periódicas de ESET Endpoint Security para evitar vulnerabilidades y amenazas de seguridad. ESET Endpoint Security encaja en una etapa específica del ciclo de vida del producto como cualquiera de los demás productos ESET. Lea más sobre la [Política del fin de la vida útil \(productos comerciales\)](#).

Para obtener más información sobre los cambios en ESET Endpoint Security, 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.

Problemas comunes de instalación

Si ocurren problemas durante la instalación, consulte nuestra lista de [errores comunes de instalación y soluciones](#) para encontrar una solución a su problema.

Falló la activación

En caso de que la activación de ESET Endpoint Security no se lleve a cabo correctamente, los escenarios posibles más frecuentes son:

- La clave de licencia ya está en uso.
- Clave de licencia no válida. Error en el formulario de activación del producto.
- No es válida o falta información adicional necesaria para la activación.
- Falló la comunicación con la base de datos de activación. Intente volver a activar en 15 minutos.
- 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](#)

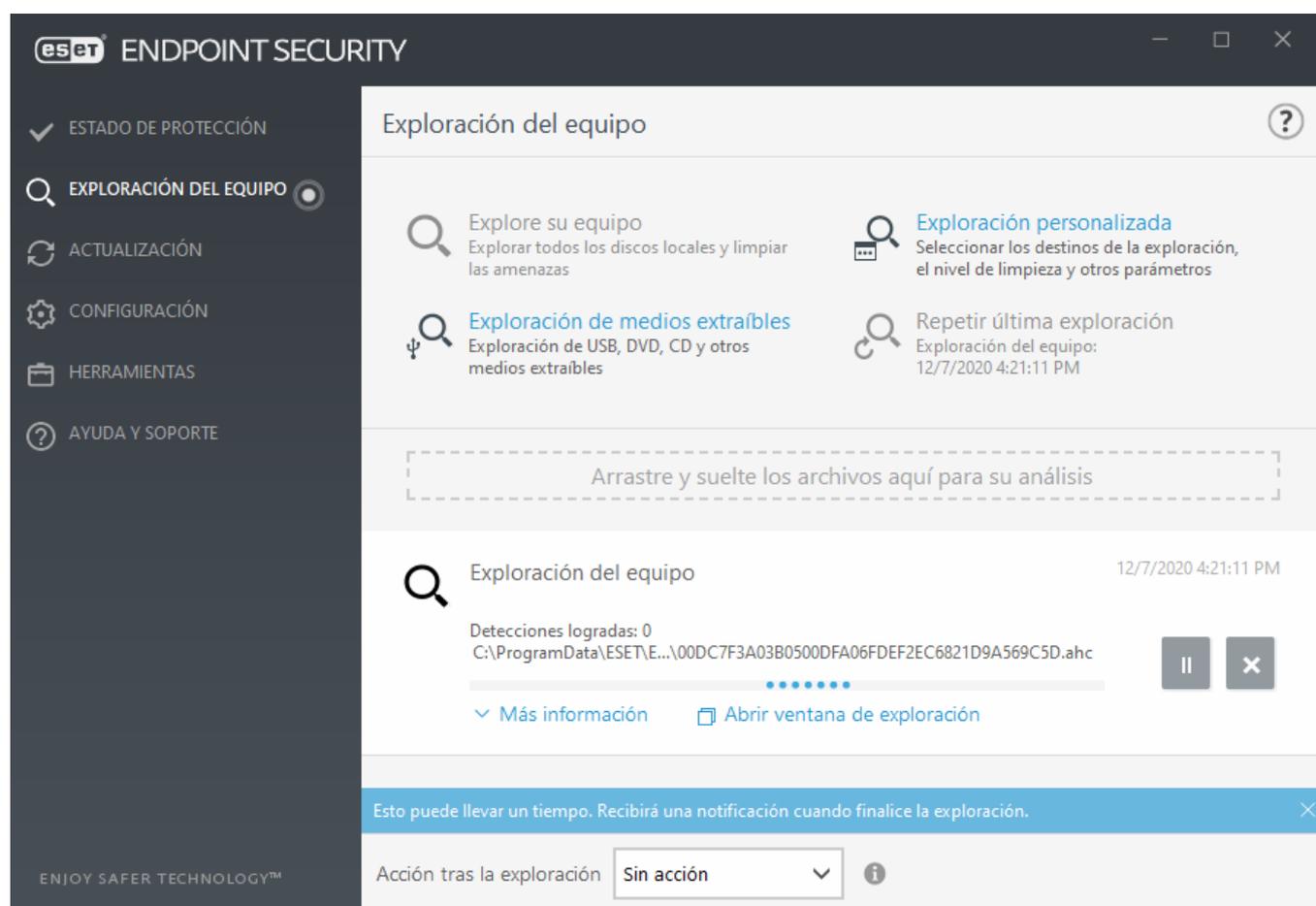
Activación del producto

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

Seleccione uno de los métodos disponibles para activar ESET Endpoint Security. Consulte [Cómo activar ESET Endpoint Security](#) para obtener más información.

Exploración del equipo

Le recomendamos realizar exploraciones regulares del equipo, o [programar una exploración regular](#), para buscar amenazas. Desde la ventana principal del programa, haga clic en **Exploración del equipo** y luego haga clic en **Exploración inteligente**. Para obtener más información sobre las exploraciones del equipo, consulte la sección [Exploración del equipo](#).



Guía para principiantes

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

La interfaz del usuario

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

principal de la izquierda.

A continuación se describen las opciones del menú principal:

Estado de protección – proporciona información sobre el estado de protección de ESET Endpoint Security.

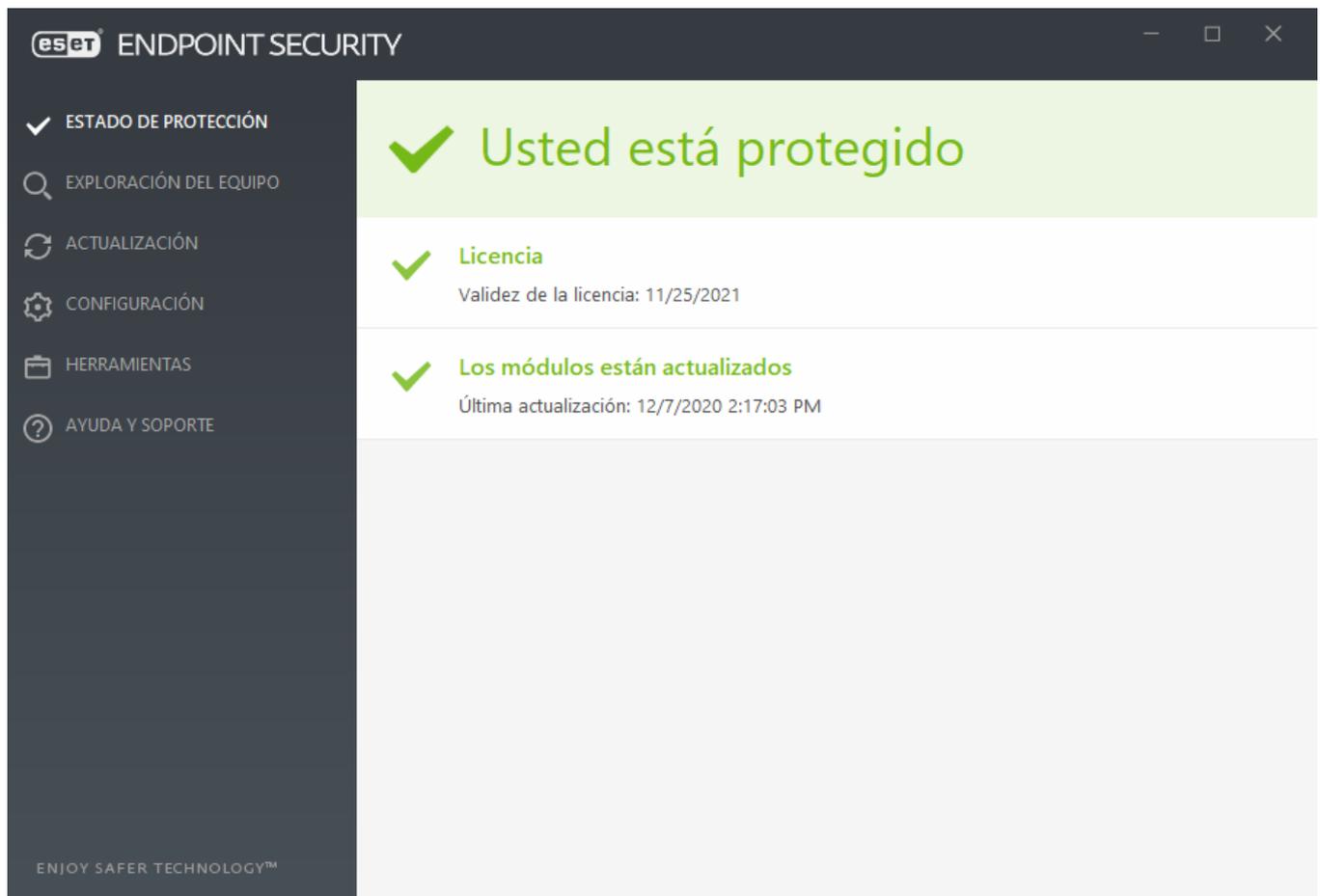
Exploración del equipo – esta opción le permite configurar y ejecutar la Exploración inteligente, la Exploración personalizada o la Exploración de medios extraíbles. También puede repetir la última exploración que se ejecutó.

Actualización: muestra información sobre el motor de detección y permite comprobar si hay actualizaciones de manera automática.

Configuración – seleccione esta opción para ajustar la configuraciones de seguridad de su Equipo, Red o Internet y correo electrónico.

Herramientas – proporciona acceso a los Archivos de registro, las Estadísticas de protección, la Visualización de la actividad, las Tareas programadas, la Cuarentenas conexiones de red,, ESET SysInspector y ESET SysRescue para crear un CD de recuperación. También puede enviar una muestra para su análisis.

Ayuda y soporte: brinda acceso a los archivos de ayuda, a la [Base de conocimiento de ESET](#) y al sitio Web de la empresa ESET. También se encuentran disponibles los enlaces para abrir una solicitud de soporte técnico, herramientas de soporte e información acerca de la activación de productos.



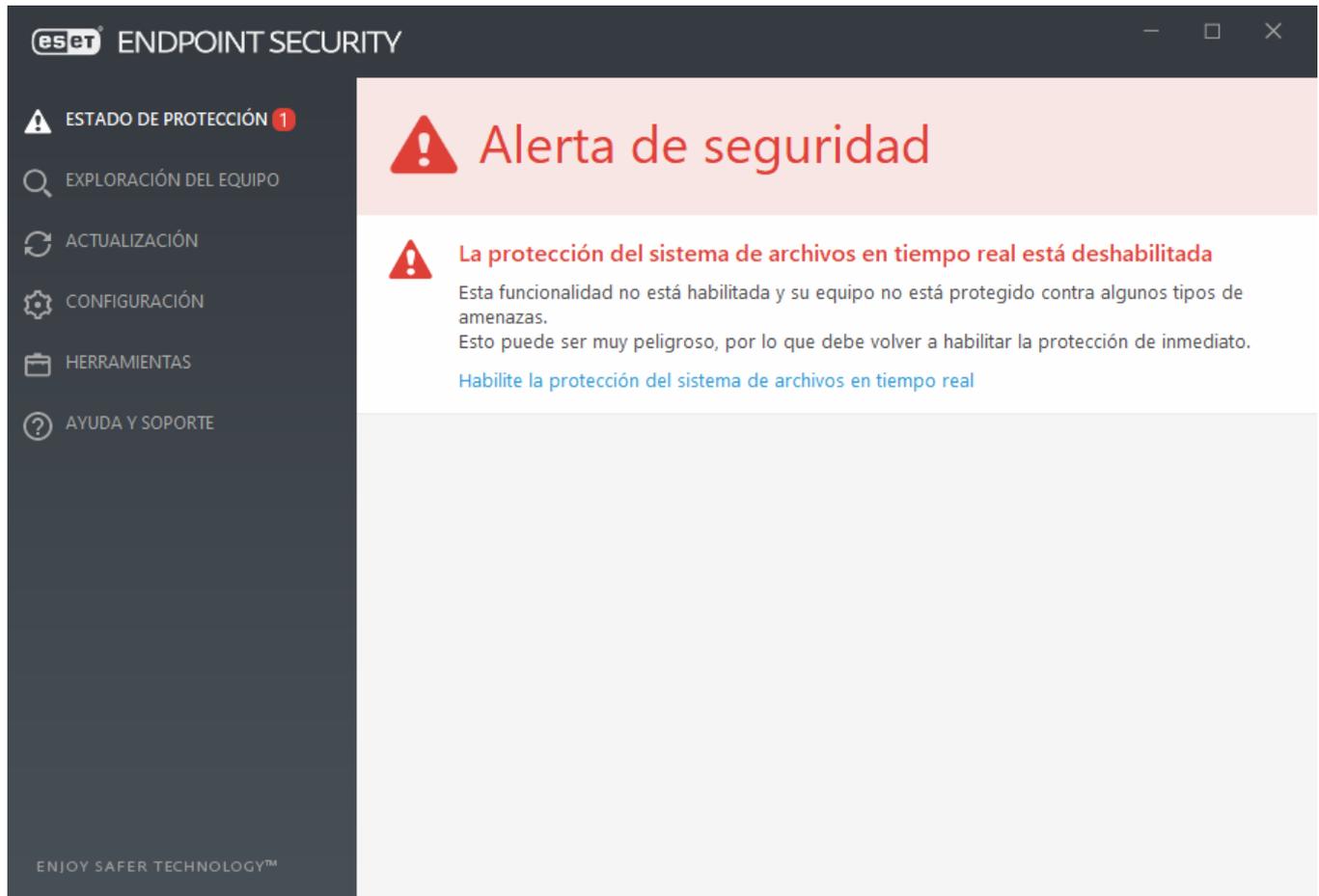
La pantalla **Estado de protección** le brinda información sobre el nivel de protección actual de su equipo y la seguridad. El estado **Protección máxima**, en color verde, indica que la máxima protección está asegurada.

La ventana de estado también muestra enlaces rápidos a funciones de uso frecuente en ESET Endpoint Security e

información acerca de la última actualización.

¿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 Security 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 Firewall de ESET está deshabilitado** – Este problema se indica mediante un ícono rojo y una notificación de seguridad ubicada junto al elemento **Red**. Haga clic en **Habilitar el modo filtrar** para volver a habilitar la

protección de red.

- **Falló la inicialización del Firewall** – El Firewall personal se deshabilitó a causa de problemas de integración del sistema. Reinicie su computadora lo antes posible.
- **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 La licencia está vencida** – Se indica mediante un icono rojo de estado de protección. Una vez que se vence la licencia, el programa no se podrá actualizar. Siga las instrucciones en la ventana de alerta para renovar la licencia.
- **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 desde Configuración avanzada. Su computadora no está protegida contra algunos tipos de amenazas y debe volver a habilitarse la protección inmediatamente haciendo clic en **Habilitar HIPS**.
- **ESET LiveGrid® está inhabilitado** – Este problema se indica cuando ESET LiveGrid® está inhabilitado en Configuración avanzada.
- **No se programaron actualizaciones regulares** – ESET Endpoint Security no buscará o recibirá actualizaciones importantes a menos que usted programe la tarea de actualización.
- **Anti-Stealth se inhabilitó** – Haga clic en **Habilitar Anti-Stealth** para volver a habilitar esta funcionalidad.
- **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 ESMC. 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** – Se indica mediante el ícono de estado de protección, que muestra 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.
- **Se pausó la protección contra botnets** – Haga clic en **Habilitar la protección contra botnets** para volver a habilitar esta característica.
- **Se pausó la protección contra ataques en la red (IDS)** – Haga clic en **Habilitar la protección contra ataques en la red (IDS)** para volver a habilitar esta característica.
- **Se pausó la protección Antispam** – Haga clic en **Habilitar la protección Antispam** para volver a habilitar esta característica.
- **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 Security, consulte [Estados de la aplicación](#).

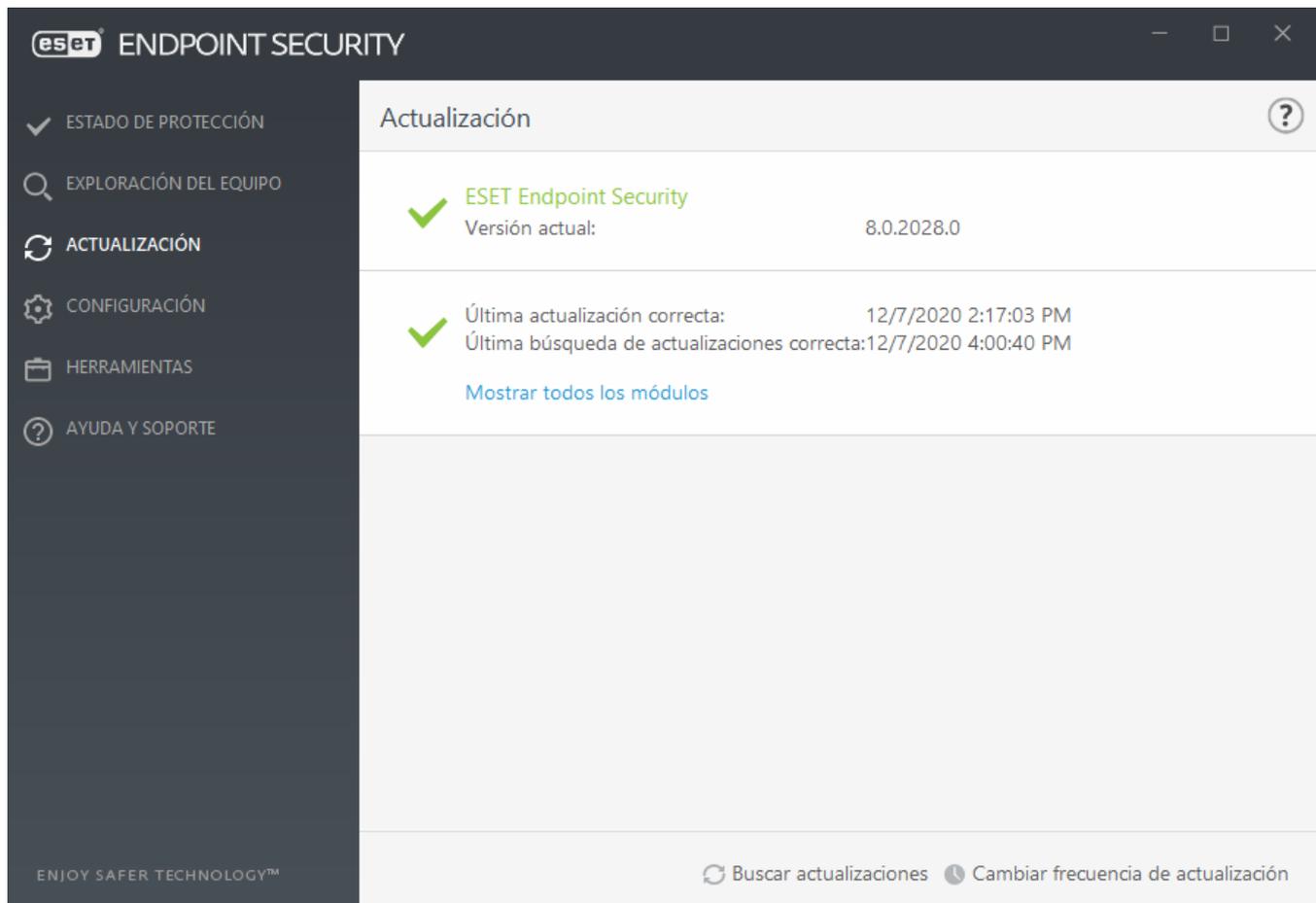
Si no puede solucionar el problema mediante las sugerencias, haga clic en **Ayuda y soporte** para acceder a los archivos de ayuda o buscar en la [base de conocimiento de ESET](#). Si aún necesita asistencia, puede enviar una petición de soporte. El Soporte técnico de ESET responderá rápidamente a sus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

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

Configuración de la actualización

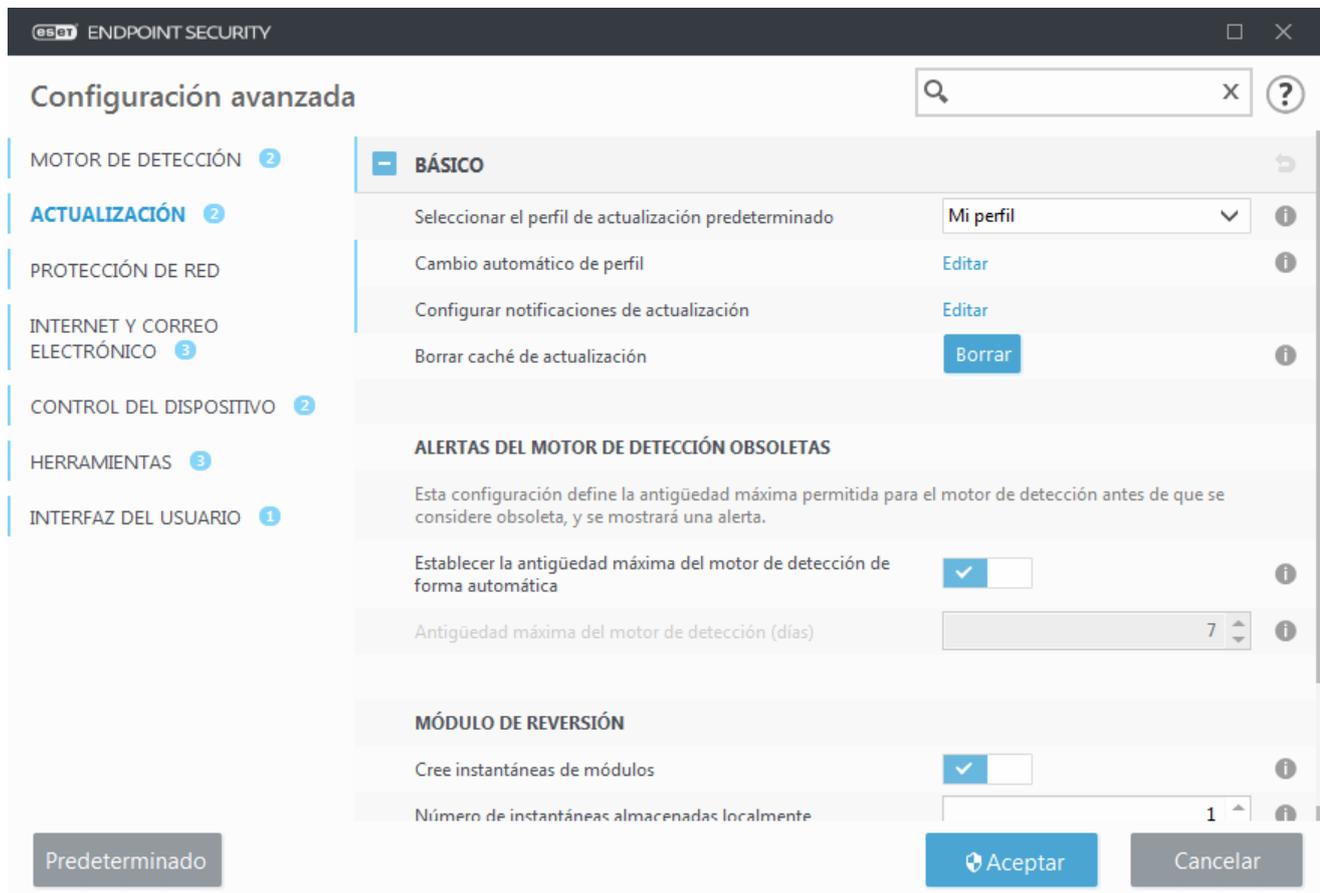
La actualización de los módulos es una parte fundamental para mantener una protección completa contra códigos maliciosos. Preste suma atención a la configuración de actualización y su funcionamiento. Desde el menú principal, seleccione **Actualizar > Comprobar actualizaciones** y verifique si existe una actualización del módulo más reciente.

Si aún no ha ingresado su **Clave de licencia**, no podrá recibir nuevas actualizaciones y se le solicitará que active su producto.



La ventana Configuración avanzada (haga clic en **Configuración** > **Configuración avanzada** en el menú principal o presione la tecla **F5** del teclado) contiene opciones adicionales de actualización. Para configurar las opciones avanzadas de actualización, como el modo de actualización, el acceso al servidor proxy, las conexiones LAN y la configuración de creación de copia del motor de detección, haga clic en **Actualizar** en el árbol de configuración Avanzada.

- Si experimenta alguna dificultad con una actualización, haga clic en **Borrar** para borrar la caché de los archivos de actualización temporales.



- La opción **Elegir de manera automática** en **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.
- Si no quiere que aparezca la notificación de bandeja de sistema de actualización correcta en el extremo inferior derecho de la pantalla, amplíe **Perfiles > Actualizaciones**, haga clic en **Editar** junto a **Seleccionar notificaciones de actualizaciones recibidas** y, luego, ajuste las casillas de verificación correspondientes a la notificación **El motor de detección se actualizó correctamente**.

Para un funcionamiento óptimo, es importante que el programa se actualice automáticamente. Esto solo será posible si se ingresa la **Clave de licencia** correcta en **Ayuda y soporte > Activar el producto**.

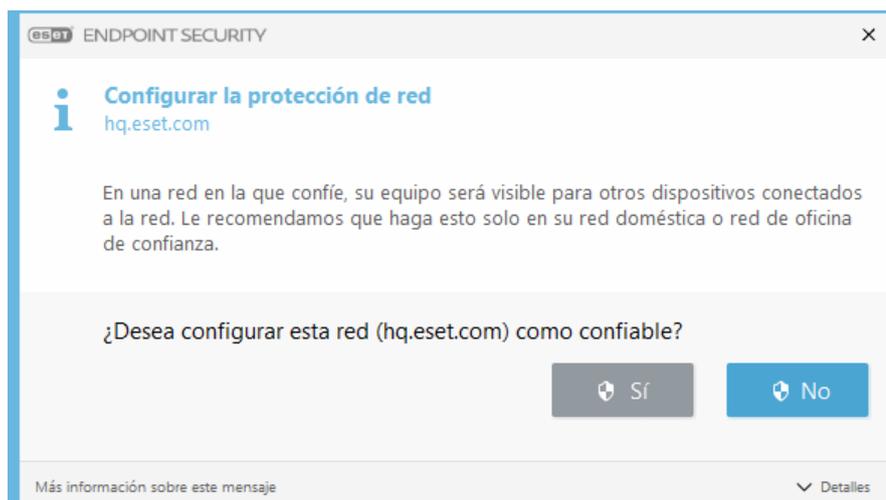
Si no ingresó su **Clave de licencia** luego de la instalación, puede hacerlo en cualquier momento. Para obtener información más detallada acerca de la activación, consulte [Cómo activar ESET Endpoint Security](#) e ingrese las credenciales que recibió con su producto de seguridad ESET en la ventana **Detalles de licencia**.

Configuración de zonas

Es necesario configurar las Zonas de confianza para proteger el equipo en un entorno de red. Puede permitir que otros usuarios accedan a su equipo mediante la configuración de una Zona de confianza a fin de permitir el uso compartido. Haga clic en **Configuración avanzada (F5) > Protección de la red > Firewall > Avanzado > Zonas** para acceder a las configuraciones de las Zonas de confianza.

La detección de la Zona de confianza se realiza luego de la instalación de ESET Endpoint Security y cada vez que el equipo se conecta a una nueva red. Por lo tanto, generalmente no es necesario definir la Zona de confianza. En

forma predeterminada, se muestra una ventana de diálogo al detectar una nueva zona, donde el usuario puede establecer el nivel de protección para dicha zona.



Una configuración incorrecta de la zona de confianza puede constituir un riesgo de seguridad para el equipo.

En forma predeterminada, las estaciones de trabajo de una zona de confianza cuentan con permiso de acceso a los archivos e impresoras compartidos, tienen la comunicación RPC entrante habilitada y tienen disponible el uso compartido del escritorio remoto.

Para obtener más detalles sobre esta característica, lea el siguiente artículo de la base de conocimiento de ESET:

- [Nueva conexión de red detectada ESET Endpoint Security](#)

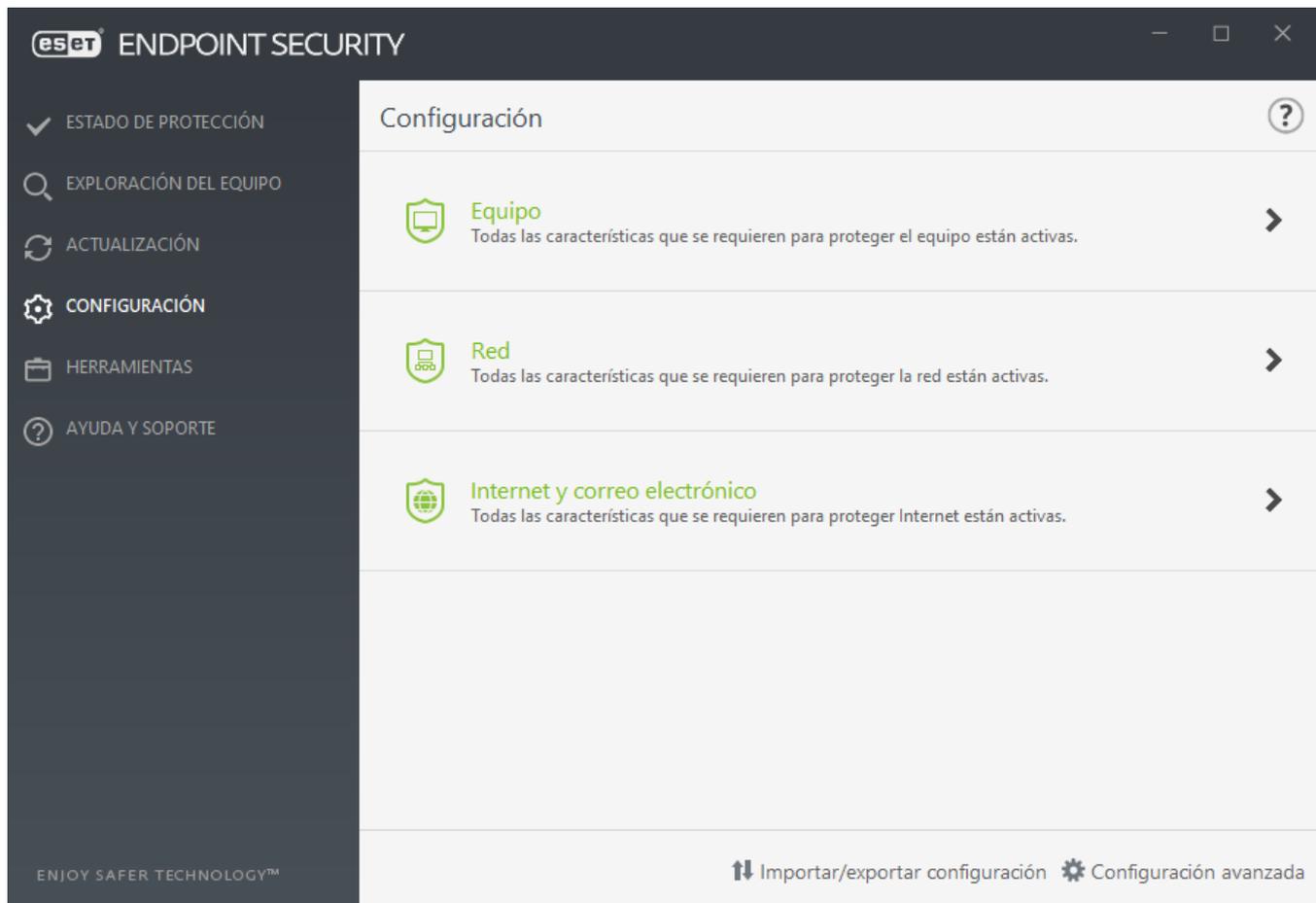
Herramientas de control Web

Si ya habilitó el Control Web en ESET Endpoint Security, debe configurar también el Control Web para las cuentas de usuario que desee con el fin de que funcione correctamente el Control Web. Consulte el capítulo [Control Web](#) para obtener instrucciones acerca de cómo crear restricciones específicas para sus estaciones de trabajo cliente con el fin de protegerlas contra material potencialmente ofensivo.

Trabajar con ESET Endpoint Security

Las opciones de configuración de ESET Endpoint Security le permiten ajustar el nivel de protección para su equipo, Internet, correo electrónico y red.

Cuando cree una política desde la Consola Web de ESET PROTECT o ESET Security Management Center, 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**

La sección Equipo permite habilitar o deshabilitar los siguientes componentes:

- **Protección del sistema de archivos en tiempo real** – Se exploran todos los archivos en busca de códigos maliciosos cuando se abren, crean o ejecutan.
- **Control 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. Obtenga 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](#).

La sección **Protección de la red** le permite configurar el [Firewall](#), la Protección contra ataques a la red (IDS) y la [Protección contra Botnet](#).

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

- **Navegador seguro** – protege sus datos confidenciales durante la navegación por Internet (por ejemplo, datos financieros durante transacciones en línea).
- **Control web** – bloquea las páginas Web que puedan contener material potencialmente ofensivo. Además, los administradores del sistema pueden especificar preferencias de acceso para 27 categorías de sitios Web predefinidos.
- **Protección del acceso a la Web** – si se encuentra habilitada, todo el tráfico que pase a través de HTTP o HTTPS se explora en busca de software malicioso.
- **Protección del cliente de correo electrónico** – monitorea las comunicaciones recibidas a través de los protocolos POP3 e IMAP.
- **Protección antispam** – explora en busca de correo electrónico no solicitado o spam.
- **Protección Anti-Phishing** – Lo protege de sitios web ilegítimos disfrazados de legítimos que intentan obtener contraseñas, datos bancarios y demás información confidencial.

Para deshabilitar temporalmente los módulos individuales, haga clic en el interruptor verde  junto al módulo deseado. Tenga en cuenta que esto puede disminuir el nivel de protección del equipo.

Para volver a habilitar la protección de un componente de seguridad deshabilitado, haga clic en el interruptor rojo  para regresar un componente a su estado de habilitado.

Cuando se aplique la política de ESET PROTECT/ESMC, verá el ícono de candado  al lado de un componente específico. La política aplicada por ESET Security Management Center o 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](#).

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

Para acceder a la configuración detallada para un componente de seguridad específico, haga clic en la rueda de

engranaje  junto a cualquier componente.

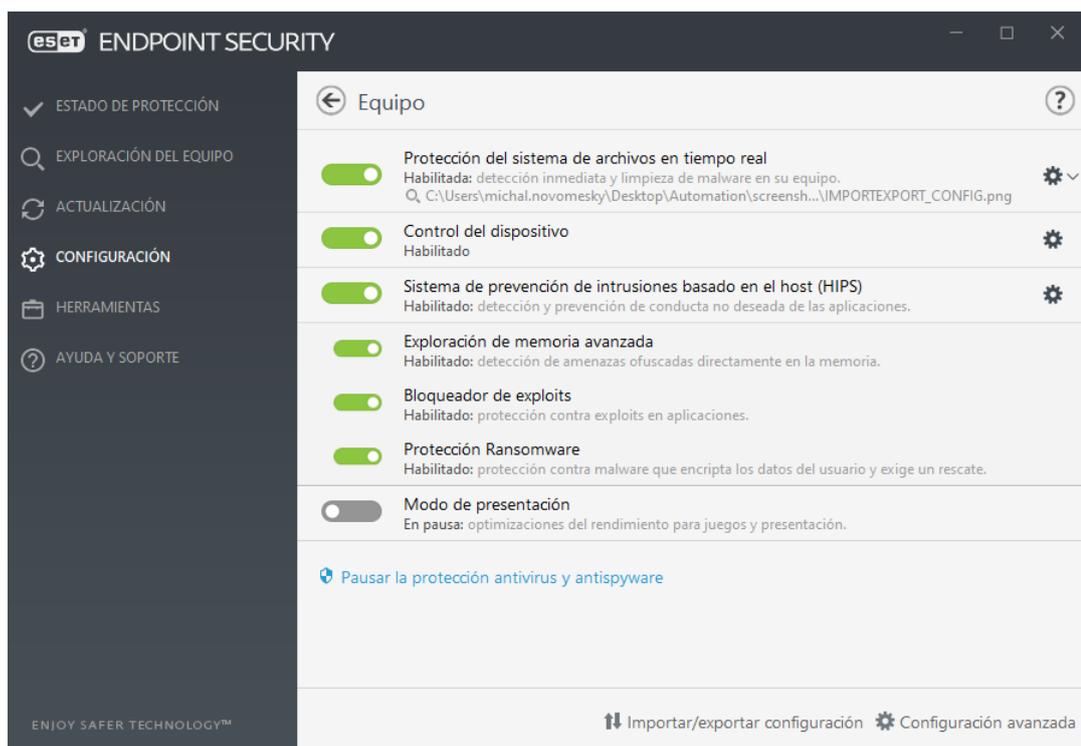
Hay opciones adicionales en la parte inferior de la ventana de configuración. Para cargar los parámetros de configuración mediante un archivo de configuración `.xml` o para guardar los parámetros de configuración actuales en un archivo de configuración, use la opción **Importar/exportar configuración**. Consulte [Importar/Exportar ajustes](#) en busca de información más detallada.

Para ver opciones más detalladas, haga clic en **Configuración avanzada** o presione la tecla **F5**.

Equipo

El módulo **Equipo** se puede encontrar bajo **Configuración > Equipo**. Muestra una vista general de los módulos de protección que se describen en el [capítulo anterior](#). En esta sección, las siguientes configuraciones están disponibles:

Haga clic en la rueda 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**.



La sección **Equipo** permite habilitar o deshabilitar los siguientes componentes:

- **Protección del sistema de archivos en tiempo real** – se exploran todos los archivos en busca de códigos maliciosos cuando se abren, crean o ejecutan en el equipo.
- **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. Obtenga 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**.

Motor de detección

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

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

En esta sección:

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



A partir de la versión 7.2, la sección del motor de detección ya no cuenta con interruptores de ENCENDIDO/APAGADO [como la versión 7.1 y anteriores](#). Los botones de ENCENDIDO/APAGADO han sido reemplazados por cuatro umbrales: Intenso, Balanceado, Cauteloso y Desactivado.

Categorías de protección en tiempo real y con aprendizaje automático

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

- **Malware** – Un virus informático es un código malicioso que puede agregarse al principio o al final de archivos existentes en su ordenador. Sin embargo, el término “virus” suele utilizarse en forma errónea. “Malware” (software malicioso) es un término más preciso. La detección de malware se realiza mediante la combinación del módulo del motor de detección con el componente de aprendizaje automático. Obtenga más información sobre estos tipos de aplicaciones en el [Glosario](#).
- **Aplicaciones potencialmente no deseadas** – Grayware o Aplicación Potencialmente no Deseada (PUA) 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](#).
- **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](#).
- **Aplicaciones sospechosas**: incluyen programas comprimidos con [empaquetadores](#) o protectores. Estos tipos de protectores por lo general son vulnerados por autores de malware para evadir la detección.

ESET ENDPOINT SECURITY

Configuración avanzada

MOTOR DE DETECCIÓN 2

- Protección del sistema de archivos en tiempo real
- Protección basada en la nube
- Exploración de malware

HIPS 2

ACTUALIZACIÓN 2

PROTECCIÓN DE RED

INTERNET Y CORREO ELECTRÓNICO 3

CONTROL DEL DISPOSITIVO 2

HERRAMIENTAS 3

INTERFAZ DEL USUARIO 1

Predeterminada

PROTECCIÓN EN TIEMPO REAL Y CON APRENDIZAJE AUTOMÁTICO

	Intenso	Balance...	Cauteloso	Desactiv...	i
Malware					
Informar	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="button" value="i"/>
Protección	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="button" value="i"/>
Aplicaciones potencialmente no deseadas					
Informar	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="button" value="i"/>
Protección	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="button" value="i"/>
Aplicaciones sospechosas					
Informar	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="button" value="i"/>
Protección	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="button" value="i"/>
Aplicaciones potencialmente no seguras					
Informar	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="button" value="i"/>
Protección	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="button" value="i"/>

Aceptar Cancelar

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

Exploración de malware

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

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 Security.

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

1. Malware
2. Aplicaciones potencialmente no deseadas
3. Potencialmente no seguro
4. Aplicaciones sospechosas

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

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

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

☐ [Disponibilidad de módulos de protección de ESET Endpoint Security](#)

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

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

* Disponibles en ESET Endpoint Security versión 7.2 y posteriores.

** No recomendado

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

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

Notas importantes

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

- El umbral **Balanceado** se recomienda para la mayoría de las configuraciones.
- El umbral **Cauteloso** representa un nivel de protección comparable con el de versiones anteriores de ESET Endpoint Security (versión 7.1 y anteriores). Se recomienda para entornos en los que la prioridad se enfoca en minimizar los objetos identificados en forma errónea por el software de seguridad.
- Mientras más alto sea el umbral de informes, más alta será la tasa de detección pero habrá más probabilidades de objetos identificados en forma errónea.
- Desde el punto de vista del mundo real, no existen garantías de una tasa de detección del 100 % ni tampoco 0 % de probabilidades de evitar la categorización incorrecta de objetos no infectados como malware.
- [Mantenga actualizados ESET Endpoint Security y sus módulos](#) para maximizar el equilibrio entre desempeño, precisión de tasas de detección y cantidad de objetos informados en forma errónea.

Configuración de protección

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

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

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

[Cuadro de conversión de política de ESET PROTECT para ESET Endpoint Security versión 7.1 y anteriores](#)

Desde ESET PROTECT, el editor de política para la configuración del explorador ya no contiene interruptores de ENCENDIDO/APAGADO para cada CATEGORÍA. A continuación se incluye un cuadro que detalla la conversión entre el umbral de protección y el estado final del [interruptor en ESET Endpoint Security versión 7.1 y anteriores](#).

Estado de umbral de CATEGORÍA	Intenso	Balanceado	Cauteloso	Desactivado
-------------------------------	---------	------------	-----------	-------------

Interruptor de CATEGORÍA aplicado	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/> x
-----------------------------------	-------------------------------------	-------------------------------------	-------------------------------------	----------------------------

Al actualizar desde la versión 7.1 y anteriores a la versión 7.2 y posteriores, el nuevo estado del umbral será el siguiente:

Interruptor de categoría antes de la actualización	<input checked="" type="checkbox"/>	<input type="checkbox"/> x
Nuevo umbral de CATEGORÍA después de la actualización	Balanceado	Desactivado

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 Security.
- 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.

Opciones avanzadas del motor de detección

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

Activar exploración avanzada mediante AMSI – la herramienta Microsoft Antimalware Scan Interface que permite a los desarrolladores de las aplicaciones habilitar nuevas defensas de malware (solo Windows 10).

Infiltración detectada

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

Conducta estándar

Como ejemplo general de la forma en que ESET Endpoint Security 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](#)

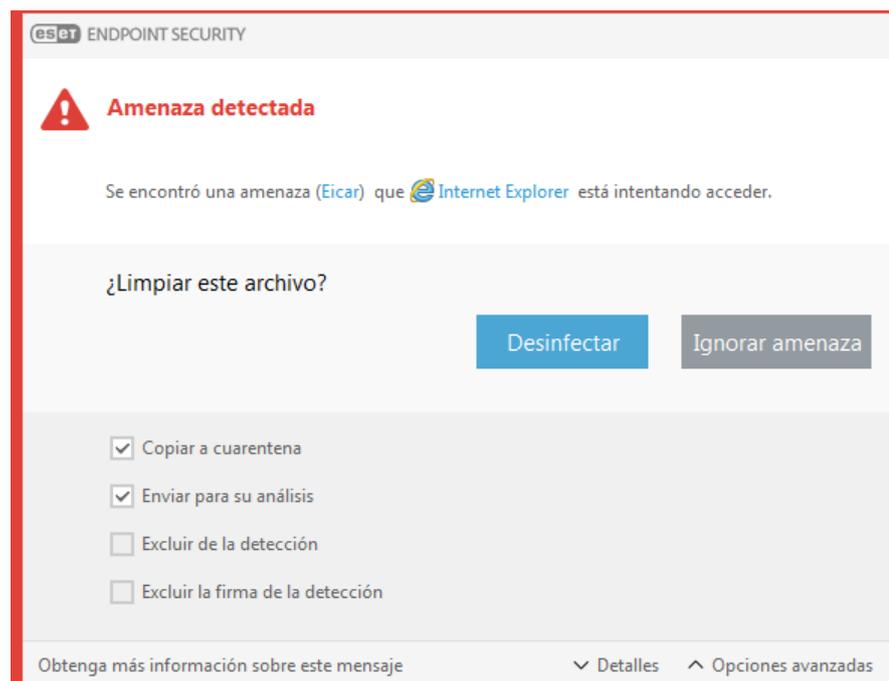
Cada uno utiliza el nivel de desinfección estándar e intentará desinfectar el archivo y moverlo a [Cuarentena](#) o finalizar la conexión. Una ventana de notificación se muestra en el área de notificaciones en la esquina inferior derecha de la pantalla. Para obtener información detallada sobre los objetos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

Caché local compartido

El caché local compartido puede incrementar el rendimiento en entornos aislados (p. ej., máquinas virtuales) al eliminar la exploración duplicada en la red. Esto garantiza que cada archivo solo se explorará una vez y se almacenará en el caché compartido.

Primero debe instalar y configurar ESET Shared Local Cache.

- [Descargar ESET Shared Local Cache](#).
- Para obtener más información, consulte el [Ayuda en línea de ESET Shared Local Cache](#).

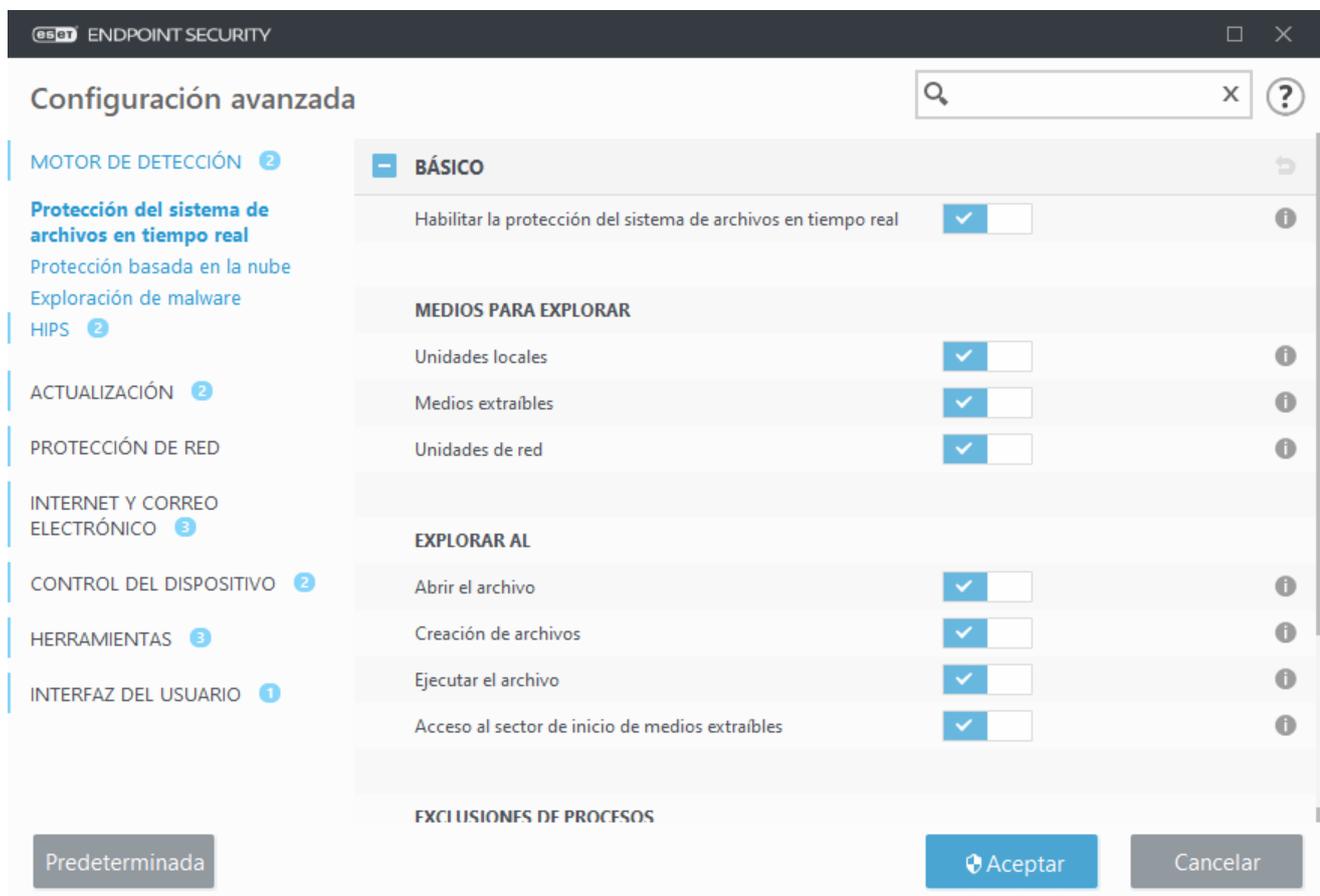
Encienda el interruptor de **Habilitar caché local** para guardar información sobre la exploración de archivos y carpetas de su red en ESET Shared Local Cache. Si realiza una exploración, ESET Endpoint Security buscará archivos explorados en ESET Shared Local Cache. Si los archivos coinciden, no se incluirán en la exploración.

La configuración del **Servidor del caché** contiene lo siguiente:

- **Nombre de host** – Nombre de host o dirección IP del equipo en el que se aloja ESET Shared Local Cache.
- **Puerto** – Número del puerto que se utiliza para la comunicación (el mismo que se configuró en ESET Shared Local Cache).
- **Contraseña** – Especifica la contraseña para ESET Shared Local Cache de ser necesario.

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 abrirlos, crearlos o ejecutarlos.



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

Medios para explorar

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

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

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

Explorar al

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

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

Procesos que no se explorarán – Lea más sobre este tipo de exclusión en el capítulo [Exclusiones de procesos](#).

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

Para asegurar el mínimo impacto en el sistema al usar la protección en tiempo real, los archivos que ya se exploraron no se vuelven a explorar reiteradamente (a menos que se hayan modificado). Se exploran los archivos nuevamente inmediatamente después de cada actualización del motor de detección. Este comportamiento se controla mediante el uso de la **Optimización inteligente**. Si se deshabilita esta **Optimización inteligente**, se exploran todos los archivos cada vez que se accede a los mismos. Si desea modificar esta configuración, presione la tecla **F5** para abrir la Configuración avanzada y expanda **Motor de detección > Protección del sistema de archivos en tiempo real**. Haga clic en **Parámetros de ThreatSense > Otros** y seleccione o anule la selección de **Habilitar la optimización inteligente**.

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.

Cuándo modificar la configuración de la protección en tiempo real

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

Luego de la instalación de ESET Endpoint Security, todas las configuraciones se optimizan para proporcionar el máximo nivel de seguridad del sistema para los usuarios. Para restaurar la configuración predeterminada, haga clic  al lado de cada pestaña en la ventana (**Configuración avanzada > Motor de detección > Protección del sistema de archivos en tiempo real**).

Qué hacer si la protección en tiempo real no funciona

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

La protección en tiempo real está deshabilitada

Si un usuario desactiva la protección en tiempo real sin darse cuenta, debe reactivar la función. Para reactivar la protección en tiempo real, vaya a **Configuración** en la ventana principal del programa y haga clic en **Protección del equipo > Protección del sistema de archivos en tiempo real**.

Si la protección en tiempo real no se activa durante el inicio del sistema, es posible que se deba a que **Habilitar la protección del sistema de archivos en tiempo real** está deshabilitada. Para asegurarse de que esta opción esté habilitada, vaya a **Configuración avanzada (F5)** y haga clic en **Motor de detección > Protección del sistema de archivos en tiempo real**.

Si la protección en tiempo real no detecta ni desinfecta infiltraciones

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

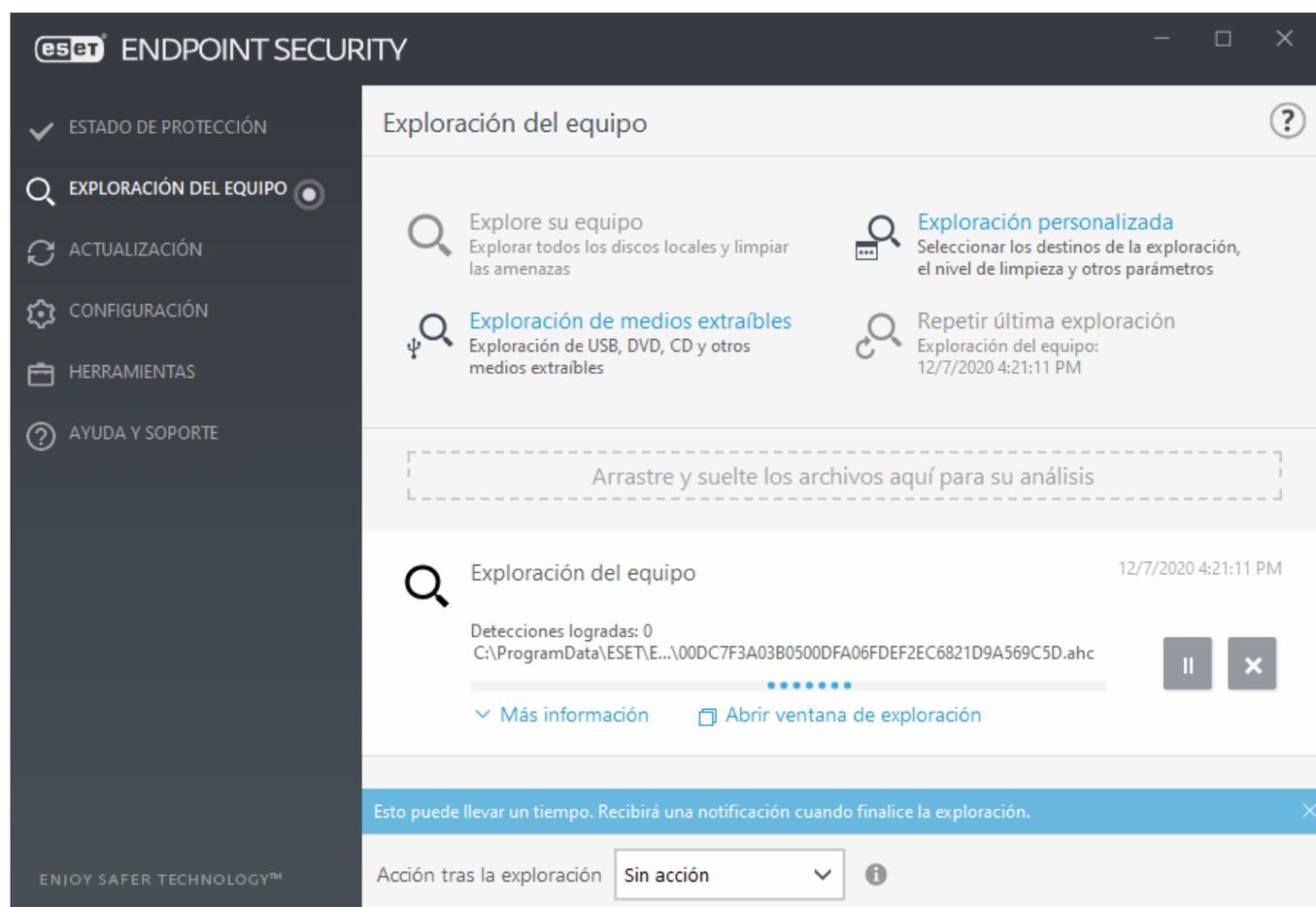
La protección en tiempo real no se inicia

Si la protección en tiempo real no se activa al iniciar el sistema (y está activada la opción **Activar protección del sistema de archivos en tiempo real**), es posible que se deba a conflictos con otros programas. Para obtener ayuda a fin de resolver este problema, póngase en contacto con el soporte técnico de ESET. La creación de un registro de SysInspector y su envío al Soporte técnico de ESET para su análisis puede ayudar a solucionar el problema. Para obtener más información, lea el siguiente artículo de la [base de conocimiento de ESET](#).

Exploración del equipo

El módulo de exploración bajo demanda es una parte importante de ESET Endpoint Security. 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

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

Exploración personalizada

La exploración personalizada es una solución ideal si desea especificar los parámetros de exploración, tales como los objetos para explorar y los métodos de exploración. La ventaja de la exploración personalizada es la capacidad de configurar los parámetros detalladamente. Es posible guardar las configuraciones en perfiles de exploración definidos por el usuario, lo que resulta útil si la exploración se efectúa reiteradamente con el uso de los mismos parámetros.

Para elegir los objetos para explorar, seleccione **Exploración del equipo > Exploración personalizada** y seleccione una opción en el menú desplegable **Objetos para explorar** o seleccione objetos específicos desde la estructura con forma de árbol. El objeto para explorar también puede definirse mediante el ingreso de la ruta de las carpetas o archivos que desea incluir. Si solo le interesa explorar el sistema sin realizar acciones adicionales de desinfección, seleccione **Explorar sin desinfectar**. Al realizar una exploración, puede elegir tres niveles de desinfección mediante un clic en **Configuración > Parámetros ThreatSense > Desinfección**.

La opción de realizar exploraciones del equipo mediante la Exploración personalizada es apropiada para usuarios avanzados con experiencia previa en la utilización de programas antivirus.

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.

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.

Puede seleccionar **Ninguna acción**, **Apagar**, **Reiniciar** o **Reiniciar en caso de ser necesario** del menú desplegable **Acción tras la exploración**. Las acciones **Suspender** o **Hibernar** están disponibles según la configuración de energía del sistema operativo de su equipo o las capacidades del equipo/equipo portátil. La acción seleccionada comenzará tras finalizar las exploraciones en ejecución. Cuando selecciona **Apagar**, se mostrará una ventana de diálogo de confirmación del apagado con una cuenta regresiva de 30 segundos (haga clic en **Cancelar** para desactivar el apagado solicitado). Consulte [Opciones avanzadas de exploración](#) para obtener más información.

 Se recomienda ejecutar una exploración del equipo al menos una vez al mes. La exploración se puede configurar como una tarea programada desde **Herramientas > Tareas programadas**. [¿Cómo programo una exploración semanal del equipo?](#)



Iniciador de la exploración personalizada

Si solo desea explorar un objeto específico, puede usar la herramienta de Exploración personalizada al hacer clic en **Exploración del equipo** > **Exploración personalizada** y, luego, seleccione una opción del menú desplegable  > **Objetos para explorar**, o bien seleccione los objetos específicos desde la estructura (de árbol) de la carpeta.

La ventana de objetos para explorar le permite definir qué objetos (memoria, unidades, sectores, archivos y carpetas) se exploran en busca de infiltraciones.

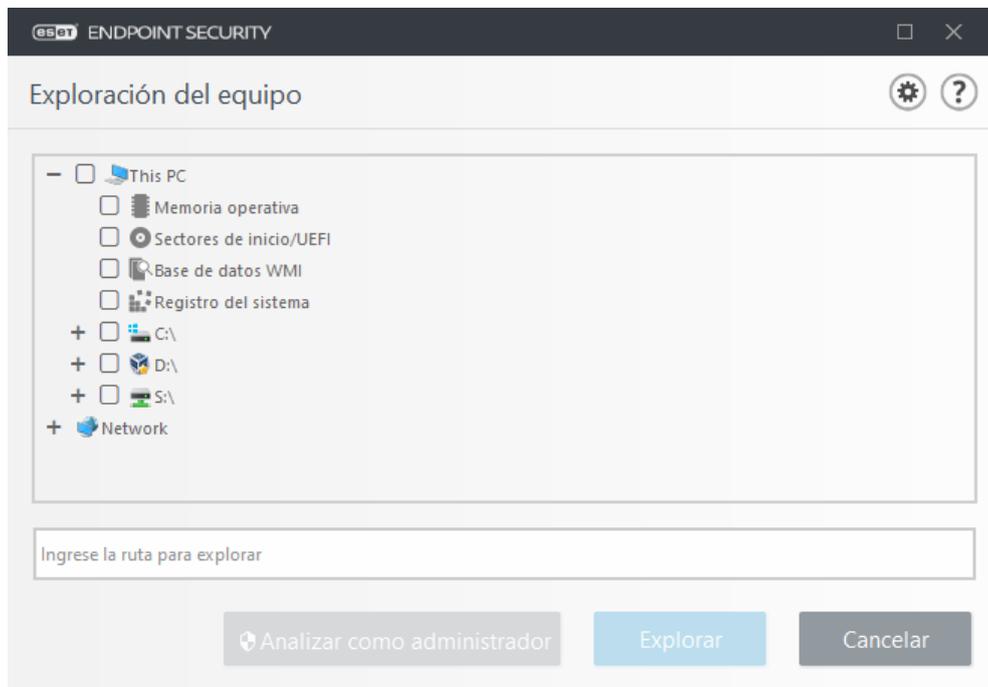
El menú desplegable **Objetos para explorar** permite seleccionar los objetos predefinidos que se explorarán.

- **Por configuración de perfil:** selecciona los objetos especificados en el perfil de exploración seleccionado.
- **Medios extraíbles** – selecciona disquetes, dispositivos de almacenamiento USB, CD, DVD.
- **Unidades locales** – selecciona todos los discos rígidos del sistema.
- **Unidades de red** – selecciona todas las unidades de red asignadas.
- **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 referencia 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 hasta un objeto para explorar o para agregar carpetas o archivos de destino, ingrese e directorio de destino en el campo vacío debajo de la lista de carpetas.



Los elementos infectados no se desinfectan automáticamente. Puede usar la exploración sin desinfección cuando desee obtener una visión general del estado actual de la protección. Además, puede elegir entre tres niveles de desinfección al hacer clic en **Configuración avanzada > Motor de detección > Exploración bajo demanda > Parámetros de ThreatSense > Desinfección**. Si solo le interesa explorar el sistema sin realizar acciones adicionales de desinfección, seleccione **Explorar sin desinfectar**. El historial de exploraciones se guarda en el registro de exploraciones.

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

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

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

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.

Exploración del equipo ?

8/15/2018 7:18:10 PM

 Amenazas detectadas: 0
C:\Documents and Settings\John\Desktop\7.0.2074\ees_nt64.exe

|| X

[^ Menos información](#)

Usuario: John-PC\John
Objetos explorados: 5435
Duración: 0:00:30

C:\Documents and Settings\All Users\Microsoft\Crypto\RSA\MachineKeys\905f6e1d2cc2166bc55cce340c0a622d_a110f29a-833e-446a-bfdb-195863caba6e - no se ...

C:\Documents and Settings\All Users\Microsoft\Crypto\RSA\MachineKeys\ade8d9c0a1372972e71c3366525ec64c_a110f29a-833e-446a-bfdb-195863caba6e - no se...

C:\Documents and Settings\All Users\Microsoft\Crypto\RSA\MachineKeys\c3a84c6dd0bf0eb5da5d84a4742f6f35_a110f29a-833e-446a-bfdb-195863caba6e - no se...

C:\Documents and Settings\All Users\Microsoft\Crypto\RSA\MachineKeys\dc558a410ecc71a25c9884a937c89d6e_a110f29a-833e-446a-bfdb-195863caba6e - no se...

C:\Documents and Settings\All Users\Microsoft\Crypto\RSA\MachineKeys\ee0066ce8768d9c2afe613dcf61232c8_a110f29a-833e-446a-bfdb-195863caba6e - no se ...

C:\Documents and Settings\All Users\Microsoft\Crypto\RSA\MachineKeys\ef73ed1b2f5151d2486cbcc4721be893_a110f29a-833e-446a-bfdb-195863caba6e - no se...

C:\Documents and Settings\All Users\Microsoft\Crypto\RSA\MachineKeys\f080183c2cf12a3df6bcl8a14723fdb_a110f29a-833e-446a-bfdb-195863caba6e - no se ...

C:\Documents and Settings\All Users\Microsoft\Diagnosis\DownloadedSettings\telemetry.ASM-WindowsDefault.json - no se puede abrir [4]

C:\Documents and Settings\All Users\Microsoft\Diagnosis\DownloadedSettings\utc.app.json - no se puede abrir [4]

C:\Documents and Settings\All Users\Microsoft\Diagnosis\events00.rbs - no se puede abrir [4]

C:\Documents and Settings\All Users\Microsoft\Diagnosis\events01.rbs - no se puede abrir [4]

C:\Documents and Settings\All Users\Microsoft\Diagnosis\events10.rbs - no se puede abrir [4]

C:\Documents and Settings\All Users\Microsoft\Diagnosis\events11.rbs - no se puede abrir [4]

Desplazarse por el registro de exploración Cerrar

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.

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

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

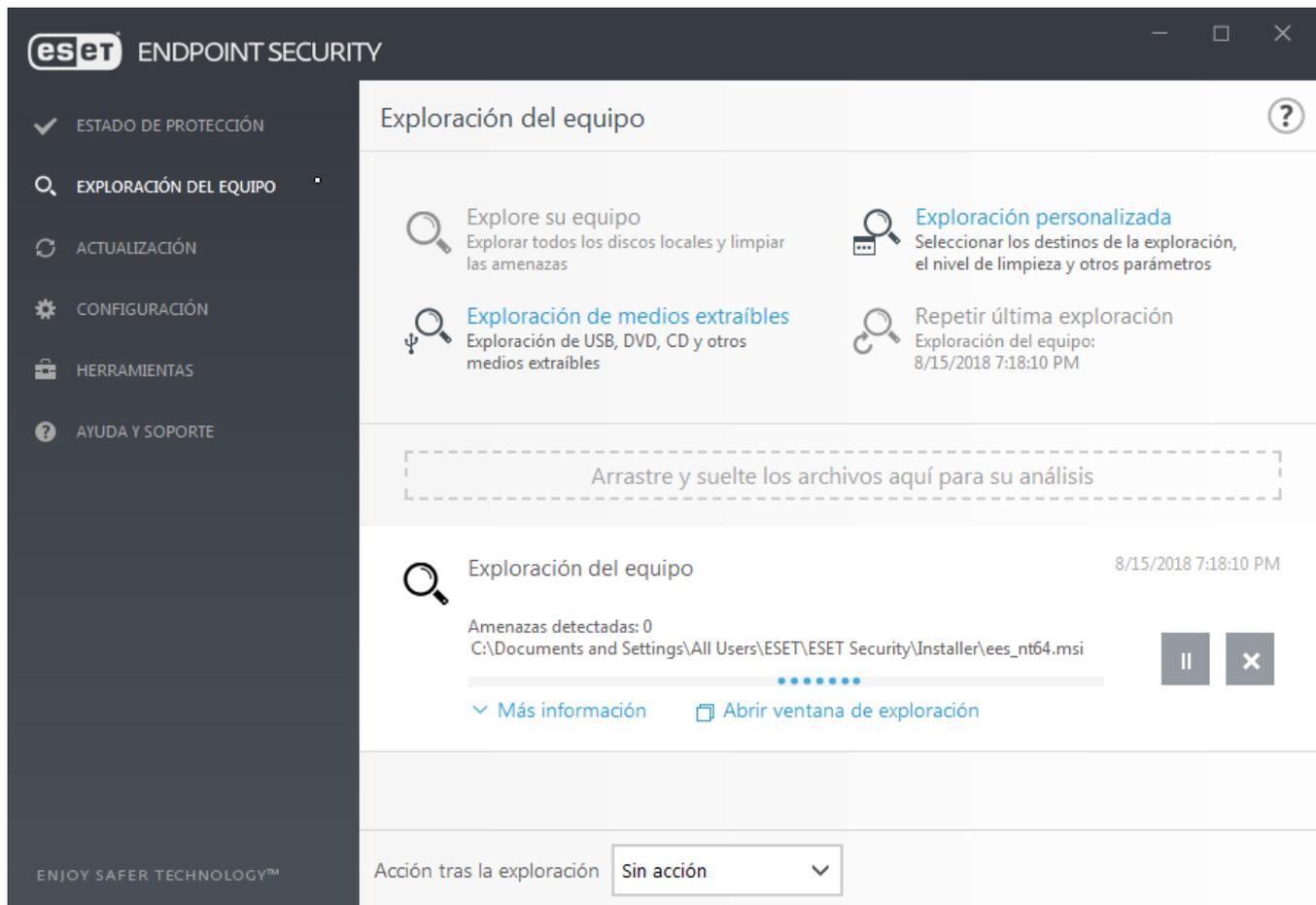
Amenazas encontradas – muestra el número total de amenazas encontradas durante una exploración.

Pausar – pone una exploración en pausa.

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

Detener – finaliza la exploración.

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



Registro de exploración del equipo

El [registro de exploración del equipo](#) le brinda información general de la exploración, como:

- Fecha y hora de la exploración
- Discos, carpetas y archivos explorados
- Cantidad de objetos explorados
- Cantidad de amenazas detectadas
- Hora de finalización
- Tiempo total de exploración

Exploración de malware

Es posible acceder a la sección **Exploración de malware** desde el menú de configuración avanzada. Presione la tecla **F5**, haga clic en **Motor de detección > Exploración de malware** y allí obtendrá opciones para seleccionar los parámetros de exploración. Esta sección incluye las siguientes opciones:

- **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.

- **Protección de acuerdo a las necesidades y con aprendizaje automático** – Consulte [Motor de detección \(versión 7.2 y posteriores\)](#).
- **Destinos de exploración**: si solo desea explorar un objeto específico, puede hacer clic en **Editar** junto a **Destinos de exploración** y elegir una opción del menú desplegable o puede seleccionar los objetos específicos desde la estructura (de árbol) de la carpeta. Consulte [Destinos de exploración](#) para obtener información detallada.
- **Parámetros de ThreatSense**: en esta sección se encuentran las opciones de configuración avanzada, tales como las extensiones de los archivos que desea controlar, los métodos de detección utilizados, etc. Haga clic para abrir una pestaña con las opciones avanzadas del explorador.

Exploración en estado inactivo

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

Exploración en estado inactivo

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

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

Encienda el interruptor **Habilitar registro** en la Configuración avanzada para registrar el resultado de la exploración del equipo en la sección [Archivos de registro](#) (desde la ventana principal del programa haga clic en **Herramientas > Archivos de registro** y seleccione **Exploración del equipo** en el menú desplegable **Registro**).

Detección en estado inactivo

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

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

Perfiles de exploración

Hay cuatro perfiles de exploración predefinidos en ESET Endpoint Security:

- **Análisis inteligente** – Es el perfil de exploración avanzada predeterminado. El perfil de análisis inteligente utiliza la tecnología de optimización inteligente, que excluye los archivos que se encontraron limpios en una exploración anterior y que no se han modificado desde esa exploración. Esto permite tener tiempos de exploración más bajos con un impacto mínimo en la seguridad del sistema.
- **Exploración del menú contextual** – Puede iniciar la exploración del menú contextual de cualquier archivo desde el menú contextual. El perfil de exploración del menú contextual le permite definir una configuración

de exploración que se utilizará cuando se ejecuta la exploración de esta manera.

- **Exploración exhaustiva** – El perfil de exploración exhaustiva no utiliza la optimización inteligente de forma predeterminada, por lo que no se excluye ningún archivo de la exploración mediante este perfil.
- **Exploración del equipo** – Es el perfil predeterminado utilizado en la exploración estándar del equipo.

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

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

i Suponga que desea crear su propio perfil de exploración y la configuración de **Explore su equipo** es parcialmente adecuada, pero no desea explorar [empaquetadores en tiempo real](#) o [aplicaciones potencialmente no seguras](#) y, además, quiere aplicar una **Desinfección estricta**. 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

La ventana de objetos para explorar le permite definir qué objetos (memoria, unidades, sectores, archivos y carpetas) se exploran en busca de infiltraciones.

El menú desplegable **Objetos para explorar** permite seleccionar los objetos predefinidos que se explorarán.

- **Por configuración de perfil:** selecciona los objetos especificados en el perfil de exploración seleccionado.
- **Medios extraíbles** – selecciona disquetes, dispositivos de almacenamiento USB, CD, DVD.
- **Unidades locales** – selecciona todos los discos rígidos del sistema.
- **Unidades de red** – selecciona todas las unidades de red asignadas.
- **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 referencia 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 hasta un objeto para explorar o para agregar carpetas o archivos de destino, ingrese e directorio de destino en el campo vacío debajo de la lista de carpetas.

Opciones avanzadas de exploración

En esta ventana puede especificar las opciones avanzadas para una tarea de exploración del equipo programado. Puede configurar una acción para que se lleve a cabo automáticamente después de la finalización de la exploración mediante el menú desplegable:

- **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:** cierra todos los programas abiertos y reinicia el equipo si lo requiere el análisis.
- **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.
- **Sin acción** – después de la finalización de la exploración, no se llevará a cabo ninguna acción.

i Tenga en cuenta que un equipo en suspensión aún es un equipo en funcionamiento. Aún ejecuta las funciones básicas y utiliza electricidad cuando funciona con la energía de la batería. Para preservar la vida útil de la batería, como cuando viaja fuera de su oficina, recomendamos utilizar la opción Hibernar.

Seleccione **El usuario no puede cancelar la acción** para denegarles a los usuarios sin privilegios la capacidad de detener las medidas que se tomaron 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.

También consulte el capítulo [Progreso de la exploración](#).

Control del dispositivo

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

Dispositivos externos admitidos:

- Almacenamiento en discoHDD, disco extraíble USB)
- CD/DVD
- impresora USB
- FireWire Almacenamiento
- Dispositivo Bluetooth
- Lector de tarjeta inteligente
- Dispositivo de imagen
- Módem
- LPT/COM puerto
- Dispositivo portátil
- Todos los tipos de dispositivos

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

Al encender el interruptor ubicado junto a **Habilitar control del dispositivo**, se activa la característica de Control del dispositivo en ESET Endpoint Security; necesitará reiniciar su equipo para que se aplique este cambio. Una vez que se habilita el Control del dispositivo, se activarán las **Reglas**, lo cual le permite abrir la ventana [Editor de reglas](#).

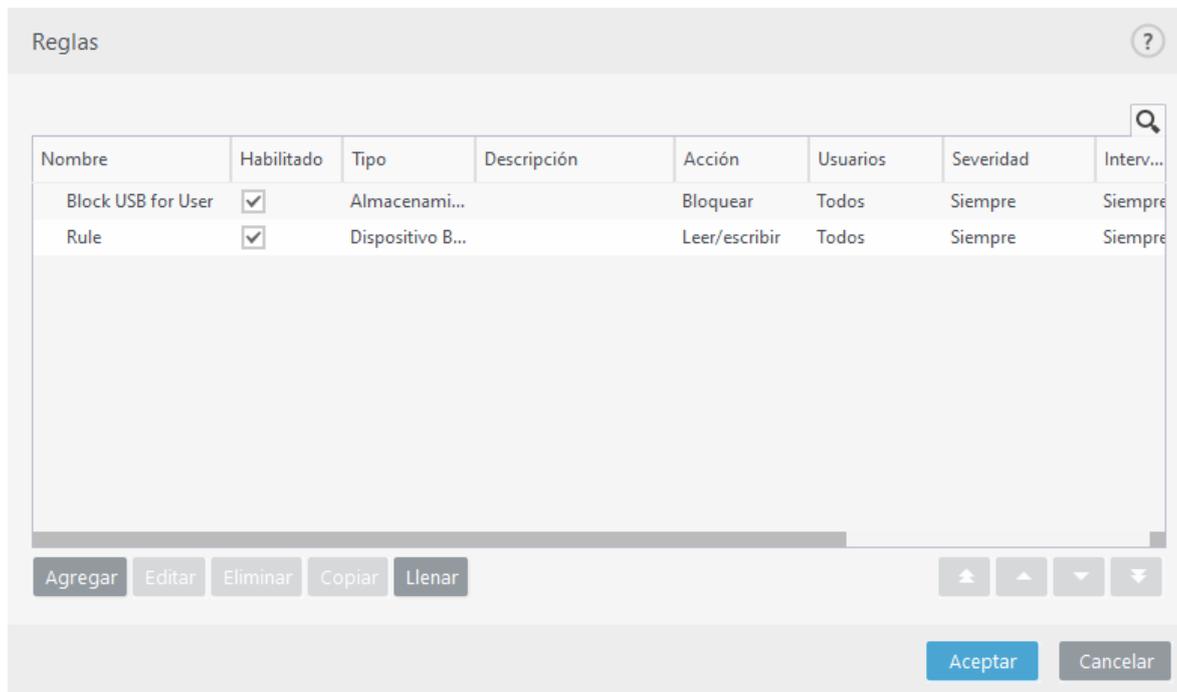
Si se inserta un dispositivo bloqueado por una regla existente, se visualizará una ventana de notificación y no se otorgará el acceso al dispositivo.

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. Consulte también [Agregar reglas del control del dispositivo](#).

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 Security 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).

Si se selecciona un dispositivo (en la lista de Dispositivos detectados) y se hace clic en **Aceptar**, aparece una ventana del editor de reglas con información predefinida (se pueden ajustar todas las configuraciones).

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 con una lista de dispositivos que desee visualizar 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 haciendo clic en **ACEPTAR**.

Elementos de control

Agregar – puede agregar un grupo al ingresar su nombre, o un dispositivo a un grupo existente (de manera opcional, puede especificar detalles como nombre del proveedor, modelo y número de serie), dependiendo de la parte de la ventana en la que ha hecho 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 debe comenzar 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).

Cuando haya finalizado la personalización, haga clic en **Aceptar**. Haga clic en **Cancelar** si desea salir de la ventana **Grupos de dispositivos** sin guardar los cambios.

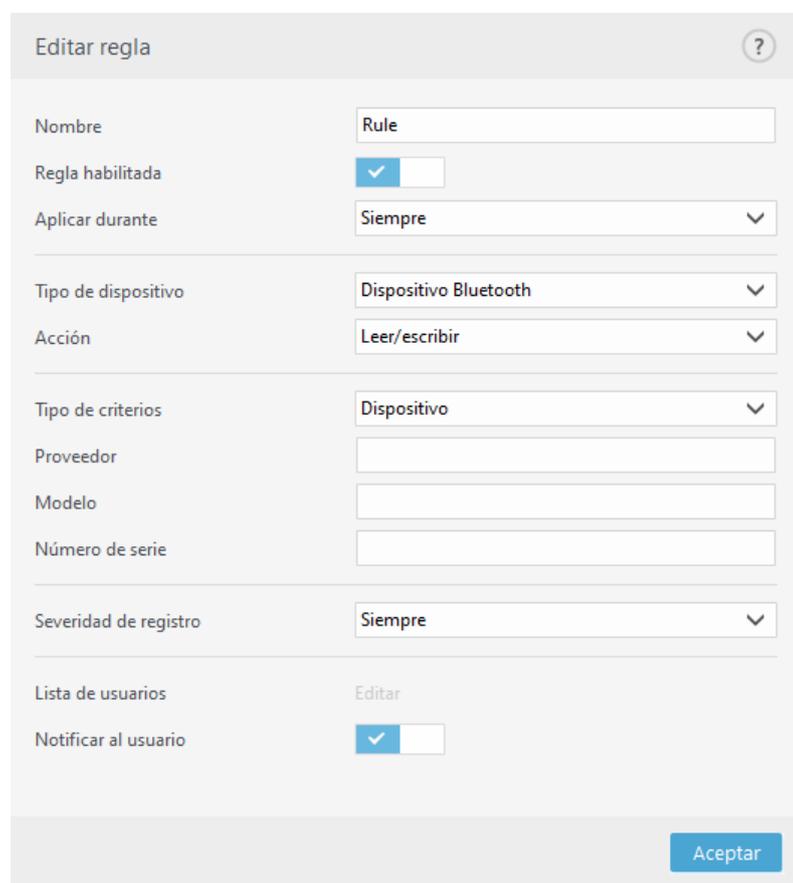
 Puede crear distintos grupos de dispositivos para los que se aplicarán reglas diferentes. También puede crear solo un grupo de dispositivos para el que se aplicará la regla con la acción **Lectura/Escritura** o **Solo lectura**. Esto garantiza que el Control de dispositivos bloquee los dispositivos no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

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, **Solo lectura** no está disponible para Bluetooth, por lo que los dispositivos Bluetooth solo se pueden permitir, bloquear o advertir).

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.



Editar regla ?

Nombre	<input type="text" value="Rule"/>
Regla habilitada	<input checked="" type="checkbox"/>
Aplicar durante	<input type="text" value="Siempre"/>
Tipo de dispositivo	<input type="text" value="Dispositivo Bluetooth"/>
Acción	<input type="text" value="Leer/escribir"/>
Tipo de criterios	<input type="text" value="Dispositivo"/>
Proveedor	<input type="text"/>
Modelo	<input type="text"/>
Número de serie	<input type="text"/>
Severidad de registro	<input type="text" value="Siempre"/>
Lista de usuarios	<input type="text" value="Editar"/>
Notificar al usuario	<input checked="" type="checkbox"/>

Ingrese 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. Obtenga más información [sobre los 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:

- **Lectura/escritura** – se permitirá el acceso total al dispositivo.
- **Bloquear** – se bloqueará el acceso al dispositivo.
- **Solo lectura** – 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, **Solo lectura** 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**.

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

- **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.

i Si no se definen estos parámetros, la regla ignorará estos campos mientras realiza la coincidencia. Los parámetros de filtrado en todos los campos de texto no distinguen mayúsculas de minúsculas y no aceptan caracteres globales (*, ?).

i 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.

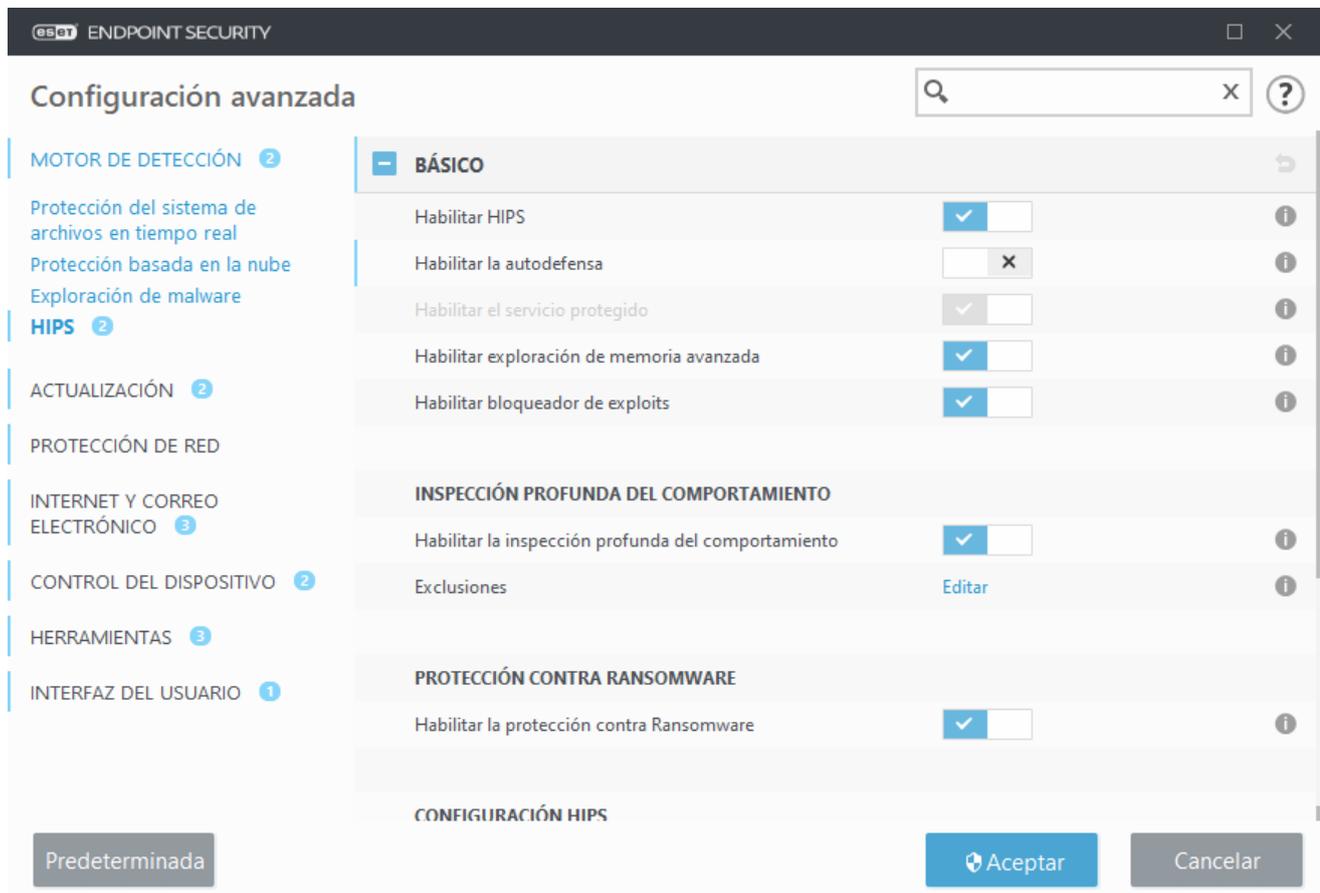
 No todos los dispositivos se pueden filtrar por reglas del usuario, (por ejemplo: los dispositivos de imagen no proporcionan información sobre usuarios, únicamente sobre acciones).

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

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

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

La configuración de HIPS se puede encontrar en **Configuración avanzada (F5) > Motor de detección > HIPS > Básico**. El estado de HIPS (habilitado/deshabilitado) se muestra en la ventana principal del programa de ESET Endpoint Security, en **Configuración > Equipo**.



Básico

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

Habilitar la autodefensa: ESET Endpoint Security 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 los procesos cruciales del sistema y de ESET, las claves de registro y los archivos contra la posibilidad 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. Obtenga 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 sobre este tipo de protección aquí.](#)

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 Security. Esta opción está disponible solo en ESET PROTECT o en el editor de configuración de la política de ESMC.

Configuración HIPS

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

Modo de filtrado	Descripción
Modo automático	Las operaciones están habilitadas, excepto las que se encuentran bloqueadas por las reglas predefinidas que protegen su sistema.
Modo inteligente	Se notificará al usuario solo en caso de eventos muy sospechosos.
Modo interactivo	El programa le solicitará al usuario que confirme las operaciones.
Modo basado en políticas	Bloquea todas las operaciones que no están definidas por una regla específica que las permite.
Modo de aprendizaje	Las operaciones están habilitadas y se crea una regla luego de cada operación. Las reglas creadas en este modo se pueden ver en el editor de reglas HIPS , pero su prioridad es inferior a la de las reglas creadas manualmente o en el modo automático. Cuando selecciona el Modo de aprendizaje en el menú desplegable Modo de filtrado , la configuración del modo de aprendizaje finalizará cuando esté disponible. Seleccione el intervalo de tiempo durante el que desea activar el modo de aprendizaje; el tiempo máximo es de 14 días. Cuando el tiempo especificado haya pasado, se le solicitará que edite las reglas creadas por HIPS mientras estuvo en el modo de aprendizaje. También puede elegir un modo de filtrado diferente, o posponer la decisión y continuar utilizando el modo de aprendizaje.

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

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

Ventana interactiva de HIPS

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

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

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

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

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

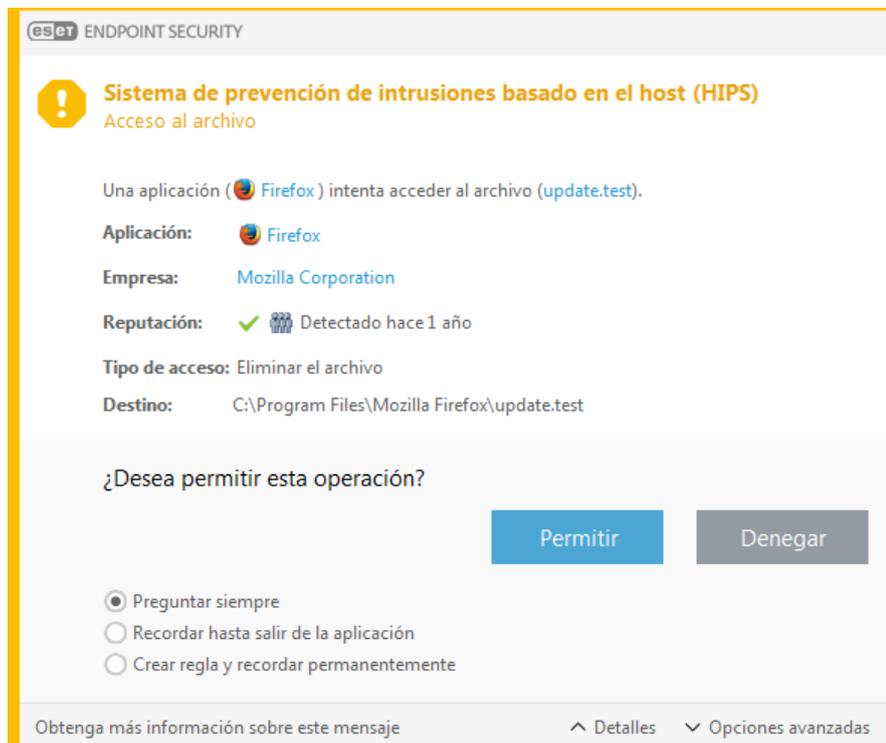
Haga clic en **Detalles** al pie para ver qué aplicación activa la operación, cuál es la reputación del archivo o qué tipo de operación se le pide autorizar o rechazar.

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

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



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



Se detectó un comportamiento ransomware potencial

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

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

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

Administración de reglas del HIPS

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 del HIPS](#) Consulte también [Principios generales del 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 emergente pequeña en la esquina inferior derecha.

Elementos de control

Agregar – crea una regla nueva.

Editar – le permite editar las entradas seleccionadas.

Quitar – quita las entradas seleccionadas.

Prioridad para reglas del HIPS

No hay opciones para ajustar el nivel de prioridad de las reglas del HIPS utilizando los botones arriba/abajo (como las [reglas de firewall](#) que se ejecutan desde arriba hacia 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 este interruptor 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 – cuando se acciona un suceso, aparece una ventana emergente pequeña en la esquina inferior derecha.

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

Aplicaciones de origen—la regla solo se utilizará si esta aplicación o estas aplicaciones accionan el evento.

Seleccione **Aplicaciones específicas** en el menú desplegable y haga clic en **Agregar** para agregar archivos nuevos, o puede seleccionar **Todas las aplicaciones** en el menú desplegable para agregar todas las aplicaciones.

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

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

Entradas de registro– la regla solo se utilizará si la operación está relacionada con este destino. Seleccione **Entradas específicas** en el menú desplegable y haga clic en **Agregar** para 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.

i No es posible interceptar las operaciones del proceso en la versión de 64 bits de Windows XP.

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.

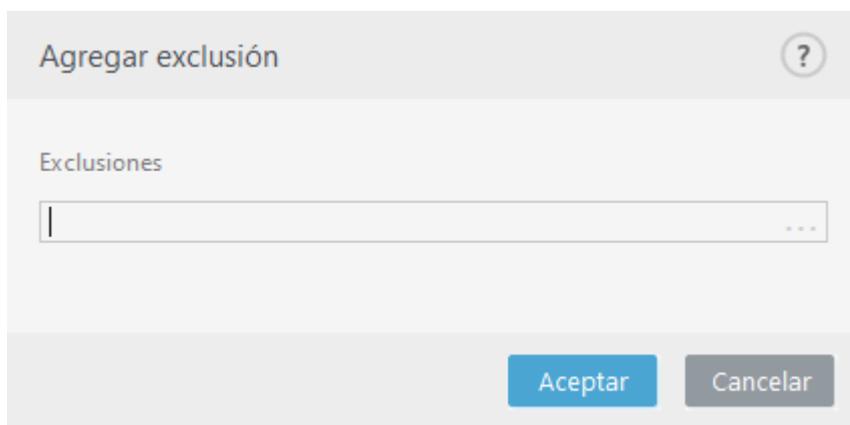
i Crear reglas dirigidas a la clave HKEY_CURRENT_USER

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.



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 del sistema HIPS.

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.

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 emergentes 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. Cuando está habilitado, todas las ventanas emergentes se deshabilitan y las tareas programadas no se ejecutan. La protección del sistema seguirá ejecutándose en segundo plano, pero no requerirá ninguna interacción por parte del usuario.

Haga clic en **Configuración > Equipo** y luego en el interruptor junto al **Modo de presentación para habilitar el modo de presentación en forma manual**. En **Configuración avanzada (F5)**, haga clic en **Herramientas > Modo de presentación** y, luego, haga clic en el interruptor junto a **Habilitar el modo de presentación automáticamente al ejecutar aplicaciones en modo de pantalla completa para que ESET Endpoint Security active en forma automática el modo de presentación cuando se ejecutan las aplicaciones de pantalla completa**. 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 habilitado** aparecerá en naranja.

Cuando **Habilitar el modo de presentación automáticamente al ejecutar aplicaciones de pantalla completa está activo**, el modo de presentación se iniciará siempre que abra una aplicación de pantalla completa y se detendrá automáticamente después de que salga de la aplicación. Es útil, en especial, para iniciar el modo de presentación inmediatamente luego de empezar un juego, abrir una aplicación de pantalla completa o iniciar una presentación.

También puede seleccionar **Deshabilitar el modo de presentación automáticamente después de** para definir la cantidad de tiempo en minutos luego de la cual el modo de presentación se deshabilitará automáticamente.

i Si el Firewall está en el modo interactivo y el modo de presentación se encuentra habilitado, quizá surjan inconvenientes para conectarse a Internet. Esto puede ocasionar problemas si comienza un juego que se conecta a Internet. Bajo circunstancias normales, el programa le solicitaría que confirme dicha acción (si no se definió ninguna regla o excepción para la comunicación); pero en el modo de presentación, la interacción del usuario está deshabilitada. La solución es definir una regla de comunicación para cada aplicación que pueda entrar en conflicto con esta conducta o usar un [Modo de filtrado](#) diferente en el Firewall. Recuerde que si el modo de presentación está habilitado, al intentar abrir una página o aplicación que constituya un riesgo para la seguridad, es posible que se bloquee, pero no aparecerá explicación o advertencia alguna, ya que la interacción con el usuario está deshabilitada.

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 las actualizaciones de los módulos. Esta exploración depende de la [Configuración y de las tareas en Tareas programadas](#).

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

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

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 secreto. 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 archivos a escanear son fijas para cada grupo antes mencionado.

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

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

Protección de documentos

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

Para activar la protección de documentos, abra la ventana **Configuración avanzada** (presione **F5**) > **Motor de detección** > **Exploración de malware** > **Protección de documentos** y haga clic en el interruptor **Habilitar la protección de documentos**.



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

Exclusiones

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

Las [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.

En la [versión 7.1 y anteriores](#), Exclusiones de rendimiento y Exclusiones de la detección, se fusionaron en una categoría.

No debe confundirse con otros tipos de exclusiones:

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

Exclusiones de rendimiento

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

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

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

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.

Exclusiones de rendimiento

Excluir ruta	Comentario
C:\Backup*	
C:\pagefile.sys	

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":"7.2.2055","path":"plugins.01000600.settings.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.

Editar exclusión ?

Ruta i

Comentario

Aceptar Cancelar

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 utilizando los botones de arriba/abajo (como las [reglas de firewall](#) que se ejecutan desde arriba hacia 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%`

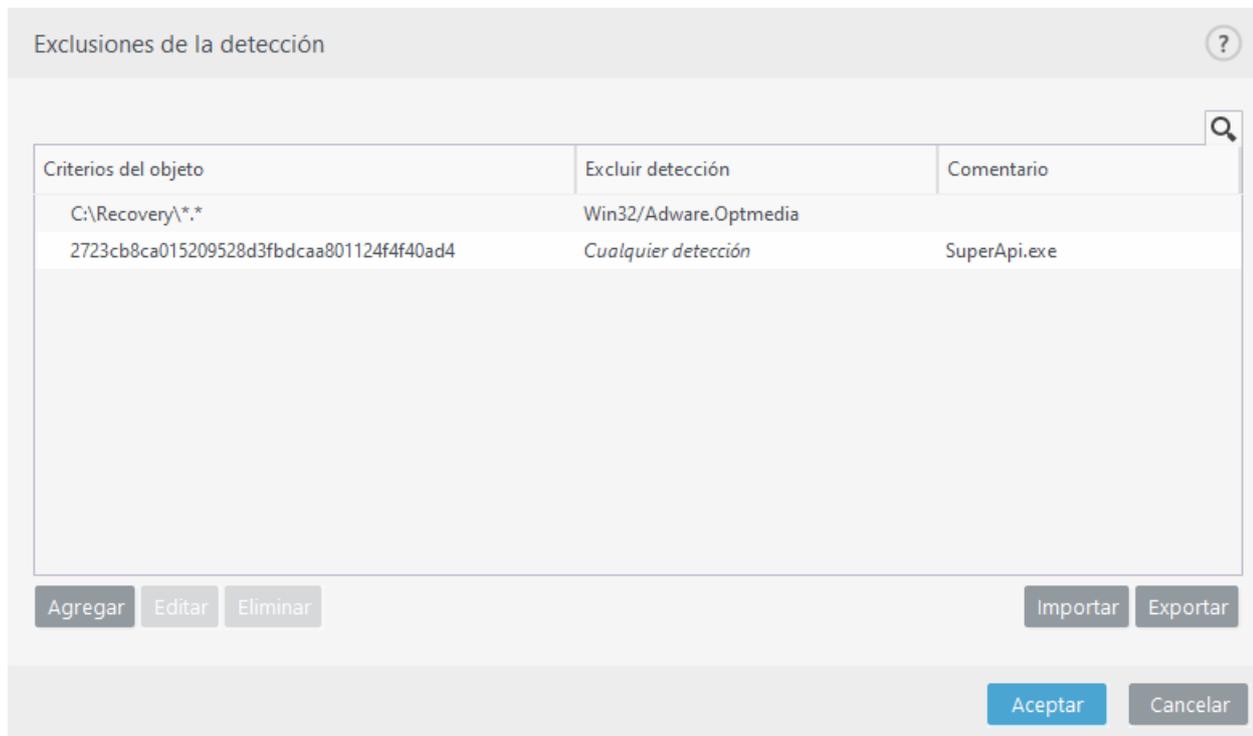
No se admiten las variables del sistema específicas del usuario (p. ej., `%TEMP%` o `%USERPROFILE%`) ni las variables de entorno (p. ej., `%PATH%`).

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.

Puede añadir archivos y carpetas a la lista de exclusiones, **Configuración avanzada (F5) > 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":"7.2.2055","path":"Settings.ExclusionsManagement.DetectionExclusions","columns":["Id","Path","ThreatName","Description","FileHash"]}
```

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

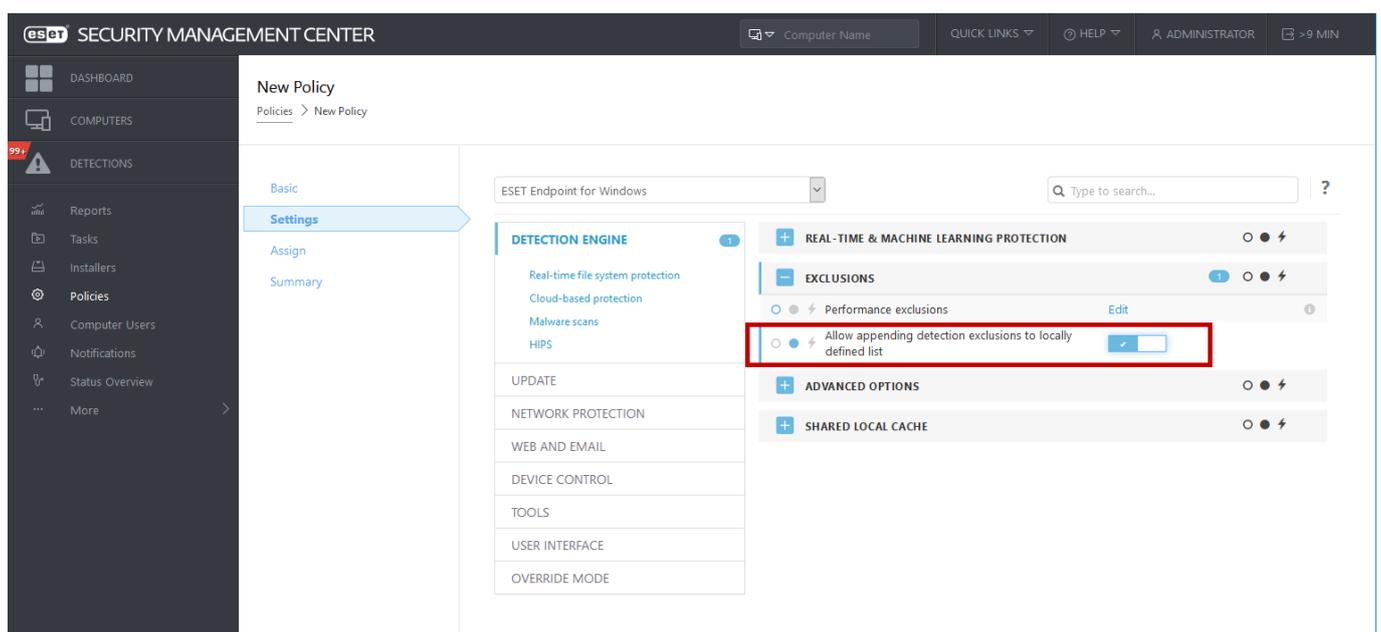
```
2c362ac8-a630-496e-9665-c76d00000001,C:\Recovery\*.*;Win32/Adware.Optmedia,,
```

Configuración de exclusiones de la detección en ESET PROTECT

ESMC 7.1 y ESET PROTECT 8.0 incluye un [nuevo asistente para la administración de exclusiones de la detección](#) — 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.



The screenshot displays the ESET Security Management Center (ESMC) interface. The main window is titled 'New Policy' and shows the configuration for a policy named 'ESET Endpoint for Windows'. The 'EXCLUSIONS' section is highlighted with a red box, and the checkbox 'Allow appending detection exclusions to locally defined list' is checked. The interface includes a sidebar with navigation options like 'Dashboard', 'Computers', 'Detections', 'Reports', 'Tasks', 'Installers', 'Policies', 'Computer Users', 'Notifications', 'Status Overview', and 'More'. The top navigation bar shows 'Computer Name', 'Quick Links', 'Help', 'Administrator', and '>9 MIN'.

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 Security. 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](#).



Editar exclusión

Ruta: C:\Recovery*.*

Hash:

Nombre de detección: Win32/Adware.Optmedia

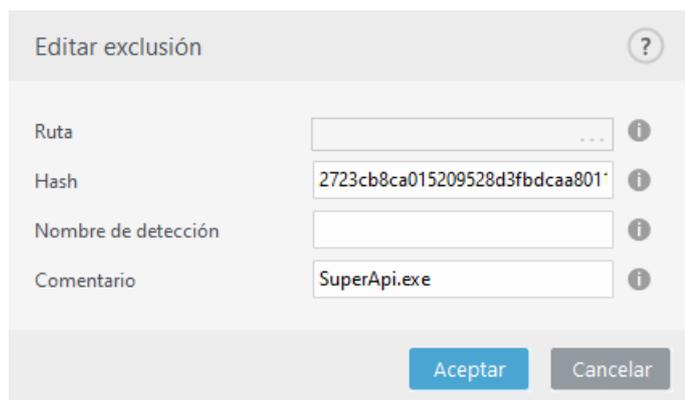
Comentario:

Aceptar Cancelar

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

Excluir hash

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



Editar exclusión

Ruta:

Hash: 2723cb8ca015209528d3fbdcaa801

Nombre de detección:

Comentario: SuperApi.exe

Aceptar Cancelar

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 Security:

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

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

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

Elementos de control

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

Asistente para crear exclusiones de la detección

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

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

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

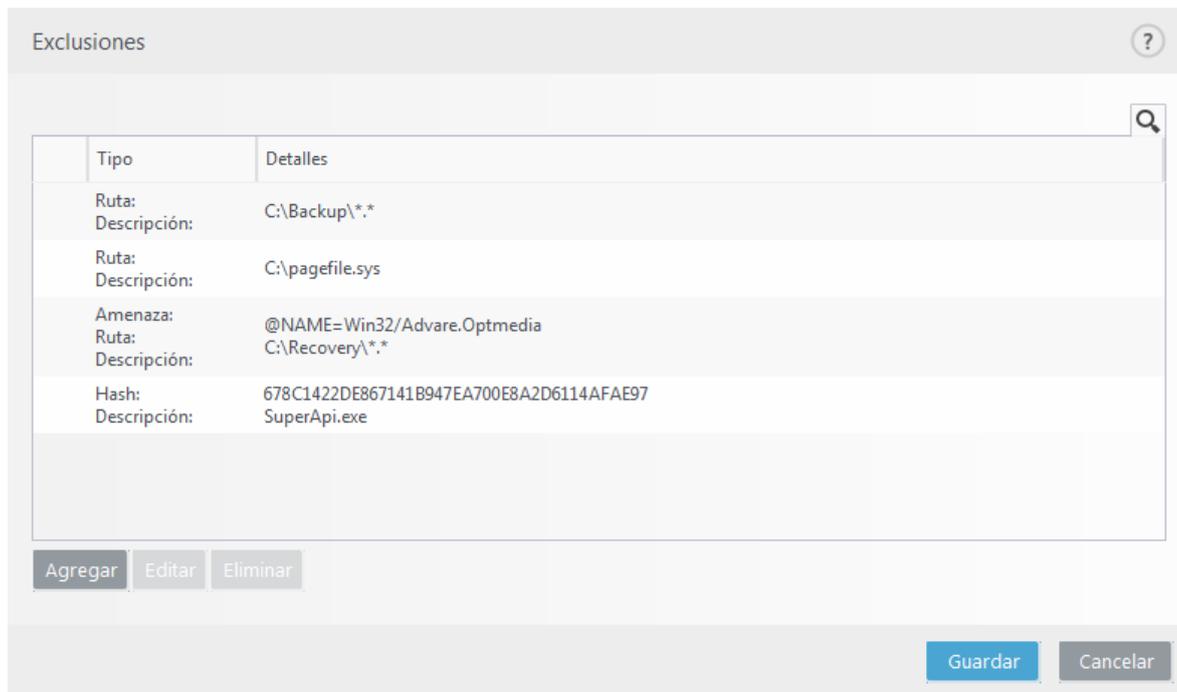
- **Archivos exactos** – Excluir cada archivo por hash SHA-1.
- **Detección** – Excluir cada archivo por nombre de detección.
- **Ruta + Detección** – Excluir cada archivo por ruta y nombre de detección, incluido el nombre del archivo (p. ej., *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*).

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

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

Exclusiones (versión 7.1 y anteriores)

En la versión 7.1 y anteriores, [Exclusiones de rendimiento](#) y [Exclusiones de la detección](#) se fusionaron en una categoría.



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. Ocurren problemas similares cuando se intenta realizar migraciones en vivo de equipos virtuales. 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.

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

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

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

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



Tan pronto se agrega el archivo .exe a las exclusiones, la actividad de este proceso no se somete a la monitorización de ESET Endpoint Security 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 Security 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.

Exclusiones de HIPS

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

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.



Consulte el capítulo [Exclusiones](#).

ThreatSense parámetros

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

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

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

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

- Protección del sistema de archivos en tiempo real
- 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 comprimidos 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 Security 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 los parámetros de ThreatSense permite definir los tipos de archivos que se van a explorar.

Otros

Cuando se configuran los valores de los parámetros del motor ThreatSense para una exploración del equipo bajo demanda, las siguientes opciones en la sección **Otros** también están disponibles:

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

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

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

Habilitar la optimización inteligente – cuando la opción para habilitar la optimización inteligente está

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

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

Límites

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

Configuración de los objetos

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

Tiempo máximo de exploración para el objeto (s): 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. Valor predeterminado: ilimitado.

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

Niveles de desinfección

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

La protección en tiempo real y otros módulos de protección presentan los siguientes niveles de corrección (es decir, desinfección).

Corrección ESET Endpoint Security 8

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

Extensiones de archivos que no se analizarán

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

i No debe confundirse con otros tipos de [Exclusiones](#).

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 hubiera) de un archivo en un sistema operativo de Windows, debe anular la selección de la opción **Ocultar las extensiones de los tipos de archivo conocidos** en **Panel de control > Opciones de carpeta > Ver** (pestaña) y aplicar este cambio.

Parámetros adicionales de ThreatSense

Parámetros adicionales de ThreatSense para los nuevos archivos creados y modificados – la probabilidad de infección de los nuevos archivos creados o en los modificados es mayor al compararla con la correspondiente a los archivos existentes. Por ese motivo, el programa verifica esos archivos con parámetros adicionales de exploración. Junto con los métodos comunes de exploración basados en firmas, se utiliza la heurística avanzada, que puede detectar las nuevas amenazas antes del lanzamiento de la actualización del motor de detección. Además de los nuevos archivos creados, la exploración se realiza en los archivos de autoextracción (.sfx) y los empaquetadores de tiempo de ejecución (archivos ejecutables comprimidos internamente). En forma predeterminada, los archivos comprimidos se exploran hasta el décimo nivel de anidado y se verifican independientemente de su tamaño real. Para modificar la configuración de la exploración de los archivos comprimidos, desactive **Configuración predeterminada para la exploración de archivos comprimidos**.

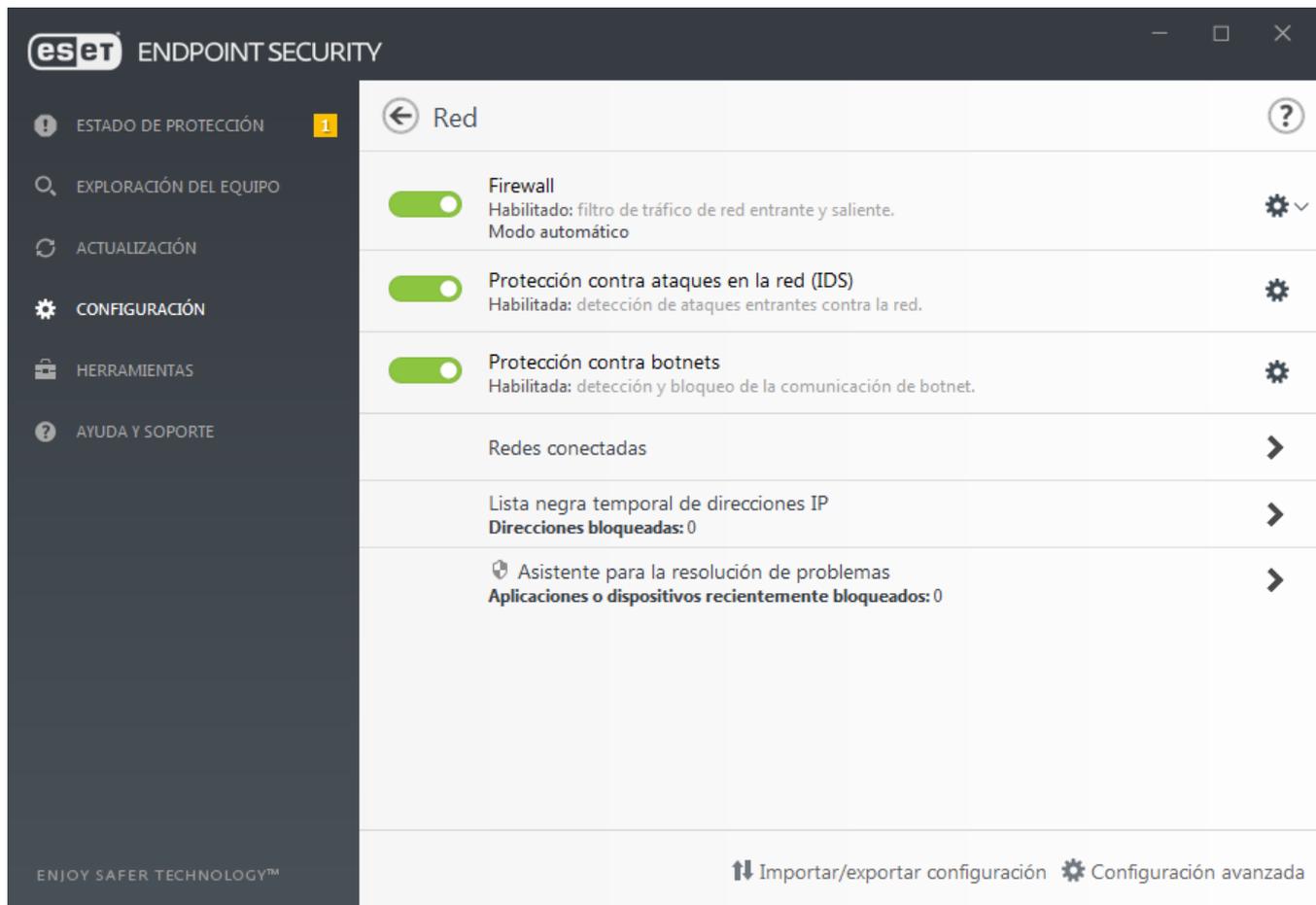
Para obtener más información acerca de los Empaquetadores de tiempo de ejecución, los Archivos de autoextracción y la Heurística avanzada, consulte [Configuración de los parámetros del motor ThreatSense](#).

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

Red

La sección **Red** le permite tener acceso rápido a los siguientes componentes o ajustes en la **configuración avanzada**:

- **Firewall** – Aquí puede ajustar el modo de filtrado para el [Firewall de ESET](#). Para acceder a configuraciones más detalladas, haga clic en la rueda de engranaje  > **Configurar** junto a **Firewall**, o presione **F5** a fin de acceder a la **Configuración avanzada**.
- [Protección contra ataques a la red \(IDS\)](#) – Analiza el contenido del tráfico de red y protege de ataques en la red. Todo tráfico considerado perjudicial será bloqueado. ESET Endpoint Security le informará cuando se conecte 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. Para deshabilitar la Protección contra Botnet durante un periodo de tiempo específico, haga clic en .
- **Redes conectadas** – muestra las redes a las que están conectados los adaptadores de red. Después de hacer clic en la rueda de engranaje, se le instará a que seleccione un tipo de protección para la red a la que está conectado mediante su adaptador de red. En esta ventana también puede ver **Adaptadores de red** en la esquina inferior derecha. Puede ver cada adaptador de red y su perfil de firewall y zona de confianza asignados. Para obtener más información, consulte [Adaptadores de red](#).
- **Lista negra temporal de direcciones IP**: muestra una lista de direcciones IP que se han detectado como fuente de ataques y, por tanto, se han agregado a la lista negra para bloquear conexiones por un cierto periodo de tiempo. Para más información, haga clic en esta opción y presione F1.
- **Asistente para la resolución de problemas** – le ayuda a resolver los problemas de conectividad causados por el firewall de ESET. Para obtener información más detallada, consulte el [Asistente para la resolución de problemas](#).



Haga clic en la rueda de engranaje  junto al **Firewall** para acceder a las siguientes configuraciones:

- **Configurar** – abre la ventana del Firewall en la Configuración avanzada, donde puede definir cómo el firewall manejará la comunicación de redes.
- **Bloquear todo el tráfico** – todas las comunicaciones entrantes y salientes serán bloqueadas por el Firewall. Use esta opción solo si sospecha que existe un riesgo crítico de seguridad que requiere desconectar el sistema de la red. Para restablecer el firewall a su funcionamiento normal mientras el filtrado del tráfico de red está en modo **Bloquear todo el tráfico**, haga clic en **Detener el bloqueo de todo el tráfico** .
- **Pausar firewall (permitir todo tráfico)**: lo opuesto a bloquear todo el tráfico de red. Al seleccionarla, se desactivan todas las opciones de filtrado del firewall y se permiten todas las conexiones entrantes y salientes. Haga clic en **Habilitar el firewall** a fin de restablecer el firewall mientras el filtrado del tráfico de red está en este modo.
- **Modo automático** – (cuando otro modo de filtrado está habilitado) – Haga clic para cambiar del modo de filtrado al modo de filtrado automático (con reglas definidas por el usuario).
- **Modo interactivo** – (cuando otro modo de filtrado está habilitado) – Haga clic para cambiar del modo de filtrado al modo de filtrado interactivo.

Firewall

El firewall controla todo el tráfico de red que sale del sistema y que ingresa a él. Para ello, permite o deniega las conexiones de red individuales según las reglas de filtrado especificadas. Brinda protección frente a ataques desde equipos remotos y bloquea ciertos servicios potencialmente amenazantes.

Básico

Habilitar el firewall

Le recomendamos dejar habilitada esta función para garantizar la seguridad de su sistema. Con el firewall activado, el tráfico de red se explora en ambas direcciones.

Evalúe también las reglas del firewall de Windows

En el modo automático, también permitir el tráfico entrante permitido por las reglas del firewall de Windows, a menos que sea explícitamente bloqueado por las reglas de ESET.



Las reglas del firewall de Windows que se configuraron mediante el uso de Directiva de Grupo (GPO) no se evaluaron.

Modo de filtrado

La conducta del firewall cambia de acuerdo con el modo de filtrado. Los modos de filtrado también influyen en el nivel requerido de interacción del usuario.

Los siguientes son los modos de filtrado disponibles para el firewall de ESET Endpoint Security:

Modo de filtrado	Descripción
Modo automático	Modo automático – es el modo predeterminado. Este modo resulta adecuado para los usuarios que prefieren un uso sencillo y conveniente del firewall sin la necesidad de definir reglas. Se pueden crear reglas personalizadas y definidas por el usuario, pero no se requieren en el modo automático . El modo automático da lugar al tráfico saliente para un sistema determinado y bloquea la mayoría del tráfico entrante, a excepción de una cantidad de tráfico de la Zona de confianza (según se especifica en sistema de detección de intrusiones y opciones avanzadas/servicios permitidos) y respuestas a las comunicaciones entrantes recientes.
Modo interactivo	permite crear una configuración personalizada para el Firewall. Cuando se detecta una comunicación y no existe ninguna regla que se aplique a ella, se mostrará una ventana de diálogo para informar sobre la existencia de una conexión desconocida. La ventana de diálogo da la opción de permitir o denegar la comunicación y dicha decisión puede guardarse como una nueva regla para el Firewall. Si elige crear una nueva regla, todas las conexiones futuras de este tipo se permitirán o bloquearán de acuerdo con dicha regla.
Modo basado en políticas	bloquea todas las conexiones que no están definidas por una regla específica que las permita. Este modo hace posible que los usuarios avanzados definan reglas para permitir solo las conexiones deseadas y seguras. El Firewall bloqueará todas las demás conexiones que no estén especificadas.
Modo de aprendizaje	Crea y guarda las reglas automáticamente; este modo se recomienda para la configuración inicial del firewall, pero no se debe dejar encendido durante períodos prolongados. No se requiere la interacción del usuario porque ESET Endpoint Security guarda las reglas según los parámetros predefinidos. El modo de aprendizaje solo debe usarse hasta que se hayan creado todas las reglas para las comunicaciones requeridas y se puedan evitar inconvenientes de seguridad.

Los [Perfiles](#) se pueden utilizar para personalizar la conducta del Firewall de ESET Endpoint Security al especificar diferentes conjuntos de reglas en situaciones distintas.

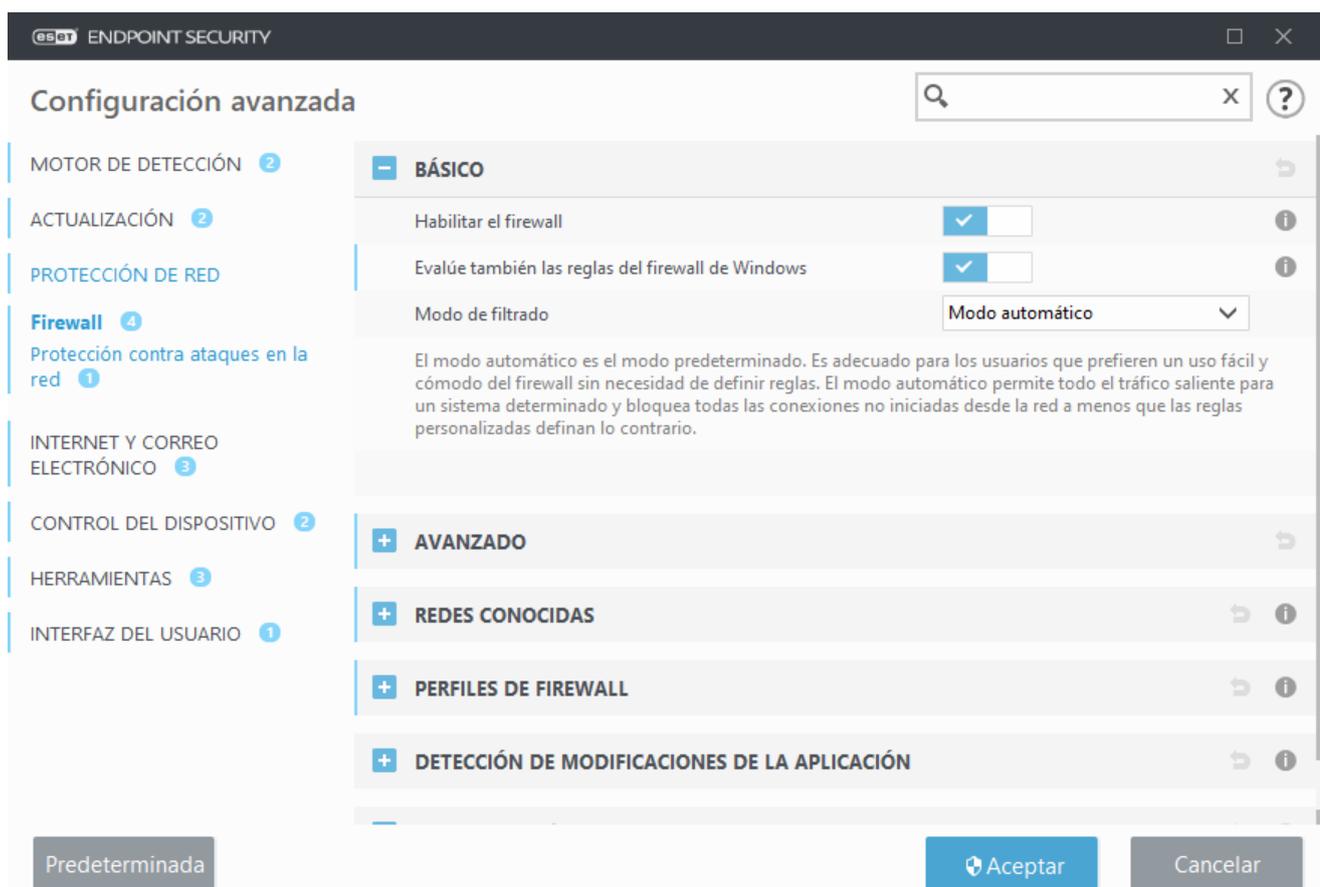
Avanzado

Reglas

La configuración de reglas le permite ver todas las reglas que se aplican al tráfico generado por cada aplicación individual dentro de las zonas de confianza e Internet.

Zonas

Una zona representa una colección de direcciones de red que crean un grupo lógico.



i Puede crear una regla IDS cuando un [Botnet](#) ataca su equipo. Se puede modificar una excepción en **Configuración avanzada (F5) > Protección de red > Protección contra los ataques de red > Reglas IDS** con clic en **Editar**.

Modo de aprendizaje

El modo de aprendizaje crea y guarda automáticamente una regla por cada comunicación que se ha establecido en el sistema. No se requiere la interacción del usuario porque ESET Endpoint Security guarda las reglas según los parámetros predefinidos.

Este modo puede exponer su sistema a riesgos, y solo se recomienda para la configuración inicial del Firewall.

Seleccione **Modo de aprendizaje** en el menú desplegable en **Configuración avanzada (F5) > Firewall > Básico >**

Modo de filtrado para activar las **opciones del modo de aprendizaje**. Esta sección contiene los siguientes elementos:

 El Firewall no filtra la comunicación cuando el modo de aprendizaje está activado. Se permiten todas las comunicaciones entrantes y salientes. En este modo, el equipo no cuenta con la protección completa del Firewall.

Modo configurado después del vencimiento del modo de aprendizaje: defina a qué modo de filtrado se ESET Endpoint Security restablecerá el firewall una vez finalizado el período para el modo de aprendizaje. Obtenga más información sobre los [Modos de filtrado](#). Después del vencimiento, la opción Preguntar al usuario requiere privilegios administrativos para realizar un cambio en el modo de filtrado del firewall.

Tipo de comunicación – seleccione los parámetros de creación de reglas específicas para cada tipo de comunicación. Existen cuatro tipos de comunicación:

-  **Tráfico entrante de una zona de confianza** – un ejemplo de una conexión entrante dentro de la zona de confianza es un equipo remoto de una zona de confianza que intenta establecer una comunicación con una aplicación activa en el equipo local.
-  **Tráfico saliente a una zona de confianza** – una aplicación remota que intenta establecer una conexión con otro equipo dentro de la red local o dentro de una red de la zona segura.
-  **Tráfico de Internet entrante** – un equipo remoto que intenta comunicarse con una aplicación ejecutada en el equipo.
-  **Tráfico de Internet saliente** – una aplicación local que intenta establecer una conexión con otro equipo.

Cada sección le permite definir los parámetros que se agregarán a las reglas recién creadas:

Agregar puerto local – incluye el número del puerto local de la comunicación de red. Para comunicaciones salientes, normalmente se generan números aleatorios. Por este motivo, es recomendable activar esta opción solo para las comunicaciones entrantes.

Agregar aplicación – incluye el nombre de la aplicación local. Esta opción es útil para reglas futuras en el nivel de las aplicaciones (reglas que definen la comunicación para una aplicación completa). Por ejemplo, puede activar la comunicación solo para un navegador Web o para un cliente de correo electrónico.

Agregar puerto remoto – incluye el número del puerto remoto de la comunicación de red. Por ejemplo, puede permitir o denegar un servicio específico asociado a un número de puerto estándar (HTTP – 80, POP3 – 110, etc.).

Agregar dirección IP remota/Zona de confianza – se puede utilizar una dirección IP o zona remota como parámetro para la creación de nuevas reglas que definan todas las conexiones de red entre el sistema local y dicha dirección o zona remota. Esta opción resulta útil cuando el usuario desea definir acciones para un equipo específico o un grupo de equipos en red.

Cantidad máxima de reglas diferentes por cada aplicación – si una aplicación establece una comunicación a través de diferentes puertos, con varias direcciones IP, etc., el firewall en modo de aprendizaje crea la cantidad de reglas adecuada para dicha aplicación. Esta opción le permite limitar el número de reglas que se pueden crear para una sola aplicación.

Protección contra ataques de 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 considerado perjudicial será bloqueado.

Habilitar protección contra Botnet: 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.

Opciones avanzadas de filtrado

Las secciones de protección contra ataques de red y firewall le permiten configurar opciones avanzadas de filtrado para detectar varios tipos de ataques y vulnerabilidades que pueden llevarse a cabo contra su equipo.

i 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 opciones determinadas en Configuración avanzada (F5) > **Protección de la red** > **Firewall** y Configuración avanzada (F5) > **Protección de la red** > **Protección contra ataques en la red** puede variar según el tipo o la versión de su módulo de firewall y según la versión de su sistema operativo.

– Servicios permitidos

Las configuraciones en este grupo están destinadas a simplificar la configuración del acceso a los servicios de este equipo desde la zona de confianza. Muchas de ellas habilitan o deshabilitan las reglas predefinidas de firewall.

- **Permitir el uso compartido de archivos e impresoras en la zona de confianza** – permite a los equipos remotos de la zona de confianza acceder a sus archivos e impresoras compartidos.
- **Permitir UPnP para los servicios del sistema en la zona de confianza** – permite peticiones entrantes y salientes de protocolos UPnP para servicios del sistema. UPnP (Universal Plug and Play, también conocido como Microsoft Network Discovery) se utiliza en Windows Vista y sistemas operativos posteriores.
- **Permitir la comunicación RPC entrante en la Zona de confianza** – habilita las conexiones TCP de una Zona de confianza permitiendo el acceso al Asignador de puertos MS RPC y a los servicios RPC/DCOM.
- **Permitir el escritorio remoto en la Zona de confianza:** habilita las conexiones mediante el Protocolo de escritorio remoto de Microsoft (RDP) y permite a los equipos de la [Zona de confianza](#) acceder a su equipo por medio de un programa que usa RDP (por ejemplo, "Conexión a escritorio remoto"). Consulte también cómo [permitir conexiones de RDP fuera de la Zona de confianza](#).
- **Habilitar los registros en grupos de multidifusión a través de IGMP** – permite multidifusiones IGMP entrantes/salientes y UDP entrantes como, por ejemplo, secuencias de video generadas por aplicaciones que utilizan el protocolo IGMP (protocolo de administración de grupos de Internet).
- **Permitir la comunicación para las conexiones puente:** seleccione esta opción para evitar que finalicen las conexiones puente. Las redes puente permiten conectar una máquina virtual a una red con el adaptador Ethernet del equipo host. Si usa redes puente, la máquina virtual puede acceder a otros dispositivos en la red y viceversa, como si se tratase de un equipo físico en la red.

- **Permitir Web Services Discovery (WSD) automático para servicios del sistema en la Zona de confianza** – permite solicitudes de Web Services Discovery entrantes desde la Zona de confianza a través del firewall. WSD es el protocolo que se utiliza para localizar servicios en una red local.
- **Permitir la multidifusión para la resolución de direcciones en la zona de confianza (LLMNR)** – la LLMNR (Resolución de nombres de multidifusión local de vínculos) es un protocolo basado en el paquete DNS cuya función es permitir que tanto el host IPv4 como el IPv6 resuelvan nombres para hosts en el mismo vínculo local sin requerir la configuración del servidor o del cliente DNS. Esta opción permite solicitudes de multidifusión DNS entrantes desde la Zona de confianza a través del firewall.
- **Soporte para el Grupo Hogar de Windows** – habilita el soporte para el Grupo Hogar de Windows 7 y sistemas operativos posteriores. Una red casera tiene la posibilidad de compartir archivos e impresoras en una red doméstica. Para configurar un grupo hogar, navegue a **Inicio > Panel de control > Redes e Internet > Grupo Hogar**.

– 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](http://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).
- **Detección del ataque por envenenamiento ARP** – detección de los ataques por envenenamiento ARP iniciados por ataques interpuestos o un examen del conmutador de red. La aplicación o el dispositivo de red utilizan ARP (Protocolo de resolución de direcciones) para determinar la dirección Ethernet.
- **Detección del ataque de exploración de puerto TCP/UDP** – detecta ataques de software de exploración de puerto; una aplicación diseñada para sondear puertos abiertos de un host enviando solicitudes de cliente a un rango de direcciones de puerto, con el objetivo de encontrar puertos activos y explotar la vulnerabilidad del servicio. Lea más información sobre este tipo de ataque en el [glosario](#).
- **Bloquear la dirección no segura una vez detectado el ataque** – las direcciones IP que se han detectado como fuentes de ataques se agregan a la Lista negra para prevenir la conexión durante un cierto periodo.
- **Mostrar una notificación al detectar un ataque** – activa la notificación de la bandeja del sistema en el sector inferior derecho 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.
- **Denegar la apertura de archivos ejecutables en un servidor fuera de la Zona de confianza en el protocolo de SMB:** anula la conexión cuando intenta ejecutar un archivo ejecutable (.exe, .dll, ...) desde una carpeta compartida en el servidor que no pertenece a la zona de confianza en el firewall. Tenga en cuenta que la copia de archivos ejecutables desde fuentes de confianza puede ser legítima. Sin embargo, esta detección debería mitigar los riesgos de la apertura no deseada de un archivo en un servidor malicioso (por ejemplo, un archivo abierto mediante un clic en un hipervínculo a un archivo ejecutable malicioso compartido).
- **Denegar la autenticación de NTLM en el protocolo SMB para conectarse a un servidor dentro o fuera de la Zona de confianza** – los protocolos que usan esquemas de autenticación de NTLM (ambas versiones) están sujetos a un ataque por reenvío de credenciales (conocido como ataque de Retransmisiones SMB en el caso de un protocolo SMB). Denegar la autenticación de NTLM con un servidor fuera de la Zona de confianza debería mitigar los riesgos del reenvío de credenciales por parte de un servidor malicioso fuera de la Zona de confianza. De modo similar, puede denegar la autenticación de NTLM con servidores en la Zona de confianza.
- **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** – 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).

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 Security \(8.x\)](#)
 - [Cree reglas IDS en las estaciones de trabajo de cliente en ESET PROTECT \(8.x\)](#)

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. Las diferentes direcciones se deben delimitar con una coma.
- **Bloquear :** cada proceso de sistema tiene su propia conducta predeterminada y acción asignada (bloquear o permitir). Para anular la conducta predeterminada de ESET Endpoint Security, 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 Security](#). Seleccione **No** si no quiere recibir eventos de registro. Los valores disponibles son **Predeterminado/Sí/No**.

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.

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 excepción 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).

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 heredará la acción predeterminada aplicada por ESET Endpoint Security.
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 ataque de exploración de puertos TCP**.
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.

Amenaza sospechosa bloqueada

Esta situación puede ocurrir cuando una aplicación en su equipo está intentando transmitir tráfico malicioso a otro equipo en la red, está explotando una vulnerabilidad de seguridad, o si alguien trata de explorar puertos en su red.

Amenaza – nombre de la amenaza.

Origen – dirección de red de origen.

Destino: dirección de red de destino.

Detener bloqueo: crea una regla IDS para la amenaza sospechosa con una configuración que permite la comunicación.

Mantener bloqueo: bloquea la amenaza detectada. Para crear una regla IDS con una configuración que bloquee la comunicación para esta amenaza, seleccione **No volver a notificarme**.

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



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

Solución de problemas de firewall

El Asistente para la resolución de problemas le ayuda a resolver problemas de conectividad causados por el Firewall de ESET. 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 **La aplicación aún no funciona** y se permitirán todas las comunicaciones para ese dispositivo que estaban bloqueadas. Si el problema persiste, reinicie el equipo.

Haga clic en **Mostrar cambios** para ver las reglas creadas por el asistente. Asimismo, puede ver las reglas creadas por el asistente en **Configuración avanzada > Protección de la red > Firewall > Avanzado > Reglas**.

Haga clic en **Desbloquear otro para buscar soluciones a los problemas de comunicación con un dispositivo o aplicación diferente**.

Redes conectadas

Es posible acceder a la sección de **redes conectadas** desde la ventana principal del programa de ESET Endpoint Security haciendo clic en **Configuración > Redes > Redes conectadas**.

Muestra las redes a las que están conectados los adaptadores de red. Luego de hacer clic en el enlace debajo del nombre de la red, se le solicitará que seleccione un tipo de protección (estricta o permitida) para la red a la que está conectado a través de su adaptador de red, o puede hacer clic en la rueda dentada  para cambiar esta selección en la **Configuración avanzada**. Esta configuración define cuán accesible es su equipo a otros equipos en la red.

Puede conectarse a tres tipos de ubicación de red:

- **Red pública:** este tipo de ubicación de red es para espacios públicos y no es de confianza. Su dispositivo no estará visible en la red y no podrá ver ningún otro dispositivo de la red. La detección de redes está desactivada de forma predeterminada para las redes públicas.
- **Red doméstica o de oficina:** a diferencia de una red pública, puede compartir recursos con otros equipos en LAN en una red privada. Seleccione **Red doméstica o de oficina** cuando sepa y confíe en los dispositivos de la red.
- **Red de dominio:** el administrador de la red controla este tipo de ubicación de red y no puede seleccionar ni cambiar este tipo de red. El tipo de ubicación de red de dominio se detecta cuando el equipo local es miembro de un Active Directory Domain Services. El equipo local puede autenticarse en un controlador de dominio para ese dominio a través de una de sus conexiones de red.

Elegir una ubicación de red puede ayudar a garantizar que el equipo esté siempre configurado con un nivel de seguridad adecuado.

Hacer clic en **Adaptadores de red** en la esquina inferior derecha de la ventana le permite ver cada adaptador de red y su perfil de firewall asignado y zona de confianza. Para obtener información más detallada, consulte [Adaptadores de red](#).

i Cuando seleccione **Usar configuración de Windows** no aparecerá una ventana y la red a la que está conectado se marcará automáticamente según la configuración de Windows. Esta configuración facilitará el acceso a algunas características (por ejemplo, compartir archivos y escritorio remoto) desde las nuevas redes.

Redes conocidas

Al utilizar un equipo que se conecta con frecuencia a redes públicas o redes que están fuera de su red normal de trabajo, recomendamos que verifique la credibilidad de red de las nuevas redes a las que se conecta. Una vez que se definan las redes, ESET Endpoint Security puede reconocer las redes de confianza (Hogar/trabajo) mediante varios parámetros de red configurados en **Identificación de la red**. Los equipos suelen ingresar a redes con direcciones IP que son similares a las de la red de confianza. En esos casos, ESET Endpoint Security puede considerar que una red no conocida es de confianza (Hogar/trabajo). Recomendamos que use la **Autenticación de la red** para evitar este tipo de situaciones.

Cuando un adaptador de red se conecta a una red o se vuelven a configurar sus propiedades de red, ESET Endpoint Security buscará en la lista de redes conocidas un registro que coincida con la nueva red. Si la **Identificación de la red** y la **Autenticación de red** (opcional) coinciden, la red se marcará como conectada en esta interfaz. Cuando no se encuentre una red conocida, la configuración de identificación de red creará una nueva conexión de red para identificarla la próxima vez que se conecte con ella. En forma predeterminada, la conexión a la nueva red utiliza el tipo de protección **Red pública**. La ventana de diálogo **Nueva conexión de red detectada** le solicitará que elija entre los tipos de protección **Red pública**, **Red doméstica o de oficina** o bien **Usar configuración de Windows**. Si un adaptador de red se conecta a una red conocida y esa red se marca como **Red doméstica o de oficina**, las subredes locales del adaptador se agregarán a la Zona de confianza.

Tipo de protección de nuevas redes: seleccione cuál de las siguientes opciones: Utilizar configuración de Windows, solicitar al usuario o Marcar como pública se utiliza de manera predeterminada para las redes nuevas.

i Cuando seleccione **Usar configuración de Windows** no aparecerá un cuadro de diálogo y la red a la que está conectado se marcará automáticamente según la configuración de Windows. Esto causará facilitar el acceso a algunas características (por ejemplo, compartir los archivos y el escritorio remoto) desde las nuevas redes.

Las redes conocidas se pueden configurar en forma manual en la ventana [Editor de redes conocidas](#).

Editor de redes conocidas

Las redes conocidas se pueden configurar manualmente en **Configuración avanzada > Protección de red > Firewall > Redes conocidas** haciendo clic en **Editar** junto a **Redes conocidas**.

Columnas

Nombre – nombre de la red conocida.

Tipo de protección: muestra si la red está configurada en **Red doméstica o de oficina**, **Pública** o **Usar configuración de Windows**.

Perfil de firewall – seleccione un perfil del menú desplegable **Mostrar las reglas que se usan en el perfil** para mostrar el filtro de reglas del perfil.

Actualizar perfil – Le permite aplicar un perfil de actualización creado cuando se conecte a esta red.

Elementos de control

Agregar: crea una nueva red conocida.

Editar – haga clic para editar una red conocida existente.

Eliminar: seleccione una red y haga clic en **Eliminar** para eliminarla de la lista de redes conocidas.



Superior/Arriba/Abajo/Inferior– le permite ajustar el nivel de prioridad de las redes conocidas (las redes se evalúan desde arriba hacia abajo).

Las propiedades de configuración de red se organizan en las siguientes pestañas:

Red

Aquí podrá definir el **Nombre de la red** y seleccionar el **Tipo de protección** (Red pública, Red doméstica o de oficina o Usar configuración de Windows) de la red. Use el menú desplegable **Perfil de firewall** para seleccionar el perfil para esta red. Si la red utiliza el tipo de protección **Hogar/oficina**, todas las subredes conectadas directamente se considerarán 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 255.255.255.0, la subred 192.168.1.0/24 se agregará a la zona de confianza de dicho adaptador. Si el adaptador tiene más direcciones o subredes, todas ellas serán de confianza, independientemente de la configuración de la **Identificación de la red** conocida.

Además, las direcciones agregadas en las **Direcciones de confianza adicionales** siempre se agregan a la zona de confianza de los adaptadores conectados a esta red (independientemente del tipo de protección de la red).

Advertir sobre cifrado Wi-Fi débil – ESET Endpoint Security le informará cuando se conecte a una red inalámbrica desprotegida o a una red con protección débil.

Perfil de Firewall – seleccione el perfil de Firewall que se utilizará cuando esté conectado a esta red.

Perfil de actualización – seleccione el perfil de actualización que se utilizará cuando esté conectado a esta red.

Se deben cumplir las siguientes condiciones para que una red se marque como conectada en la lista de redes conectadas:

- **Identificación de la red** – todos los parámetros completados deben coincidir con los parámetros de conexión activos.
- **Autenticación de red** – si se selecciona el servidor de autenticación, se debe llevar a cabo una autenticación correcta con el Authentication Server de ESET.

Identificación de la red

La identificación de la red se realiza según los parámetros del adaptador de red local. Todos los parámetros seleccionados se comparan con los parámetros reales de las conexiones de red activas. Se permiten las direcciones IPv4 e IPv6.

Editar red ?

Red **Identificación de la red** Autenticación de red

Cuando el sufijo DNS actual es (ejemplo: 'empresa.com')

hq.eset.com

Cuando la dirección IP del servidor WINS es x

Cuando la dirección IP del servidor DNS es

10.196.106

Cuando la dirección IP local es

fe80::d20:3796:ddab:7f67

Cuando la dirección IP del servidor DHCP es

10.1.81.21

Autenticación de red

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 está autenticando debe coincidir con el nombre de zona establecido en las configuraciones del servidor de autenticación. El nombre diferencia entre mayúsculas y minúsculas. Especifique un nombre de servidor, un puerto de escucha del servidor y una clave pública que se corresponda con la clave del servidor privado (consulte [Autenticación de red: configuración del servidor](#)). El nombre del servidor se puede ingresar en forma de dirección IP, DNS o nombre NetBios, y se puede seguir por una ruta que especifique la ubicación de la clave en el servidor (por ejemplo, server_name_/directory1/directory2/authentication). Puede especificar servidores alternativos para usarlos al añadirlos a la ruta, separados por punto y coma.

[Descargue ESET Authentication Server.](#)

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

- La clave pública cifrada PEM (.pem) se puede generar con el ESET Authentication Server (consulte la sección [Autenticación de red: configuración del servidor](#)).
- Clave pública cifrada
- Certificado de clave pública (.crt)

Editar red ?

Red	Identificación de la red	Autenticación de red
Nombre del servidor o dirección IP	<input type="text" value="10.1.1.24"/>	
Puerto de servidor	<input type="text" value="80"/>	
Clave pública (codificado con base64)	<input type="text"/>	

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 zona 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.

Autenticación de red: configuración del servidor

Cualquier equipo o servidor conectado a la red que se debe autenticar puede realizar el proceso de autenticación. La aplicación ESET Authentication Server debe instalarse en un equipo o servidor que siempre tenga acceso para la autenticación cuando un cliente intente conectarse a la red. El archivo de instalación para la aplicación ESET Authentication Server está disponible en el sitio Web de ESET para su descarga.

Luego de instalar la aplicación ESET Authentication Server, aparecerá una ventana de diálogo (puede acceder a la aplicación al hacer clic en **Inicio > Programas > ESET > ESET Authentication Server**).

Para configurar el servidor de autenticación, ingrese el nombre de la red de autenticación, el puerto de escucha del servidor (el predeterminado es 80), así como la ubicación donde se debe almacenar el par de claves pública y privada. Luego, genere la clave pública y la clave privada que se usarán en el proceso de autenticación. La clave privada permanecerá en el servidor, mientras que la clave pública deberá importarse desde el lado del cliente en la sección de autenticación de red cuando se configure una red en la configuración del firewall.

Perfiles de firewall

Perfil global predeterminado: Si no hay ningún perfil de la red ni de la configuración del adaptador de red, se usa el perfil global predeterminado.

Lista de perfiles: Los perfiles se pueden utilizar para controlar la conducta del Firewall de ESET Endpoint Security. Al crear o editar una regla de Firewall, puede asignarla a un perfil específico o a todos los perfiles. Cuando un perfil está activo en una interfaz de red, solo se aplicarán las reglas globales (reglas sin ningún perfil especificado) y las reglas asignadas a dicho perfil. Puede crear varios perfiles con diferentes reglas asignadas a los adaptadores de red o asignadas a las redes para alterar fácilmente la conducta del Firewall.

Perfiles asignados a los adaptadores de red: se puede configurar un adaptador de red para que utilice un perfil configurado para una red específica cuando está conectado a esa red.

También puede asignar un perfil específico para usarlo en una red determinada en **Configuración avanzada (F5) > Firewall > Redes conocidas**. Seleccione una red de la lista de **Redes conocidas** y haga clic en **Editar** para asignar un perfil de firewall a la red específica desde el menú desplegable **Perfil de Firewall**. Si no se ha asignado un perfil a dicha red, se utilizará el perfil predeterminado del adaptador. Si el adaptador se configura para que no use el perfil de la red, se utilizará su perfil predeterminado independientemente de a qué red esté conectado. Si no hay ningún perfil para la red ni para la configuración del adaptador, se utiliza el perfil global predeterminado. Para asignar un perfil a un adaptador de red, seleccione el adaptador de red, haga clic en **Editar** junto a **Perfiles asignados a los adaptadores de red**, seleccione el perfil en el menú desplegable **Perfil de firewall predeterminado** y, luego, haga clic en **Guardar**.

Cuando el Firewall cambia a otro perfil, aparecerá una notificación en la esquina inferior derecha, junto al reloj del sistema.

Perfiles asignados a los adaptadores de red

Al intercambiar los perfiles, puede realizar rápidamente varios cambios en la conducta del firewall. Las reglas personalizadas se pueden establecer y aplicar para perfiles determinados. Las entradas del adaptador de red para todos los adaptadores presentes en la máquina se agregan a la lista de **Adaptadores de red** automáticamente.

Columnas

Nombre – nombre del adaptador de red.

Perfil de firewall predeterminado – el perfil predeterminado se utiliza cuando la red a la que está conectado no posee un perfil configurado, o su adaptador de red está configurado para no usar un perfil de red.

Preferir el perfil de la red: El adaptador de red puede usar un perfil de firewall configurado para la red conectada conocida. Si esa red no tiene un perfil configurado, o si el adaptador de red está configurado para no usar el perfil de la red, entonces se usa el perfil del adaptador predeterminado.

Elementos de control

Agregar: agrega un adaptador de red nuevo.

Editar – le permite editar un adaptador de red existente.

Quitar – seleccione un adaptador de red y haga clic en Eliminar si desea eliminar un adaptador de red de la lista.

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

DetECCIÓN DE MODIFICACIONES DE LA APLICACIÓN

La característica de detección de modificaciones de la aplicación muestra notificaciones si alguna aplicación modificada, para la que existe una regla de firewall, intenta establecer una conexión. Esto es útil para evitar el abuso de las reglas configuradas para alguna aplicación por parte de otra aplicación reemplazando temporal o permanentemente el archivo ejecutable original de la aplicación por otro archivo ejecutable de la aplicación, o modificando en forma maliciosa el archivo ejecutable original de la aplicación.

Tenga en cuenta que esta característica no está destinada a detectar modificaciones en cualquier aplicación en general. El objetivo es evitar el abuso de las reglas de firewall existentes, y solo se supervisan las aplicaciones para las que existen reglas de firewall específicas.

Habilitar la detección de modificaciones en las aplicaciones – si se selecciona, el programa controlará las aplicaciones en busca de cambios (actualizaciones, infecciones u otras modificaciones). Cuando una aplicación modificada intente establecer una conexión, recibirá una notificación del firewall.

Permitir la modificación de aplicaciones firmadas (de confianza) – no notifican si la aplicación tiene la misma firma digital válida antes y después de la modificación.

Lista de aplicaciones excluidas de la verificación: puede agregar o eliminar aplicaciones individuales para las cuales se permiten modificaciones sin notificación.

Aplicaciones excluidas de la detección de modificaciones

El firewall en ESET Endpoint Security detecta los cambios en las aplicaciones para las que existen reglas (consulte [Detección de modificaciones de la aplicación](#)).

En algunos casos, quizá no le interese usar esta funcionalidad para ciertas aplicaciones si desea excluirlas de la verificación que realiza el firewall.

Agregar: abre una ventana donde puede seleccionar una aplicación para agregarla a la lista de aplicaciones excluidas de la detección de modificaciones. Puede elegir de una lista de aplicaciones en ejecución con comunicación de red abierta, para la cual existen reglas de firewall, o agregar una aplicación específica.

Editar: abre una ventana donde puede cambiar la ubicación de una aplicación que se encuentra en la lista de aplicaciones excluidas de la detección de modificaciones. Puede elegir de una lista de aplicaciones en ejecución con comunicación de red abierta, para la cual existen reglas de firewall, o cambiar la ubicación de forma manual.

Quitar – quita entradas de la lista de aplicaciones excluidas de la detección de modificaciones.

Configuración y uso de reglas

Las reglas representan un grupo de condiciones usadas para evaluar todas las conexiones de red y todas las acciones asignadas a dichas condiciones. Con las reglas de Firewall, puede definir la acción a realizar cuando se establecen diferentes tipos de conexiones de red. Para acceder a la configuración del filtrado de reglas, navegue a **Configuración avanzada (F5) > Protección de la red > Firewall > Avanzado**. Algunas de las reglas predefinidas están ligadas a las casillas de verificación de los **servicios permitidos** ([Servicios permitidos y opciones avanzadas](#)) y no se pueden desactivar directamente, en cambio, puede usar esas casillas de verificación relacionadas para hacerlo.

A diferencia de la versión anterior de ESET Endpoint Security, las reglas se evalúan desde arriba hacia abajo. La acción de la primera regla que coincida se utiliza para cada conexión de red que se está evaluando. Este es un cambio de conducta importante con respecto a la versión anterior, en la que las reglas de prioridad eran automáticas y las reglas más específicas tenían una prioridad más alta que las generales.

Las conexiones pueden dividirse en entrantes y salientes. Las conexiones entrantes se inician por un equipo remoto que intenta establecer una conexión con el sistema local. Las conexiones salientes funcionan en la forma opuesta – el sistema local establece el contacto con un equipo remoto.

Si se detecta una nueva comunicación desconocida, considere cuidadosamente si la va a permitir o denegar. Las conexiones no solicitadas, no seguras o desconocidas constituyen un riesgo para el sistema. Si se establece una conexión de ese tipo, es recomendable prestar especial atención al equipo remoto y a la aplicación que trata de conectarse a su equipo. Muchas infiltraciones intentan obtener y enviar datos confidenciales, o descargar otras aplicaciones maliciosas en las estaciones de trabajo locales. El firewall permite detectar y finalizar dichas conexiones.

Lista de reglas del firewall

La lista de reglas del firewall se encuentra en **Configuración avanzada (F5) > Protección de red > Firewall > Básico**, para lo cual es necesario hacer clic en **Editar** junto a **Reglas**.

Columnas

Nombre – nombre de la regla.

Habilitada – muestra si la regla están habilitada o deshabilitada; la casilla de verificación correspondiente debe estar seleccionada para activar una regla.

Protocolo – el Internet protocolo para el que esta regla es válida.

Perfil – muestra el perfil de firewall para el que esta regla es válida.

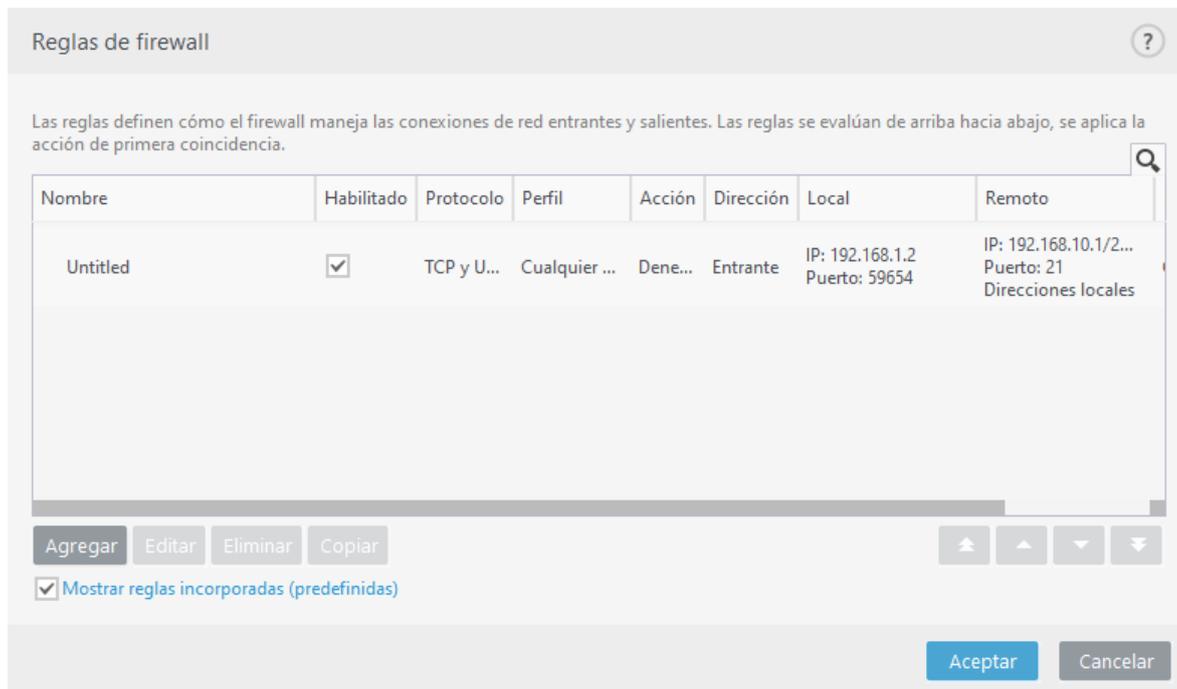
Acción – muestra el estado de la comunicación (bloquear/permitir/preguntar).

Dirección – dirección de la comunicación (entrante/saliente/ambas).

Local: dirección/rango/subred IPv4 o IPv6 remota y puerto de equipo local.

Remota: dirección/rango/subred IPv4 o IPv6 remota y puerto de equipo remoto.

Aplicaciones –la aplicación a la que se aplica la regla.



Elementos de control

Agregar – [crea una regla nueva](#).

Editar – Edita una regla existente.

Quitar: elimina una regla existente.

Copiar - crea una copia de la regla seleccionada.

Mostrar reglas incorporadas (predefinidas) – reglas predefinidas por ESET Endpoint Security que permiten o deniegan comunicaciones específicas. Puede deshabilitar estas reglas, pero no puede eliminar una regla predefinida.



Superior/Arriba/Abajo/Inferior – le permite ajustar el nivel de prioridad de las reglas (las reglas se ejecutan desde arriba hacia abajo).

i Haga clic en el icono de búsqueda  ubicado en la parte superior derecha para buscar la(s) regla(s) por nombre, protocolo o puerto.

Agregar o editar reglas del firewall

Las modificaciones son necesarias cada vez que se cambian los parámetros supervisados. Si se realizan cambios que impiden que dicha regla cumpla con las condiciones y que la acción especificada se aplique, la conexión determinada puede ser rechazada. Esto puede ocasionar problemas con el funcionamiento de la aplicación afectada por una regla. Un ejemplo es el cambio de la dirección de red o el número del puerto correspondiente al lado remoto.

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

- i** • [Crear o editar reglas del firewall en ESET Endpoint Security](#)
- [Crear o editar reglas del firewall para estaciones de trabajo de clientes en ESET Security Management Center](#)

La sección superior de la ventana contiene tres pestañas:

- **General** – especifica el nombre de una regla, la dirección de la conexión, la acción (**Permitir**, **Denegar**, **Preguntar**), el protocolo y el perfil al que se aplicará la regla.
- **Local** – muestra información sobre el lado local de la conexión, incluido el número del puerto local o rango de puertos locales, y el nombre de la aplicación que se está comunicando. También le permite agregar una zona predefinida o creada con un rango de direcciones IP aquí al hacer clic en **Agregar**.
- **Remoto** – esta pestaña contiene información sobre el puerto remoto (o el rango de puertos). Le permite definir una lista de direcciones IP o zonas remotas para una regla específica. También puede agregar una zona predefinida o creada con un rango de direcciones IP aquí al hacer clic en **Agregar**.

Al crear una nueva regla, debe ingresar un nombre para la regla en el campo **Nombre**. Seleccione la dirección a la que se aplica la regla en el menú desplegable **Dirección** y la acción que se ejecutará cuando una comunicación cumpla la regla en el menú desplegable **Acción**.

El protocolo representa el protocolo de transferencia utilizado para la regla. Seleccione en el menú desplegable qué protocolo usar para una regla determinada.

El **Tipo/Código ICMP** representa un mensaje ICMP identificado por un número (por ejemplo, 0 representa “Respuesta de eco”).

Están habilitadas todas las reglas para **Cualquier perfil** de forma predeterminada. Alternativamente, seleccione un perfil de firewall personalizado mediante el menú desplegable **Perfiles**.

Si habilita el **Severidad de registro**, la actividad conectada con la regla se guardará en un registro. Notificar al usuario: muestra una notificación cuando se aplica la regla.

Editar regla

General Local Remoto

General

Nombre: Untitled

Habilitado:

Dirección: Entrante

Acción: Denegar

Protocolo: TCP y UDP

Tipo/Código ICMP: 0

Perfil: Cualquier perfil

Severidad de registro: Diagnóstico

Aceptar



Los registros del firewall con el estado **Advertencia** [pueden recopilarse en ESET Security Management Center](#).

Creamos una nueva regla para permitir que la aplicación del navegador web Firefox tenga acceso a Internet/los sitios web de la red local. En este ejemplo, debe configurarse lo siguiente:

1. En la ficha **General**, habilite la comunicación saliente a través de los protocolos TCP y UDP.
2. Haga clic en la ficha **Local**.
3. Seleccione la ruta del archivo del navegador web que utiliza, para lo cual debe hacer clic en ... (por ejemplo, *C:\Program Files\Firefox\Firefox.exe*). NO ingrese el nombre de la aplicación.
4. En la ficha **Remoto**, habilite los números de puerto 80 y 443 si quiere habilitar la navegación estándar por Internet.



Tenga en cuenta que las reglas predefinidas se pueden modificar de forma limitada.

Regla de firewall: local

Especifique el nombre de la aplicación local y los puertos locales a los que se aplica una regla.

Puerto: números de puertos locales. Si no se especifica ningún número, la regla se aplicará a todos los puertos. Agregue un solo puerto de comunicación o un rango de puertos de comunicación.

IP – le permite agregar una dirección o direcciones remotas, un rango de direcciones, o una subred sobre la que se aplica la regla. Si no se especifica ningún valor, la regla se aplicará a todas las comunicaciones.

Zonas – lista de zonas agregadas.

Agregar – agregar una zona creada del menú desplegable. Para crear una zona, use la pestaña [Configuración de la zona](#).

Quitar – elimina zonas de la lista.

Aplicación – el nombre de la aplicación a la que se aplica la regla. Agregue la ubicación de la aplicación a la que se aplicará la regla.

Servicio – el menú desplegable muestra los servicios del sistema.



Es posible que desee crear una regla para su **Mirror** que proporcione actualizaciones a través del puerto 2221 mediante el servicio EHttp Srv para las comunicaciones en el menú desplegable.

Editar regla

General Local Remoto

Local

Puerto 59654

IP 192.168.1.2

Zonas

Agregar Editar Eliminar Importar Exportar

Aplicación C:\Program Files\Internet Explorer

Aceptar

Regla de firewall: remota

Puerto – números de puertos remotos. Si no se especifica ningún número, la regla se aplicará a todos los puertos. Agregar un solo puerto de comunicación o un rango de puertos de comunicación.

IP – le permite agregar una dirección remota, un rango de direcciones, o una subred. La dirección, el rango de direcciones, la subred o zona remota a la que se aplica la regla. Si no se especifica ningún valor, la regla se aplicará a toda la comunicación.

Zonas – lista de zonas agregadas.

Agregar – agregar una zona al seleccionarla del menú desplegable. Para crear una zona, use la pestaña [Configuración de la zona](#).

Quitar – elimina zonas de la lista.

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. Desde ESET Endpoint Security vaya a **Configuración > Protección de la red > Lista negra temporal de direcciones IP**. 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.

Zona de confianza

La zona de confianza representa un grupo de direcciones de red desde las que el Firewall permite cierto tráfico entrante mediante el uso de configuraciones predeterminadas. La configuración de funciones tales como la

compartición de archivos y el escritorio remoto dentro de la zona de confianza está determinada en [Servicios permitidos y opciones avanzadas](#).

La verdadera zona de confianza se calcula en forma dinámica y separada para cada adaptador de red en función de la red a la que actualmente está conectada el equipo. Las direcciones que estén definidas como dentro de la zona de confianza en el Editor de zonas siempre son de confianza. Si un adaptador de red está conectado a una red conocida, entonces las **Direcciones adicionales de confianza** configuradas para esa red, se agregan a la zona de confianza del adaptador. Si una red tiene el tipo de protección Hogar/trabajo, todas las subredes que se conecten directamente se incluyen en la zona de confianza. La verdadera zona de confianza para cada adaptador de red se puede visualizar desde la ventana **Configuración en Red > Adaptadores de red**.

Configuración de zonas

Una zona representa un conjunto de direcciones de red que conforman un grupo lógico de direcciones IP, útiles cuando necesita reutilizar la misma serie de direcciones en múltiples reglas. A cada dirección de un grupo dado se le asignan reglas similares, que se definieron en forma general para todo el grupo. Un ejemplo de este tipo de grupo es la **zona de confianza**. La zona de confianza representa un grupo de direcciones de red que no están bloqueadas por el firewall de ninguna manera. Estas zonas se pueden configurar en **Configuración avanzada > Protección de la red > Firewall > Avanzado** al hacer clic en **Editar** junto a **Zonas**. Para agregar una nueva zona, haga clic en **Agregar**, ingrese un **Nombre** para la zona, una **Descripción** y agregue una dirección IP remota en el campo **Dirección del equipo remoto (IPv4/IPv6, rango, máscara)**. Consulte también [Zonas del firewall](#).

Zonas de firewall

Para obtener más información acerca de las zonas, consulte la sección [Configuración de zonas](#).

Columnas

Nombre – nombre de un grupo de equipos remotos.

Direcciones IP: direcciones de IP remotas que pertenecen a una zona.

Elementos de control

Cuando **agrega** o **edita** una zona, 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.

i Tenga en cuenta que las zonas predefinidas no se pueden eliminar.

Registro del Firewall

El firewall de ESET Endpoint Security guarda todos los sucesos importantes en un archivo de registro, que se puede ver directamente desde el menú principal. Haga clic en **Herramientas > Archivos de registro** y luego seleccione **Protección de red** en el menú desplegable **Registro**. Para habilitar el registro del firewall, vaya a **Configuración avanzada > Herramientas > Archivos de registro** y configure el nivel de detalle mínimo para los registros en **Diagnóstico**. Se registrarán todas las conexiones denegadas.

Los archivos de registro se pueden utilizar para detectar errores y revelar intrusiones en su sistema. Los registros del firewall de ESET contienen los siguientes datos:

- **Hora** : fecha y hora del suceso.
- **Suceso**: nombre del suceso.
- **Origen** – dirección de red de origen.
- **Destino**: dirección de red de destino.
- **Protocolo**: protocolo de comunicación de red.
- **Nombre del gusano/regla**: regla aplicada o nombre del gusano, si se ha identificado.
- **Aplicación**: aplicación implicada.
- **Usuario**: nombre del usuario registrado al momento en que se detectó la infiltración.

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

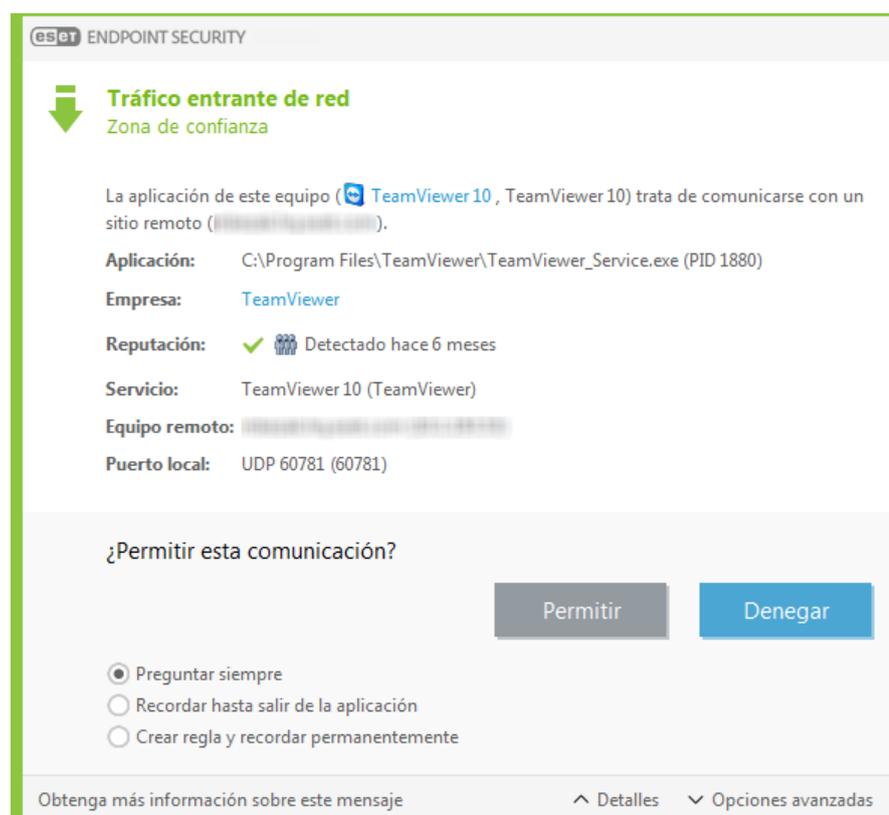
i El mensaje de ataque de vulnerabilidad a la seguridad se registra incluso cuando se soluciona la vulnerabilidad específica, ya que se detecta el intento de ataque y se lo bloquea a nivel de la red antes de que el ataque real pueda tener lugar.

Establecimiento de una conexión: detección

El firewall detecta cada nueva conexión de red que se crea. El modo de firewall activo determina las acciones que se llevan a cabo para la nueva conexión. Si el **Modo automático** o el **Modo basado en políticas** está activado, el firewall realizará acciones predefinidas sin la interacción del usuario.

El modo interactivo muestra una ventana informativa para indicar que se detectó una nueva conexión de red, complementada con información detallada sobre la conexión. Puede elegir permitir la conexión o rechazarla (bloquearla). Si permite la misma conexión en forma reiterada en la ventana de diálogo, es recomendable crear una nueva regla para esa conexión. Para ello, seleccione **Recordar acción (crear regla)** y guarde la acción como una nueva regla para el firewall. Si en el futuro el firewall reconoce la misma conexión, aplicará la regla existente sin requerir la interacción del usuario.

Recordar la acción temporalmente para el proceso hace que una acción (**Permitir / Denegar**) se utilice hasta la actualización de una aplicación, un cambio de reglas o modos de filtrado, una actualización del módulo de Firewall o un reinicio del sistema. Las reglas temporales se eliminarán después de cualquiera de estas acciones.



Sea precavido cuando crea reglas nuevas y solo permita las conexiones que usted reconoce como seguras. Si se permiten todas las conexiones, el firewall deja de cumplir su propósito. Estos son los parámetros importantes para las conexiones:

- **Ubicación remota:** solo permite las conexiones de direcciones de confianza y conocidas.
- **Aplicación local:** no es aconsejable permitir conexiones para aplicaciones y procesos desconocidos.
- **Número de puerto:** las comunicaciones en puertos comunes (por ejemplo, tráfico de Internet, número de puerto 80) deberían permitirse bajo circunstancias normales.

Para proliferar, las infiltraciones informáticas suelen usar Internet y conexiones ocultas, que las ayudan a infectar sistemas remotos. Si las reglas están configuradas correctamente, el firewall se convierte en una herramienta útil para la protección ante una diversidad de ataques de códigos maliciosos.

Resolución de problemas con el Firewall de ESET

Si experimenta problemas de conectividad con ESET Endpoint Security instalado, existen varias maneras de identificar si el Firewall de ESET es el causante del problema. Además, el Firewall 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 Firewall de ESET:

- [Asistente para la resolución de problemas](#)

- [Registro y creación de reglas o excepciones desde el registro](#)
- [Crear excepciones desde las notificaciones del firewall](#)
- [Registro avanzado de protección de red](#)
- [Resolución de problemas con el filtrado de protocolos](#)

Asistente para la resolución de problemas

El asistente para la resolución de problemas monitorea silenciosamente todas las conexiones bloqueadas, y lo guiará a través del proceso de resolución de problemas para corregir problemas del firewall con aplicaciones o dispositivos específicos. Luego, el asistente sugerirá un nuevo conjunto de reglas para aplicar si las aprueba. El **Asistente para la resolución de problemas** se puede encontrar en el menú principal bajo **Configuración > Red**.

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

- [Agregar una excepción del firewall con el asistente de solución de problemas](#)

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 el Firewall bloqueó, habilite el registro avanzado de Protección de red en la sección **Diagnósticos** de **Configuración avanzada** bajo **Herramientas > Diagnósticos**. Si ve algo en el registro que no desea que el Firewall bloquee, puede crear una regla o una regla IDS 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](#).

i Use los registros para ver el orden en que el Firewall 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 Security 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 Security debe establecerse con las siguientes configuraciones:

- ajustar el nivel de detalle mínimo para los registros a **Diagnóstico** en **Configuración avanzada (F5) > Herramientas > Archivos de registro**,

- habilitar **Mostrar notificaciones también para ataques entrantes frente a agujeros de seguridad** en **Configuración avanzada (F5) > Protección de la red > Protección contra ataques en la red > Opciones avanzadas > Detección de intrusiones.**

Crear excepciones desde las notificaciones del firewall

Cuando el Firewall de ESET detecte actividad de red maliciosa, aparecerá una ventana de notificación con la descripción del suceso. Esta notificación contiene un enlace que le permitirá obtener más información acerca del suceso para, así, establecer una excepción para este suceso si lo desea.

i Si una aplicación de red o dispositivo no implementa las normas de red correctamente, puede disparar reiteradas notificaciones del sistema de detección de intrusiones del firewall. Puede crear una excepción directamente desde la notificación para evitar que el Firewall de ESET detecte esta aplicación o dispositivo.

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. Navegue a **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 Endpoint Security\Diagnostics\`

Resolución de problemas con el filtrado de protocolos

Si experimenta problemas con su navegador o cliente de correo electrónico, el primer paso es determinar si el responsable es el filtrado de protocolos. Para hacer esto, intente deshabilitar temporalmente el filtrado de protocolos de la aplicación en la configuración avanzada (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 el filtrado de protocolos SSL habilitado, intente desactivarlo temporalmente. Si eso ayuda, puede continuar utilizando el filtrado SSL y hacer que la actualización funcione al excluir la comunicación problemática:
Cambie el modo de filtrado de protocolos SSL a interactivo. 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 del filtrado de protocolos (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 del filtrado de protocolos 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”

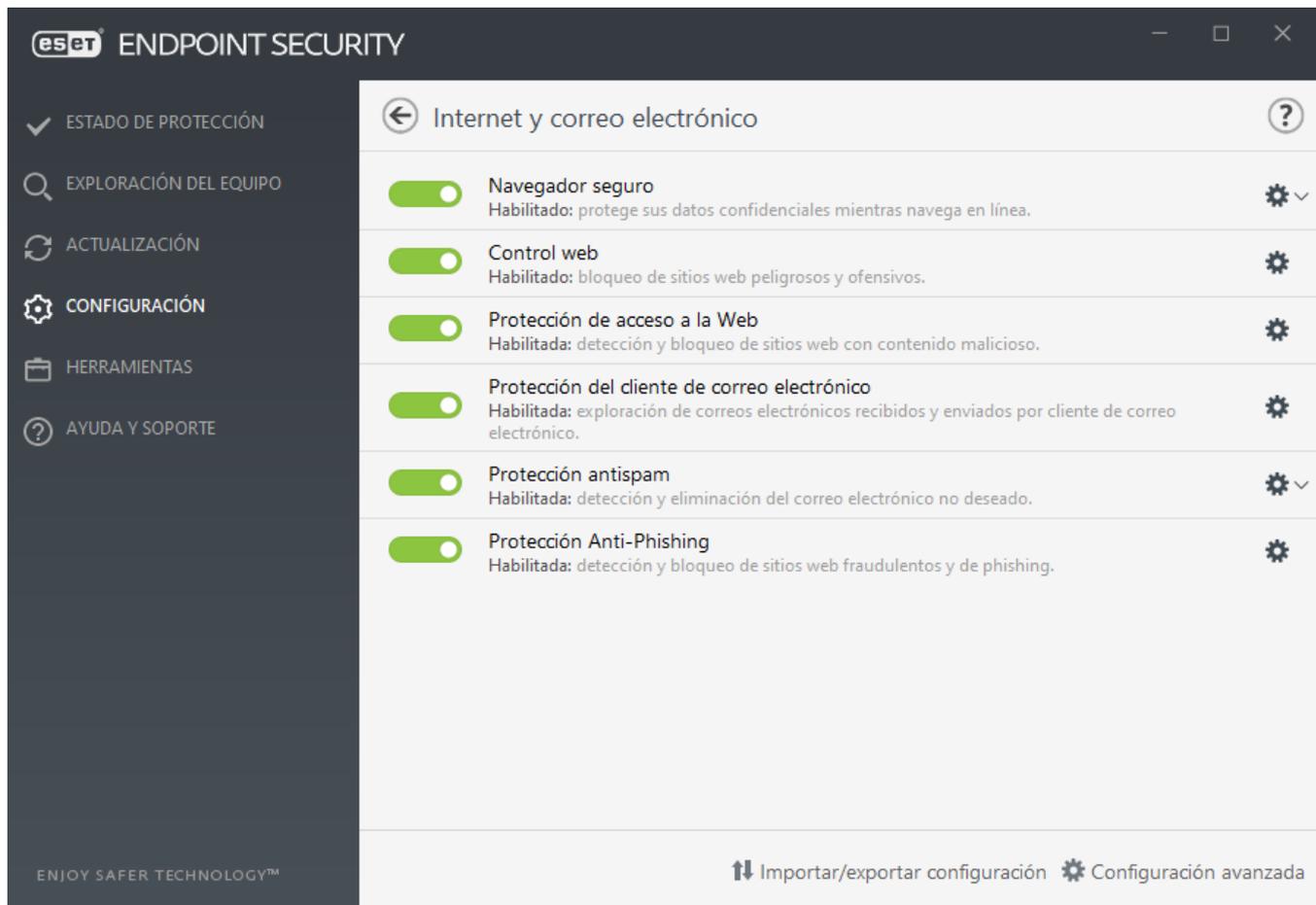
Cuando habilita el filtrado de protocolos SSL, ESET Endpoint Security se asegura de que las aplicaciones instaladas confían en la forma en que se filtra e protocolo SSL al importar un certificado a su almacén de certificados. Para ciertas aplicaciones esto no es posible mientras están activas. Esto incluye 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. Luego, deshabilite el filtrado de protocolos SSL y habilítelo nuevamente. Esto vuelve a ejecutar la importación.

Internet y correo electrónico

La configuración de Internet y del correo electrónico se puede encontrar en **Configuración > Internet y correo electrónico**. Desde aquí es posible acceder a configuraciones más detalladas del programa.



Navegador seguro – Protege sus datos confidenciales mientras navega en línea.

El módulo **Control Web** le permite ajustar las configuraciones que le proporcionan a los administradores herramientas automatizadas para proteger sus estaciones de trabajo y establecer restricciones para la navegación en Internet. El objetivo de la funcionalidad para el Control Web es evitar el acceso a las páginas con contenido inapropiado o perjudicial. Consulte [Control Web](#) para obtener más información.

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

Protección 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 Security proporciona el control de todas las comunicaciones desde el cliente de correo electrónico.

La [Protección antispam](#) filtra los mensajes de correo electrónico no solicitado.

Al hacer clic en la rueda de engranaje  junto a Protección antispam, las siguientes opciones están disponibles:

Configurar – abre las configuraciones avanzadas para la protección antispam del cliente de correo electrónico.

Lista blanca/Lista negra/Lista de excepciones del usuario – abre una ventana de diálogo donde se pueden agregar, editar o eliminar las direcciones de correo electrónico que se consideran seguras o inseguras. Según las reglas que aquí se definen, el correo electrónico desde estas direcciones no se explorará ni se tratará como spam. Haga clic en la Lista de excepciones del usuario para abrir una ventana de diálogo donde puede

agregar, editar o eliminar las direcciones de correo electrónico que pueden haberse alterado y utilizado para enviar spam. Los mensajes de correo electrónico recibidos desde las direcciones enumeradas en la lista de excepciones se explorarán siempre en busca de spam.

Protección Anti-phishing es otra capa de protección que brinda una mayor defensa frente a sitios Web ilegítimos que intentan obtener contraseñas y demás información sensible. La protección antiphishing se puede encontrar en el panel de Configuración bajo Internet y correo electrónico. Consulte [Protección antiphishing](#) para obtener más información.

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

Filtrado de protocolos

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

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

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

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

Direcciones IPv4 y máscara:

- *192.168.0.10*: agrega la dirección IP de un equipo individual al que debe aplicarse la regla.
- *192.168.0.1 a 192.168.0.99*: escriba la primera y la última dirección IP para especificar el rango de IP (de varios equipos) al que se debe aplicar la regla.
- Subred (un grupo de computadoras) definida por una dirección IP y una máscara. Por ejemplo, *255.255.255.0* es la máscara de red para el prefijo *192.168.1.0/24*, lo que implica un rango de direcciones de *192.168.1.1 a 192.168.1.254*.

Dirección IPv6 y máscara:

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

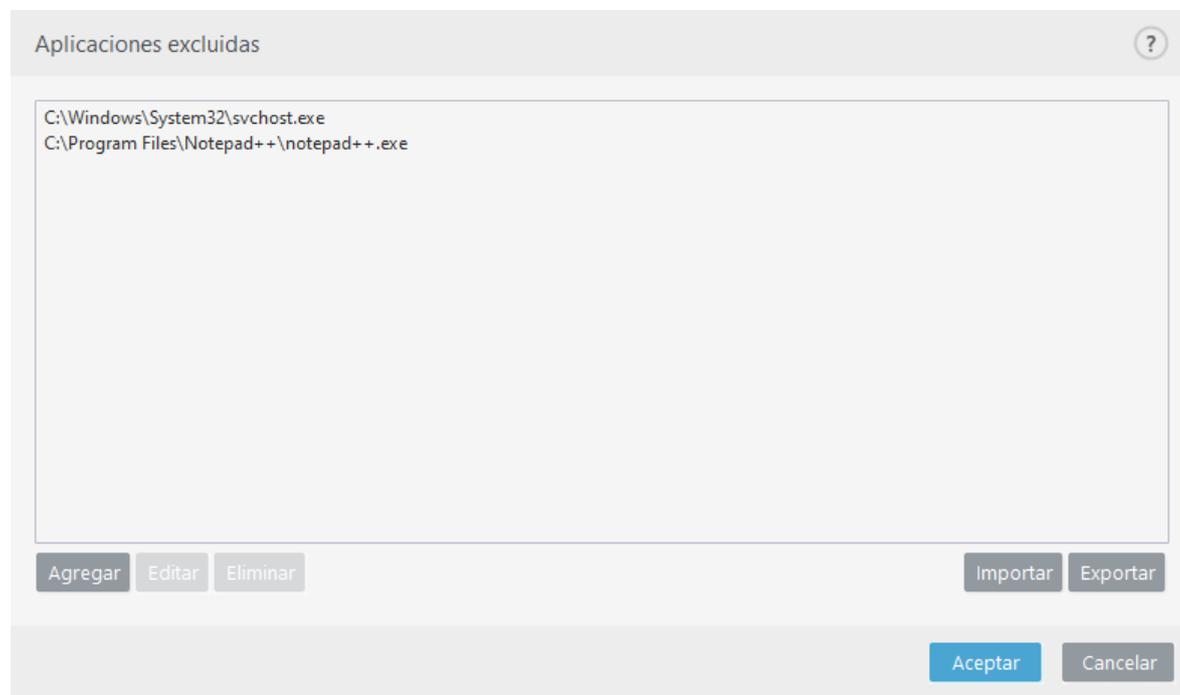
Aplicaciones excluidas

Para excluir del filtrado de protocolos las comunicaciones de aplicaciones específicas con reconocimiento de redes, agréguelas a la lista. La comunicación HTTP/POP3/IMAP de las aplicaciones seleccionadas no se verificará en busca de amenazas. Recomendamos que solo use esta técnica en los casos en que las aplicaciones no funcionen correctamente con el filtrado de protocolos habilitado.

Las aplicaciones y los servicios que ya fueron afectados por el filtrado de protocolos se mostrarán automáticamente después de hacer clic en **Agregar**.

Editar – edite las entradas seleccionadas de la lista.

Quitar – elimine las entradas seleccionadas de la lista.



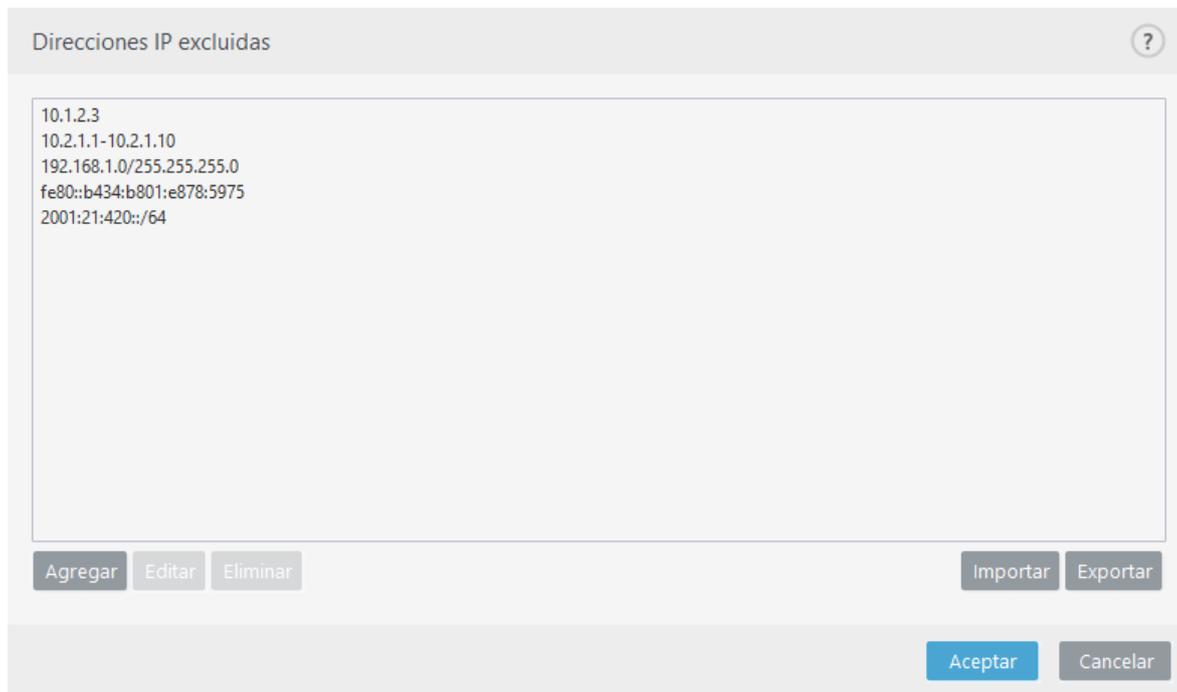
Direcciones IP excluidas

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

Agregar– 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.



SSL/TLS

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

Habilitar el filtrado del protocolo SSL/TLS: el filtrado de protocolos se habilita de manera predeterminada. Puede deshabilitar internet y correo electrónico o el filtrado de protocolos SSL/TLS en **Configuración avanzada > Internet y correo electrónico > SSL/TLS** o a través de la política. Si se deshabilita el filtrado de protocolos, el programa no explorará las comunicaciones con el protocolo SSL.

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

Modo de filtrado	Descripción
Modo automático	El modo predeterminado solo explorará las aplicaciones correspondientes, como los navegadores web y los clientes de correo electrónico. Puede anularlo si selecciona las aplicaciones para las cuales se explorarán sus comunicaciones.
Modo interactivo	Si ingresa un nuevo sitio protegido por SSL- (con un certificado desconocido), se mostrará un cuadro de diálogo para la selección de acción . Este modo le permite crear una lista de certificados/aplicaciones SSL que se excluirán de la exploración.
Modo de política	Seleccione esta opción para explorar todas las comunicaciones protegidas por SSL excepto las protegidas por certificados excluidos de la verificación. Si se establece una nueva comunicación que use un certificado firmado desconocido, no se notificará al usuario y se filtrará la comunicación en forma automática. Al acceder a un servidor con un certificado no confiable que está marcado como de confianza (se encuentra en la lista de certificados de confianza), se permite la comunicación con el servidor y se filtra el contenido del canal de comunicación.

La **Lista de aplicaciones SSL/TLS filtradas** puede usarse para personalizar la conducta de ESET Endpoint Security

para aplicaciones específicas

La **Lista de certificados conocidos** le permite personalizar la conducta de ESET Endpoint Security para certificados SSL específicos.

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

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

i Las direcciones no se filtrarán si la configuración de **Excluir la comunicación con dominios de confianza** está activada y el dominio se considera de confianza.

Certificado raíz

Certificado raíz – para que la comunicación SSL funcione correctamente en los navegadores o clientes de correo electrónico, es imprescindible agregar el certificado raíz para ESET a la lista de certificados raíz conocidos (desarrolladores). **Agregar el certificado raíz a los navegadores conocidos** deberá estar habilitada. Seleccione esta opción para agregar automáticamente el certificado raíz de ESET a los navegadores conocidos (por ejemplo, Opera y Firefox). Para los navegadores que usan el almacén de certificaciones del sistema, el certificado se agrega en forma automática (por ejemplo, en Internet Explorer).

Para aplicar el certificado en navegadores no compatibles, haga clic en **Ver el certificado > Detalles > Copiar en el archivo** y luego impórtelo manualmente al navegador.

Validez del certificado

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

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

i 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

Certificados

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

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

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

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

Tráfico de red cifrada

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

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

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



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**

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

Lista de certificados conocidos

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

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

Columnas

Nombre— nombre del certificado.

Emisor del certificado— nombre del creador del certificado.

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

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

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

Elementos de control

Añadir — se puede cargar un certificado en forma manual desde un archivo con la extensión *.cer*, *.crt* o *.pem*. Haga clic en **Archivo** para cargar un certificado local o haga clic en **URL** para especificar la ubicación de un certificado en línea.

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** para salir sin realizar cambios.

Lista de aplicaciones SSL/TLS filtradas

La **Lista de aplicaciones SSL/TLS filtradas** se puede usar para personalizar la conducta de ESET Endpoint Security para certificados SSL específicos y para recordar las acciones elegidas si se selecciona el **Modo interactivo** en el **modo de filtrado de protocolos SSL/TLS**. La lista se puede ver y editar en **Configuración avanzada (F5) > Internet y correo electrónico > SSL/TLS > Lista de aplicaciones SSL/TLS filtradas**.

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

Columnas

Aplicación – nombre de la aplicación.

Acción de exploración – seleccione **Explorar** o **Ignorar**. 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 el certificado que desea configurar y haga clic en **Editar**.

Quitar – 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.

Protección del cliente de correo electrónico

La integración de ESET Endpoint Security con los clientes de correo electrónico incrementa el nivel de protección activa frente a los códigos maliciosos en los mensajes de correo electrónico. Si su cliente de correo electrónico es compatible, esta integración se puede habilitar en ESET Endpoint Security. Cuando se integra a su cliente de correo electrónico, la barra de herramientas de ESET Endpoint Security se inserta directamente en el cliente de correo electrónico, lo que permite una protección de correo electrónico más eficaz. Las configuraciones de integración se ubican en **Configuración avanzada (F5) > Internet y correo electrónico > Protección del cliente de correo electrónico > Clientes de correo electrónico**.

The screenshot shows the 'Configuración avanzada' (Advanced Configuration) window in ESET Endpoint Security. The left sidebar lists various configuration categories, with 'Protección del cliente de correo electrónico' (Email Client Protection) selected and highlighted in blue. The main content area is titled 'CLIENTES DE CORREO ELECTRÓNICO' (Email Clients) and contains two sections: 'INTEGRACIÓN CON EL CLIENTE DE CORREO ELECTRÓNICO' (Integration with Email Client) and 'CORREO ELECTRÓNICO PARA EXPLORAR' (Email for Scanning). The integration section has four rows, each with a toggle switch: 'Integrar con Microsoft Outlook' (checked), 'Integrar con Outlook Express/Windows Mail' (checked), 'Integrar con Windows Live Mail' (checked), and 'Deshabilitar la verificación en caso de cambios en el contenido del buzón de entrada' (unchecked). The scanning section has three rows, each with a toggle switch: 'Habilitar protección de correo electrónico mediante complementos de clientes de correo' (checked), 'Correo electrónico recibido' (checked), and 'Correo electrónico enviado' (checked). At the bottom, there is a section for 'ACCIÓN PARA REALIZAR FN CORREOS ELECTRÓNICOS CON DETECCIONES' (Action for scanning emails with detections) with three buttons: 'Predeterminada' (Default), 'Aceptar' (Accept), and 'Cancelar' (Cancel).

Integración con el cliente de correo electrónico	Estado
Integrar con Microsoft Outlook	✓
Integrar con Outlook Express/Windows Mail	✓
Integrar con Windows Live Mail	✓
Deshabilitar la verificación en caso de cambios en el contenido del buzón de entrada	✗

Correo electrónico para explorar	Estado
Habilitar protección de correo electrónico mediante complementos de clientes de correo	✓
Correo electrónico recibido	✓
Correo electrónico enviado	✓
Correo electrónico leído	✓

Integración con el cliente de correo electrónico

Entre los clientes de correo electrónico actualmente compatibles, se incluyen [Microsoft Outlook](#), [Outlook Express](#), [Windows Mail](#) y Windows Live Mail. La protección de correo electrónico funciona como un complemento para estos programas. La ventaja principal de este complemento es su independencia respecto al protocolo utilizado. Cuando el cliente de correo electrónico recibe un mensaje cifrado, se descifra y se envía al módulo de exploración de virus. Si desea obtener una lista completa de los clientes de correo electrónico compatibles y sus versiones, consulte el siguiente [artículo de la Base de conocimiento de ESET](#).

Active la opción **Deshabilitar la verificación en caso de cambios en el contenido del buzón de entrada** si nota que el sistema funciona con mayor lentitud mientras recupera el correo electrónico.

Correo electrónico para explorar

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

Correo electrónico recibido: comprueba mensajes de correo electrónico que se reciben cuando está habilitada.

Correo electrónico enviado: comprueba mensajes de correo electrónico que se envían cuando está habilitada.

Correo electrónico leído: comprueba mensajes de correo electrónico que se leen cuando está habilitada.

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

Acción a realizar en correos electrónicos infectados

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

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

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

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

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

Repetir la exploración tras la actualización: vuelve a explorar los correos electrónicos infectados después de una actualización del motor de detección cuando está habilitada.

Aceptar los resultados de las exploraciones realizadas por otros módulos: permite al módulo de protección de correo electrónico usar los resultados de la exploración de otros módulos de protección en lugar de escanearlos nuevamente.

Protocolos de correo electrónico

IMAP y POP3 son los protocolos de uso más generales para recibir comunicaciones de correo electrónico en una aplicación de cliente de correo electrónico. El protocolo de acceso a mensajes de Internet (IMAP, 'Internet Message Access Protocol') es otro protocolo de Internet para la recuperación del correo electrónico. El protocolo IMAP tiene algunas ventajas sobre POP3, por ejemplo, se pueden conectar simultáneamente varios clientes al mismo buzón de correo y mantener información del estado de los mensajes: si se leyó, respondió o eliminó el mensaje, etc. El módulo de protección que proporciona este control se ejecuta automáticamente cuando se inicia el sistema y queda activo en la memoria.

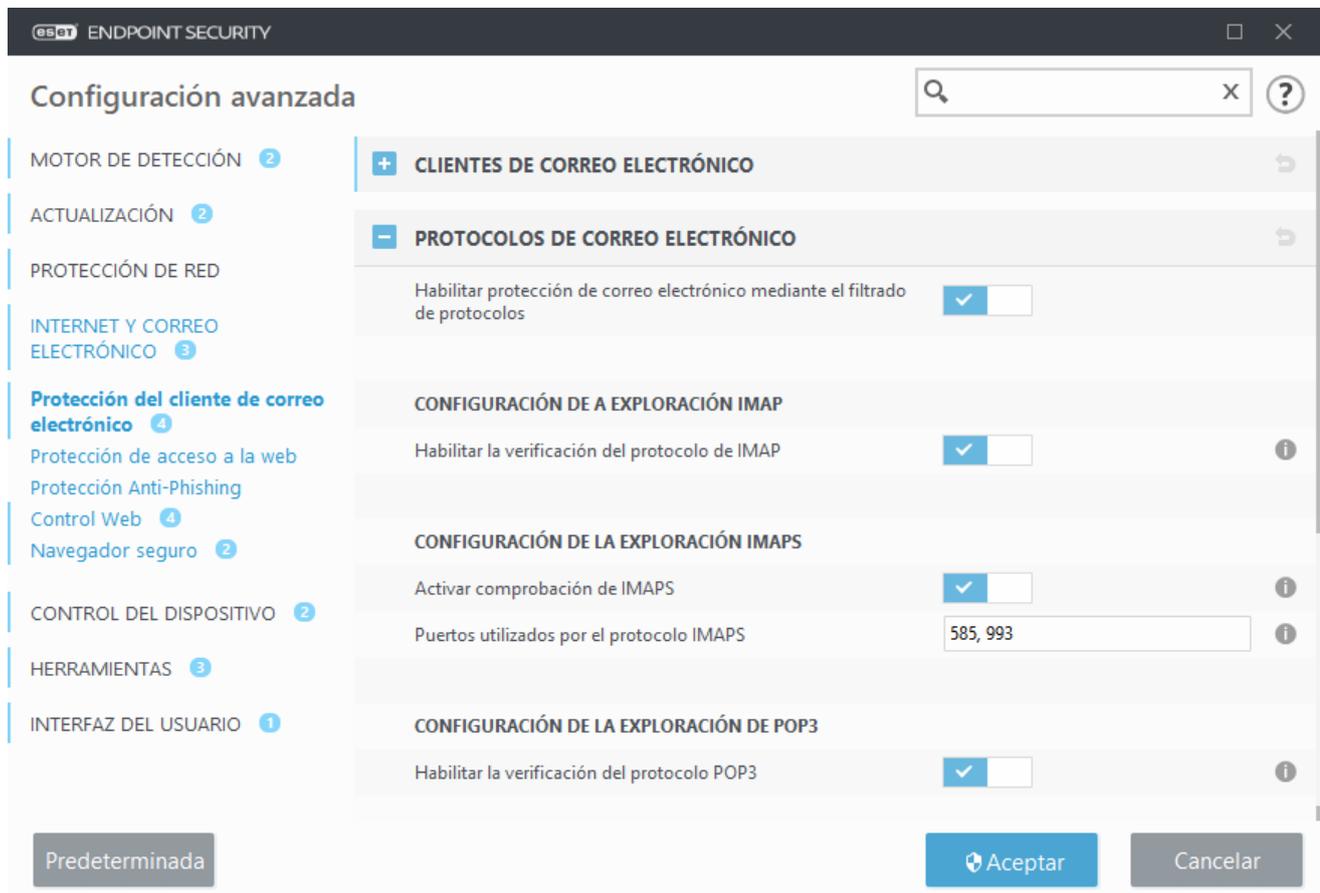
ESET Endpoint Security proporciona protección para estos protocolos, independientemente del cliente de correo electrónico usado, y sin requerir una nueva configuración del cliente de correo electrónico. De manera predeterminada, toda la comunicación mediante los protocolos POP3 y IMAP se explora, sin 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.

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

ESET Endpoint Security 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 Security verifica la comunicación mediante el SSL (protocolo de capa de conexión segura) y la TLS (seguridad de la capa de transporte). El programa solo explorará el tráfico en los puertos definidos en **Puertos utilizados por los protocolos IMAPS/POP3S**, independientemente de la versión del sistema operativo. Se pueden agregar otros puertos de comunicación, de ser necesario. Si hay varios números de puerto, estos se deben separar con una coma.

Por defecto, la comunicación encriptada será explorada. Para ver la configuración del explorador, vaya a [SSL/TLS](#) en la sección de configuración avanzada, haga clic en **Web y correo electrónico** > **SSL/TLS** y habilite la opción **Habilitar SSL/TLS el filtrado de protocolos**.



Alertas y notificaciones por correo electrónico

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

Luego de verificar el correo electrónico, se puede añadir al mensaje una notificación con el resultado de la exploración. Puede elegir **Añadir mensajes de etiqueta a los correos electrónicos recibidos y leídos** o **Añadir mensajes de etiqueta a los correos electrónicos enviados**. Tenga en cuenta que, en ocasiones raras, los mensajes de etiqueta pueden omitirse en mensajes HTML problemáticos o si los mensajes están adulterados por malware. Los mensajes de etiqueta se pueden añadir a los correos electrónicos recibidos y leídos, enviados o a ambas categorías. Se encuentran disponibles las siguientes opciones:

- **Nunca** – no se agregará ningún mensaje de etiqueta en absoluto.
- **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 asunto de correos electrónicos que fueron enviados: deshabilite esta opción si no desea que la protección de correo electrónico incluya una advertencia sobre virus en el asunto de un correo electrónico infectado. Esta característica permite realizar un filtrado simple basado en el asunto del correo electrónico infectado (si es compatible con el programa de correo electrónico). También incrementa el nivel de credibilidad para el destinatario y si se detecta una amenaza, proporciona información valiosa sobre el grado de peligro de la amenaza de un correo electrónico o remitente específicos.

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.

Integración con los clientes de correo electrónico

Entre los clientes de correo electrónico actualmente compatibles, se incluyen [Microsoft Outlook](#), [Outlook Express](#), [Windows Mail](#) y Windows Live Mail. La protección de correo electrónico funciona como un complemento para estos programas. La ventaja principal de este complemento es su independencia respecto al protocolo utilizado. Cuando el cliente de correo electrónico recibe un mensaje cifrado, se descifra y se envía al módulo de exploración de virus. Si desea obtener una lista completa de los clientes de correo electrónico compatibles y sus versiones, consulte el siguiente [artículo de la Base de conocimiento de ESET](#).

Barra de herramientas de Microsoft Outlook

El módulo de protección de Microsoft Outlook funciona como un complemento. Después de instalar ESET Endpoint Security, se agrega a Microsoft Outlook la siguiente barra de herramientas con las opciones de protección antivirus/antispam :

Spam – marca los mensajes seleccionados como spam. Después de marcarlos, se envía una “huella digital” del mensaje a un servidor central que almacena las firmas de spam. Si el servidor recibe más “huellas digitales” similares de varios usuarios, el mensaje se clasificará como spam en el futuro.

No es spam – marca los mensajes seleccionados como correo deseado.

Dirección de spam (lista negra, una lista de direcciones de spam) – agrega una nueva dirección de remitente a la [lista negra](#). Todos los mensajes recibidos de la lista se clasificarán automáticamente como spam.

 Tenga cuidado con la suplantación o falsificación de la dirección del remitente en mensajes de correo electrónico, utilizada para engañar a los destinatarios con el objetivo de que lean los correos y los respondan.

Dirección confiable (lista blanca, una lista de direcciones de confianza) – agrega una nueva dirección de remitente a la lista blanca. Todos los mensajes recibidos de las direcciones incluidas en la lista blanca nunca se clasificarán automáticamente como spam.

ESET Endpoint Security – Hacer clic en el ícono abre la ventana principal del programa de ESET Endpoint Security.

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

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

Configuración del antispam – muestra las opciones de configuración de la [Protección antispam](#).

Libretas de direcciones – abre la ventana de protección antispam, desde donde puede acceder a las listas de direcciones excluidas, de confianza y de spam.

Barra de herramientas de Outlook Express y Windows Mail

El módulo de protección de Outlook Express y Windows Mail funciona como un complemento. Después de instalar ESET Endpoint Security, se agrega a Microsoft Outlook la siguiente barra de herramientas con las opciones de protección antivirus/antispam :

Spam – marca los mensajes seleccionados como spam. Después de marcarlos, se envía una “huella digital” del mensaje a un servidor central que almacena las firmas de spam. Si el servidor recibe más “huellas digitales” similares de varios usuarios, el mensaje se clasificará como spam en el futuro.

No es spam – marca los mensajes seleccionados como correo deseado.

Dirección de spam – agrega una nueva dirección de remitente a la [lista negra](#). Todos los mensajes recibidos de la lista se clasificarán automáticamente como spam.



Tenga cuidado con la suplantación o falsificación de la dirección del remitente en mensajes de correo electrónico, utilizada para engañar a los destinatarios con el objetivo de que lean los correos y los respondan.

Dirección confiable – agrega una nueva dirección de remitente a la lista blanca. Todos los mensajes recibidos de las direcciones incluidas en la lista blanca nunca se clasificarán automáticamente como spam.

ESET Endpoint Security – Hacer clic en el ícono abre la ventana principal del programa de ESET Endpoint Security.

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

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

Configuración del antispam – muestra las opciones de configuración de la [Protección antispam](#).

Interfaz del usuario

Personalizar la apariencia – se puede modificar el aspecto de la barra de herramientas según el cliente de correo electrónico. Anule la selección de la opción para personalizar el aspecto de manera independiente a los parámetros del programa de correo electrónico.

Mostrar el texto – ver las descripciones de los íconos.

Texto a la derecha – las descripciones de las opciones se mueven del sector inferior al lado derecho de los íconos.

Íconos grandes – muestra íconos grandes para las opciones del menú.

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 Security, 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:

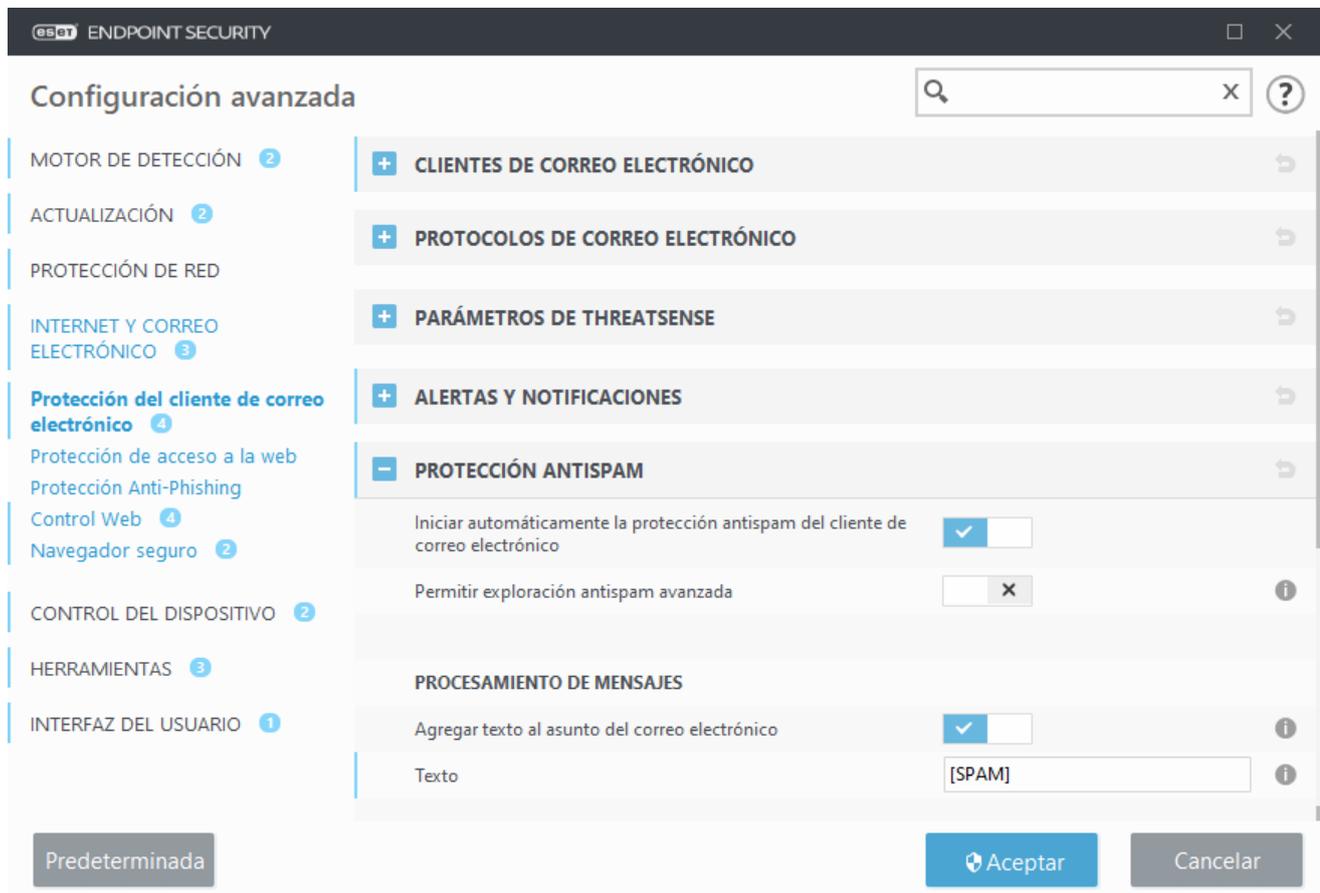
Todos los mensajes de la carpeta actual – explora los mensajes en la carpeta actualmente abierta.

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.

Protección antispam

El correo electrónico no solicitado (llamado spam) es uno de los problemas más importantes de la comunicación electrónica. El spam representa hasta 50% de todas las comunicaciones por correo electrónico. La protección antispam sirve para proteger de este problema. Mediante la combinación de varios principios de seguridad del correo electrónico, el módulo antispam proporciona un filtrado superior para mantener su buzón de entrada desinfectado.



Un principio importante para la detección del spam es la habilidad de reconocer correo electrónico no solicitado basándose en direcciones de confianza (lista blanca) y direcciones de spam (lista negra) predefinidas. Todas las direcciones de la lista de contactos se agregan en forma automática a la lista blanca, al igual que otras direcciones que usted marque como seguras.

El método principal utilizado para detectar spam es la exploración de las propiedades de los mensajes de correo electrónico. Los mensajes recibidos se exploran en búsqueda de los criterios antispam básicos (definiciones de mensajes, heurísticas estadísticas, reconocimiento de algoritmos y otros métodos exclusivos) y el valor de índice resultante determina si el mensaje es spam o no.

Iniciar automáticamente la protección antispam del cliente de correo electrónico – al habilitar esta opción, la protección antispam se activará automáticamente con cada inicio del sistema.

Permitir exploración antispam avanzada – se descargarán datos antispam adicionales en forma periódica, aumentando las capacidades antispam y produciendo mejores resultados.

La protección antispam en ESET Endpoint Security permite establecer distintos parámetros para que funcionen con las listas de distribución de correo. Las opciones son las siguientes:

Procesamiento de mensajes

Agregar texto al tema del correo electrónico – permite agregar una cadena de texto personalizada como prefijo a la línea del asunto de los mensajes clasificados como spam. El valor predeterminado es “[SPAM]”.

Mover los mensajes a la carpeta de spam – cuando esta opción está habilitada, los mensajes de spam se enviarán a la carpeta predeterminada de correo electrónico no deseado, y los mensajes reclasificados como “no es” spam se enviarán al buzón de entrada. Cuando hace clic derecho en un mensaje de correo electrónico y selecciona ESET Endpoint Security en el menú contextual, puede elegir las opciones que se aplicarán.

Usar la carpeta: especifique la carpeta personalizada a donde desea mover los correos electrónicos infectados cuando se detecten.

Marcar los mensajes de spam como leídos – habilítela para marcar automáticamente los mensajes de spam como leídos. Resulta útil para centrar su atención en los mensajes “no infectados”.

Marcar los mensajes reclasificados como no leídos – los mensajes originalmente clasificados como spam que luego se cambiaron a “no infectados” se mostrarán como no leídos.

Registro del puntaje de spam – El motor antispam de ESET Endpoint Security le asigna un puntaje de spam a cada mensaje explorado. El mensaje se guardará en el [registro antispam](#) (ESET Endpoint Security > Herramientas > Archivos de registro > Protección antispam).

- **Ninguno** – el puntaje de la exploración antispam no se registrará.
- **Reclasificado y marcado como spam** – seleccione esta opción si desea registrar un puntaje de spam para los mensajes marcados como SPAM.
- **Todos** – se guardarán en el registro todos los mensajes con su puntaje de spam.

i Cuando hace clic en un mensaje de la carpeta de correo electrónico no deseado, puede elegir **Reclasificar los mensajes seleccionados como NO ES spam**, y el mensaje se enviará al buzón de entrada. Cuando hace clic en un mensaje del buzón de entrada que considera como spam, seleccione **Reclasificar los mensajes como spam**, y el mensaje se enviará a la carpeta de correo electrónico no deseado. Puede seleccionar varios mensajes y realizar la acción sobre todos ellos al mismo tiempo.

i La protección antispam de ESET Endpoint Security es compatible con Microsoft Outlook, Outlook Express, Windows Mail y Windows Live Mail.

Libretas de direcciones antispam

La característica antispam de ESET Endpoint Security permite configurar varios parámetros para las listas de direcciones.

Libretas de direcciones

Permitir las listas de direcciones del usuario – habilite esta opción para activar la libreta de direcciones creada por el usuario en su propio cliente de correo electrónico.

Permitir las listas globales de direcciones – Habilite esta opción para activar la libreta de direcciones global compartida por todos los usuarios de esta estación de trabajo, es decir, el servicio de directorio dentro del sistema de correo electrónico. La Lista global de direcciones (GAL, por sus siglas en inglés) contiene información para todos los usuarios de correo electrónico, grupos de distribución y recursos.

Lista blanca del usuario – lista de contactos donde puede agregar, editar o eliminar direcciones que son consideradas seguras y de las que el usuario desea recibir mensajes.

Lista negra del usuario– lista de contactos donde puede agregar, editar o eliminar direcciones que no son consideradas seguras y de las que el usuario no desea recibir mensajes.

Lista de excepciones del usuario– esta lista de contactos contiene las direcciones de correo electrónico que pueden haberse alterado y utilizado para enviar spam. Consulte también [Lista de excepciones](#).

Lista blanca/Lista negra/Lista de excepciones globales– Estas listas se utilizan para aplicar políticas antispam a todos los usuarios que utilicen ESET Endpoint Security en esta estación de trabajo. Cuando ESET Endpoint Security se [administra de forma remota](#), se aplica la política ESET PROTECT/ESCM/ECA en todas las estaciones de trabajo asignadas.

Agregar a la lista blanca del usuario en forma automática

Agregar direcciones de la libreta de direcciones – agregue direcciones desde su lista de contactos a la [Lista blanca](#).

Agregar las direcciones de destinatarios desde los mensajes salientes – agregue direcciones de destinatarios desde los mensajes enviados a la Lista blanca.

Agregar las direcciones de los mensajes reclasificados como NO ES spam – agregue a la Lista blanca direcciones de remitentes desde mensajes reclasificados como NO ES spam.

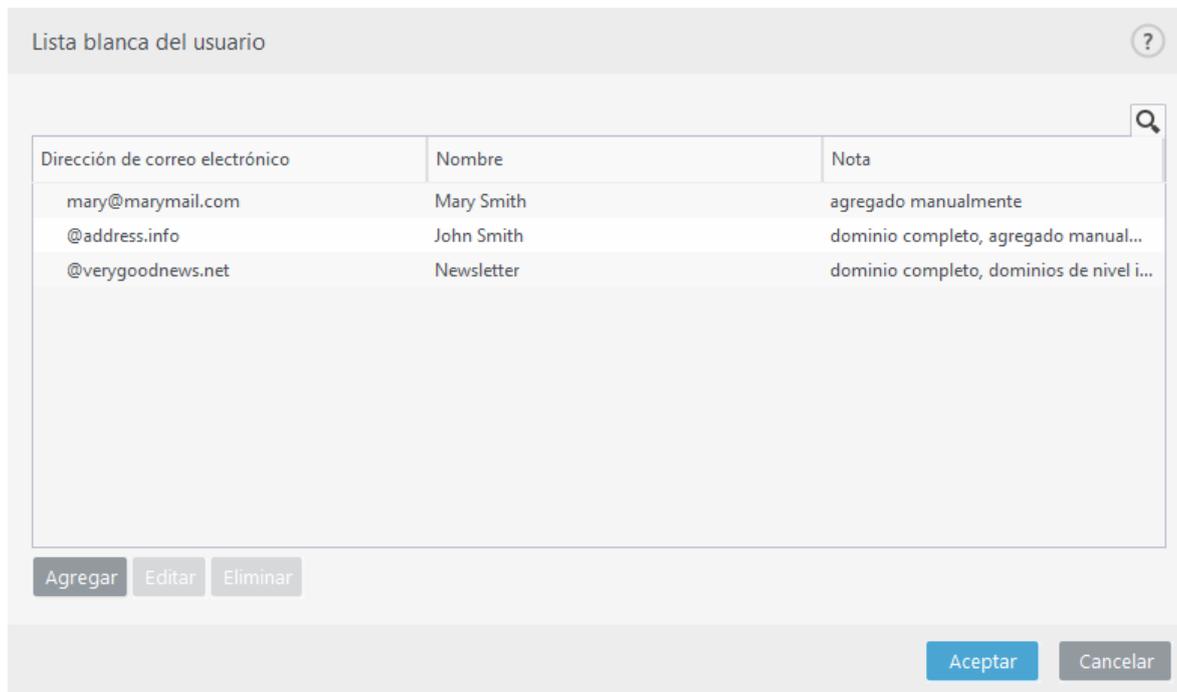
Agregar a la lista de excepciones del usuario en forma automática

Agregar direcciones de cuentas propias – agregue sus direcciones desde cuentas existentes del cliente de correo electrónico a la [Lista de excepciones](#).

Lista negra/Lista blanca/Lista de excepciones

Para proporcionar protección ante correos electrónicos no solicitados, ESET Endpoint Security le permite clasificar las direcciones de correo electrónico mediante el uso de listas especializadas. La [Lista blanca](#) contiene direcciones de correo electrónico que considera seguras. Los mensajes de usuarios que aparecen en la Lista blanca siempre están disponibles en la carpeta de correo entrante. La [Lista negra](#) contiene direcciones de correo electrónico clasificadas como spam, y todos los mensajes provenientes de remitentes en la Lista negra se marcan consecuentemente. La lista de excepciones contiene las direcciones de correo electrónico que siempre se verifican en busca de spam, pero también puede contener direcciones de mensajes de correo electrónico no solicitados disfrazados como correo deseado.

Todas las listas se pueden editar desde la ventana principal del programa de ESET Endpoint Security en **Configuración avanzada > Internet y correo electrónico > Protección del cliente de correo electrónico > Libretas de direcciones antispam** mediante el uso de los botones **Agregar**, **Editar** y **Quitar** en la ventana de diálogo de cada lista, o desde **Configuración > Internet y correo electrónico** después de hacer clic en la rueda de engranaje  junto a **Protección antispam**.



De forma predeterminada, ESET Endpoint Security agrega a la lista blanca todas las direcciones de la libreta de direcciones de los clientes de correo electrónico compatibles. La lista negra está vacía en forma predeterminada. La [Lista de excepciones](#) solo incluye en forma predeterminada las direcciones de correo electrónico propias del usuario.

Agregar/Editar lista negra/Lista blanca/Dirección de excepciones

Esta ventana le permite agregar o editar las entradas de las listas blanca y negra. Abra la ventana principal del programa de ESET Endpoint Security en **Configuración avanzada > Web y correo electrónico > Protección del cliente de correo electrónico > Libretas de direcciones antispam**.

Dirección de correo electrónico – la dirección de correo electrónico para agregar o editar.

Nombre – el nombre de la entrada.

Dominio completo – seleccione esta opción para aplicar la entrada al dominio completo del contacto (no solo a la dirección especificada en el campo Dirección de correo electrónico, sino a todas las direcciones del dominio *dirección.info*).

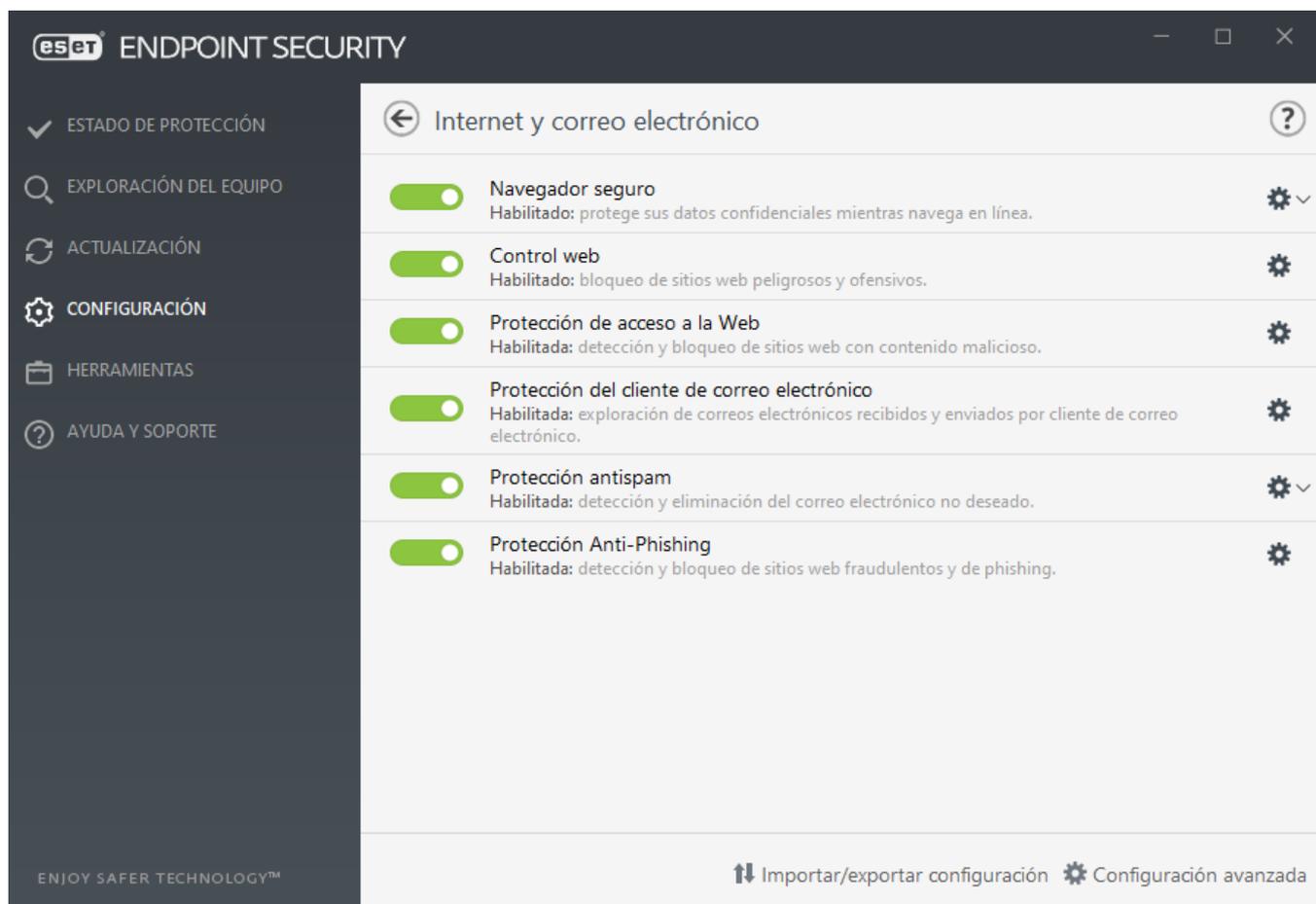
Dominios de nivel inferior – seleccione esta opción para aplicar la entrada a los dominios de nivel inferior del contacto (*dirección.info* representa el dominio, mientras que *mi.dirección.info* representa un subdominio).

Protección del acceso a la Web

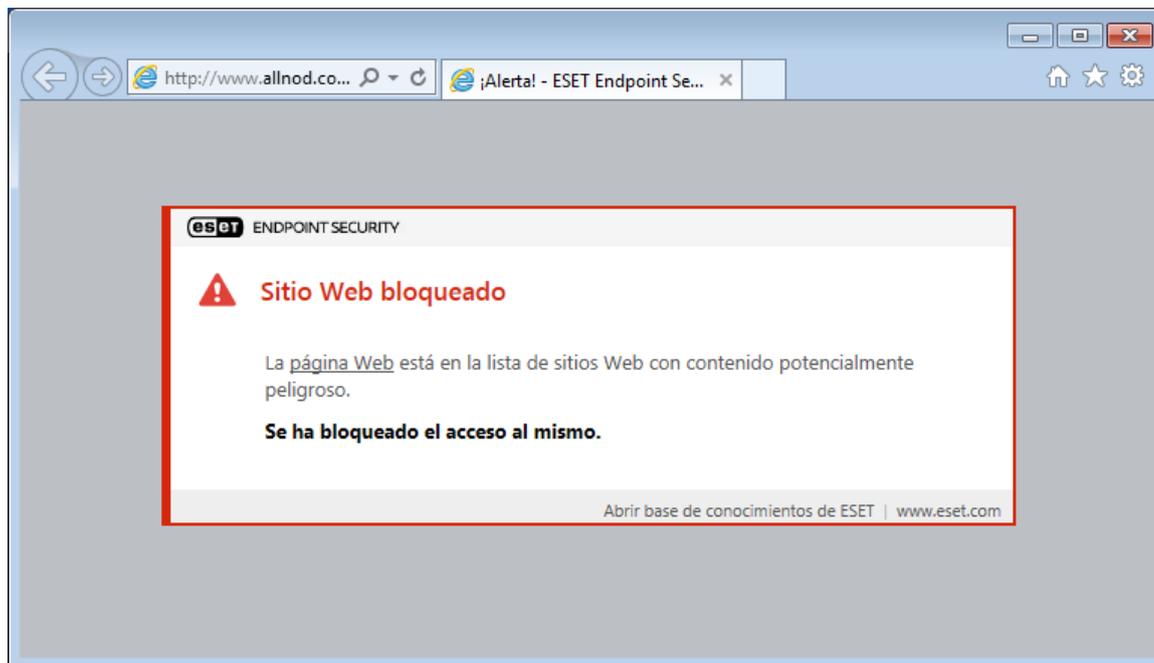
La conectividad a Internet es una función estándar del equipo personal. Lamentablemente, también se convirtió en el medio principal para transferir códigos maliciosos. La función de la protección del acceso a la Web es monitorear la comunicación entre los navegadores Web y los servidores remotos, según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

El acceso a las páginas Web que se sabe que tienen contenido malicioso se bloquea antes de que se descargue el contenido. Todas las otras páginas Web son exploradas por el motor de exploración ThreatSense cuando se cargan, y se bloquean si se detecta contenido malicioso. La protección del acceso a la Web ofrece dos niveles de protección: bloqueo según la lista negra y bloqueo según el contenido.

Se recomienda firmemente que la protección del acceso a la Web esté habilitada. Puede acceder a esta opción desde la ventana principal de ESET Endpoint Security al ir a **Configuración > Protección de Internet > Protección del acceso a la Web**.



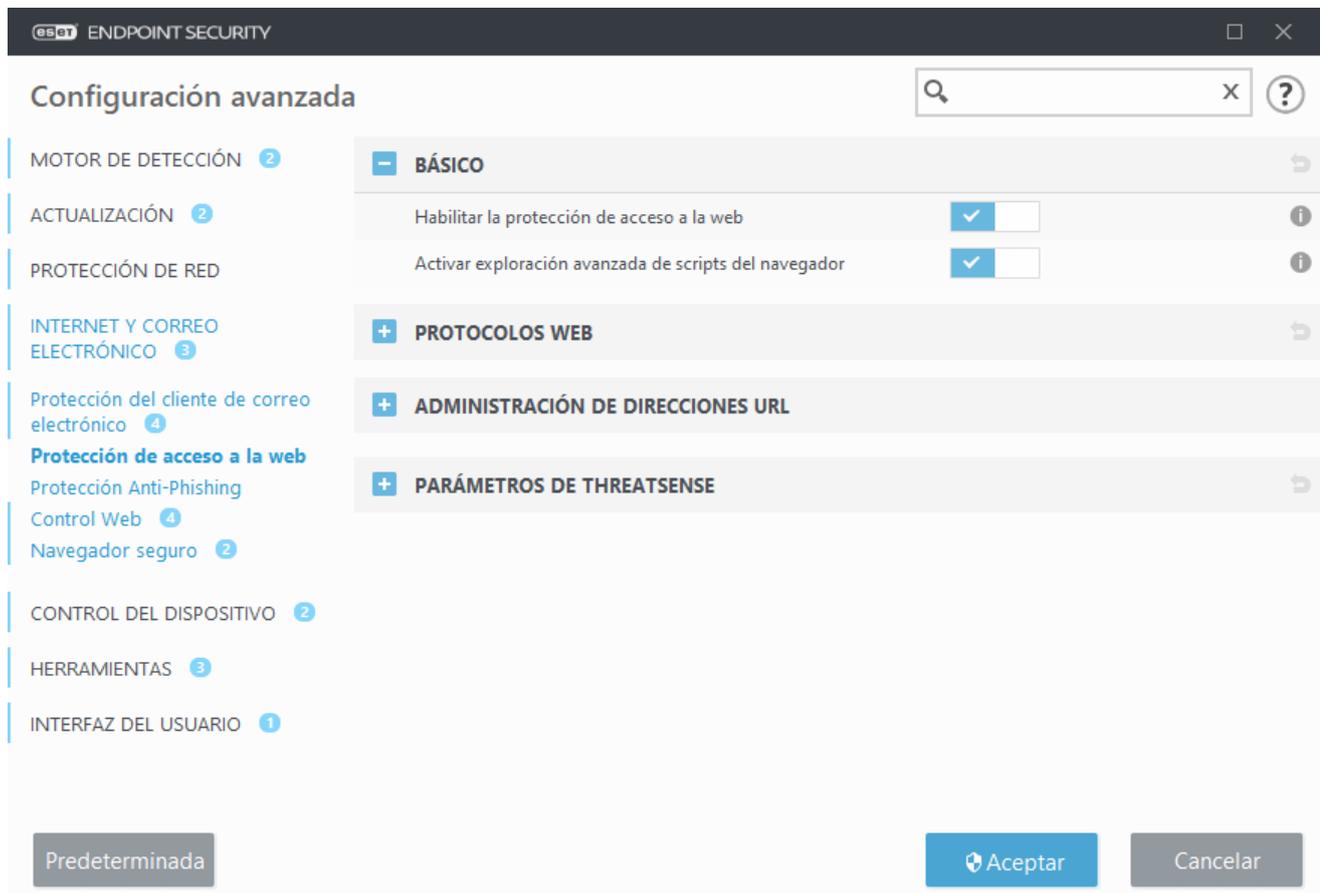
Protección de acceso a la web mostrará al siguiente mensaje en su navegador cuando el sitio web esté bloqueado:



- 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 Security](#)
 - [Desbloquear un sitio web seguro en un equipo con ESET Security Management Center](#)

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

- **Básico** – Para habilitar o deshabilitar esta función desde Configuración avanzada.
- **Protocolos de Internet** – Le permite configurar la supervisión de estos protocolos estándar, que son utilizados por la mayoría de los navegadores de Internet.
- **Administración de direcciones URL** – Le permite especificar las direcciones URL que se desea bloquear, permitir o excluir de la verificación.
- **ThreatSense parámetros:** la configuración avanzada del módulo de exploración de virus le permite configurar propiedades como, por ejemplo, los tipos de objetos que se explorarán (correos electrónicos, archivos comprimidos, etc.), los métodos de detección para la protección del acceso a la Web, etc.



Configuración avanzada de la protección de acceso a la web

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

Habilitar la protección de acceso a la web – Cuando está deshabilitada, no se ejecuta la [Protección del acceso a la web](#) ni la [Protección anti-phishing](#).

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

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

Protocolos Web

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

Configuración de la exploración de HTTP

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

Configuración de a exploración de HTTPS

ESET Endpoint Security también admite la verificación del protocolo HTTPS. La comunicación de HTTPS utiliza un canal cifrado para transferir información entre el servidor y el cliente. ESET Endpoint Security verifica la comunicación mediante los protocolos SSL (protocolo de capa de socket seguro) y TLS (seguridad de la capa de transporte). El programa solo explorará el tráfico en los puertos (443, 0-65535) definidos en **Puertos utilizados por el protocolo HTTPS**, independientemente de la versión del sistema operativo.

Por defecto, la comunicación encriptada será explorada. Para ver la configuración del explorador, vaya a [SSL/TLS](#) en la sección de configuración avanzada, haga clic en **Web y correo electrónico > SSL/TLS** y habilite la opción **Habilitar SSL/TLS el filtrado de protocolos**.

Administración de direcciones URL

La sección sobre administración de direcciones URL permite especificar las direcciones HTTP que se desean bloquear, permitir o excluir de la exploración del contenido.

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

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

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

Pueden utilizarse los símbolos especiales * (asterisco) y ? (signo de interrogación) en las listas. El asterisco sustituye a cualquier cadena de caracteres y el signo de interrogación, a cualquier símbolo. Se debe tener especial cuidado al especificar las direcciones excluidas, ya que la lista debe contener solamente 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**.

i Con la administración de direcciones URL usted puede bloquear o permitir la apertura de tipos de archivos específicos durante la navegación por Internet. Por ejemplo, si no desea que se abran los archivos ejecutables, seleccione la lista donde desea bloquearlos desde el menú desplegable y luego ingrese la máscara "***.exe".

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

Lista de direcciones ?

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

Agregar
Editar
Eliminar
Importar
Exportar

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

Aceptar
Cancelar

Elementos de control

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

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

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

Lista de direcciones URL

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

De forma predeterminada, se pueden utilizar estas tres listas:

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

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

Lista de direcciones ?

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

Agregar
Editar
Eliminar
Importar
Exportar

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

Aceptar
Cancelar

- i** 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 Security](#)
 - [Desbloquear un sitio web seguro en un equipo con ESET Security Management Center](#)

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

Crear nueva lista de direcciones URL

Esta sección le permitirá indicar las listas de direcciones/máscaras URL que se bloquearán, permitirán o excluirán de la verificación.

Al crear una lista nueva, las siguientes opciones de configuración se encuentran disponibles:

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

- **Excluida de la verificación** – no se comprobará la existencia de códigos maliciosos en ninguna de las direcciones agregadas a esta lista.
- **Bloqueadas** – el usuario no tendrá acceso a las direcciones incluidas en esta lista.
- **Permitidas** – Si su política está configurada para usar esta característica y se agrega el valor del comodín (*) a esta lista, se le permitirá el acceso a las direcciones de esta lista incluso si esas direcciones también están presentes en la lista bloqueada.

Nombre de la lista – especifique el nombre de la lista. Este campo no estará disponible si está editando una de las tres listas predefinidas.

Descripción de la lista – Ingrese una descripción breve para la lista (opcional). Este campo no estará disponible si está editando una de las tres listas predefinidas.

Lista activa – seleccione la barra deslizante para activar la lista.

Notificar al aplicar – seleccione la barra deslizante si desea que se le notifique cuando se utiliza esta lista en la evaluación de un sitio HTTP que usted visitó. Por ejemplo, se emitirá una notificación cuando un sitio web esté

bloqueado o permitido por estar incluido en la lista de direcciones bloqueadas o permitidas. La notificación mostrará el nombre de la lista para la lista que especifique el sitio web.

Severidad de registro – seleccione la severidad de registro del menú desplegable. ESMC o ESET PROTECT puede recopilar los registros con el nivel de detalle de Advertencia.

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 es posible para las direcciones creadas con **Agregar**.

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

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

Cómo agregar una máscara URL

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

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

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

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

Una primera secuencia “*.” se trata de modo especial si se utiliza al comienzo del nombre del dominio. Primero, el comodín * no coincide con carácter de barra (“/”) es 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 mediante una sola máscara. Por ejemplo la máscara *.domain.com también coincide con *http://domain.com*. Utilizar **domain.com* sería incorrecto, ya que también coincidiría con *http://anotherdomain.com*.

Protección antiphishing

El término phishing define una actividad criminal que utiliza la ingeniería social (manipula a los usuarios para obtener información confidencial). El phishing suele utilizarse para obtener el acceso a datos confidenciales, como números de cuentas bancarias, códigos de identificación personal, etc. Obtenga más información sobre esta actividad en el [glosario](#). ESET Endpoint Security incluye protección antiphishing, que bloquea las páginas web conocidas por distribuir este tipo de contenido.

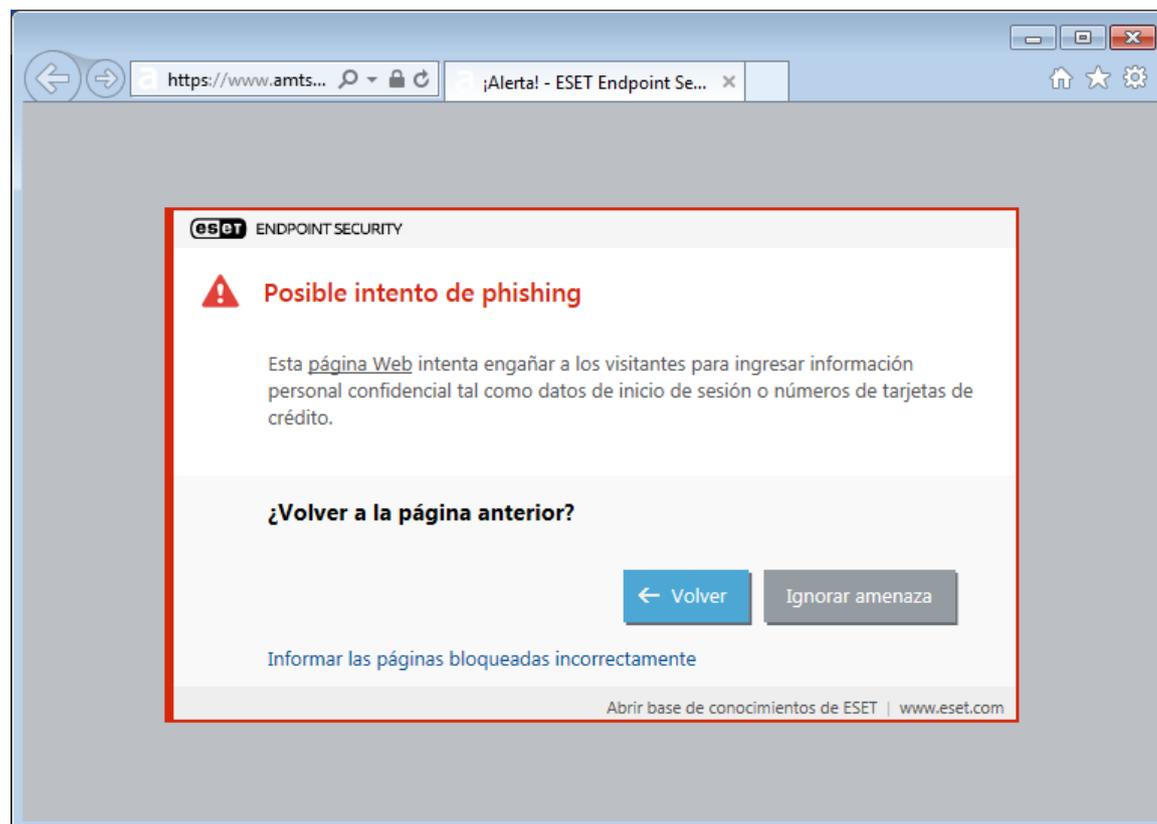
Se recomienda firmemente habilitar Anti-Phishing en ESET Endpoint Security. Para hacerlo, abra **Configuración**

avanzada (F5) y vaya a **Internet y correo electrónico > Protección antiphishing**.

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

Acceso a un sitio Web de phishing

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



Los posibles sitios Web de phishing de la lista blanca se vencerán, de forma predeterminada, luego de algunas horas. Para permitir un sitio Web de manera permanente, use la herramienta [Administración de direcciones URL](#). En **Configuración avanzada (F5)** expanda **Internet y correo electrónico > Protección del acceso a la web > Administración de direcciones URL > Lista de direcciones**, haga clic en **Editar**, y luego agregue a la lista el sitio web que desea editar.

Informe de un sitio de phishing

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

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

- el programa directamente no detecta el sitio Web,
- el programa detecta erróneamente el sitio Web como una amenaza. En este caso, puede [Informar un sitio de phishing falso positivo](#).

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

Configuración avanzada de navegador seguro

Esta configuración está disponible en **Configuración avanzada (F5) > Internet y correo electrónico > Navegador seguro**.

Básico

Habilitar navegador seguro: una vez que se habilita, se activa la lista de sitios web protegidos, lo cual le permite abrir la ventana [Sitios web protegidos](#).

Redireccionamiento de sitios web

Habilitar la redirección de sitios web protegidos – Si se habilita, se redirigirán los sitios de la lista de sitios web protegidos y banca por internet interna al navegador seguro.

Sitios Web protegidos: una lista de sitios Web para los que puede elegir cual navegador (normal o seguro) se abre. Se mostrará el logotipo de ESET en el marco del navegador para indicar que la navegación segura está activada.

Páginas seguras de banca y pagos en línea: deshabilitadas en forma predeterminada. Además de la lista en [Sitios web protegidos](#), los sitios Web de la lista interna de ESET se redireccionarán al navegador con protección de ESET. Los sitios Web identificados por ESET se actualizan con regularidad.

Navegador seguro

Habilitar la protección de memoria optimizada – Si se habilita, se protegerá la memoria del navegador seguro contra inspecciones de otros procesos.

Habilitar protección con el teclado: Si se habilita, la información ingresada con el teclado en el navegador seguro estará oculta para otras aplicaciones. Esta opción aumenta la protección contra [registradores de pulsaciones](#).

Configurar alertas interactivas de navegador seguro: le permite abrir la ventana [Alertas interactivas](#).

Sitios Web protegidos

ESET Endpoint Security contiene una lista incorporada de sitios web predeterminados que harán que se abra un navegador protegido. Puede agregar un sitio web o editar el listado de sitios web dentro de la configuración del producto.

Se puede visualizar y editar la lista de **Sitios Web protegidos** en **Configuración avanzada (F5) > Internet y correo electrónico > Navegador seguro > Básica > Sitios Web protegidos > Editar**.

La ventana consiste en:

Columnas

Sitio Web: Sitio Web protegido.

Navegador seguro: el logotipo de ESET se mostrará en el borde del navegador durante la navegación segura.

Navegador normal: seleccione esta opción para continuar en el navegador web predeterminado (por ejemplo, una transacción bancaria).

Elementos de control

Agregar: le permite agregar un sitio Web a las lista de sitios Web conocidos.

Editar: le permite editar las entradas seleccionadas.

Quitar – quita las entradas seleccionadas.

Control Web

La sección Control Web permite configurar las opciones que protegen a su empresa del riesgo de responsabilidad legal. El Control Web puede regular el acceso a sitios Web que violan los derechos de propiedad intelectual. El objetivo es prevenir que los empleados accedan a páginas con contenido inapropiado o perjudicial o páginas que puedan tener un impacto negativo en la productividad.

El Control Web permite bloquear 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.

De forma predeterminada, el control web está deshabilitado. Para activarlo:

- 1.Presione la tecla **F5** e ingrese a **Configuración avanzada** y amplíe la sección **Internet y correo electrónico** > **Control de acceso web**.
- 2.Seleccione **Habilitar el control web** para activar el control web en ESET Endpoint Security.
- 3.Para configurar el acceso a páginas web específicas, haga clic en **Editar** junto a las **Reglas** para acceder a la ventana [Editor de reglas de control web](#).

Configuración avanzada

MOTOR DE DETECCIÓN 2

ACTUALIZACIÓN 2

PROTECCIÓN DE RED

INTERNET Y CORREO ELECTRÓNICO 3

Protección del cliente de correo electrónico 4

Protección de acceso a la web

Protección Anti-Phishing

Control Web 4

Navegador seguro 2

CONTROL DEL DISPOSITIVO 2

HERRAMIENTAS 3

INTERFAZ DEL USUARIO 1

BÁSICO

Habilitar control web

Reglas [Editar](#)

Grupos de categoría [Editar](#)

Grupos de URL [Editar](#)

Mensaje de la página web bloqueada

Gráfico de la página web bloqueado

Predeterminada [Aceptar](#) Cancelar

Los campos **Mensaje de la página web bloqueada** y **Gráfico de la página web bloqueada** permiten [personalizar fácilmente el mensaje que se muestra](#) cuando se bloquea un sitio web.

i En caso de que desee bloquear todas las páginas web y dejar disponibles solo algunas, utilice la opción [Gestión de direcciones URL](#).

Reglas del control Web

La ventana del editor de **Reglas** muestra las reglas existentes basadas en la URL o basadas en la Categoría.

Habilitado	Nombre	Tipo	URL/Categoría	Usuarios	Derechos ...	Severidad	Intervalos ...
<input checked="" type="checkbox"/>	Block page	Acción basada ...	www.blockedpa...	Todos	Bloquear	Siempre	Siempre
<input checked="" type="checkbox"/>	Allow this page	Acción basada ...	www.allowedpa...	Todos	Permitir	Siempre	Siempre
<input checked="" type="checkbox"/>	Group all harmf...	Acción basada ...	Desnudez	Todos	Bloquear	Siempre	Siempre

La lista de reglas contiene varias descripciones de reglas como nombre, tipo de bloqueo, acción a realizar después de hacer coincidir una regla de control Web con la severidad del registro.

Haga clic en **Agregar** o **Editar** para administrar una regla. Haga clic en **Copiar** para crear una regla nueva con opciones predefinidas utilizadas para otra regla seleccionada. Al presionar **Ctrl** y hacer clic, puede seleccionar múltiples reglas y eliminar todas las reglas seleccionadas. La casilla de verificación **Habilitada** deshabilita o habilita una regla; esto puede ser útil si no desea eliminar una regla de forma permanente dado que puede utilizarla en el futuro.

Las reglas se clasifican en función de su prioridad. Las reglas con mayor prioridad se ubican más arriba. Para cambiar la prioridad de una regla, selecciónela y haga clic en el botón de la flecha a fin de aumentar o reducir la prioridad de la regla. Haga clic en la flecha doble para mover la regla hacia abajo o hacia arriba de la lista.

Obtenga más información [sobre la creación de reglas](#).

Agregado de reglas de control Web

La ventana de Reglas de control web le permite crear o modificar manualmente una regla de filtrado del control web existente.

Nombre

Ingrese una descripción de la regla en el campo **Nombre** para lograr una mejor identificación.

Habilitado

Haga clic en el interruptor **Habilitado** para habilitar o deshabilitar la regla. Esto puede resultar útil si no quiere eliminar la regla en forma permanente.

Acción

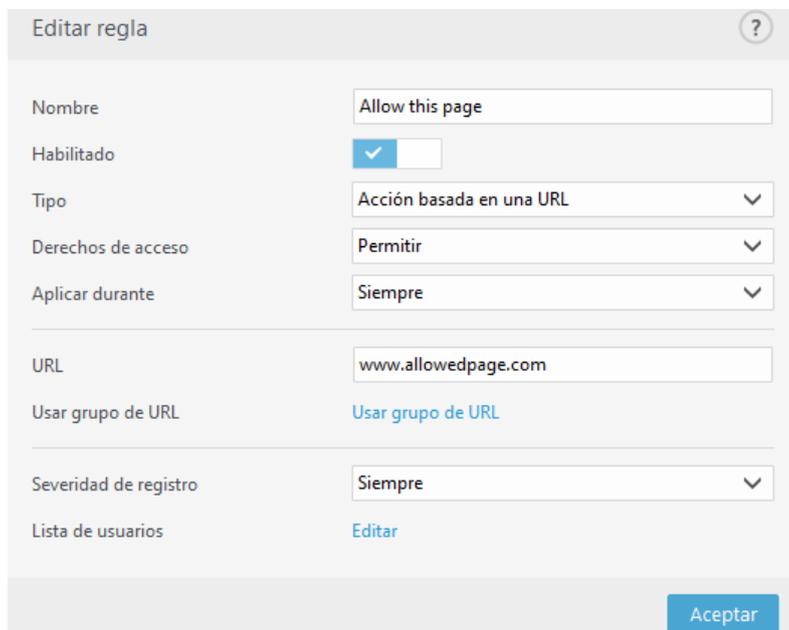
Elija entre **Acción basada en una URL** o **Acción basada en una categoría**:

 [Acción basada en una URL](#)

para las reglas que controlan el acceso a un sitio web determinado, ingrese la URL en el campo **URL**.

Pueden usarse los símbolos especiales * (asterisco) y ? (signo de interrogación) no se pueden utilizar en la lista de direcciones URL. Al crear un grupo de URL que contiene un sitio web con múltiples dominios de nivel superior (TLD), cada TLD se debe agregar por separado. Si agrega un dominio al grupo, todo el contenido ubicado en este dominio y todos los subdominios (por ejemplo, *sub.examplepage.com*) se bloquearán o permitirán en función de su elección de la acción basada en la URL.

URL o **Usar grupo de URL**: utiliza el vínculo URL o el [grupo URL](#) de vínculos para permitir, bloquear o advertir al usuario cuando se detecta una de estas URL.



 [Acción basada en una categoría](#)

Cuando se selecciona esta opción, configure la categoría para su acción mediante el uso del menú desplegable.

Categoría de URL o **Usar grupo**: utiliza la categoría del sitio web o los [grupos de categoría](#) de categorías para permitir, bloquear o advertir al usuario cuando se detecta uno de estos grupos.

Derechos de acceso

- **Permitir** – se otorgará acceso a la dirección/categoría URL.
- **Advertir** – advierte al usuario acerca de la dirección o categoría URL.
- **Advertir siempre**: advierte al usuario acerca de la categoría o dirección URL. Puede continuar al sitio web, pero se notificará al administrador.

- **Bloquear** – bloquea la dirección o la categoría URL.

Aplicar durante

Le permite aplicar la regla creada durante el tiempo especificado. En el menú desplegable, seleccione el intervalo de tiempo creado.

- [Para obtener más información sobre los intervalos de tiempo](#)

Severidad de registro

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

 La severidad de registro se puede configurar por separado para cada lista. ESET Security Management Center puede recopilar los registros con el estado **Advertencia**.

Lista de usuarios

- **Agregar** – abre la ventana de diálogo **Seleccionar usuarios o grupos**, que le permite seleccionar los usuarios deseados. Cuando no se ingresa ningún usuario, la regla se aplica a todos los usuarios.
- **Quitar** – quita el usuario seleccionado del filtro.

Grupos de categoría

La ventana Grupos de categoría se divide en dos partes. La parte izquierda de la ventana contiene una lista de Grupos de categoría.

- **Agregar**: haga clic para crear un nuevo Grupo de categoría.
- **Editar**: haga clic para editar un Grupo de categoría existente.
- **Quitar**: seleccione y haga clic aquí para quitar un grupo de categoría existente de la lista de Grupos de categorías.

En la parte derecha de la ventana, se incluye una lista de categorías y subcategorías. Seleccione una categoría de la Lista de categorías para mostrar sus subcategorías. Cada grupo contiene la subcategoría adulto y/o las subcategorías generalmente inapropiadas, así como las categorías que generalmente se consideran aceptables. Cuando abre la ventana de Grupos de categoría y hace clic en el primer grupo, puede agregar o quitar categorías o subcategorías de la lista de grupos apropiados (por ejemplo, Violencia o Armas). Las páginas Web con contenido inapropiado se pueden bloquear, o se puede informar a los usuarios después de que se crea una regla con acciones predefinidas.

Seleccione la casilla de verificación para agregar o quitar una subcategoría en un grupo determinado.

Grupos de categoría

Agrupe las categorías de sitios web para simplificar el trabajo con los mismos al definir reglas, por ej. en base a su aceptabilidad para u organización.

Grupos

- Grupo 1
- Grupo 2
- Grupo 3

Agregar Editar Quitar

- Actividades criminales
- Alcohol y tabaco
- Archivos compartidos
- Bienes raíces
- Búsqueda laboral
- Compras
- Comunicación y redes sociales
- Deportes peligrosos
- Educación

Aceptar Cancelar

Estos son algunos ejemplos de categorías con las que podrían no estar familiarizados los usuarios:

Varios – por lo general, direcciones IP privadas (locales), como intranet, 192.168.0.0/16, etc. Cuando recibe un código de error 403 o 404, el sitio Web también coincidirá con esta categoría.

No resuelto – esta categoría incluye páginas Web no resueltas debido a un error de conexión con el motor de la base de datos de control Web.

No categorizado – páginas Web desconocidas que aún no forman parte de la base de datos de control Web.

Proxies – pueden usarse páginas Web como anonimadores, redirectores o servidores proxy públicos para acceder (en forma anónima) a páginas Web generalmente prohibidas por el filtro de control Web.

Uso compartido de archivos – estas páginas Web contienen grandes cantidades de datos, como fotos, videos o libros electrónicos. Existe el riesgo de que estos sitios contengan material para adultos o potencialmente ofensivo.

i Una subcategoría puede pertenecer a cualquier grupo. Existen algunas subcategorías que no se incluyen en los grupos predefinidos (por ejemplo, Juegos). Para hacer coincidir una subcategoría deseada por medio del filtro de control Web, agréguela al grupo que desea.

Grupos de URL

Los grupos de URL le permiten crear un grupo que contiene varios vínculos URL para los que desea crear una regla (permitir/no permitir un sitio web particular).

Crear un nuevo grupo de URL

Para crear un nuevo grupo de URL, haga clic en **Agregar** e ingrese el nombre del nuevo grupo de URL.

Usar un grupo de URL puede ser útil cuando el administrador desea crear una regla para más páginas web (bloqueadas o permitidas según su elección).

Agregar direcciones URL a la lista de grupos de URL: de forma manual

Para agregar una nueva dirección URL a la lista, seleccione un grupo de URL y haga clic en **Agregar** en el extremo inferior derecho de la ventana.

No se pueden usar símbolos especiales * (asterisco) y ? (signo de pregunta) en la lista de direcciones URL.

No es necesario ingresar el nombre completo del dominio con http:// o https://.

Si agrega un dominio al grupo, todo el contenido ubicado en este dominio y todos los subdominios (por ejemplo, *sub.examplepage.com*) se bloquearán o permitirán según su acción elegida basada en la URL.

En caso de conflicto entre las dos reglas, en el sentido de que la primera regla bloquea el dominio y la segunda lo permite, la dirección IP o el dominio específico se bloquearán de todos modos. Para obtener más información sobre la creación de reglas, [consulte la acción basada en la URL](#).

Agregar direcciones URL a la lista de grupos de URL: importar usando un archivo .txt

Haga clic en **Importar** para importar un archivo con una lista de direcciones URL (separar valores con un salto de línea, por ejemplo, el archivo .txt que usa codificación UTF-8). No se pueden usar símbolos especiales * (asterisco) y ? (signo de pregunta) en la lista de direcciones URL.

Uso de grupos de URL en el control web

Si desea establecer una acción para que lleve a cabo un grupo de URL específico, abra el [editor de reglas de control web](#), seleccione su grupo de URL con el menú desplegable, ajuste otros parámetros y luego haga clic en **Aceptar**.

i El hecho de bloquear o permitir una página Web específica puede ser más preciso que bloquear o permitir una categoría completa de páginas Web. Tenga precaución al modificar estas opciones y agregar una categoría o página Web a la lista.

Personalización de mensajes de la página web bloqueada

Los campos **Mensaje de la página web bloqueada** y **Gráfico de la página web bloqueada** permiten personalizar fácilmente el mensaje que se muestra cuando se bloquea un sitio web.

Este es el mensaje predeterminado y el diseño de la notificación del navegador cuando un usuario intenta acceder

a un sitio web bloqueado:

Uso

Bloqueemos la categoría de sitio web de “Armas”.

A continuación se incluye un ejemplo de mensaje de la página web bloqueada:

Se bloqueó la página web %URL_OR_CATEGORY% porque se considera que no es apropiada o que incluye contenido nocivo.
Comuníquese con su administrador para obtener detalles.

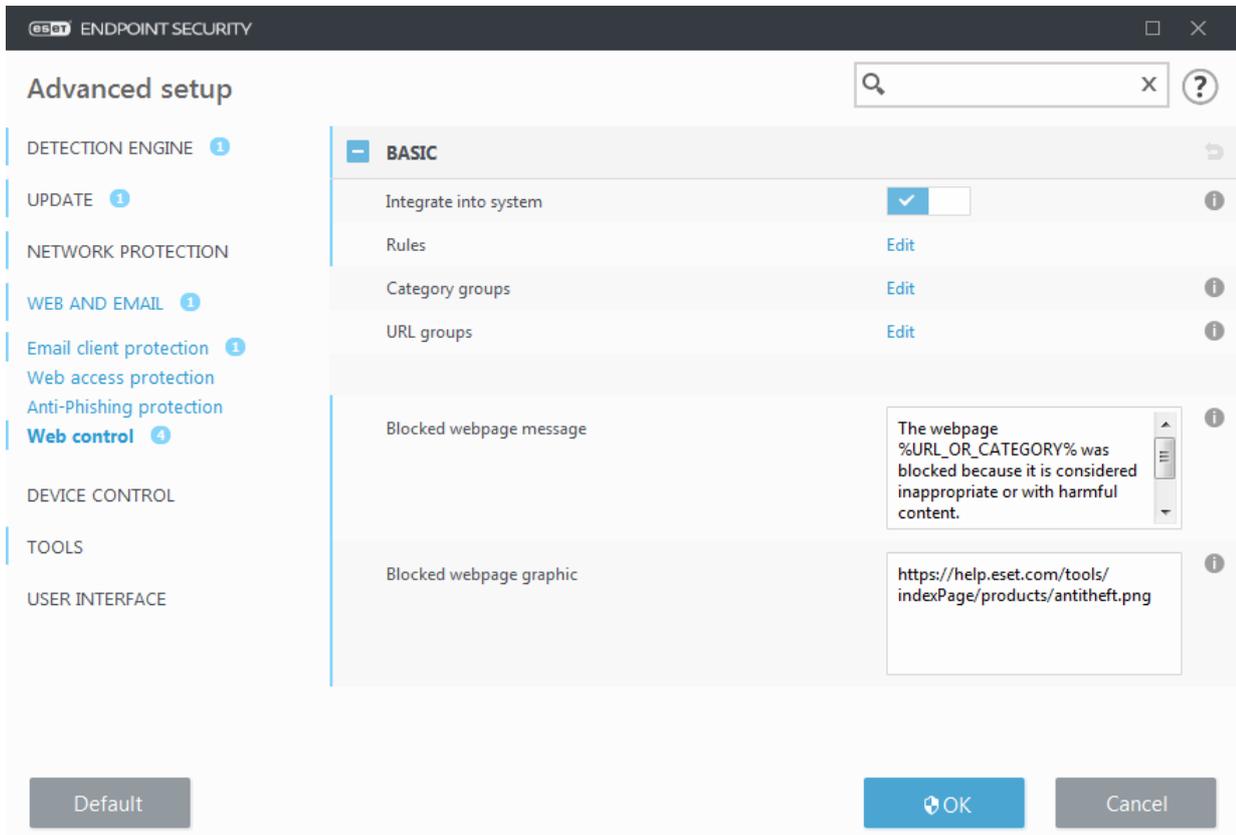
Variable	Descripción
%CATEGORY%	Categoría de control Web bloqueada.
%URL_OR_CATEGORY%	El sitio o categoría con control Web bloqueados (depende de la regla de bloqueo del control Web).
%STR_GOBACK%	Valor del botón “Atrás”.
%product_name%	Nombre del producto de ESET (ESET Endpoint Security)
%product_version%	Versión del producto de ESET.

Ejemplo del gráfico de la página web bloqueada:

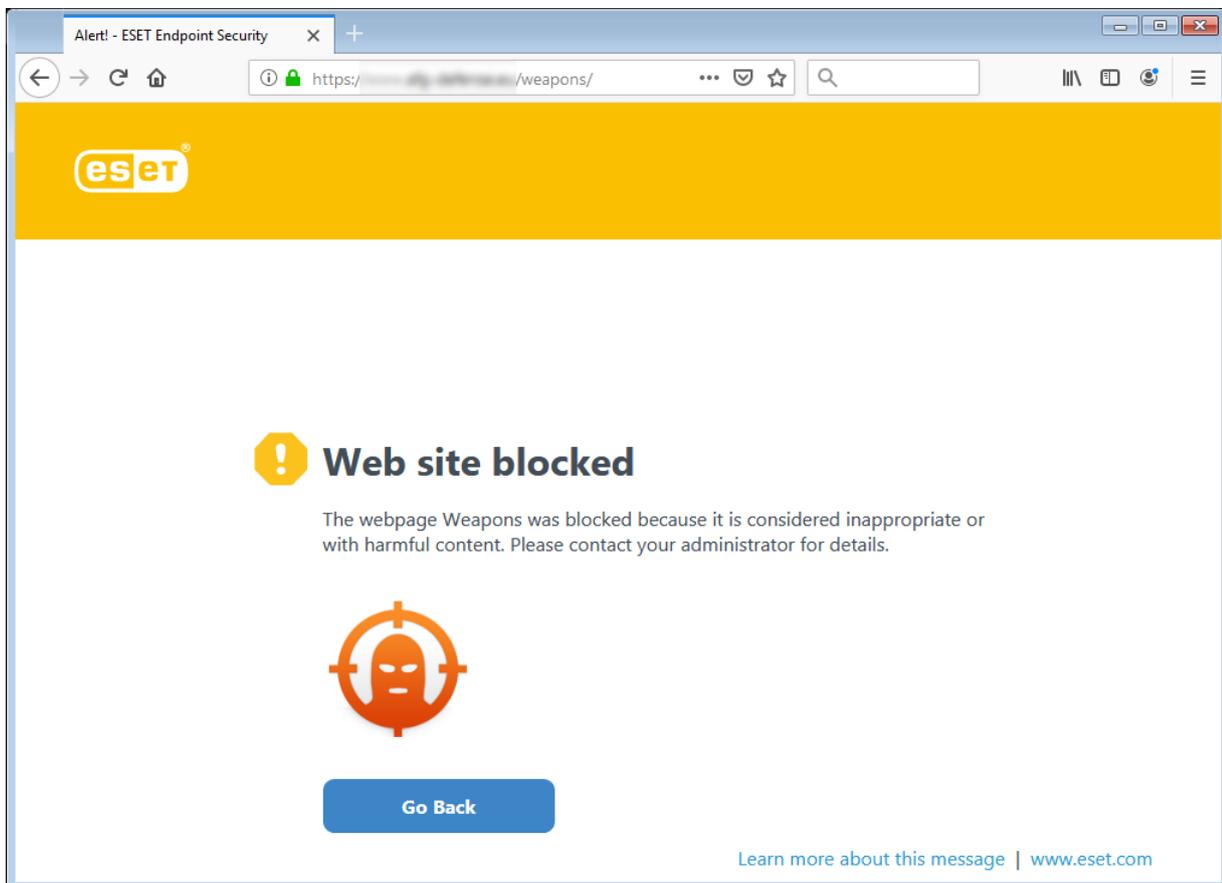
<https://help.eset.com/tools/indexPage/products/antitheft.png>

El tamaño de la imagen (ancho/alto) se escalará automáticamente si está demasiado alto.

La configuración ESET Endpoint Security se verá así:



La notificación personalizada del navegador cuando un usuario intenta acceder a un sitio web bloqueado se verá de la siguiente manera:



Actualización del programa

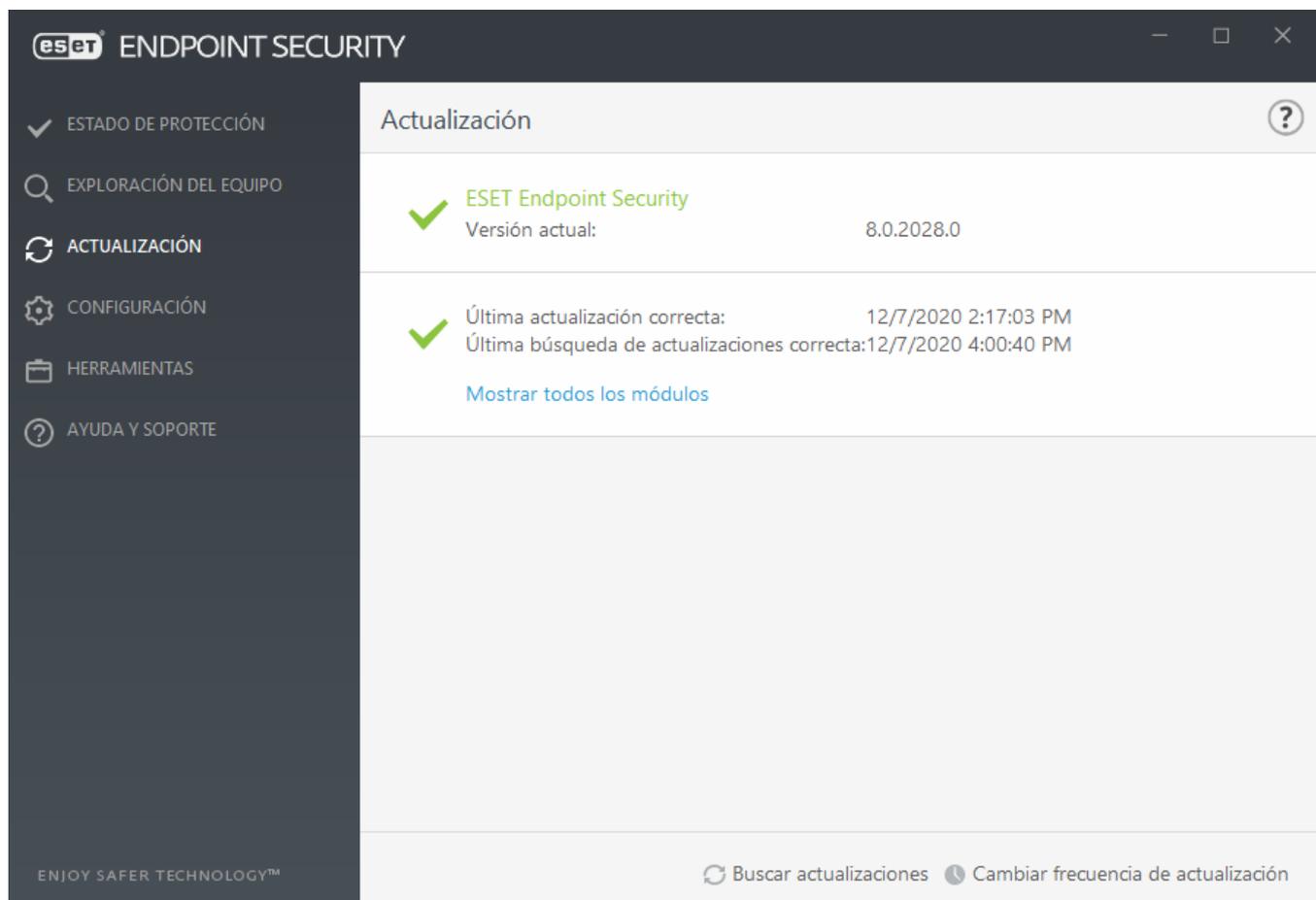
La actualización habitual de ESET Endpoint Security es la mejor forma de obtener el máximo nivel de seguridad en el equipo. El módulo de actualización garantiza que el programa esté siempre al día de dos maneras: actualizando el motor de detección y los componentes del sistema. Las actualizaciones se realizan de manera automática y en forma predeterminada cuando se activa el programa.

Al hacer clic en **Actualización** en la ventana principal del programa, encontrará el estado actual de la actualización, incluyendo la fecha y la hora de la última actualización correcta y si es necesario actualizar. También puede hacer clic en el enlace **Mostrar todos los módulos** para abrir la lista de módulos instalados y comprobar la versión y la última actualización de un módulo.

Además, se encuentra disponible la opción de iniciar el proceso de actualización en forma manual, **Comprobar actualizaciones**. La actualización del motor de detección de virus así como la actualización de componentes del programa constituyen una parte fundamental para mantener una protección completa contra códigos maliciosos. Preste atención a su configuración y funcionamiento. Si no ingresó los detalles de su licencia durante la instalación, puede ingresar su clave de licencia mediante un clic en **Activar producto** cuando realiza una actualización para acceder a los servidores de actualización de ESET.

Si activa ESET Endpoint Security 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.

 ESET le provee su clave de licencia después de la compra de ESET Endpoint Security.



The screenshot shows the 'Actualización' (Update) window of ESET Endpoint Security. The window title is 'Actualización' with a help icon. The main content area displays the following information:

- ESET Endpoint Security** (indicated by a green checkmark)
- Versión actual: 8.0.2028.0
- Última actualización correcta: 12/7/2020 2:17:03 PM
- Última búsqueda de actualizaciones correcta: 12/7/2020 4:00:40 PM

Below this information is a blue link: [Mostrar todos los módulos](#)

At the bottom of the window, there are two buttons: [Buscar actualizaciones](#) and [Cambiar frecuencia de actualización](#).

The left sidebar contains the following menu items: ESTADO DE PROTECCIÓN, EXPLORACIÓN DEL EQUIPO, ACTUALIZACIÓN, CONFIGURACIÓN, HERRAMIENTAS, and AYUDA Y SOPORTE.

The ESET logo and 'ENDPOINT SECURITY' are visible at the top left of the window. The tagline 'ENJOY SAFER TECHNOLOGY™' is at the bottom left.

Versión actual – el ESET Endpoint Security número de compilación.

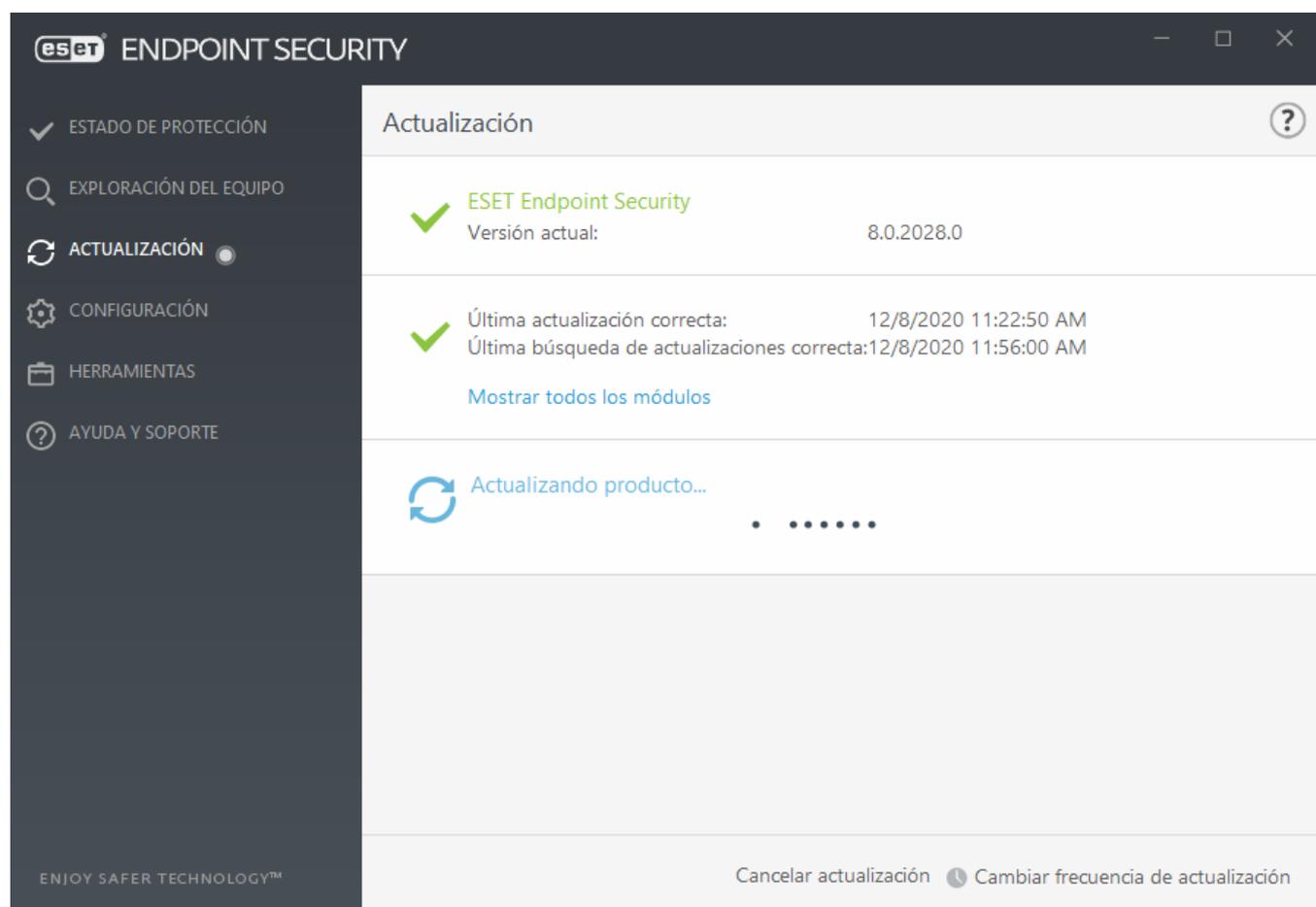
Última actualización exitosa: la fecha y hora de la última actualización exitosa. Asegúrese de que la fecha sea reciente, lo que significa que el motor de detección está al día.

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**.



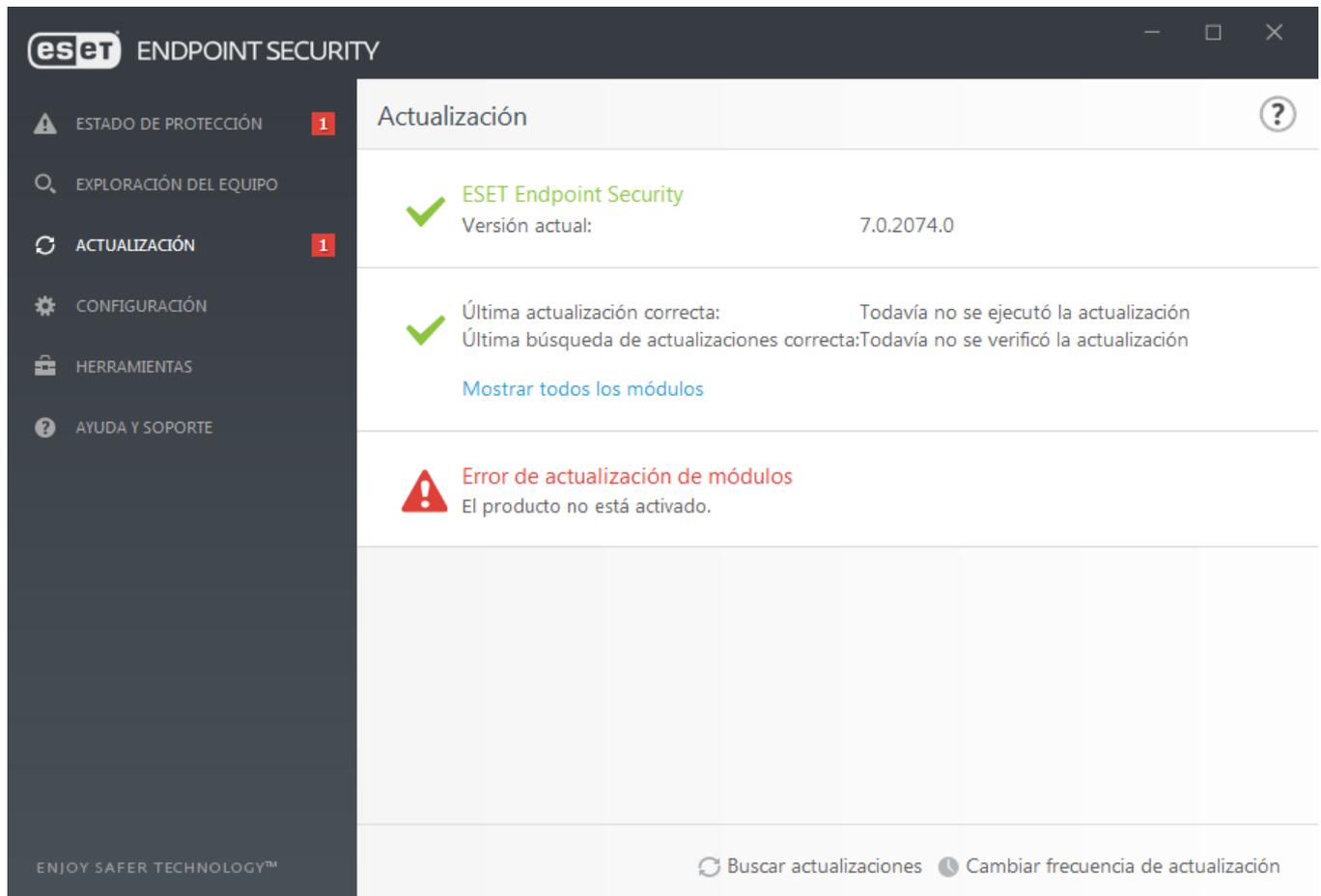
En circunstancias normales, los módulos se actualizan varias veces al día. Si este no es el caso, el programa está desactualizado y más vulnerable a una infección. Actualice los módulos lo antes posible.

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

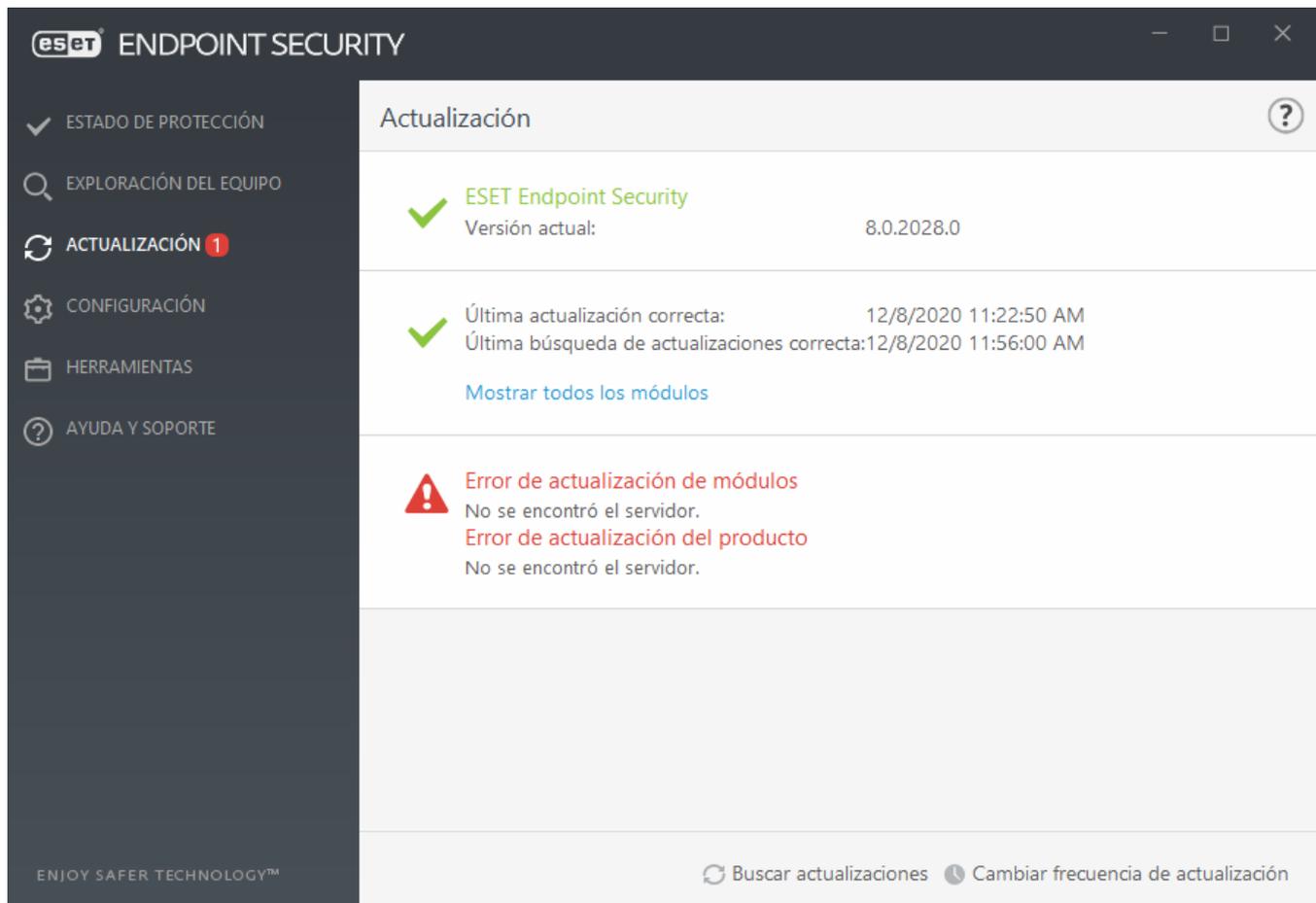
La notificación anterior está relacionada con los dos mensajes siguientes **Falló la actualización de los módulos**

sobre actualizaciones insatisfactorias que se detallan a continuación:

1. **Licencia no válida** – la clave de licencia no se ha ingresado correctamente en la configuración de actualización. Recomendamos que verifique sus datos de autenticación. La ventana Configuración avanzada (haga clic en **Configuración** en el menú principal y luego en **Configuración avanzada** o presione la tecla F5 del teclado) contiene opciones adicionales de actualización. 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. Consulte el problema con su proveedor de servicios de Internet (ISP) si su conexión está inactiva.



 Para obtener más información, visite este [artículo de la Base de conocimiento de ESET](#).

Configuración de la actualización

Actualizar opciones de configuración está disponible en el árbol de **Configuración avanzada** (F5) bajo **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).

Básico

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 [Perfiles](#).

Cambio automático de perfil: asigna un perfil de actualización en función de las redes conocidas en el firewall. El cambio automático de perfil permite que se modifique el perfil de una red específica según los ajustes de Tareas programadas. Consulte las páginas de ayuda para obtener más información.

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 obsoletas del motor de detección

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.

Endpoint Security

Configuración avanzada

- MOTOR DE DETECCIÓN 2
- ACTUALIZACIÓN 2**
- PROTECCIÓN DE RED
- INTERNET Y CORREO ELECTRÓNICO 3
- CONTROL DEL DISPOSITIVO 2
- HERRAMIENTAS 3
- INTERFAZ DEL USUARIO 1

BÁSICO

- Seleccionar el perfil de actualización predeterminado: Mi perfil
- Cambio automático de perfil: Editar
- Configurar notificaciones de actualización: Editar
- Borrar caché de actualización: **Borrar**

ALERTAS DEL MOTOR DE DETECCIÓN OBSOLETAS

Esta configuración define la antigüedad máxima permitida para el motor de detección antes de que se considere obsoleto, y se mostrará una alerta.

- Establecer la antigüedad máxima del motor de detección de forma automática:
- Antigüedad máxima del motor de detección (días): 7

MÓDULO DE REVERSIÓN

- Cree instantáneas de módulos:
- Número de instantáneas almacenadas localmente: 1

Predeterminada

Aceptar Cancelar

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 estableces 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.

The screenshot shows the 'Configuración avanzada' window of ESET Endpoint Security. The left sidebar lists various configuration categories, with 'ACTUALIZACIÓN' selected. The main panel shows the 'BÁSICO' section expanded to 'PERFILES'. Under 'Mi perfil', the 'ACTUALIZACIONES' section is expanded, showing the following settings:

- Tipo de actualización: Actualización normal
- Habilitar la optimización de entrega de actualización:
- Preguntar antes de descargar la actualización: (with an 'X' icon)
- Preguntar si un archivo de actualización es más grande que (kB): 0
- ACTUALIZACIONES DE MÓDULO: Elegir automáticamente:
- Servidor personalizado: Elegir automáticamente

At the bottom, there are buttons for 'Predeterminada', 'Aceptar', and 'Cancelar'.

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 de 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
```

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
```

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

Actualización de componentes del programa

Vea [Actualización de componentes del programa](#).

Opciones de conexión

Vea [Opciones de conexión](#).

Mirror de actualización

Vea [Mirror de actualización](#).

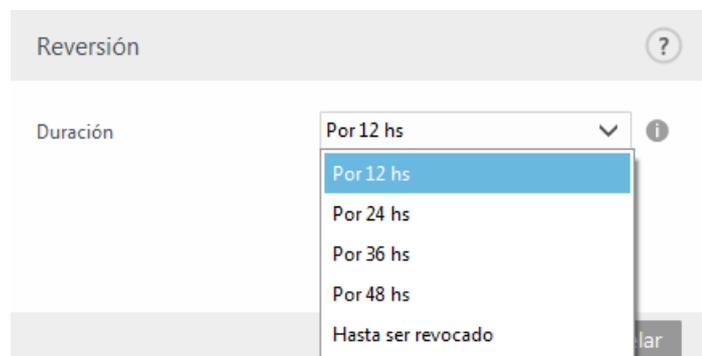
Actualizar reversión

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 Security 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.

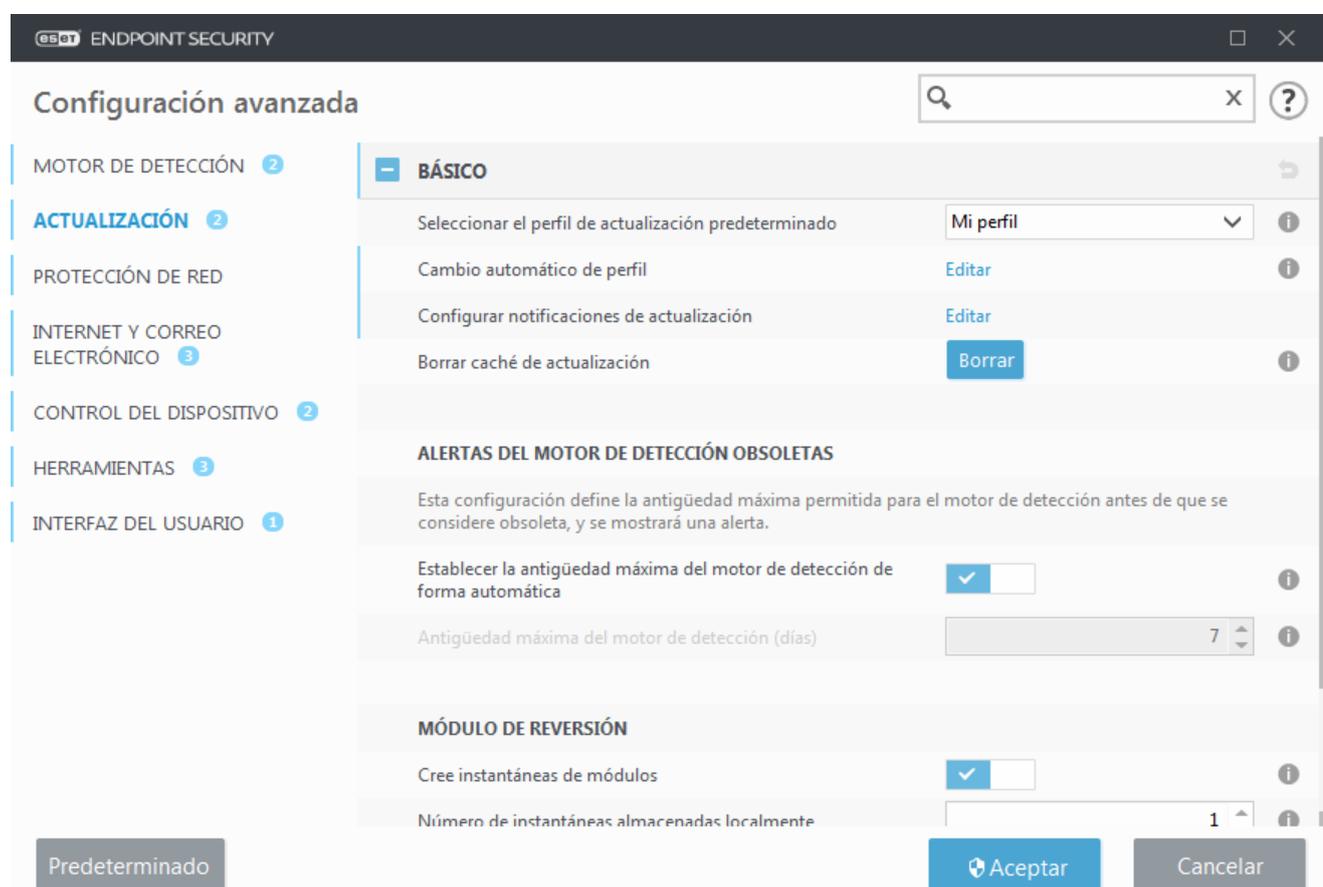
i Cuando se alcanza la cantidad máxima de instantáneas (por ejemplo, tres), la instantánea más antigua se reemplaza con una nueva cada 48 horas. ESET Endpoint Security revierte las versiones de actualización del motor de detección y del módulo del programa a la instantánea más antigua.

Si hace clic en **Revertir (Configuración avanzada (F5) > Actualizar > Básico > Reversión de módulo)**, debe seleccionar un intervalo de tiempo en el menú desplegable **Duración**.



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

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

Actualización de componentes del programa

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

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

En el menú desplegable **Modo de actualización**, hay tres opciones disponibles:

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

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

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

1. Defina la ruta para la actualización de componentes del programa 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 de componente del programa mediante el uso de una actualización estándar de ESET Endpoint Security.

i 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 programa podría provocar serios daños.

Opciones de conexión

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

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

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

Seleccione **No usar servidor proxy** para indicar que no se usará ningún servidor proxy para actualizar ESET Endpoint Security.

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 Security. 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 Security se conectará a un servidor proxy para descargar las actualizaciones.
- El equipo está conectado a Internet mediante un servidor proxy. Durante la instalación del programa, la configuración se copia de Internet Explorer, pero si se cambia (p. ej., cambia el ISP), verifique desde esta ventana que la configuración del proxy sea la correcta. De lo contrario, el programa no podrá conectarse con los servidores de actualización.

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

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

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.

Mirror de actualización

ESET Endpoint Security 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 reflejado 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.



Para minimizar el tráfico de Internet en redes donde se utiliza ESET PROTECT para administrar una gran cantidad de clientes, recomendamos que use Apache HTTP Proxy en lugar de configurar un cliente como servidor reflejado. Apache HTTP Proxy se puede instalar con ESET PROTECT usando el instalador todo en uno o como componente independiente. Para obtener más información y conocer las diferencias entre 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 la Configuración avanzada en **Actualización**. Para acceder a esta sección presione **F5** para acceder a Configuración avanzada, haga clic en

Actualizar > Perfiles y seleccione la pestaña **Actualizar reflejo**.

Configuración avanzada

MOTOR DE DETECCIÓN 2

ACTUALIZACIÓN 5

PROTECCIÓN DE RED

INTERNET Y CORREO ELECTRÓNICO 3

CONTROL DEL DISPOSITIVO 1

HERRAMIENTAS 2

INTERFAZ DEL USUARIO 1

Crear replicación de actualización

ACCEDER A LOS ARCHIVOS DE ACTUALIZACIÓN

Carpeta de almacenamiento
C:\ProgramData\ESET\ESET Smart Security Premium\mirror **Borrar**

Habilitar servidor HTTP

Nombre de usuario

Contraseña

ACTUALIZACIÓN DE COMPONENTES DEL PROGRAMA

Archivos **Editar**

Actualizar componentes automáticamente

Actualizar los componentes ahora **Actualización**

SERVIDOR HTTP

OPCIONES DE CONEXIÓN

Predeterminado **Aceptar** Cancelar

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 Security\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 y la contraseña se deben ingresar con el formato *Dominio/Usuario* o *Grupo de trabajo/Usuario*. Recuerde que debe proporcionar las contraseñas correspondientes.

Actualización de componentes del programa

Archivos – al configurar el Mirror, también puede especificar las versiones de idiomas de las actualizaciones que desea descargar. Los idiomas seleccionados deben ser compatibles con el servidor reflejado configurado por el usuario.

Actualizar componentes automáticamente – permite la instalación de nuevas funciones y las actualizaciones de las funciones ya existentes. Puede realizarse una actualización automáticamente sin la intervención del usuario, pero también se puede elegir recibir una notificación. Luego de instalar la actualización de componentes del programa, es posible que sea necesario reiniciar el equipo.

Actualizar componentes ahora – actualiza los componentes de su programa a la versión más reciente.

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.

i 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.

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 Security 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 > Actualizar > Perfiles > Actualizar Mirror** y que 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:

- Acceda a **Configuración avanzada** (F5) y haga clic en **Actualizar > Perfiles > Actualizaciones > Actualizaciones del 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 Security 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 ESET Endpoint Security **Configuración avanzada** (F5) 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 ESET Endpoint Security **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/era6`

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 activa **Actualizar los componentes del programa**, 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 componente del programa.

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 Security 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 Security 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 Security 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 Security 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.

Cómo crear tareas de actualización

Las actualizaciones pueden accionarse manualmente con un clic en **Buscar actualizaciones** en la ventana primaria que se muestra al hacer clic en **Actualizar** en el menú principal.

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

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

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

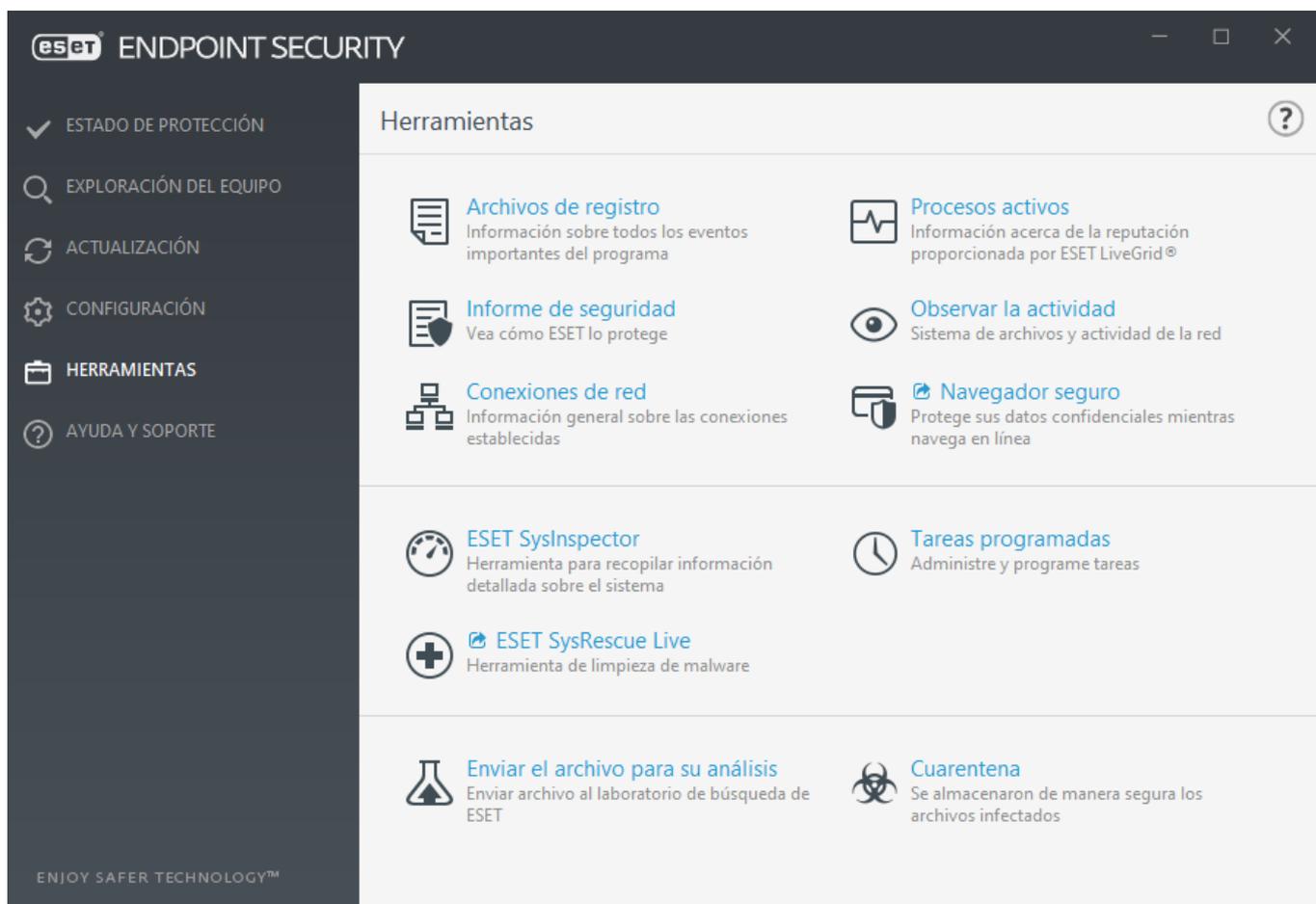
Herramientas

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

Este menú incluye las siguientes herramientas:

- [Archivos de registro](#)
- [Informe de seguridad](#) (para puntos de conexión no administrados)
- [Procesos activos](#) (si ESET LiveGrid® está habilitado en ESET Endpoint Security)
- [Observar la actividad](#)

- [Tareas programadas](#)
- [Conexiones de red](#) (si el [Firewall](#) se encuentra habilitado en ESET Endpoint Security)
- [Navegador seguro](#) (deshabilitado en ESET Endpoint Security de forma predeterminada)
- [ESET SysInspector](#)
- [ESET SysRescue Live](#) – lo redirecciona a la página de ESET SysRescue Live, donde puede descargar la imagen de ESET SysRescue Live .iso para CD/DVD.
- [Cuarentena](#)
- [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).



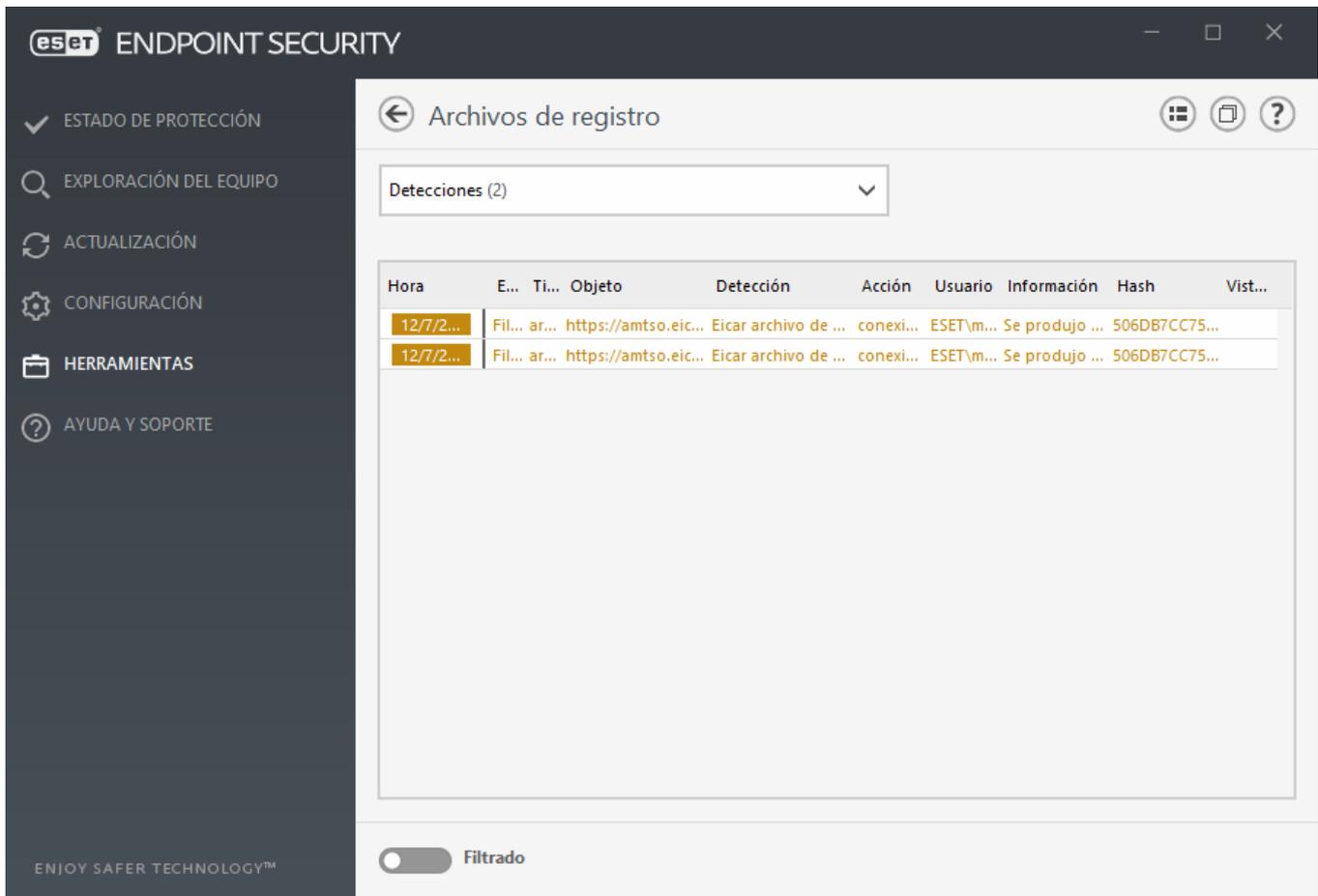
Archivos de registro

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. Es posible ver los mensajes de texto y los registros directamente desde el entorno de ESET Endpoint Security. 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 Security. 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 Security 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 Dynamic Threat Defense](#) 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 la red** – El registro del firewall muestra todos los ataques remotos detectados por la [protección contra ataques de red](#) o el [firewall](#). 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 firewall puede ayudarlo a detectar a tiempo los intentos de infiltraciones en el sistema para prevenir el acceso no autorizado. Para obtener más detalles sobre los ataques de red particular, consulte [IDS y opciones avanzadas](#).
- **Sitios Web filtrados** – Esta lista es útil si desea ver una lista de los sitios Web bloqueados por la [Protección del acceso a la Web](#) o el [Control 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.
- **Protección antispam** – contiene historiales relacionados con los mensajes de correo electrónico que se marcaron como spam.

- **Control Web** – muestra las direcciones URL bloqueadas o permitidas y los detalles acerca de cómo están categorizadas. La columna Acción realizada explica cómo se aplicaron las reglas de filtrado.
- **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, la ventana [Filtrado de registros](#) le permitirá definir los criterios de filtrado para entradas de registros específicas.
- **Habilitar filtro** – activa las configuraciones de los filtros.

- **Deshabilitar el filtro** – borra todas las configuraciones del filtro (descritas arriba).
- **Copiar/Copiar todo** – copia la información sobre todos los historiales que aparecen en la ventana.
- **Eliminar/Eliminar todo** – elimina los historiales seleccionados o todos los historiales mostrados (esta acción requiere privilegios de administrador).
- **Exportar** – exporta información sobre los historiales en formato XML.
- **Exportar todo** – exporta información sobre todos los registros en formato XML.
- **Buscar/Buscar siguiente/Buscar anterior**: después de hacer clic en esta opción, la ventana Filtrado de registros le permite definir los criterios de filtrado para resaltar la entrada específica.
- **Crear exclusión** – Cree una nueva [Exclusión de la detección con un asistente](#) (no disponible para la detección de malware).

Filtrado de registros

Haga clic en **Filtre** en **Herramientas > Archivos de registro** para definir los criterios de filtrado.

La característica de filtrado de registros lo ayudará a encontrar la información que busca, en particular, cuando hay muchos registros. Le permite acotar los registros, por ejemplo, si busca un tipo de evento, un estado o un periodo de tiempo específicos. Puede filtrar los registros al especificar ciertas opciones de búsqueda y solo se mostrarán los registros que sean pertinentes (en función de dichas opciones de búsqueda) en la ventana Archivos de registro.

Escriba la palabra clave que está buscando en el campo **Buscar texto**. Utilice el menú desplegable **Buscar en columnas** para acotar la búsqueda. Elija uno o más registros del menú desplegable **Tipos de registro**. Defina el **periodo de tiempo** para el que quiere que se muestren los resultados. También puede usar otras opciones de búsqueda, como **Solo coincidir palabras completas** o **Coincidir mayúsculas y minúsculas**.

Buscar el texto

Escriba una cadena (palabra o una parte de una palabra). Solo se mostrarán los registros que contengan dicha cadena. Se omitirán otros registros.

Buscar en columnas

Seleccione qué columnas se tomarán en cuenta en la búsqueda. Puede marcar una o más columnas para utilizar en la búsqueda.

Tipos de historiales

Elija uno o más tipos de registro del menú desplegable:

- **Diagnóstico** – registra la información necesaria para ajustar el programa y todos los historiales antes mencionados.
- **Informativo** – registra los mensajes de información, que incluyen los mensajes de actualizaciones correctas, y todos los historiales antes mencionados.
- **Advertencias** – registra los errores críticos y los mensajes de advertencia.
- **Errores** – se registrarán errores tales como “Error al descargar el archivo” y los errores críticos.

- **Crítico** – registra solo los errores críticos (error al iniciar la protección antivirus,

Período de tiempo

Defina el momento a partir del cual desea que se muestren los resultados.

- **Sin especificar** (predeterminado): no busca en un periodo de tiempo, sino en todo el registro.
- **Ayer**
- **Última semana**
- **El mes pasado**
- **Período de tiempo**: puede especificar el periodo de tiempo exacto (Desde: y Hasta:) para filtrar únicamente los registros del periodo de tiempo especificado.

Solo coincidir palabras completas

Utilice la casilla de verificación si quiere buscar palabras completas para resultados más precisos.

Coincidir mayúsculas y minúsculas

Habilite esta opción si es importante para usted usar letras mayúsculas o minúsculas al filtrar. Una vez que haya configurado las opciones de filtrado/búsqueda, haga clic en **Aceptar** para mostrar los registros filtrados o en **Buscar** para comenzar a buscar. Los archivos de registro se buscan de arriba hacia abajo, comenzado por su posición actual (el registro que está resaltado). La búsqueda se detiene cuando encuentra el primer registro coincidente. Presione **F3** para buscar el siguiente registro o haga clic con el botón secundario y seleccione **Buscar** para refinar las opciones de búsqueda.

Configuración de registro

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

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

- **Diagnóstico** – registra la información necesaria para ajustar el programa y todos los historiales antes mencionados.
- **Informativo** – registra los mensajes de información, que incluyen los mensajes de actualizaciones correctas, y todos los historiales antes mencionados.
- **Advertencias** – registra los errores críticos y los mensajes de advertencia.
- **Errores** – se registrarán errores tales como “Error al descargar el archivo” y los errores críticos.
- **Crítico** – registra solo los errores críticos (error al iniciar la protección antivirus, el firewall integrado, etc...).



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. Todas las entradas de registro vacías se eliminan para mejorar el rendimiento y la velocidad de procesamiento del registro. Esta mejora se observa más claramente cuanto mayor sea el número de entradas de los registros.

Habilitar protocolo del texto habilita el almacenamiento de los registros en otro formato de archivo distinto del de los [Archivos de registro](#):

- **Directorio de destino** – 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.



Para ayudar a resolver los problemas más rápidamente, ESET le puede solicitar que proporcione los registros de su equipo. El ESET Log Collector le facilita la recopilación de la información necesaria. Para obtener más información acerca del ESET Log Collector, visite nuestro [artículo de la Base de conocimiento de ESET](#).

Registros de auditorías

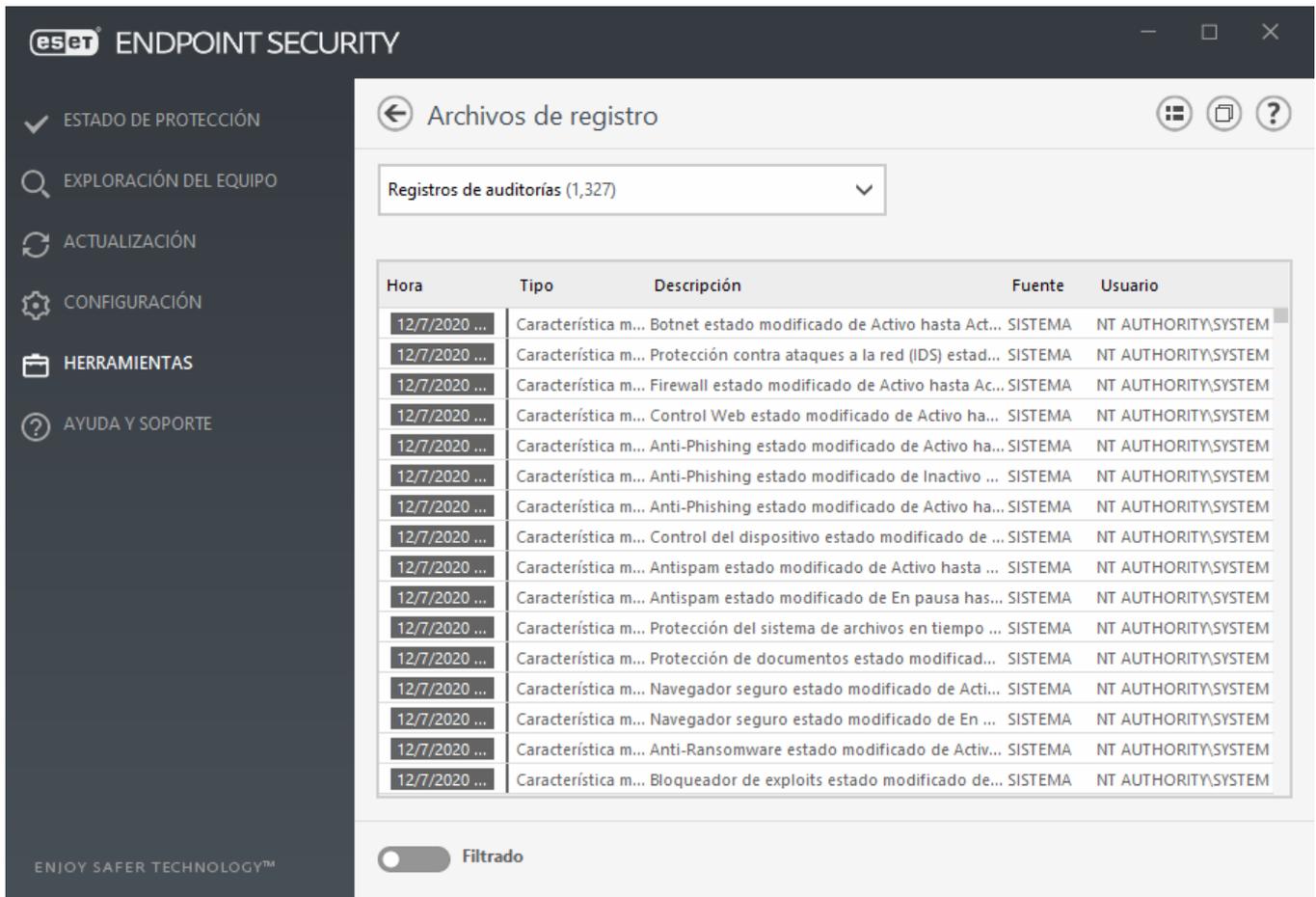
En un entorno empresarial, suele haber varios usuarios con derechos de acceso definidos para configurar puntos de conexión. Debido a que la modificación en la configuración del producto puede afectar de manera significativa su modo de funcionamiento, resulta fundamental que los administradores lleven 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 de ESET Endpoint Security versión 7.1 y una solución 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 ESMC o 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.

Tareas programadas

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

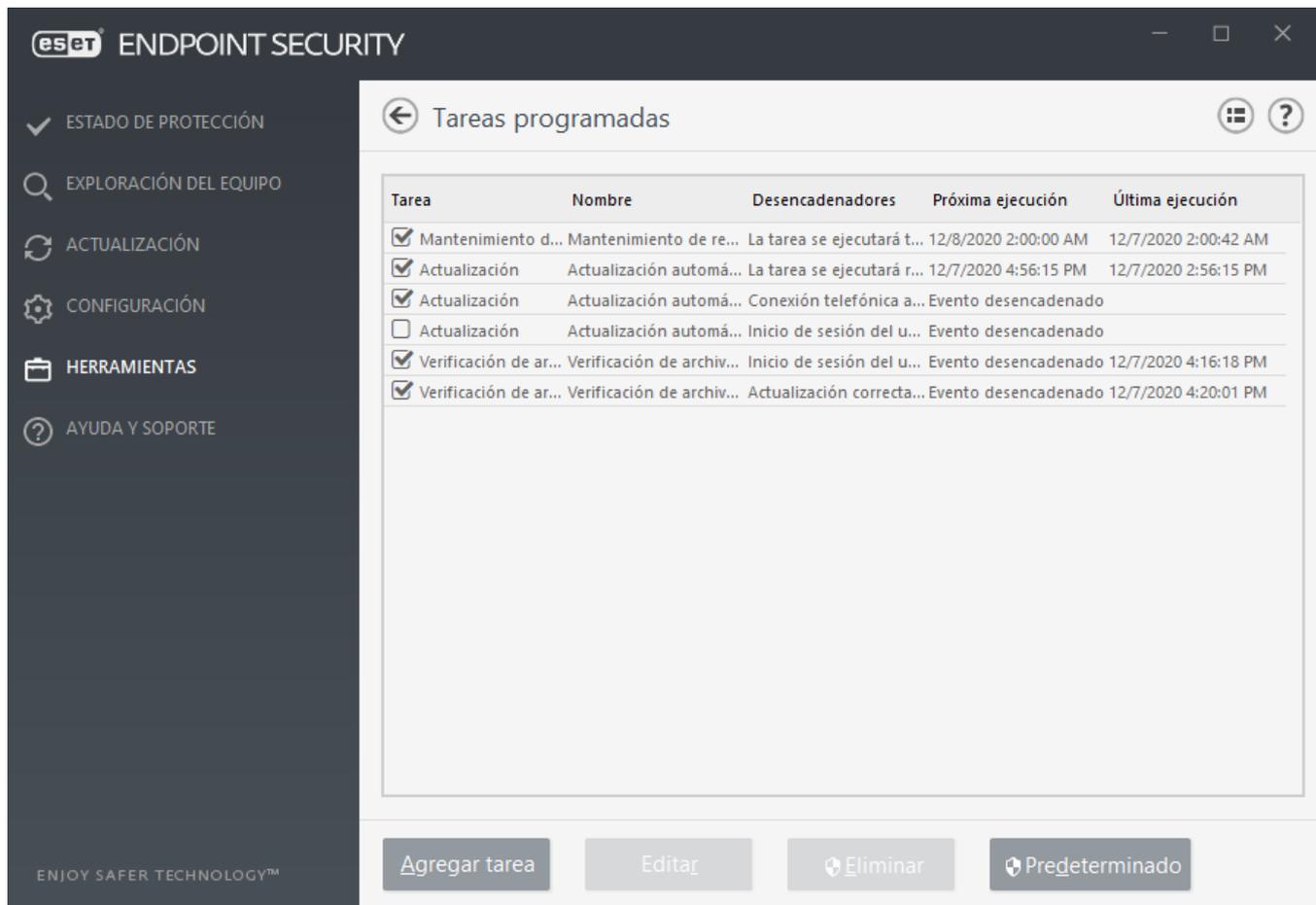
Puede acceder a las tareas programadas desde la ventana principal del programa ESET Endpoint Security, al hacer clic en **Herramientas > Tareas programadas**. La sección **Tareas programadas** contiene una lista de todas las tareas programadas y propiedades de configuración, como la fecha y la hora predefinidas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

Esta sección sirve para programar las siguientes tareas: 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)

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

1. Haga clic en **Agregar tarea** en el sector inferior de la ventana.
2. Escriba el nombre de la tarea.
3. Seleccione la tarea deseada desde el menú desplegable:
 - **Ejecutar aplicación externa** – programa la ejecución de una aplicación externa.
 - **Mantenimiento de registros**: los archivos de registro también contienen remanentes de historiales eliminados. Esta tarea optimiza los historiales de los archivos de registro en forma habitual para que funcionen eficazmente.
 - **Verificación de archivos de inicio del sistema**: verifica los archivos que tienen permiso para ejecutarse al iniciar el sistema o tras el registro del usuario.
 - **Crear una instantánea de estado del equipo**: crea una instantánea del equipo de ESET SysInspector, que recopila información detallada sobre los componentes del sistema (por ejemplo, controladores, aplicaciones) y evalúa el nivel de riesgo de cada componente.
 - **Exploración del equipo a pedido**: realiza una exploración del equipo de los archivos y las carpetas de su equipo.
 - **Actualización** – programa una tarea de actualización mediante la actualización del motor de detección y los módulos del programa.

4. 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**)

Puede rever la tarea programada al hacer clic con el botón secundario y clic en **Mostrar detalles de la tarea**.

Resumen general de tareas programadas ?

Nombre de tarea
Actualización automática tras el registro del usuario

Tipo de tarea
Actualización

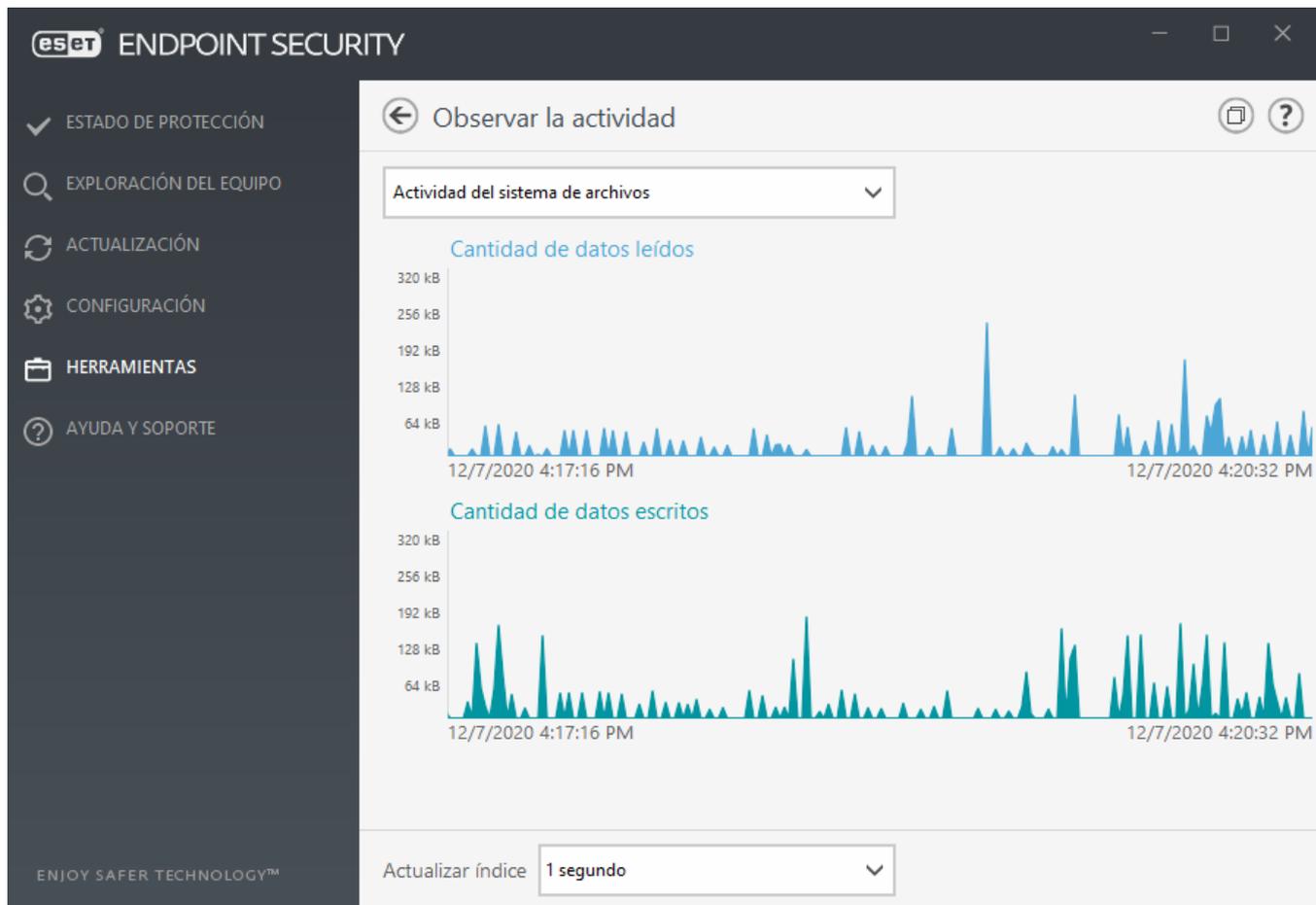
Ejecutar la tarea
El usuario inicie la sesión (una vez cada hora como máximo)

Acción en caso de que la tarea no se ejecute en el momento especificado
A la siguiente hora programada

Aceptar

Observar la actividad

Para observar la **Actividad del sistema de archivos** actual en forma de gráfico, haga clic en **Herramientas > Observar la actividad**. En el sector inferior del gráfico hay una línea de tiempo que registra la actividad del sistema de archivos en tiempo real conforme al intervalo de tiempo seleccionado. Para cambiar el intervalo de tiempo, seleccione **Actualizar índice** en el menú desplegable.



Se encuentran disponibles las siguientes opciones:

- **Paso: 1 segundo** – el gráfico se actualiza cada segundo y la línea de tiempo abarca los últimos 10 minutos.
- **Paso: 1 minuto (últimas 24 horas)** – el gráfico se actualiza cada minuto y la línea de tiempo abarca las últimas 24 horas.
- **Paso: 1 hora (último mes)** – el gráfico se actualiza cada hora y la línea de tiempo abarca el último mes.
- **Paso: 1 hora (el mes seleccionado)** – el gráfico se actualiza cada hora y la línea de tiempo abarca los últimos X meses seleccionados.

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

También puede seleccionar la **Actividad de la red** en el menú desplegable. La visualización del gráfico y las opciones para la **Actividad del sistema de archivos** y la **Actividad de la red** son las mismas, con la excepción de que la segunda muestra la cantidad de datos recibidos (en azul) y la cantidad de datos enviados (en turquesa).

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. [También consulte la Guía del usuario en línea para ESET SysInspector.](#)

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

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

Están disponibles las siguientes opciones:

- **Mostrar** – abre el registro creado. También puede hacer clic derecho en un archivo de registro determinado y seleccionar **Mostrar** en el menú contextual.
- **Comparar** – compara dos registros existentes.
- **Crear** – crea un nuevo registro. Espere hasta que ESET SysInspector finalice (el estado de registro se visualizará como **Creado**) antes de intentar acceder al registro.
- **Eliminar** – elimina los registros seleccionados de la lista.

Los siguientes elementos están disponibles en el menú contextual cuando se seleccionan uno o más archivos de registro:

- **Mostrar** – abre el registro seleccionado en ESET SysInspector (equivale a hacer doble clic en el registro).
- **Comparar** – compara dos registros existentes.
- **Crear** – crea un nuevo registro. Espere hasta que ESET SysInspector finalice (el estado de registro se visualizará como **Creado**) antes de intentar acceder al registro.
- **Eliminar**: elimina el registro seleccionado.
- **Eliminar todo** – elimina todos los registros.
- **Exportar** – exporta el registro a un archivo .xml o .xml comprimido.

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.

Hay tres opciones:

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

El sistema de reputación ESET LiveGrid® proporciona listas blancas y listas 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 Security 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 Security puede responder más rápido a las nuevas amenazas que una actualización del motor de detección cuando ESET LiveGrid® está habilitado.

i 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 Security.

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

Para acceder a la configuración de ESET LiveGrid®, presione **F5** para ingresar a la Configuración avanzada y expanda **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 Dynamic Threat Defense (no visible en ESET Endpoint Security): ESET Dynamic Threat Defense es un servicio pago prestado 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. Recuerde que no recibirá respuesta alguna de ESET a menos que se necesite información adicional.

The screenshot shows the 'Configuración avanzada' (Advanced Configuration) window in ESET Endpoint Security. The window title is 'ESET ENDPOINT SECURITY'. On the left, there is a navigation menu with categories: MOTOR DE DETECCIÓN (2), ACTUALIZACIÓN (2), PROTECCIÓN DE RED, INTERNET Y CORREO ELECTRÓNICO (3), CONTROL DEL DISPOSITIVO (2), HERRAMIENTAS (3), and INTERFAZ DEL USUARIO (1). The 'MOTOR DE DETECCIÓN' category is expanded, showing sub-items: Protección del sistema de archivos en tiempo real, Protección basada en la nube (selected), and Exploración de malware. The 'PROTECCIÓN BASADA EN LA NUBE' section is expanded, showing the following settings:

Configuración	Estado	Acción
Habilitar ESET LiveGrid® sistema de reputación (recomendado)	<input checked="" type="checkbox"/>	i
Habilitar el sistema de comentarios de ESET LiveGrid®	<input checked="" type="checkbox"/>	i
Enviar informes de error y datos de diagnóstico	<input checked="" type="checkbox"/>	i
Enviar estadísticas anónimas	<input checked="" type="checkbox"/>	i
Correo electrónico de contacto (opcional)	<input type="text"/>	i

Below this section is the 'ENVÍO DE MUESTRAS' (Sample Submission) section, which is currently collapsed. At the bottom of the window, there are three buttons: 'Predeterminada' (Default), 'Aceptar' (Accept), and 'Cancelar' (Cancel).

Envío de muestras

Envío manual de muestras: activa la opción de enviar muestras a ESET manualmente desde el menú contextual, [Cuarentena](#) o [Herramientas > Enviar muestra para su análisis](#).

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 detectó. Por ejemplo, las muestras que casi no se detectan o alguno de los [módulos de protección](#) de ESET Endpoint Security 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](#)

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

Exclusiones

El [filtro de exclusión](#) le permite excluir ciertos 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.

ESET Dynamic Threat Defense

Para habilitar el servicio de ESET Dynamic Threat Defense en una máquina de cliente que usa la consola web ESET PROTECT, consulte [Configuración de EDTD para ESET Endpoint Security](#).

Si usted ya utilizó antes 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

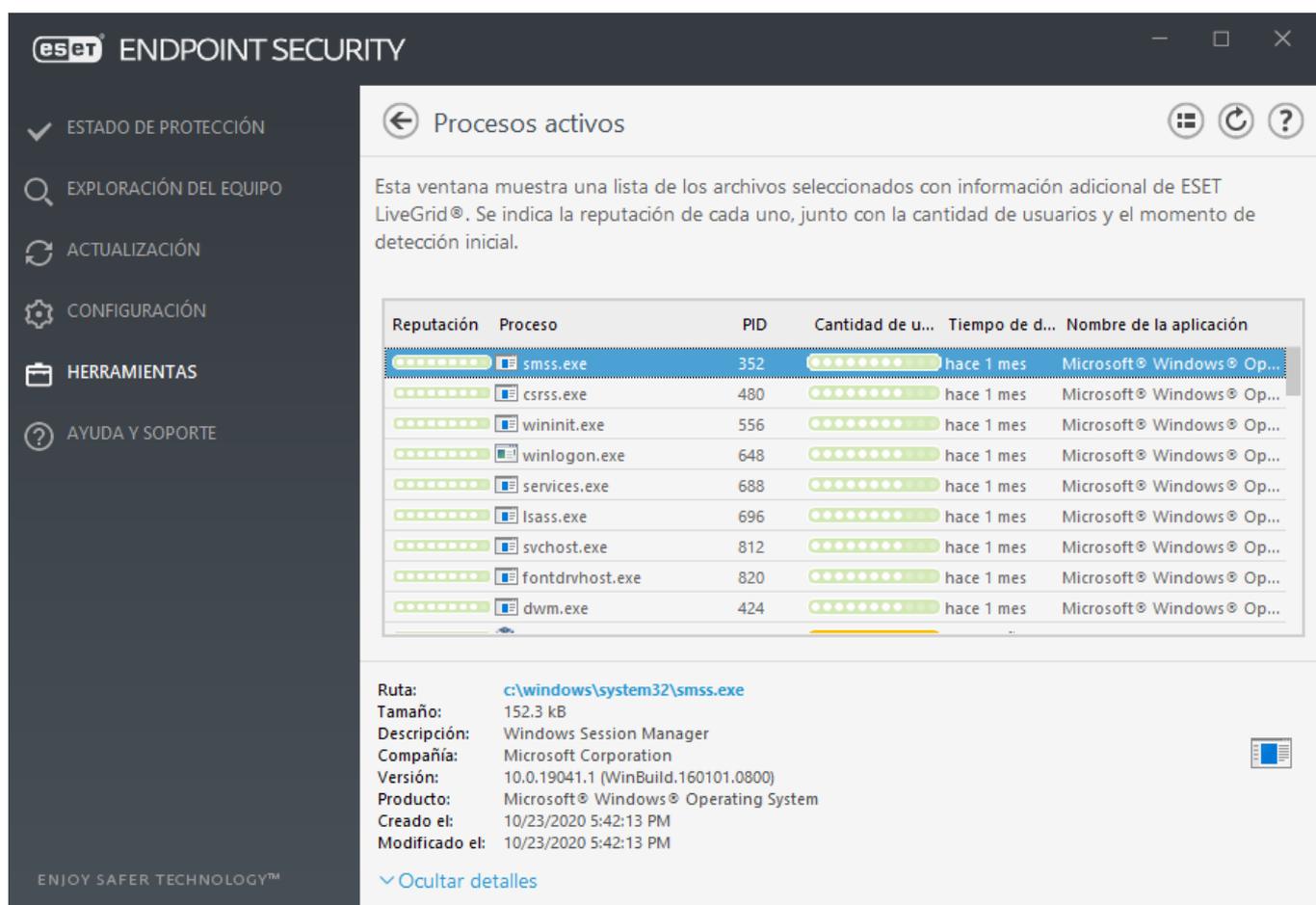
El filtro de exclusión permite excluir ciertos archivos o carpetas del envío de muestras. Los archivos incluidos en la lista nunca se enviarán a los laboratorios de ESET para su análisis, aunque contengan un código sospechoso. Los tipos de archivo comunes (tales como .doc, etc.) se excluyen de forma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

i 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, vaya a **Configuración avanzada > Protección basada en la nube > Envío de muestras > Exclusiones** y agregue la exclusión .download.domain.com.

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 Security proporciona información detallada sobre los procesos activos para proteger a los usuarios con la tecnología [ESET LiveGrid®](#) habilitada.



eset ENDPOINT SECURITY

✓ ESTADO DE PROTECCIÓN
🔍 EXPLORACIÓN DEL EQUIPO
🔄 ACTUALIZACIÓN
⚙️ CONFIGURACIÓN
📁 HERRAMIENTAS
🔗 AYUDA Y SOPORTE

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 d...	Nombre de la aplicación
🟢🟢🟢🟢🟢🟢🟢	smss.exe	352	🟢🟢🟢🟢🟢🟢🟢	hace 1 mes	Microsoft® Windows® Op...
🟢🟢🟢🟢🟢🟢🟢	csrss.exe	480	🟢🟢🟢🟢🟢🟢🟢	hace 1 mes	Microsoft® Windows® Op...
🟢🟢🟢🟢🟢🟢🟢	wininit.exe	556	🟢🟢🟢🟢🟢🟢🟢	hace 1 mes	Microsoft® Windows® Op...
🟢🟢🟢🟢🟢🟢🟢	winlogon.exe	648	🟢🟢🟢🟢🟢🟢🟢	hace 1 mes	Microsoft® Windows® Op...
🟢🟢🟢🟢🟢🟢🟢	services.exe	688	🟢🟢🟢🟢🟢🟢🟢	hace 1 mes	Microsoft® Windows® Op...
🟢🟢🟢🟢🟢🟢🟢	lsass.exe	696	🟢🟢🟢🟢🟢🟢🟢	hace 1 mes	Microsoft® Windows® Op...
🟢🟢🟢🟢🟢🟢🟢	svchost.exe	812	🟢🟢🟢🟢🟢🟢🟢	hace 1 mes	Microsoft® Windows® Op...
🟢🟢🟢🟢🟢🟢🟢	fontdrvhost.exe	820	🟢🟢🟢🟢🟢🟢🟢	hace 1 mes	Microsoft® Windows® Op...
🟢🟢🟢🟢🟢🟢🟢	dwm.exe	424	🟢🟢🟢🟢🟢🟢🟢	hace 1 mes	Microsoft® Windows® Op...

Ruta: [c:\windows\system32\smss.exe](#)
Tamaño: 152.3 kB
Descripción: Windows Session Manager
Compañía: Microsoft Corporation
Versión: 10.0.19041.1 (WinBuild.160101.0800)
Producto: Microsoft® Windows® Operating System
Creado el: 10/23/2020 5:42:13 PM
Modificado el: 10/23/2020 5:42:13 PM

🔍 Ocultar detalles

ENJOY SAFER TECHNOLOGY™

Reputación – en la mayoría de los casos, la tecnología ESET Endpoint Security 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.

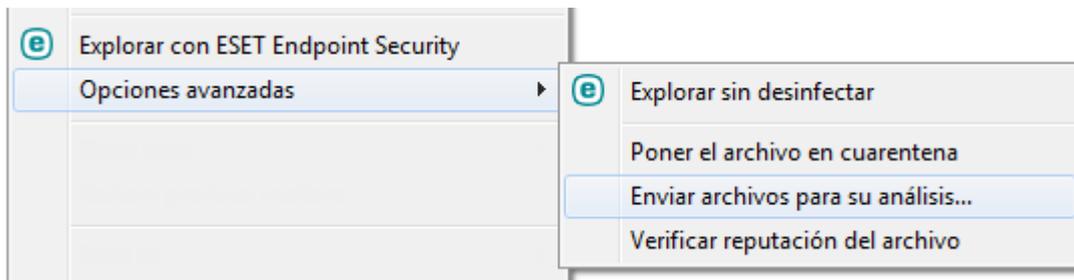
i Si una aplicación está marcada como nivel de seguridad desconocido (naranja), no significa necesariamente que sea software malicioso. Por lo general, solo se trata de una aplicación nueva. Si no está seguro con respecto al archivo, use la función [enviar el archivo para su análisis](#) para enviar 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.
- **Tamaño** – tamaño del archivo ya sea en kB (kilobytes) o MB (megabytes).
- **Descripción** – características del archivo según la descripción proporcionada por el sistema operativo.
- **Empresa** – nombre del proveedor o del proceso de la aplicación.
- **Versión** – información proporcionada por el desarrollador de la aplicación.
- **Producto** – nombre de la aplicación y/o nombre comercial.
- **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.

Páginas web bloqueadas con control de acceso web – Muestra el número de páginas web bloqueadas con el [control de acceso web](#).

PUA detectadas – Muestra el número de [aplicaciones potencialmente no deseadas](#) (PUA).

Spam de correo electrónico detectado – Muestra el número de correos electrónicos de spam detectados.

Documentos revisados – 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.

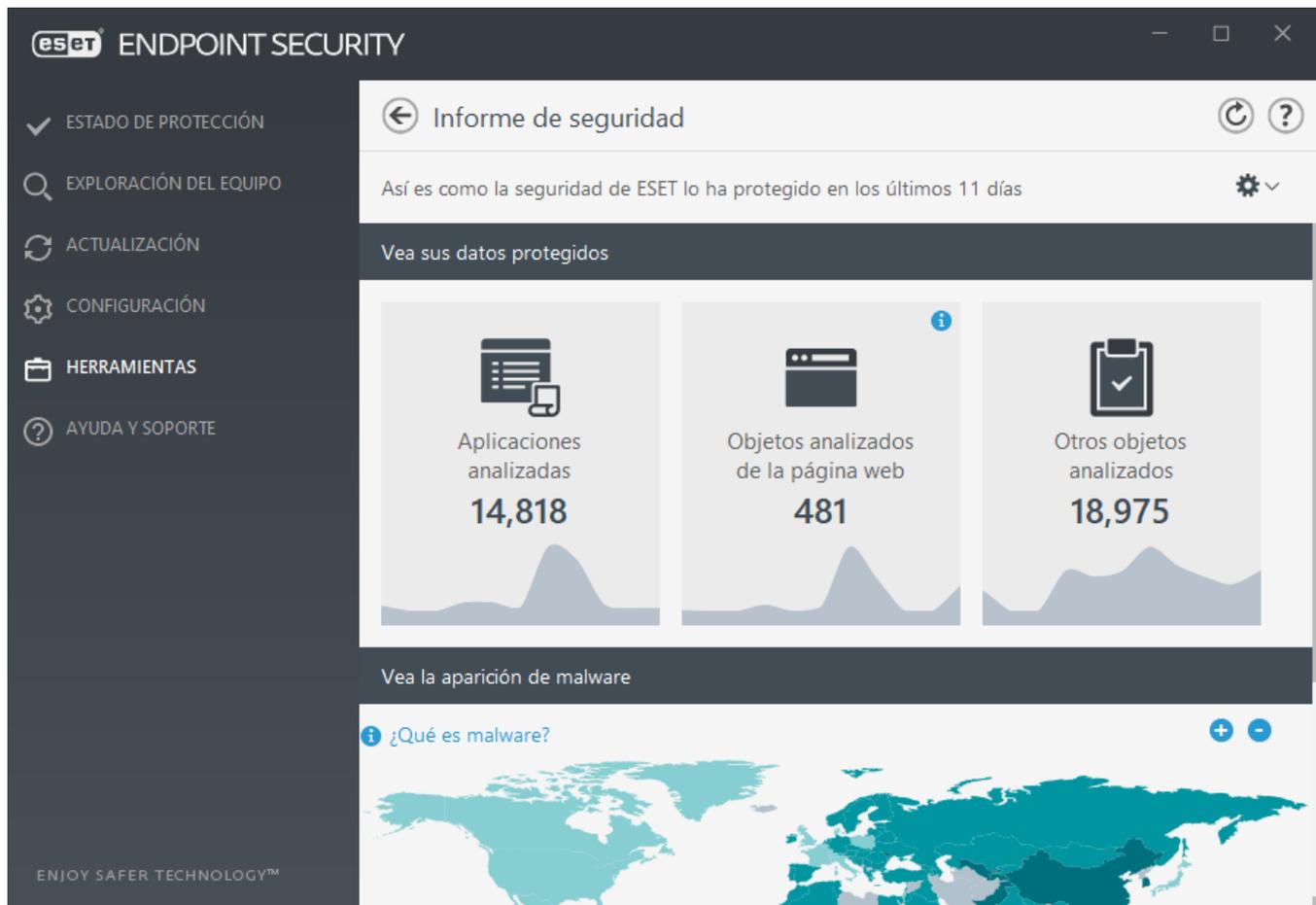
Objetos de páginas web explorados: muestra el número de objetos explorados de la página web.

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.

Debajo de las categorías, puede ver la situación actual del virus con el mapa del mundo. La presencia de virus en cada país se indica con el color (mientras más oscuro sea el color, mayor será el número). Los países sin datos aparecen en gris. Pase el cursor por encima del país para ver los datos del país seleccionado. Puede seleccionar el continente específico para que se amplíe automáticamente.

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 Security 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 > Interfaz del usuario > Alertas y cuadros de mensajes > Mensajes de confirmación**.

Conexiones de red

En la sección Conexiones de red, verá una lista de las conexiones activas y pendientes. Sirve para controlar todas las aplicaciones que establecen conexiones salientes.

eset ENDPOINT SECURITY

✓ ESTADO DE PROTECCIÓN
 🔍 EXPLORACIÓN DEL EQUIPO
 ↻ ACTUALIZACIÓN
 ⚙️ CONFIGURACIÓN
 📁 HERRAMIENTAS
 ? AYUDA Y SOPORTE

ENJOY SAFER TECHNOLOGY™

Conexiones de red

Aplicación/IP local	IP remota	Protoc...	Aument...	Disminui...	Enviado	Recibido
+ System			0 B/s	0 B/s	165 kB	453 kB
+ wininit.exe			0 B/s	0 B/s	0 B	0 B
+ services.exe			0 B/s	0 B/s	0 B	0 B
+ lsass.exe			0 B/s	0 B/s	59 kB	86 kB
+ svchost.exe			0 B/s	0 B/s	0 B	0 B
+ svchost.exe			0 B/s	0 B/s	0 B	0 B
+ svchost.exe			0 B/s	0 B/s	0 B	0 B
+ spoolsv.exe			0 B/s	0 B/s	0 B	0 B
+ svchost.exe			0 B/s	0 B/s	37 kB	62 kB
+ svchost.exe			0 B/s	0 B/s	3 kB	11 kB
+ svchost.exe			0 B/s	0 B/s	19 kB	66 kB
+ SearchApp.exe			0 B/s	0 B/s	110 kB	108 kB
+ YourPhone.exe			0 B/s	0 B/s	923 B	7 kB
+ WinStore.App.exe			0 B/s	0 B/s	10 kB	141 kB

Mostrar detalles

La primera línea muestra el nombre de la aplicación y la velocidad de la transferencia de datos. Para ver una lista de las conexiones establecidas por la aplicación (así como información más detallada), haga clic en +.

Columnas

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

IP remota – dirección IP y número de puerto del equipo remoto específico.

Protocolo – protocolo de transferencia utilizado.

Aumentar velocidad/Disminuir velocidad – la velocidad actual de los datos salientes y entrantes.

Enviado/Recibido – cantidad de datos intercambiados en la conexión.

Mostrar detalles – elija esta opción para mostrar información detallada sobre la conexión seleccionada.

Seleccione una aplicación o dirección IP en la Pantalla de conexiones de red, y al hacer clic derecho sobre la misma, se mostrará el menú contextual con la siguiente estructura:

Resolver nombres de host – si es posible, todas las direcciones de red se muestran en el formato de nombre DNS, no en el formato numérico de dirección IP.

Mostrar solo las conexiones TCP – la lista muestra únicamente las conexiones pertenecientes al grupo de protocolos TCP.

Mostrar las conexiones de escucha – seleccione esta opción para mostrar únicamente aquellas conexiones para las que aún no se estableció comunicación alguna, pero para las que el sistema ha abierto un puerto y está esperando establecer una conexión.

Mostrar las conexiones dentro del equipo – seleccione esta opción para mostrar únicamente aquellas conexiones en las que el lado remoto es un sistema local; es decir, las llamadas conexiones localhost.

Haga un clic derecho en una conexión para ver opciones adicionales, entre las que se incluyen:

Denegar las comunicaciones para la conexión – finaliza la comunicación establecida. Esta opción está disponible solo luego de hacer clic en una conexión activa.

Actualizar la velocidad – elija la frecuencia para actualizar las conexiones activas.

Actualizar ahora – actualiza la ventana de Conexiones de red.

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

Denegar temporalmente las comunicaciones para el proceso – rechaza las conexiones actuales de la aplicación determinada. Si se establece una nueva conexión, el firewall usa una regla predefinida. Puede encontrar una descripción de la configuración en la sección [Reglas y zonas](#).

Permitir temporalmente las comunicaciones para el proceso – permite las conexiones actuales de la aplicación determinada. Si se establece una nueva conexión, el firewall usa una regla predefinida. Puede encontrar una descripción de la configuración en la sección [Reglas y zonas](#).

ESET SysRescue Live

ESET SysRescue Live es una utilidad gratis que le permite crear un rescate reinicialable en CD/DVD o una unidad USB. Puede reiniciar un equipo infectado desde su medio de rescate para explorar el malware y limpiar los archivos infectados.

La ventaja principal de ESET SysRescue Live es que la solución se ejecuta en forma independiente del sistema operativo del host, pero cuenta con acceso directo al disco y al sistema de archivos. De esta forma, es posible quitar las infiltraciones que normalmente no se podrían eliminar; por ejemplo, mientras el sistema operativo está activo, etc.

- [Ayuda en línea para ESET SysRescue Live](#)

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.
3. Para denunciar spam, falsos positivos de spam o sitios web mal categorizados por el módulo de control web, consulte nuestro [artículo incluido en la base de conocimientos 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.

i No obtendrá una respuesta de ESET a menos que se requiera más información, ya que nuestros servidores reciben decenas de miles de archivos por día, lo que hace imposible responder a todos los envíos. Si la muestra resulta ser una aplicación maliciosa o sitio malicioso, se agregará su detección a una de las próximas actualizaciones de ESET.

Seleccionar muestra para su análisis: archivo sospechoso

Signos y síntomas observados de infección de malware – ingrese una descripción sobre la conducta de los archivos sospechosos observada en el equipo.

Origen del archivo (dirección URL o proveedor) – ingrese el origen del archivo (la procedencia) e indique cómo lo encontró.

Notas e información adicional – aquí puede ingresar información adicional o una descripción útil para el proceso de identificación del archivo sospechoso.

i Aunque solo el primer parámetro, **Signos y síntomas observados de infección de malware**, es obligatorio, el suministro de información adicional ayudará en forma significativa a nuestros laboratorios en 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.

Notificaciones

Para administrar la manera en que ESET Endpoint Security comunica eventos con el usuario, vaya a **Configuración avanzada** (F5) > **Herramientas** > **Notificaciones**. Esta ventana de configuración le permite definir los siguientes tipos de notificaciones:

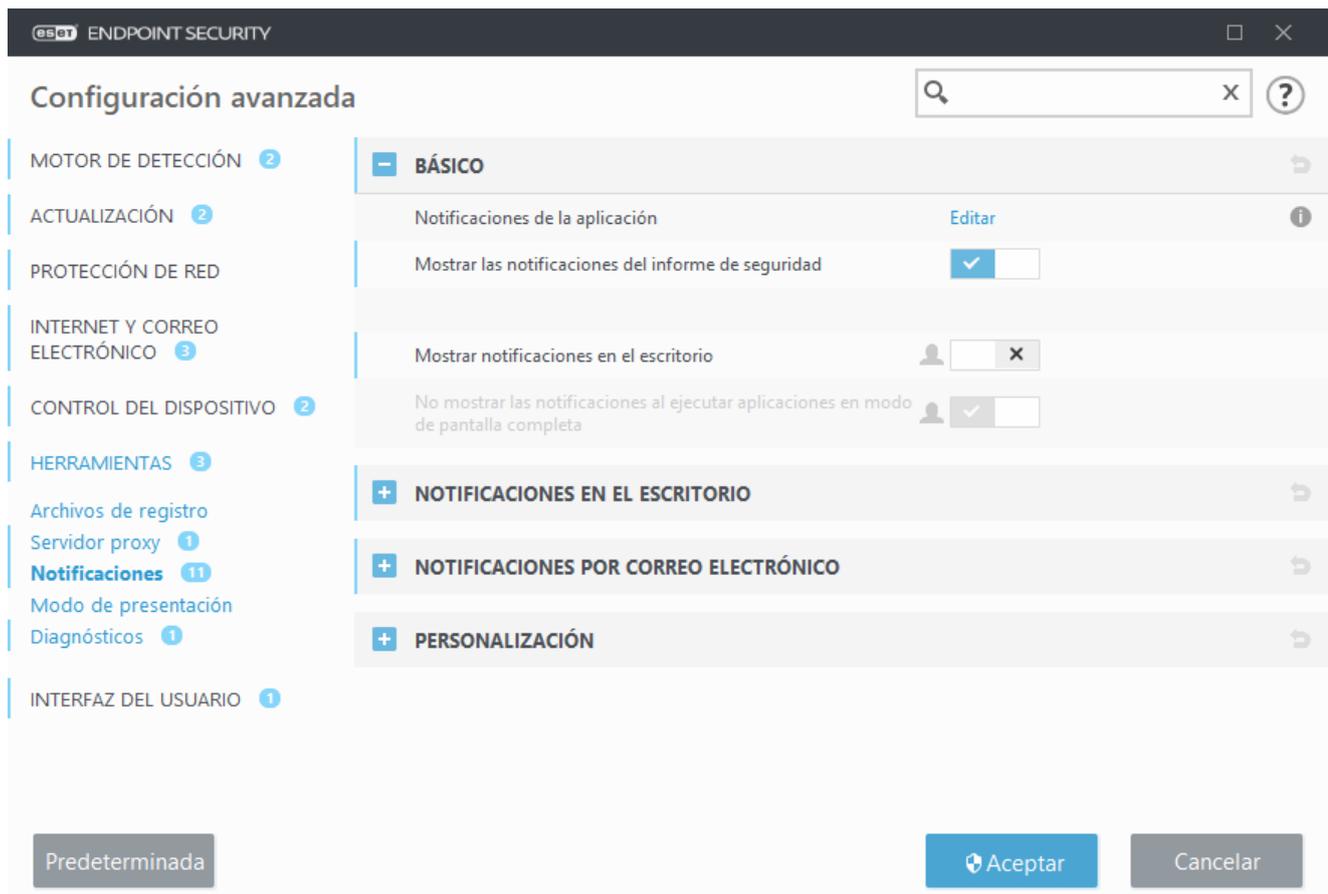
- **Notificaciones de la aplicación** : aparece directamente en la ventana principal del programa.
- **Notificaciones de escritorio** : notificación de escritorio que se muestra como ventana emergente junto a la barra de tareas del sistema.
- **Notificaciones por correo electrónico** : las notificaciones 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.

En la sección **Básico**, utilice los botones correspondientes para ajustar lo siguiente:

Botón	Predeterminada	Descripción
Mostrar notificaciones en el escritorio	<input checked="" type="checkbox"/>	Deshabilitar para ocultar las notificaciones emergentes junto a la barra de tareas del sistema. Le recomendamos mantener esta opción habilitada para que el producto le informe cuando tenga lugar un nuevo suceso.
No mostrar las notificaciones al...	<input checked="" type="checkbox"/>	Conservar No mostrar las notificaciones al ejecutar aplicaciones en el modo de pantalla completa habilitado para suprimir las notificaciones no interactivas.
Mostrar las notificaciones del informe de seguridad	<input type="checkbox"/>	Habilitar para recibir una notificación cuando se genera una nueva versión del Informe de seguridad (disponible solo si no se administra con ESET Security Management Center).
Mostrar las notificaciones acerca de la actualización correcta	<input type="checkbox"/>	Habilitar para recibir una notificación cuando el producto actualiza sus componentes y los módulos del motor de detección.
Enviar notificaciones de sucesos por correo electrónico	<input type="checkbox"/>	Habilitar para activar las Notificaciones por correo electrónico .

Para habilitar o deshabilitar [notificaciones de la aplicación](#) específicas, haga clic en **Editar** junto a **Notificaciones**

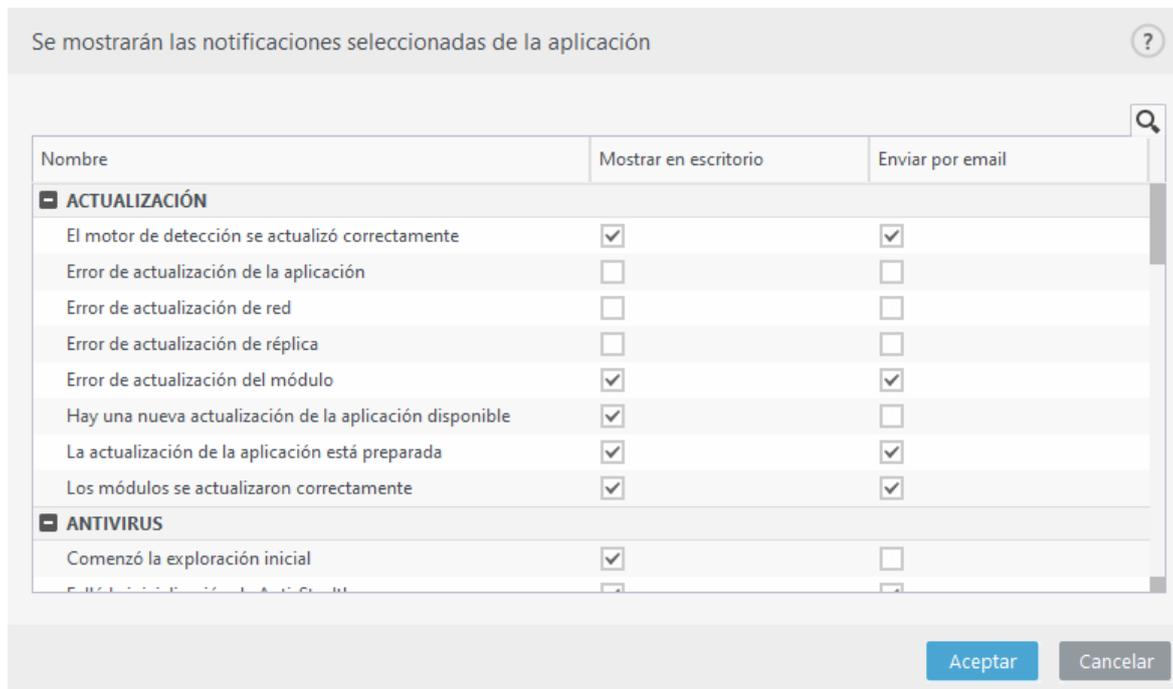
de la aplicación.



Notificaciones de la aplicación

Para ajustar la visibilidad de las notificaciones de la aplicación (que se muestran en el extremo inferior derecho de la pantalla), vaya a **Herramientas > Notificaciones > Básico > Notificaciones de la aplicación** del árbol de configuración Avanzada de ESET Endpoint Security.

La lista de notificaciones se divide en tres columnas. Los nombres de las notificaciones se clasifican por categorías en la primera columna. Para cambiar la manera en que el producto notifica sobre los nuevos sucesos de la aplicación, marque las casillas de verificación en las columnas correspondientes **Mostrar en el escritorio** y **Enviar por correo electrónico**.



Para definir las configuraciones generales de las notificaciones de escritorio, por ejemplo, durante cuánto tiempo se mostrará un mensaje o la cantidad mínima de detalles para mostrar de los sucesos, consulte [Notificaciones de escritorio](#) en **Configuración avanzada > Herramientas > Notificaciones**.

Para definir el formato del mensaje que se envía por correo electrónico y configurar los ajustes del servidor de SMTP, vaya a [Notificaciones por correo electrónico](#) en **Configuración avanzada > Herramientas > Notificaciones**.

i Si desea configurar notificaciones de **Archivo analizado** y **Archivo no analizado** mientras usa ESET Dynamic Threat Defense, se debe configurar la [protección proactiva](#) en **Bloquear ejecución hasta recibir el resultado del análisis**.

Notificaciones en el escritorio

La notificación de escritorio está representada por una pequeña ventana emergente 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 Security 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.

La sección **Notificaciones de escritorio** permite personalizar el comportamiento de las notificaciones emergentes. Pueden definirse los siguientes atributos:

Duración : define durante cuánto tiempo se muestra el mensaje de notificación. El valor debe ubicarse en un rango de 3 a 30 segundos.

Transparencia : define la transparencia del mensaje de notificación en porcentajes. El rango admitido es de 0 (sin transparencia) a 80 (transparencia muy alta).

Detalles mínimos de sucesos para mostrar : en el menú desplegable, seleccione el nivel de severidad de inicio de las notificaciones que han de mostrarse:

- **Diagnóstico** – registra la información necesaria para ajustar el programa y todos los historiales antes

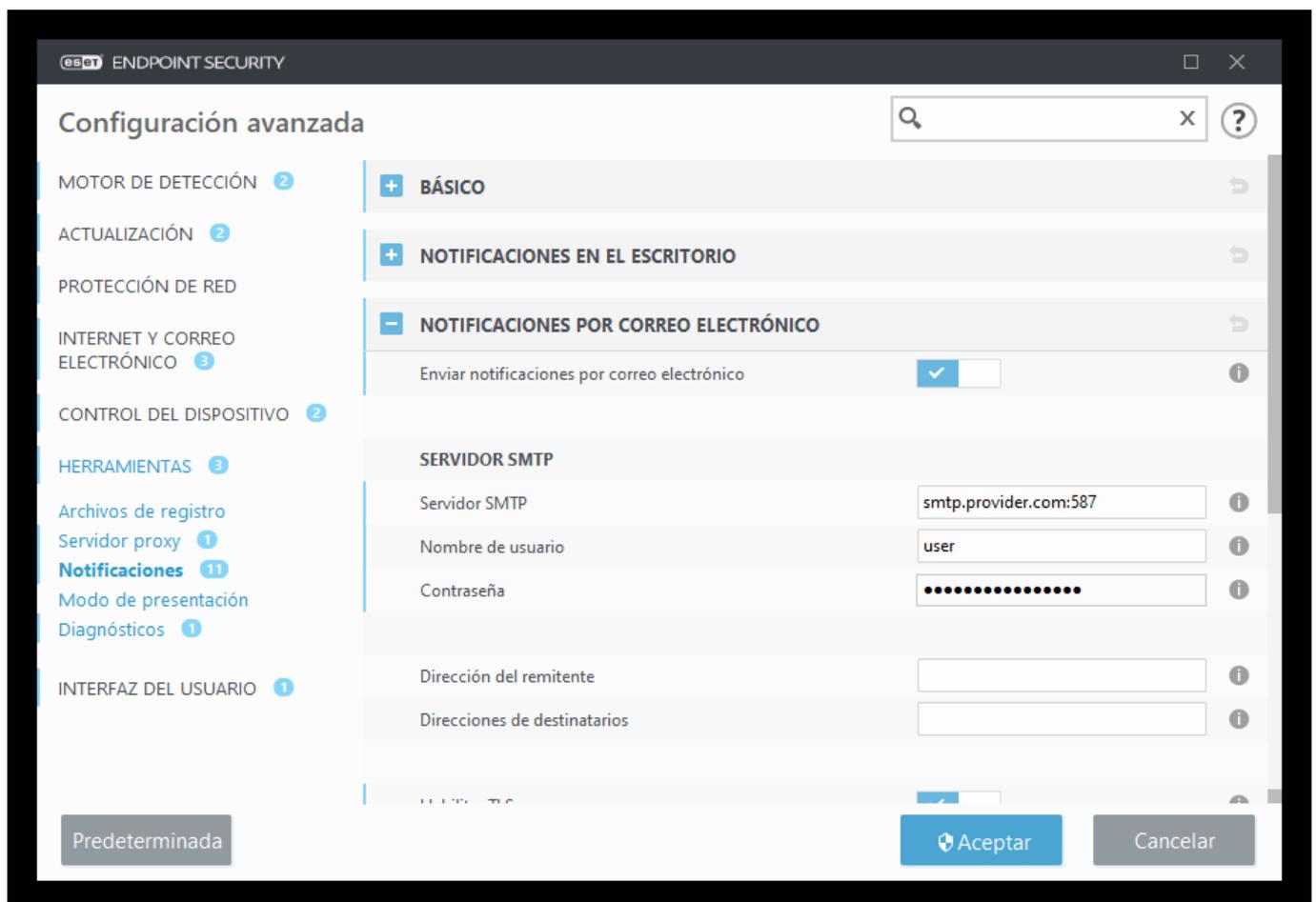
mencionados.

- **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 (Antisteach no se está ejecutando de forma adecuada o hubo un error en 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 los sistemas de múltiples usuarios, se muestran las notificaciones en la pantalla de este usuario : escriba los nombres completos de la cuenta de los usuarios que deberían autorizarse para recibir notificaciones de escritorio. Por ejemplo, si utiliza un equipo con otra cuenta de administrador y quiere mantenerse informado sobre eventos de nuevos productos.

Notificaciones por correo electrónico

ESET Endpoint Security puede enviar automáticamente correos electrónicos de notificación si ocurre un suceso con el nivel de detalle de los sucesos seleccionado. En la sección [Básico](#), habilite **Enviar notificaciones de sucesos por correo electrónico** para activar las notificaciones por correo electrónico.



Servidor SMTP

Servidor SMTP – el servidor SMTP utilizado para enviar notificaciones (por ej. *smtp.provider.com:587*, el puerto predeterminado es 25).

i Los servidores SMTP con cifrado TLS son admitidos por ESET Endpoint Security.

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.

Configuración de 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 (Antisteam no se está ejecutando de forma adecuada o hubo un error en 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.

Enviar cada notificación en un correo electrónico por separado – cuando se habilite, el destinatario recibirá un correo electrónico nuevo por cada notificación individual. Esto puede dar como resultado un gran número de correos electrónicos recibidos en un corto 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.

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

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.

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.

Amenazas

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 amenaza** para usar mensajería de notificación personalizada.

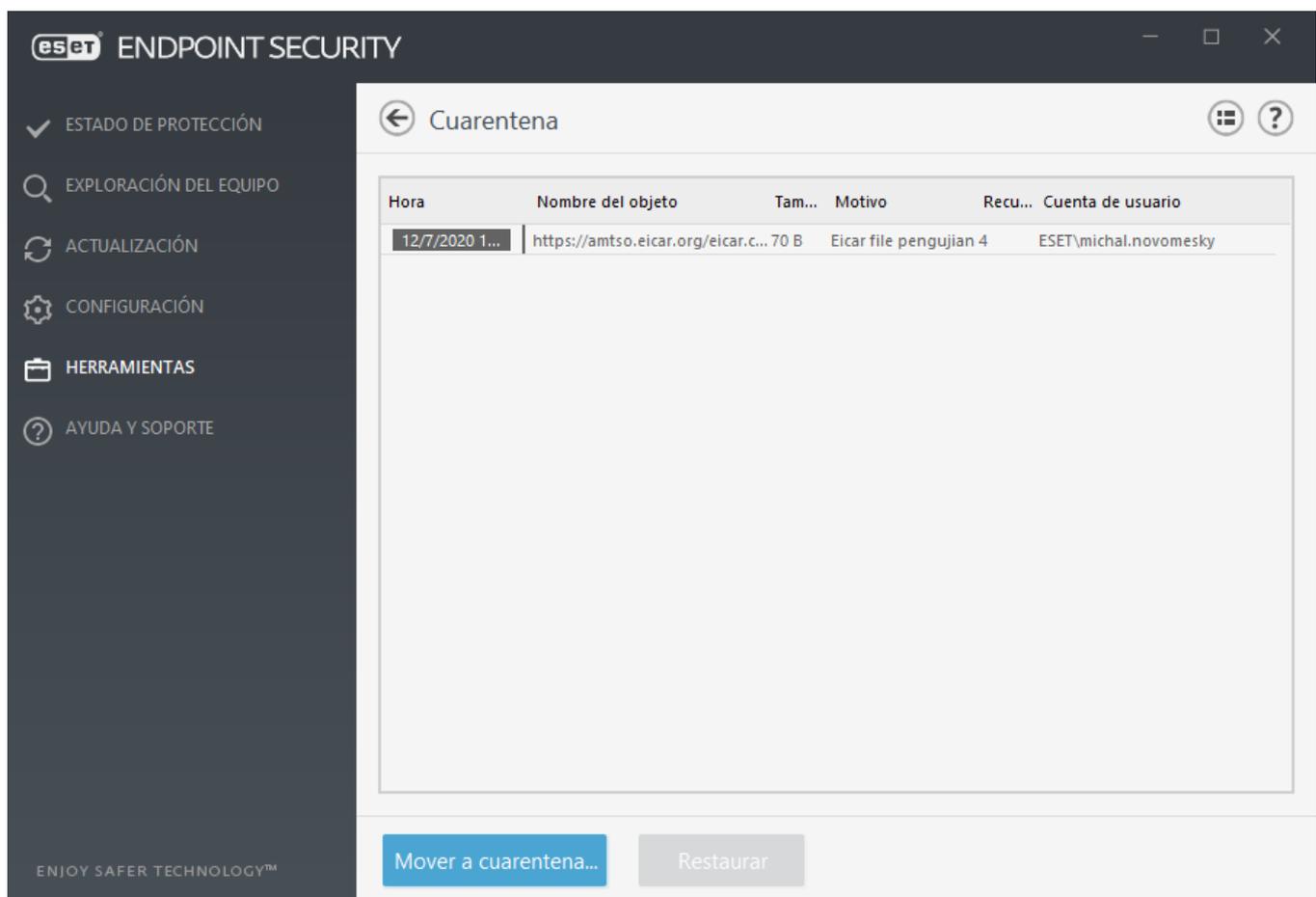
Cuarentena

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 Security 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 Security dispone los archivos eliminados en cuarentena de manera automática (si usted no canceló esta opción en la [ventana de alerta](#)).

Los archivos adicionales deberían ponerse en cuarentena si:

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

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

- a.use la función Arrastrar y soltar para poner un archivo en cuarentena manualmente al hacer clic en el archivo, mover el puntero del mouse hacia el área marcada al mismo tiempo que mantiene el botón pulsado, y luego lo suelta. Después de eso, la aplicación se mueve al primer plano.
- b.Haga clic en **Mover a cuarentena** en la ventana principal del programa.
- c.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.

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

- [Administrar la cuarentena en ESET PROTECT \(8.x\)](#)
- [Mi producto ESET me envió una notificación sobre una detección. ¿Qué debo hacer?](#)

Configuración del servidor proxy

En redes de LAN muy extensas, la comunicación entre su equipo e Internet puede tener como intermediario un servidor proxy. Al utilizar esta configuración, será necesario definir las siguientes opciones de configuración. De lo contrario, el programa no podrá actualizarse en forma automática. En ESET Endpoint Security, la configuración del servidor proxy está disponible en dos secciones diferentes del árbol de Configuración avanzada.

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

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

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

i En la configuración del **Servidor proxy**, debe ingresar su Nombre de usuario y Contraseña en forma manual.

Use conexión directa si el proxy no está disponible – Si ESET Endpoint Security está configurado para usar proxy y no puede llegar al proxy, ESET Endpoint Security evadirá el proxy y se comunicará directamente con los servidores ESET.

La configuración del servidor proxy también puede establecerse desde Configuración avanzada de la actualización (**Configuración avanzada > Actualizar > Perfiles > Actualizaciones > Opciones de conexión** seleccionando **Conexión a través de un servidor proxy** del menú desplegable **Modo de proxy**). Esta configuración se aplica al perfil de actualización determinado y se recomienda para equipos portátiles, ya que suelen recibir las actualizaciones del motor de detección desde ubicaciones remotas. Para obtener más información sobre esta configuración, consulte [Configuración de actualización avanzada](#).

Configuración avanzada

x ?

MOTOR DE DETECCIÓN 2

ACTUALIZACIÓN 5

PROTECCIÓN DE RED

INTERNET Y CORREO ELECTRÓNICO 3

CONTROL DEL DISPOSITIVO 2

HERRAMIENTAS 3

Archivos de registro

Servidor proxy 1

Notificaciones por correo electrónico 3

Modo de presentación

Diagnósticos

INTERFAZ DEL USUARIO 1

SERVIDOR PROXY

Usar servidor proxy	<input checked="" type="checkbox"/>	i
Servidor proxy	<input type="text"/>	i
Puerto	<input type="text" value="3128"/>	
El servidor proxy requiere autenticación <input type="checkbox"/> x i		
Nombre de usuario	<input type="text"/>	i
Contraseña	<input type="text"/>	i
Detectar el servidor proxy	<input type="button" value="Detectar"/>	
Utilice una conexión directa si el proxy no está disponible <input checked="" type="checkbox"/>		

Predeterminado

Aceptar

Cancelar

Intervalos de tiempo

Se pueden crear intervalos de tiempo y luego asignarlos a reglas para el **Control de dispositivos** y **Control de acceso web**. 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.

Intervalos de tiempo ?

Q

Nombre	Descripción
Work time	Weekdays 8:00-17:00
Off-work	Evenings & weekends

Agregar
Editar
Eliminar

Aceptar
Cancelar

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, éste se mostrará en el menú desplegable **Aplicar durante** en la [ventana del editor de reglas del control de dispositivos](#) o [en la ventana del editor de reglas de control de acceso web](#).

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 Security 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.

Verificación de intervalo de licencia

ESET Endpoint Security se conecta a los servidores de ESET de manera automática. Para cambiar esta configuración, vaya a **Configuración avanzada (F5) > Herramientas > Licencia**. De manera predeterminada, la opción **Verificación de licencia** se encuentra configurada en **Automática** y el servidor de ESET Licence verifica el producto varias veces por hora. En caso de que haya mayor tráfico de red, cambie la configuración a **Limitada** para disminuir la sobrecarga. Cuando la opción **Limitada** está seleccionada, ESET Endpoint Security verifica el 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 Business Account/ESET MSP Administrator pueden demorar hasta un día en aplicar las configuraciones de ESET Endpoint Security.

Interfaz del usuario

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

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

Para brindar la máxima seguridad de su software de seguridad, puede evitar los cambios no autorizados mediante la herramienta [Configuración de acceso](#).

En la configuración de los [Cuadros de alertas y mensajes](#) y [Notificaciones](#), puede cambiar el comportamiento de las alertas de detección y las notificaciones del sistema. Dichos mensajes se pueden personalizar de acuerdo a sus necesidades.

Si elige no mostrar algunas notificaciones, se mostrarán en **Elementos de la interfaz de usuario > Estados de aplicaciones**. Aquí puede verificar su estado o, como alternativa, evitar que se muestren estas notificaciones.

La [Integración en el menú contextual](#) aparece cuando se hace un clic derecho en el objeto seleccionado. Use esta herramienta para integrar los elementos de control de ESET Endpoint Security al menú contextual.

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 Security](#) (útil para entornos administrados).

Elementos de la interfaz del usuario

Las opciones de configuración de la interfaz del usuario en ESET Endpoint Security permiten ajustar el entorno de trabajo conforme a sus necesidades. Puede acceder a estas opciones de configuración en la sección **Interfaz del usuario > Elementos de la interfaz del usuario** en el árbol de Configuración avanzada de ESET Endpoint Security.

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.

i 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 Security** como administrador, o puede hacerlo mediante ESET Security Management Center con una [política](#).

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

Para que ESET Endpoint Security 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 Security al menú contextual.

Estados

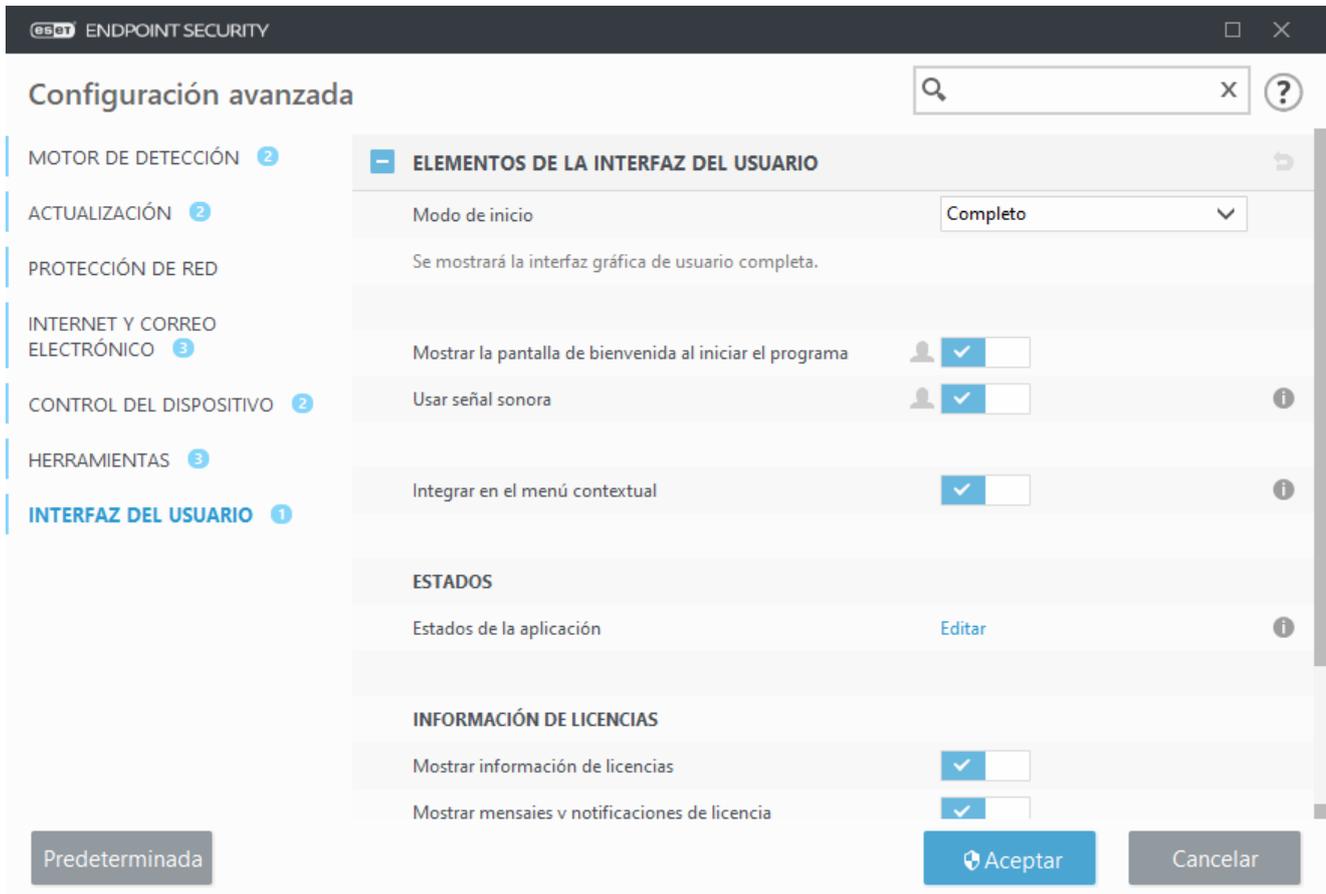
Estados de aplicaciones – haga clic en el botón **Editar** para administrar (deshabilitar) los estados que se muestran en el panel **Estado de protección** en el menú principal.

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**.

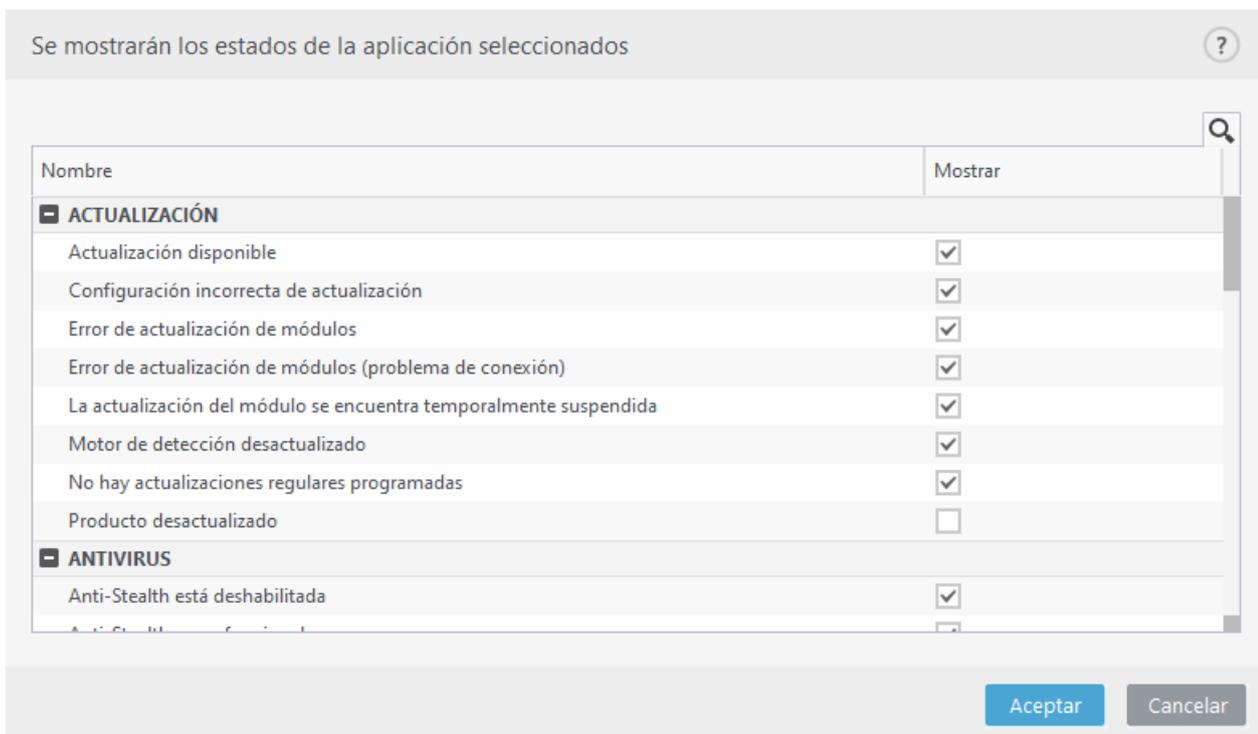
Mostrar mensajes y notificaciones de licencia – cuando están deshabilitados, las notificaciones y los mensajes solo se mostrarán cuando la licencia expire.

i La configuración de información de licencia se aplica pero no está accesible para ESET Endpoint Security activado con licencia MSP.



Estados de la aplicación

Para ajustar los estados del producto en el primer panel de ESET Endpoint Security, vaya a **Interfaz del usuario > Elementos de la interfaz del usuario > Estados de la aplicación** del árbol de configuración Avanzada de ESET Endpoint Security.



Habilite o deshabilite los estados de las aplicaciones que se mostrarán o no. Por ejemplo, cuando detiene la protección antivirus y antispyware, o cuando habilita el modo de presentación. Un estado de aplicaciones también se mostrará si su producto no está activado o si su licencia ha vencido. Esta configuración puede cambiarse mediante las políticas de [ESET Security Management Center](#).

Configuración del acceso

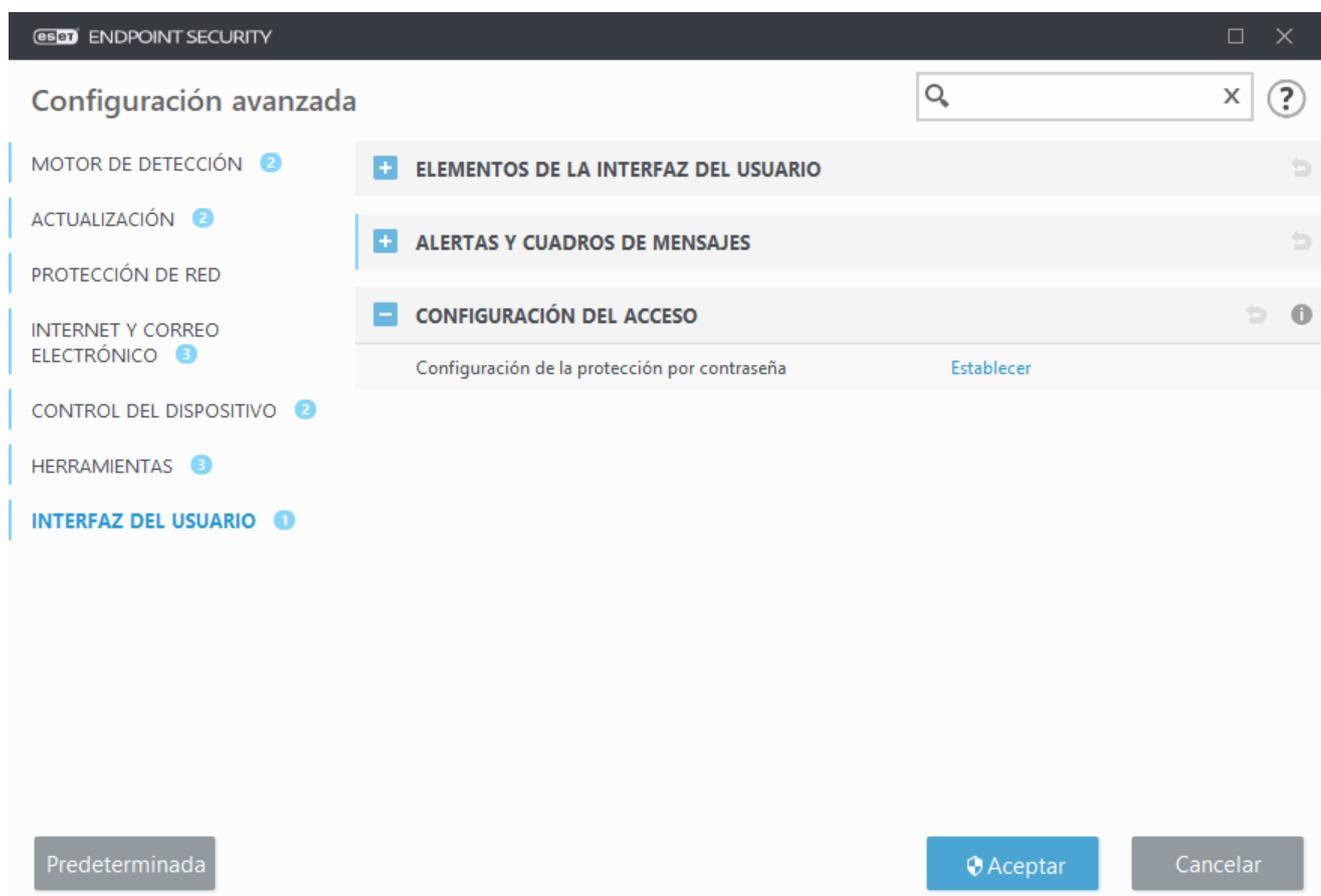
Para proporcionarle a su sistema la máxima seguridad, es esencial que ESET Endpoint Security esté configurado correctamente. Cualquier cambio no calificado puede provocar la pérdida de datos importantes. Para evitar las modificaciones no autorizadas, los parámetros de configuración de ESET Endpoint Security pueden protegerse con una contraseña.

Entornos administrados

El administrador puede crear una política para proteger con contraseña la configuración de ESET Endpoint Security en los equipos cliente conectados. Para crear una nueva política, consulte [Configuraciones protegidas de las contraseñas](#).

Sin administración

La configuración para la protección con contraseña se encuentra en **Configuración avanzada (F5)** en **Interfaz del usuario > Configuración del acceso**.



Configuración de la protección por contraseña – indique la configuración de la contraseña. Haga clic para abrir la ventana de Configuración de la contraseña.

Si desea establecer o modificar una contraseña para proteger los parámetros de configuración, haga clic en **Establecer**.

Contraseña para configuración avanzada

Para proteger los parámetros de configuración de ESET Endpoint Security y evitar una modificación no autorizada, se debe establecer una nueva contraseña.

Entornos administrados

El administrador puede crear una política para proteger con contraseña la configuración de ESET Endpoint Security 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 Security.

Si olvida la contraseña, se puede restaurar el acceso a la configuración avanzada.

- [Restaurar con el método "Restaurar contraseña" \(versión 7.1 y posteriores\)](#)
- [Restaurar con ESET Unlock Tool \(versión 7.0 y anteriores\)](#)

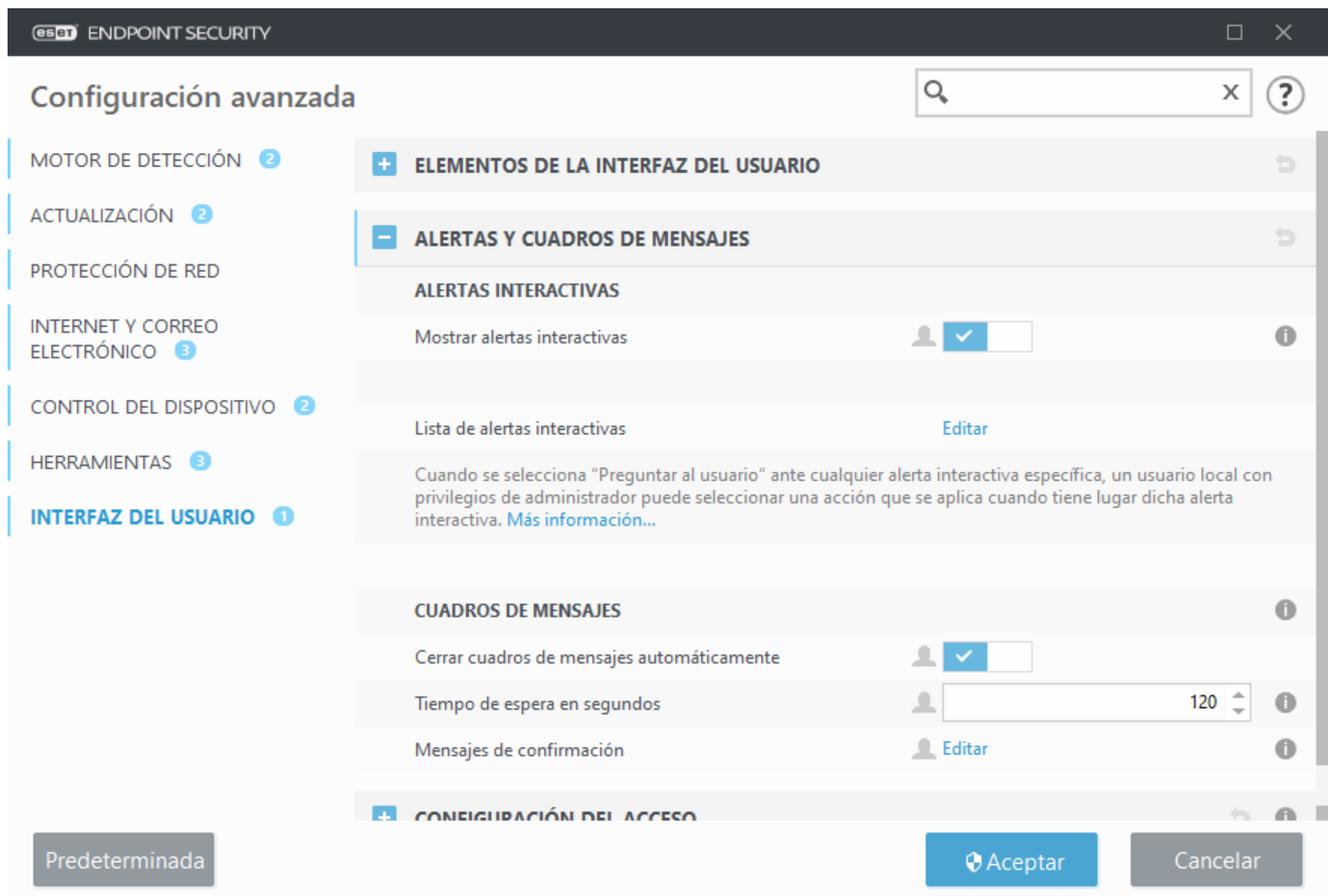
[Obtenga más información si olvidó su clave de licencia emitida por ESET](#), la fecha de vencimiento de su licencia u otro tipo de información de ESET Endpoint Security.

Alertas y cuadros de mensajes

¿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](#)

La sección **Alertas y cuadros de mensajes** en **Interfaz del usuario** le permite configurar cómo ESET Endpoint Security trata las detecciones en las que el usuario debe tomar una decisión (p. ej., posibles sitios web de phishing).



Alertas interactivas

Aparecerán ventanas de alerta interactivas si se encuentran amenazas o si se requiere la intervención del usuario.

Mostrar alertas interactivas

ESET Endpoint Security versión 7.2 y posteriores:

- 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](#).

Deshabilitar **Mostrar alertas interactivas** ocultará todas las ventanas de alerta y los mensajes en el navegador. Se seleccionará automáticamente una acción predeterminada (p. ej., se bloqueará un “posible sitio web de phishing”).

ESET Endpoint Security versión 7.1 y anteriores:

El nombre de esta configuración es **Mostrar alertas** y no es posible personalizar acciones predefinidas para ventanas de alerta interactivas y específicas.

Notificaciones en el escritorio

Las [notificaciones en el escritorio](#) y los globos de sugerencias son solo a título informativo y no requieren interacción del usuario. La sección **Notificaciones de escritorio** se movió a **Herramientas > Notificaciones** en Configuración avanzada (versión 7.1 y posteriores).

Cuadros de mensajes

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

Mensajes de confirmación – le muestra una [lista de mensajes de confirmación](#) que puede seleccionar para que se muestren o no.

Alertas interactivas

Esta sección describe distintas ventanas de alerta interactivas que ESET Endpoint Security muestra antes de realizar una acción.

Para ajustar el comportamiento de las alertas interactivas configurables, vaya a **Interfaz del usuario > Alertas y cuadros de mensajes > Lista de alertas interactivas** del árbol de configuración avanzada de ESET Endpoint Security y haga clic en **Editar**.



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.

Vea también los [estados de la aplicación](#) del producto.

Selecciónar la alerta interactiva que se mostrará

Nombre	Solicitar al usuario	Acción aplicada cuando no se muestra
ACTUALIZAR		
Está disponible la actualización	<input checked="" type="checkbox"/>	Ninguno
ALERTAS DEL NAVEGADOR WEB		
Se encontró contenido potencialmente no deseado	<input checked="" type="checkbox"/>	Bloquear
Sitio web bloqueado debido a phishing	<input checked="" type="checkbox"/>	Bloquear
EQUIPO		
Reiniciar equipo (recomendado)	<input checked="" type="checkbox"/>	Ninguno
Reiniciar equipo (requerido)	<input checked="" type="checkbox"/>	Ninguno
MEDIOS EXTRAÍBLES		

Aceptar Cancelar

Consulte otras secciones de ayuda para obtener referencias para una ventana de alerta interactiva específica:

Medios extraíbles

- [Se detectó un nuevo dispositivo](#)

Navegador seguro

- [Permitir continuar en un navegador predeterminado](#)

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

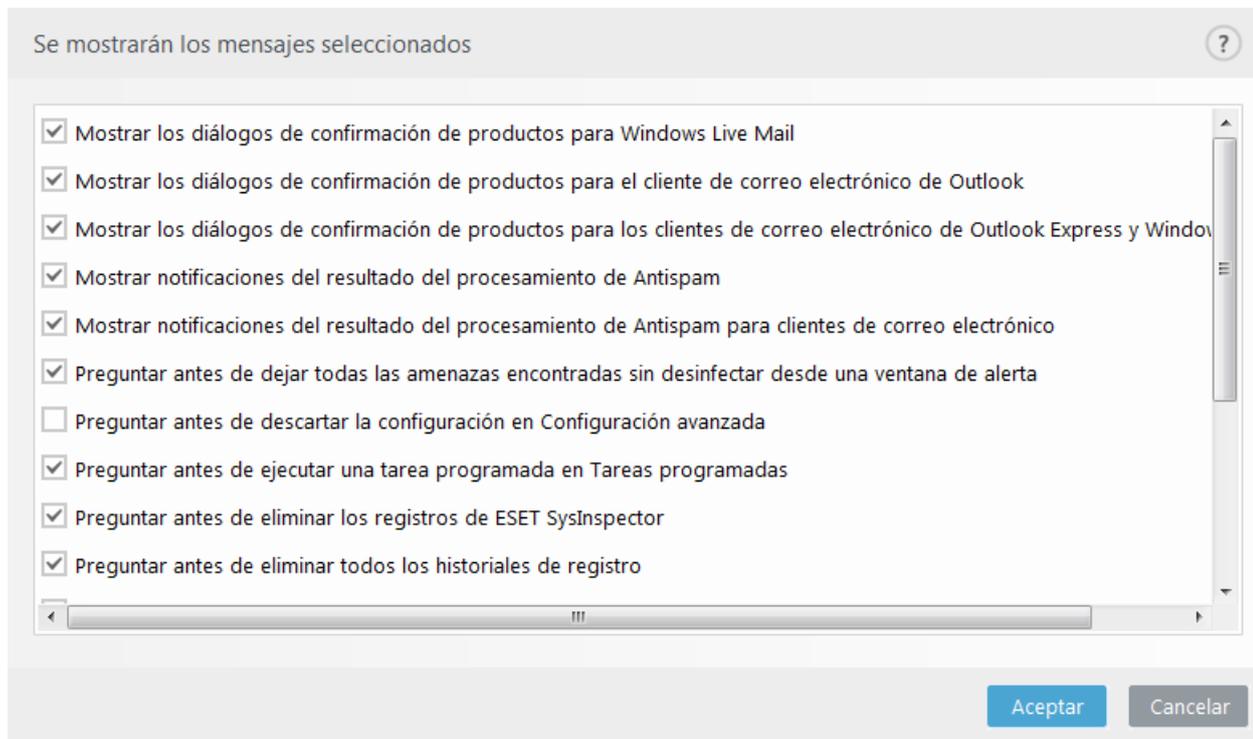
La presencia de estas alertas cambiará el color de la interfaz del usuario a naranja:

- [Reiniciar equipo \(requerido\)](#)
- [Reiniciar equipo \(recomendado\)](#)

i 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 **Interfaz del usuario > Alertas y cuadros de mensajes > Mensajes de confirmación** del árbol de configuración avanzada de ESET Endpoint Security y haga clic en **Editar**.



Esta ventana de diálogo muestra mensajes de confirmación que ESET Endpoint Security 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 los registros de ESET SysInspector](#)
- [Preguntar antes de eliminar todos los registros de ESET SysInspector](#)
- [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 notificaciones del resultado del procesamiento de Antispam](#)
- [Mostrar notificaciones del resultado del procesamiento de Antispam para clientes de correo electrónico](#)

- [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

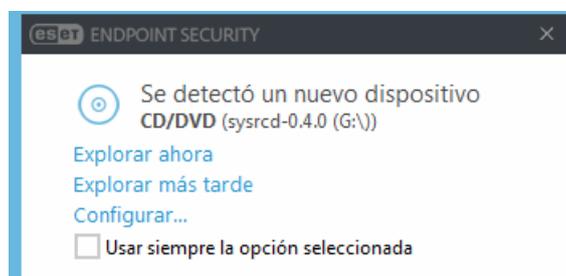
Este error puede ocurrir si algún componente (por ejemplo, HIPS o Firewall) y el usuario crean las reglas en modo interactivo o de aprendizaje al mismo tiempo.

Recomendamos cambiar el modo de filtrado por el **Modo automático** predeterminado si desea crear sus propias reglas. Obtenga más información sobre el [Modo de aprendizaje de ESET Firewall](#). Obtenga más información sobre [HIPS y los modos de filtrado de HIPS](#).

Medios extraíbles

ESET Endpoint Security proporciona la exploración automática de los medios extraíbles (CD/DVD/USB/...) al insertarlos en un equipo. Resulta útil si el administrador del equipo desea prevenir que los usuarios utilicen medios extraíbles con contenido no solicitado.

Cuando se inserten medios extraíbles y se configure **Mostrar las opciones de exploración** en ESET Endpoint Security, se mostrará el siguiente cuadro de diálogo:



Opciones para este diálogo:

- **Explorar ahora** – desencadenará la exploración de los medios extraíbles.
- **Explorar más tarde** – se pospone la exploración de los medios extraíbles.
- **Configuración:** abre la sección **Configuración avanzada**.
- **Usar siempre la opción seleccionada** – de seleccionarse, se llevará a cabo la misma acción cuando se inserte un medio extraíble en el futuro.

Además, ESET Endpoint Security 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](#).

ESET Endpoint Security 7.2 y versiones posteriores

Para acceder a los ajustes de análisis de medios extraíbles, abra Configuración avanzada (F5) > **Interfaz del usuario** > **Alertas y cuadros de mensajes** > **Alertas interactivas** > **Lista de alertas interactivas** > **Editar** > **Nuevo dispositivo detectado**.

Si la opción **Solicitar al usuario** no está seleccionada, elija la acción deseada luego de introducir un medio extraíble en un equipo:

- **No explorar:** no se realizará ninguna acción y no se abrirá la ventana **Se detectó un nuevo dispositivo**.
- **Exploración automática del dispositivo:** se llevará a cabo una exploración del equipo en los dispositivos de medios extraíbles insertados.
- **Mostrar opciones de exploración:** abre la sección de configuración de **Alertas interactivas**.

ESET Endpoint Security versión 7.1 y anteriores

Para acceder a la configuración de la exploración de medios extraíbles, abra Configuración avanzada (F5) > **Motor de detección** > **Exploraciones de malware** > **Medios extraíbles**.

Acción para realizar tras insertar un medio: seleccione la acción predeterminada que se realizará cuando se inserte un medio extraíble en el equipo (CD/DVD/USB). Seleccione la acción deseada luego de insertar un medio extraíble en un equipo:

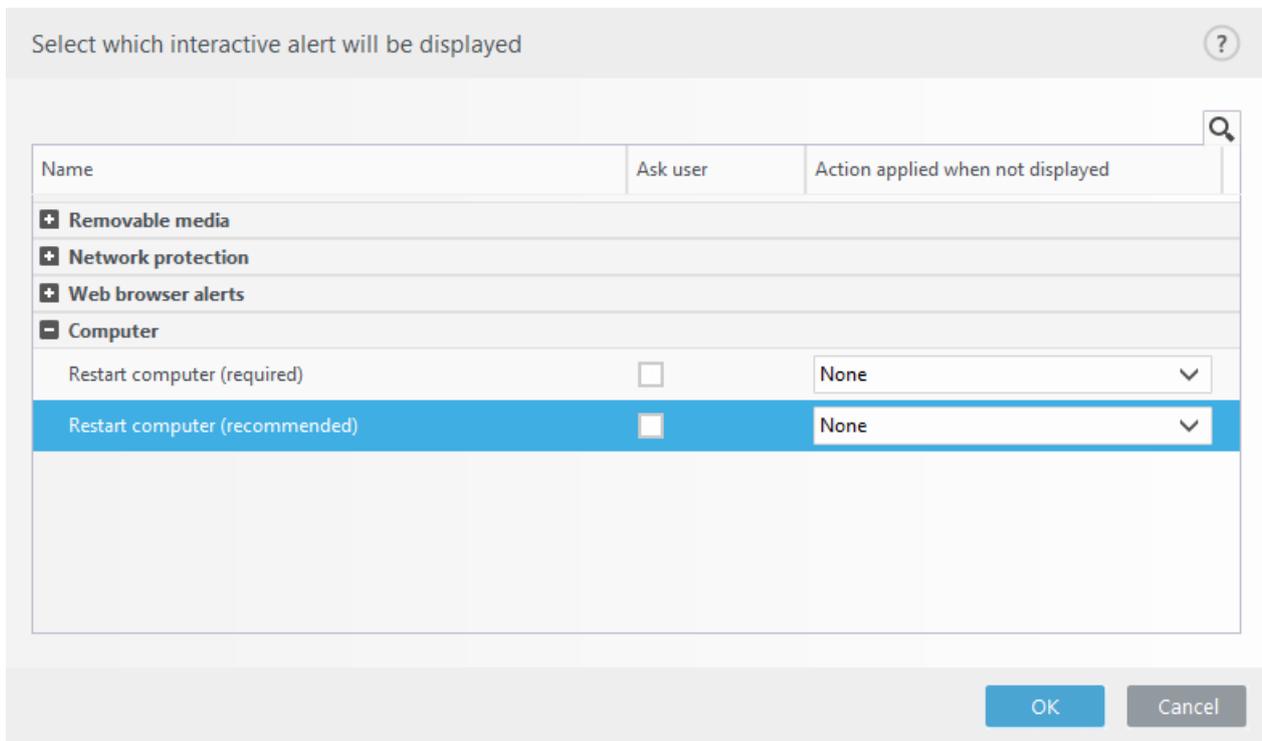
- **No explorar:** no se realizará ninguna acción y no se abrirá la ventana **Se detectó un nuevo dispositivo**.
- **Exploración automática del dispositivo:** se llevará a cabo una exploración del equipo en los dispositivos de medios extraíbles insertados.
- **Mostrar las opciones de exploración** – abre la sección de configuración de **medios extraíbles**.

Se requiere el reinicio

Si las máquinas de punto de conexión reciben una alerta roja “Se requiere el reinicio”, puede deshabilitar la visualización de las alertas.

Para deshabilitar la alerta “Se requiere el reinicio” o “Se recomienda el reinicio”, siga los pasos a continuación:

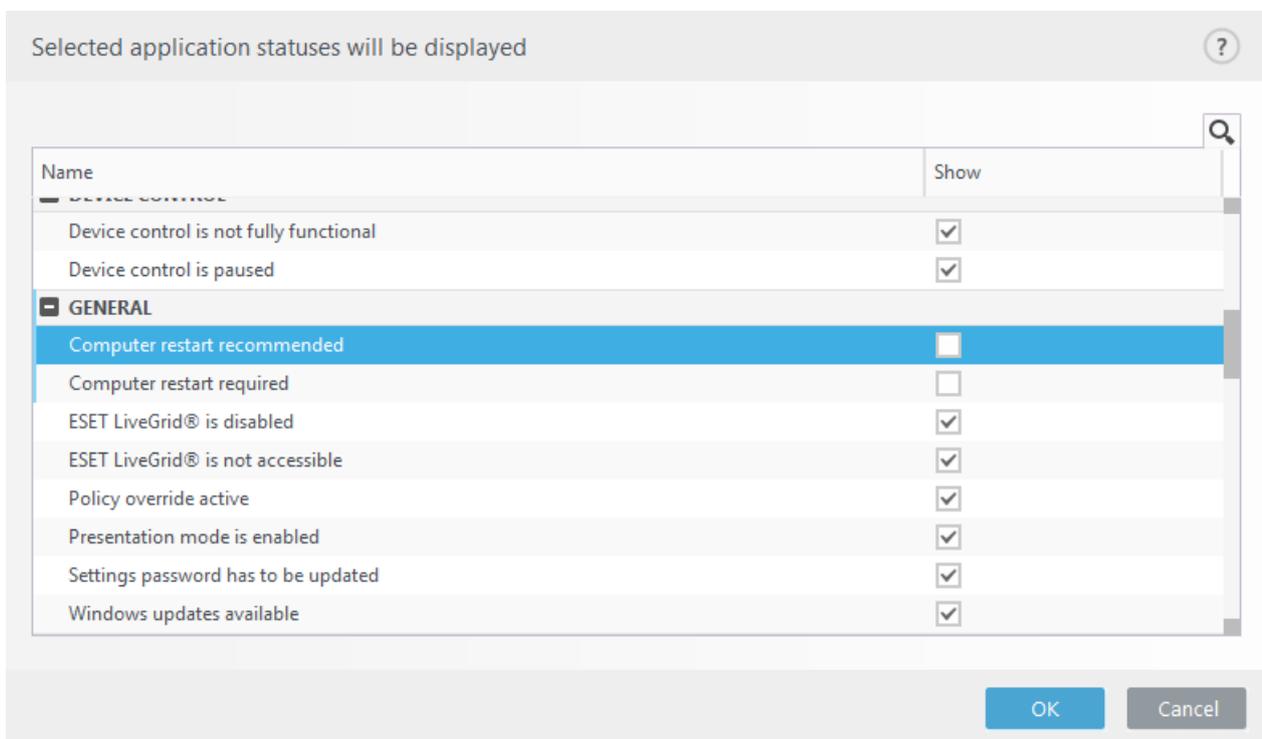
1. Presione la tecla **F5** para ingresar en Configuración avanzada y amplíe la sección **Alertas y cuadros de mensajes**.
2. Haga clic en **Editar** junto a **Lista de alertas interactivas**. En la sección **Equipo**, anule la selección de las casillas de verificación junto a **Reiniciar equipo (requerido)** 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 Security, 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

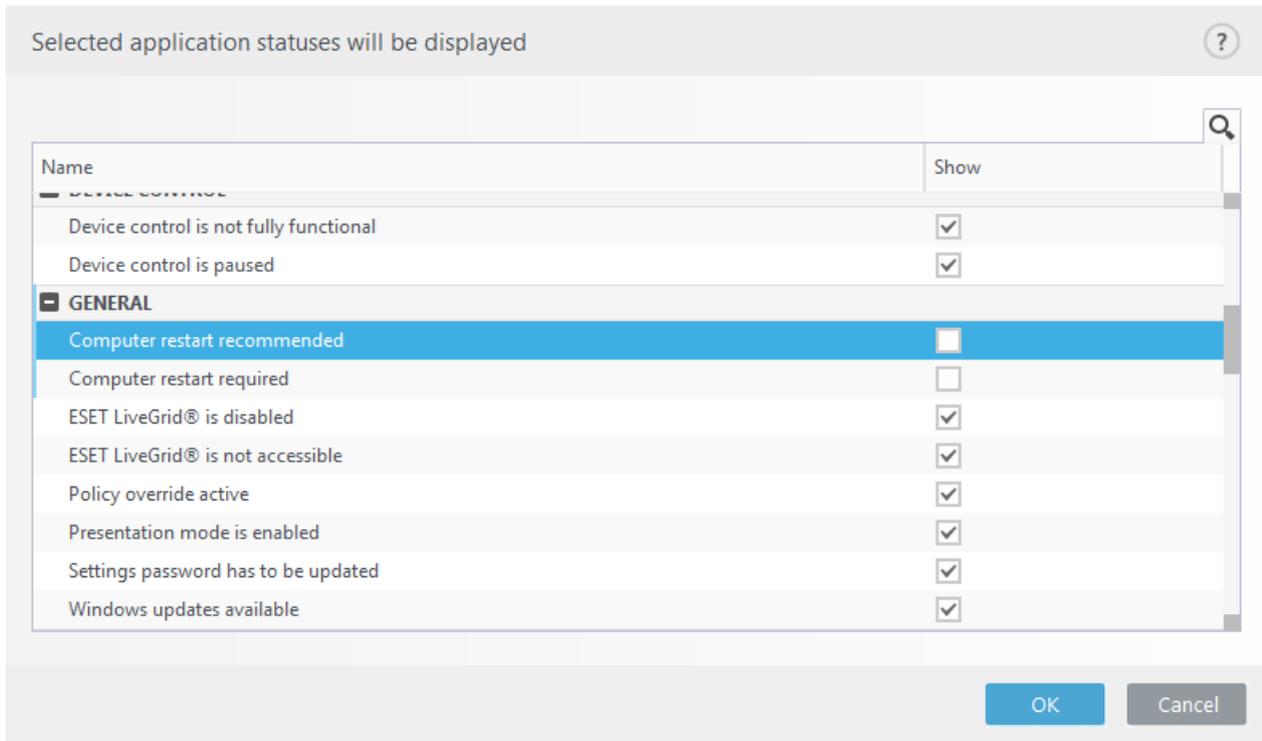
Si las máquinas de punto de conexión reciben una alerta amarilla “Se recomienda el reinicio”, puede deshabilitar la visualización de las alertas.

Para deshabilitar la alerta “Se requiere el reinicio” o “Se recomienda el reinicio”, siga los pasos a continuación:

1. Presione la tecla **F5** para ingresar en Configuración avanzada y amplíe la sección **Alertas y cuadros de mensajes**.
2. Haga clic en **Editar** junto a **Lista de alertas interactivas**. En la sección **Equipo**, anule la selección de las casillas de verificación junto a **Reiniciar equipo (requerido)** y **Reiniciar equipo (recomendado)**.

Name	Ask user	Action applied when not displayed
+ Removable media		
+ Network protection		
+ Web browser alerts		
- Computer		
Restart computer (required)	<input type="checkbox"/>	None
Restart computer (recommended)	<input type="checkbox"/>	None

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 Security, 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**.



Ícono de la bandeja del sistema

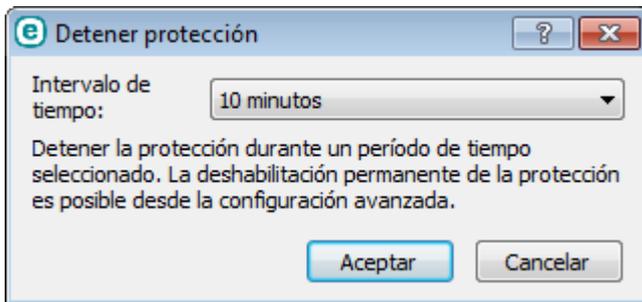
Algunas de las opciones de configuración y funciones más importantes están disponibles al hacer clic derecho en el ícono de la bandeja del sistema .

i Para acceder al menú del ícono de la bandeja del sistema, 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.

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



Pausar firewall (permitir todo tráfico) – cambia el firewall a un estado inactivo. Consulte [Red](#) para obtener más información.

Bloquear todo el tráfico de red – el firewall bloqueará todo el tráfico de la red y de Internet, tanto saliente como entrante. Para volver a habilitarlo, haga clic en **Detener el bloqueo de todo el tráfico de red**.

Configuración avanzada – seleccione esta opción para ingresar en el árbol de **Configuración avanzada**. También puede acceder a la Configuración avanzada al presionar la tecla F5 o al ir a **Configuración > Configuración avanzada**.

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 infiltraciones.

Abrir ESET Endpoint Security: abre la ventana principal del programa ESET Endpoint Security desde el ícono de la bandeja.

Restablecer la disposición de la ventana – restablece la ventana de ESET Endpoint Security a su tamaño y posición predeterminados en la pantalla.

Buscar actualizaciones – comienza a actualizar los módulos del programa para garantizar su nivel de protección frente a un código malicioso.

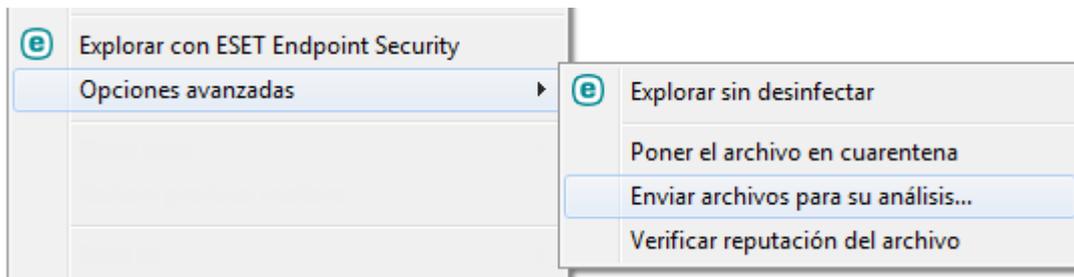
Acerca de – proporciona información del sistema, detalles sobre la versión instalada de ESET Endpoint Security y los módulos del programa instalados, como así también la fecha de vencimiento de su licencia. La información acerca de su sistema operativo y recursos del sistema se puede encontrar en la parte inferior de la página.

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.

Es posible integrar los elementos de control de ESET Endpoint Security al menú contextual. Las opciones de configuración para esta función están disponibles en el árbol de Configuración avanzada, en **Interfaz del usuario > Elementos de la interfaz del usuario**.

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



Ayuda y soporte

ESET Endpoint Security contiene herramientas de solución de problemas e información de soporte que lo ayudarán a resolver los problemas que pueda encontrar.

Producto instalado

- **Acerca de ESET Endpoint Security** – muestra información acerca de una copia de [ESET Endpoint Security](#).
- **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 Security.

[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. En función de su configuración, se [mostrará la](#) ventana de datos de envío de datos de configuración del sistema antes de rellenar el formulario web.
- **Detalles de Soporte técnico:** cuando se lo solicite, puede copiar y enviar información a Soporte técnico de ESET (como el nombre del producto, la versión del producto, el sistema operativo y tipo de procesador).
- **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.



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 Security

Esta ventana brinda detalles sobre la versión instalada de ESET Endpoint Security, su sistema operativo y los recursos del sistema.

Haga clic en **Componentes instalados** para ver la información sobre la lista de los módulos de programas instalados y sus versiones. Puede copiar información sobre los módulos al portapapeles al hacer clic en **Copiar**. Puede resultar útil durante la solución de problemas o al ponerse en contacto con el soporte técnico.

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 Security, 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.

Cuando envía el formulario web, los datos de configuración de su sistema se enviarán a ESET. Seleccione **Enviar siempre esta información** si desea recordar esta acción para este proceso. Para enviar el formulario sin enviar los

datos, haga clic en **No enviar datos**, y puede contactar a Soporte Técnico de ESET mediante el formulario de soporte en línea.

Esta configuración también se puede establecer en **Configuración avanzada > Herramientas > Diagnóstico > Soporte técnico**.

i Si decidió enviar los datos del sistema, es necesario completar y enviar el formulario web. De lo contrario, no se creará su comprobante y se perderán los datos de su sistema.

Soporte técnico

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.

Administrador de perfiles

El administrador de perfiles se usa en dos partes de ESET Endpoint Security – en la sección **Exploración del equipo a pedido** y en **Actualización**.

Exploración del equipo a petición

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

Para crear un nuevo perfil, abra la ventana de Configuración avanzada (F5) y haga clic en **Antivirus > Exploración del equipo a pedido** y luego **Editar** junto a **Lista de perfiles**. El menú desplegable **Actualizar perfil** enumera los

perfiles de exploración existentes. Para obtener ayuda sobre cómo crear un perfil de exploración acorde a sus necesidades, consulte la sección [Configuración de los parámetros del motor ThreatSense](#), donde obtendrá la descripción de cada parámetro de la configuración de la exploración.

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

Actualización

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

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

Actualizar perfil – El perfil de actualización utilizado actualmente. Para cambiarlo, elija un perfil del menú desplegable.

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

Accesos directos del teclado

Para una mejor navegación en ESET Endpoint Security, se pueden usar los siguientes accesos directos desde el teclado:

Accesos directos desde teclado	Medida tomada
F1	abre las páginas de ayuda
F5	abre la configuración avanzada
Up/Down	permite la navegación en el producto por los elementos
TAB	mueve el cursor 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

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 Security.

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 del motor Antispam: registra todos los eventos que ocurren durante el análisis antispam. Esto puede ayudar a los desarrolladores a diagnosticar y corregir problemas relacionados al motor de Antispam de ESET.

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 protección de documentos: graba todos los eventos que ocurren en la protección de documentos para diagnosticar y solucionar 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 (disponible en la versión 7.2 y posteriores).

Habilitar el registro avanzado de licencias: registra todas las comunicaciones del producto con la activación de ESET y los servidores de ESET Business Account.

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.

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.

Habilitar el registro avanzado del filtrado de protocolos: registra todos los datos que pasan a través del motor de filtrado de protocolos con el formato PCAP para ayudar a los desarrolladores a diagnosticar y solucionar problemas relacionados con el filtrado de protocolos.

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 del control Web: registra todos los eventos que ocurren durante el control web. Esto puede ayudar a los desarrolladores a diagnosticar y solucionar problemas relacionados con el control web.

Ubicación de los archivos de registro

C:\ProgramData\ESET\ESET Endpoint Security\Diagnostics

Exploración de la línea de comandos.

El módulo antivirus de ESET Endpoint Security 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	saltar 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	usar el MODO de desinfección para objetos infectados Se encuentran disponibles las siguientes opciones: <ul style="list-style-type: none"> • none (predeterminado): no se realizará desinfección automática alguna. • standard: ecls.exe intentará desinfectar o eliminar en forma automática los archivos infectados. • estricta: ecls.exe intentará desinfectar o eliminar en forma automática los archivos infectados sin la intervención del usuario (no se le notificará antes de que se eliminen los archivos). • rigurosa: ecls.exe eliminará los archivos sin intentar desinfectarlos, independientemente de qué archivo sea. • eliminar: ecls.exe eliminará los archivos sin intentar desinfectarlos, pero se abstendrá de eliminar los archivos importantes, como los archivos del sistema de Windows.
/quarantine	copiar los archivos infectados (si fueron desinfectados) a cuarentena (complementa la acción realizada durante la desinfección)
/no-quarantine	no copiar los archivos infectados a cuarentena

Opciones generales

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

Códigos de salida

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

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

ESET CMD

Esta es una característica que habilita los comandos avanzados `ecmd`. Le permite exportar e importar la configuración mediante la línea de comando (`ecmd.exe`). Hasta ahora, solo era posible exportar configuraciones usando la interfaz gráfica del usuario, [GUI](#). ESET Endpoint Security la configuración puede exportarse al archivo `.xml`.

Cuando haya habilitado ESET CMD, existen dos métodos de autorización disponibles:

- **Ninguno** – sin autorización. No le recomendamos este método porque permite la importación de cualquier configuración no firmada, lo cuál es un riesgo potencial.
- **Contraseña de configuración avanzada**: se requiere una contraseña para importar una configuración de un archivo `.xml`, este archivo debe estar firmado (consulte la firma del archivo de configuración `.xml` más abajo). La contraseña especificada en [Configuración de acceso](#) se debe brindar antes de poder importar una nueva configuración. Si no tiene acceso a la configuración habilitada, su contraseña no coincide o el archivo de configuración `.xml` no está firmado, la configuración no se importará.

Una vez habilitado ESET CMD, puede usar la línea de comandos para exportar/importar ESET Endpoint Security configuraciones. Puede hacerlo manualmente o crear una secuencia de comandos con fines de automatización.

i 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.

i Los comandos `ecmd` avanzados solo pueden ejecutarse localmente. Ejecutar una tarea de cliente **Ejecutar comando** mediante ESET PROTECT o ESMC no funcionará.

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`:

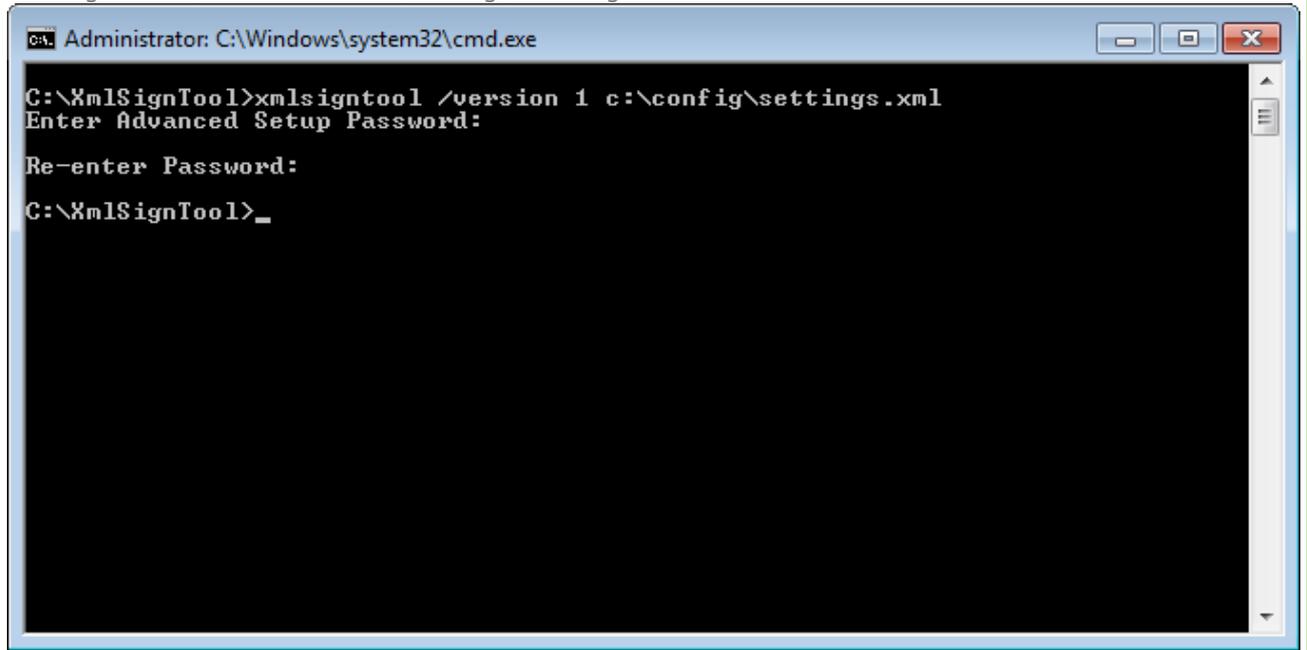
1. Descargar el [XmlSignTool](#) ejecutable.
2. Abra el símbolo del sistema de Windows (`cmd`) mediante **Ejecutar como administrador**.
3. Navegar a la ubicación de guardar de `xmlsigntool.exe`
4. Ejecute un comando para firmar el archivo de configuración `.xml`, uso: `xmlsigntool /version 1|2 <xml_file_path>`

i El valor del parámetro `/version` depende de la versión que tenga instalada de ESET Endpoint Security. 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 Security con ESET CMD utilizando el método de autorización con contraseña.

Firme el comando de archivo de configuración exportado:
`xmldsigntool /version 2 c:\config\settings.xml`



i 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 Security 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	<code>ecmd /setfeature onaccess pause</code>	<code>ecmd /setfeature onaccess enable</code>
Protección de documentos	<code>ecmd /setfeature document pause</code>	<code>ecmd /setfeature document enable</code>
Control del dispositivo	<code>ecmd /setfeature devcontrol pause</code>	<code>ecmd /setfeature devcontrol enable</code>
Modo de presentación	<code>ecmd /setfeature presentation pause</code>	<code>ecmd /setfeature presentation enable</code>

Característica de seguridad	Comando de pausa temporal	Habilitar comando
Tecnología Anti-Stealth	ecmd /setfeature antistealth pause	ecmd /setfeature antistealth 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
Protección antispam	ecmd /setfeature antispam pause	ecmd /setfeature antispam enable
Protección antiphishing	ecmd /setfeature antiphishing pause	ecmd /setfeature antiphishing habilitar

Detección en estado inactivo

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

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

Use los interruptores de cada estado correspondiente para habilitar o deshabilitar los desencadenantes de la detección en estado inactivo.

Importación y exportación de una configuración

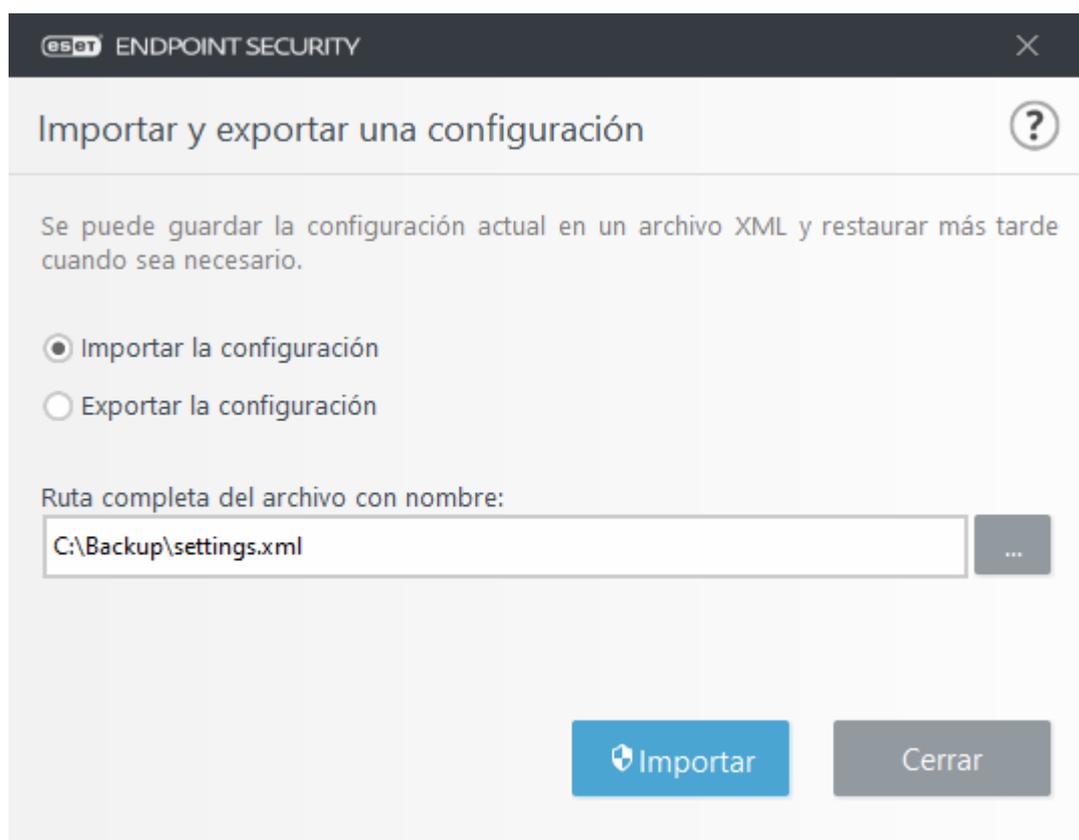
Puede importar o exportar su archivo de configuración personalizado ESET Endpoint Security .xml desde el menú **Configuración**.

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

Es muy fácil importar una configuración. En la ventana principal del programa, haga clic en **Configuración > Importar/Exportar ajustes**, ay luego seleccione **Importar ajustes**. Ingrese el nombre del archivo de configuración o haga clic en el botón ... para buscar el archivo de configuración que desea importar.

Los pasos para exportar una configuración son muy similares. En la ventana principal del programa, haga clic en **Configuración > Importar/Exportar ajustes**. Seleccione **Exportar configuraciones** e ingrese el nombre del archivo de la configuración (es decir *export.xml*). Use el botón de exploración para elegir la ubicación en el equipo donde desea guardar el archivo de configuración.

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.



Restauración de todas las configuraciones a las predeterminadas

En Configuración avanzada (F5), haga clic en **Predeterminada** para revertir toda la configuración del programa para todos los módulos. Se restablecerá el estado que tendrían después de una nueva instalación.

Consulte también [Importar y exportar configuración](#).

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.

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 Security 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 remotos ESET Endpoint Security](#)

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

Remote monitoring management is run using the command line interface. The default ESET Endpoint Security installation contains the file ermm.exe located in the Endpoint application within the directory *c:\Program Files\ESET\ESET Security*.

Run the Command Prompt (cmd.exe) as an Administrator and navigate to the mentioned path. (To open Command Prompt, press Windows button + R on your keyboard, type a cmd.exe into the Run window and press Enter.)

The command syntax is: `ermm context command [options]`

Also note that the log parameters are case sensitive.

```

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 uses three basic contexts: Get, Start and Set. In the table below you can find examples of commands syntax. Click the link in the Command column to see the further options, parameters, and usage examples. After successful execution of command, the output part (result) will be displayed. To see an input part, add parameter --debug at the of the command.

Context	Command	Description
get	Get information about products	
	información de la aplicación	Get information about product
	Información de licencia	Get information about license
	estado de protección	Get protection status
	registros	Get logs
	información de exploración	Get information about running scan
	configuración	Get product configuration
	Estado de la actualización	Get information about update
	estado de activación	Get information about last activation
start	Start task	
	Exploración	Start on demand scan

Context	Command	Description
	activación	Start activation of product
	desactivación	Start deactivation of product
	actualización	Start update of product
set		Set options for product
	configuración	Set configuration to product

In the output result of every command, the first information displayed is result ID. To understand better the result information, check the table of IDs below.

Error ID	Error	Description
0	Success	
1	Command node not present	"Command" node not present in input json
2	Command not supported	Particular command is not supported
3	General error executing the command	Error during execution of command
4	Task already running	Requested task is already running and has not been started
5	Invalid parameter for command	Bad user input
6	Command not executed because it's disabled	RMM isn't enabled in advanced settings or isn't started as an administrator

Lista de los comandos ERMM JSON

- [Obtener estado de protección](#)
- [Obtener información de la aplicación](#)
- [Obtener información de licencia](#)
- [Obtener registros](#)
- [Obtener estado de activación](#)
- [Obtener información de la exploración](#)
- [Obtener configuración](#)
- [Obtener estado de actualización](#)
- [Comenzar exploración](#)
- [Comenzar activación](#)
- [Comenzar desactivación](#)
- [Comenzar actualización](#)
- [Establecer configuración](#)

get protection-status

Get the list of application statuses and the global application status

Command line

```
ermm.exe get protection-status
```

Parameters

None

Example

call

```
{
  "command": "get_protection_status",
  "id": 1,
  "version": "1"
}
```

result

```
{
  "id": 1,
  "result": {
    "statuses": [
      {
        "id": "EkrnNotActivated",
        "status": 2,
        "priority": 768,
        "description": "Product not activated"
      }
    ],
    "status": 2,
    "description": "Security alert"
  },
  "error": null
}
```

get application-info

Get information about the installed application

Command line

```
ermm.exe get application-info
```

Parameters

None

Example

call

```
{  
  "command": "get_application_info",  
  "id": 1,  
  "version": "1"  
}
```

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 antispysware 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":"ANTISTEALTH32",
      "description":"Anti-Stealth support module",
      "version":"1106",
      "date":"2016-10-17"
    },{
      "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

Command line

```
ermm.exe get license-info
```

Parameters

None

Example

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

Command line

```
ermm.exe get logs --name warnlog --start-date "2017-04-04 06-00-00" --end-date "2017-04-04 12-00-00"
```

Parameters

Name	Value
name	{ all, virlog, warnlog, scanlog, blocked, hipslog, urllog, devctrlog } : 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])

Example

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, error }

Command line

```
ermm.exe get activation-status
```

Parameters

None

Example

call

```
{  
  "command": "get_activation_status",  
  "id": 1,  
  "version": "1"  
}
```

result

```
{  
  "id": 1,  
  "result": {  
    "status": "success"  
  },  
  "error": null  
}
```

get scan-info

Get information about running scan.

Command line

```
ermm.exe get scan-info
```

Parameters

None

Example

call

```
{  
  "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 }

Command line

```
ermm.exe get configuration --file C:\\tmp\\conf.xml --format xml
```

Parameters

Name	Value
file	the path where the configuration file will be saved
format	format of configuration: json, xml. Default format is xml

Example

```
call
```

```
{
  "command": "get_configuration",
  "id": 1,
  "version": "1",
  "params": {
    "format": "xml",
    "file": "C:\\tmp\\conf.xml"
  }
}
```

result

```
{
  "id": 1,
  "result": {
    "configuration": "PD94bWwgdmVyc2lvbj0iMS4w=="
  },
  "error": null
}
```

get update-status

Get information about the update. Result of status may be { success, error }

Command line

```
ermm.exe get update-status
```

Parameters

None

Example

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

Command line

```
ermm.exe start scan --profile "profile name" --target "path"
```

Parameters

Name	Value
profile	Profile name of On-demand computer scan defined in product
target	Path to be scanned

Example

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

Command line

```
ermm.exe start activation --key "activation key" | --offline "path to offline file"
```

Parameters

Name	Value
------	-------

key	Activation key
offline	Path to offline file

Example

```
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

Command line

```
ermm.exe start deactivation
```

Parameters

None

Example

```
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

Command line

```
ermm.exe start update
```

Parameters

None

Example

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 }

Command line

```
ermm.exe set configuration --file C:\tmp\conf.xml --format xml --password pass
```

Parameters

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)

Example

call

```
{
  "command": "set_configuration",
  "id": 1,
  "version": "1",
  "params": {
    "format": "xml",
    "file": "C:\\tmp\\conf.xml",
    "password": "pass"
  }
}
```

result

```
{
  "id": 1,
  "result": {
  },
  "error": null
}
```

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 Security](#)
- [Cómo activar ESET Endpoint Security](#)
- [Cómo usar las credenciales actuales para activar un producto nuevo](#)
- [Cómo quitar un virus del equipo](#)
- [Cómo permitir la comunicación para una aplicación específica](#)
- [Cómo crear una nueva tarea en Tareas programadas](#)
- [Cómo programar una exploración semanal del equipo](#)
- [Cómo conectar mi producto a ESET Security Management Center](#)
- [Cómo utilizar el modo anulación](#)
- [Procedimiento para aplicar una política recomendada para ESET Endpoint Security](#)
- [Cómo configurar un servidor reflejado](#)
- [Cómo actualizo a Windows 10 con ESET Endpoint Security](#)
- [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 Security](#)

Si el problema no está contemplado en la lista de páginas de ayuda precedente, intente buscarlo en las Páginas de ayuda de ESET Endpoint Security 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.

- [Mejores prácticas para protegerse contra malware tipo Filecoder \(ransomware\)](#)
- [Preguntas frecuentes sobre ESET Endpoint Security y ESET Endpoint Antivirus](#)
- [Crear o editar una regla firewall para permitir conexiones RDP en ESMC](#)
- [¿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.

Cómo actualizar ESET Endpoint Security

La actualización de ESET Endpoint Security 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** (consulte [más información sobre las Tareas programadas](#)).

Cómo activar ESET Endpoint Security

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.).

Para activar su copia de ESET Endpoint Security directamente desde el programa, abra la ventana principal del programa de ESET Endpoint Security y, en el menú principal, haga clic en **Ayuda y soporte técnico > Activar producto** o en **Estado de protección > Activar producto**.

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

- **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 Business Account:** una cuenta creada en el portal de [ESET Business Account](#) con credenciales

(dirección de correo electrónico + contraseña). Este método le permite administrar múltiples licencias desde una ubicación.

- **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 Security Management Center. También puede utilizar esta opción si desea activar este cliente más tarde.

Si tiene un nombre de usuario y una contraseña que utilizó para activaciones anteriores de productos de ESET, y no sabe cómo activar ESET Endpoint Security, [convierta sus credenciales anteriores en una clave de licencia](#).

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

Podrá cambiar la licencia del producto en cualquier momento. Para realizar esto, haga clic en **Ayuda y soporte** > **Cambiar licencia** en la ventana principal del programa. Verá la identificación de la licencia pública utilizada para identificar su licencia con el soporte de ESET. El nombre de usuario bajo el cual su equipo está registrado se almacena en la sección **Acerca de** que puede ver al hacer clic derecho en el ícono de la bandeja del sistema .

 ESET Security Management Center 7.2 o ESET PROTECT 8 puede activar equipos cliente de manera silenciosa con el uso de licencias que el administrador pone a disposición. Para obtener instrucciones sobre cómo hacer esto, consulte la [Ayuda en línea de ESET PROTECT](#).

Ingreso de su clave de licencia durante la activación

Las actualizaciones automáticas son importantes para su seguridad. ESET Endpoint Security 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.

Inicie sesión en ESET Business Account

La cuenta de Security Admin es una cuenta creada en el portal ESET Business Account con su **dirección de correo electrónico** y **contraseña**, que puede ver todas las autorizaciones de puestos. Una cuenta de Security Admin le permite administrar múltiples licencias. Si no posee una cuenta de Security Admin, haga clic en **Crear cuenta** y se lo redireccionará al portal ESET Business Account donde se puede registrar con sus credenciales.

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

Procedimiento para usar credenciales de la licencia para activar un producto de punto de conexión de ESET más reciente.

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.

Cómo quitar un virus del equipo

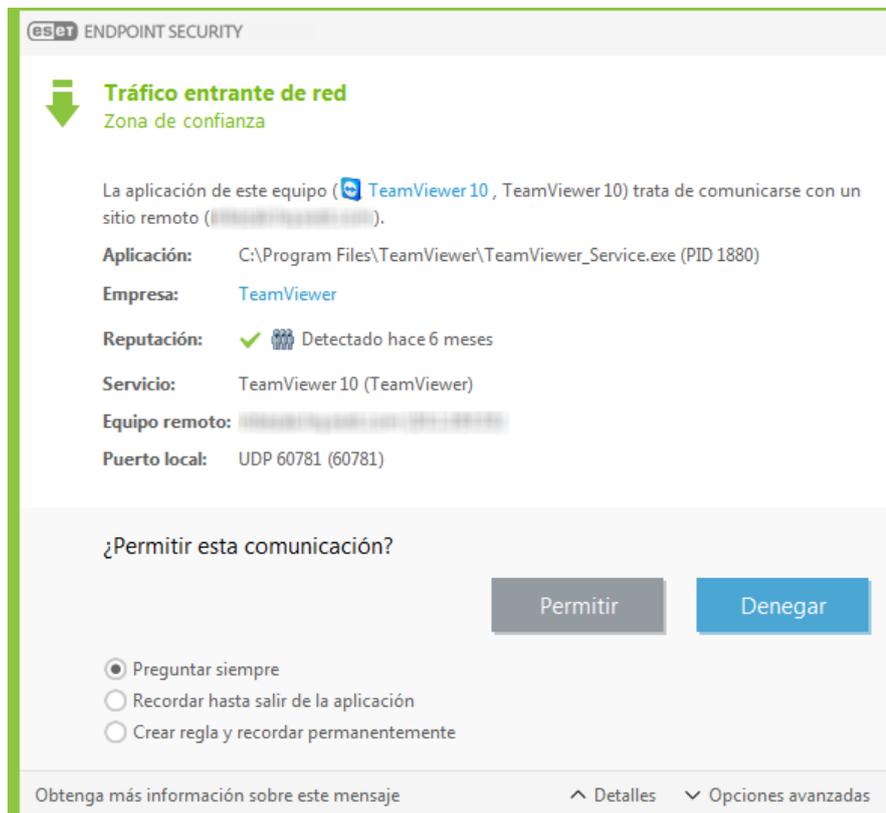
Si su equipo muestra síntomas de infección por malware; por ejemplo, funciona más lento o con frecuencia no responde, se recomienda hacer lo siguiente:

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 permitir la comunicación para una aplicación específica

Si se detecta una nueva conexión en el modo interactivo y no hay ninguna regla coincidente, el programa le solicitará que permita o deniegue la conexión. Si desea que ESET Endpoint Security realice la misma acción cada vez que la aplicación intente establecer una conexión, seleccione la casilla de verificación **Recordar acción (crear regla)**.



Puede crear nuevas reglas de firewall para las aplicaciones antes de que ESET Endpoint Security las detecte en la ventana de configuración del firewall. Abra la ventana principal del programa > **Configuración** > **Red** > **Firewall** > haga clic en la rueda dentada > **Configurar...** > **Avanzado** > **Reglas** haciendo clic en **Editar**.

Haga clic en **Agregar** para agregar la regla. En la pestaña **General**, ingrese el nombre, la dirección y el protocolo de comunicación para la regla. Esta ventana permite definir la acción que se tomará cuando se aplique la regla.

Ingrese la ruta al archivo ejecutable de la aplicación y el puerto de comunicación local en la pestaña **Local**. Haga clic en la pestaña **Remoto** para ingresar la dirección y el puerto remotos (de ser necesario). La nueva regla creada se aplicará en cuanto la aplicación vuelva a intentar comunicarse.

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 habitual, abra la ventana principal del programa y haga clic en **Herramientas > Tareas programadas**. La siguiente guía le indicará cómo programar una tarea que explorará sus unidades locales todas las semanas. Lea nuestro [artículo de la base de conocimiento](#) para obtener instrucciones más detalladas.

Para programar una tarea de exploración:

1. Haga clic en **Agregar** en la pantalla principal de Tareas programadas.
2. 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 Security al ESET PROTECT

Cuando haya instalado ESET Endpoint Security 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 ESMC.

- [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 Security](#)

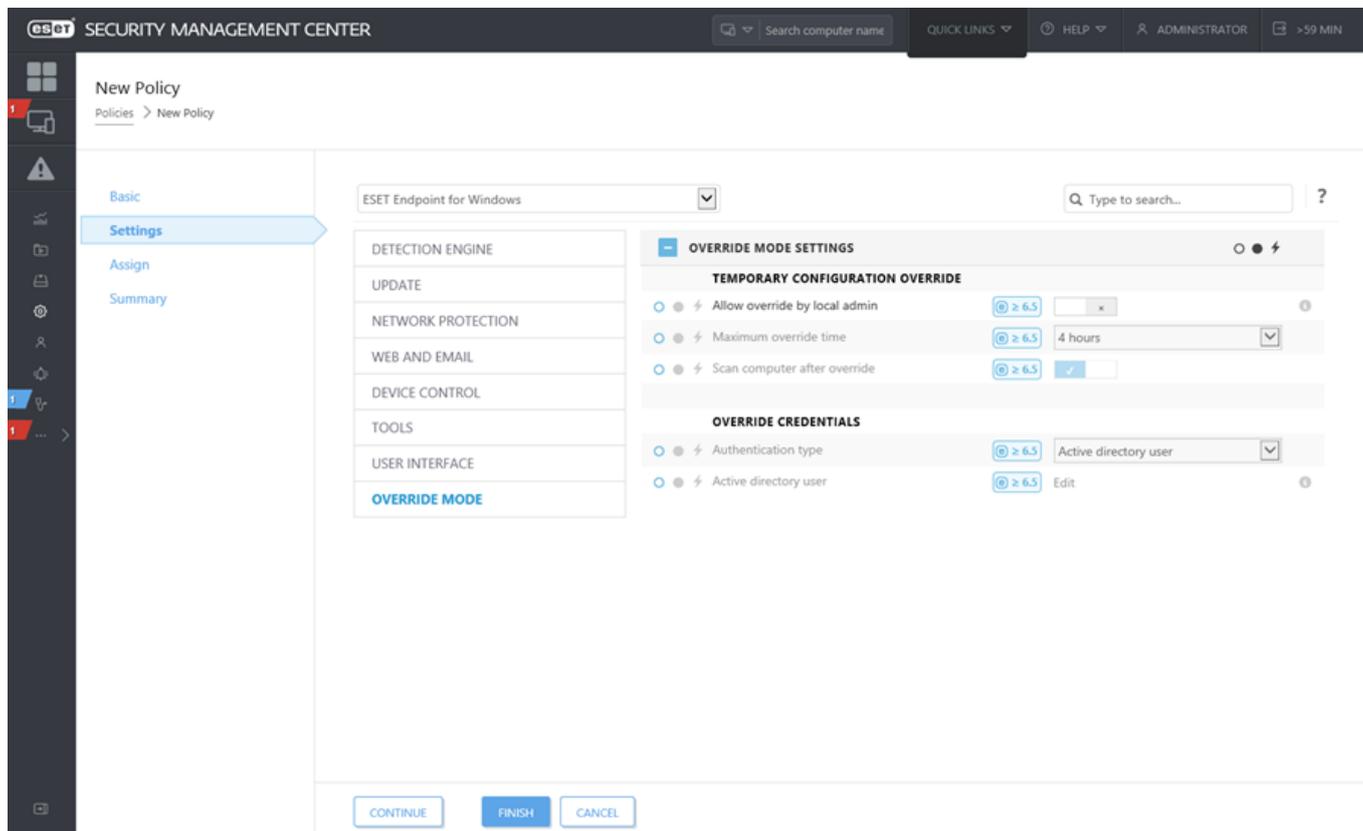
Cómo utilizar el modo anulación

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 ESMC 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 Security.
- La autenticación de grupo de Active Directory es compatible con la versión 7.0.2100.4 de ESET Endpoint Security y posteriores.

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.



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 ESMC 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 ESMC, 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 Security

La práctica recomendada después de conectar ESET Endpoint Security con ESET Security Management Center es aplicar una [política](#) recomendada o una personalizada.

Hay varias políticas incorporadas para ESET Endpoint Security:

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 ESET LiveGrid® 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 menos la conexión ESMC y EEI	Bloquear todo el tráfico, excepto la conexión con ESET Security Management Center y el servidor de ESET Enterprise Inspector (ESET Endpoint Security únicamente).
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 Threatsense 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 interfaz gráfica de usuario y la integración con el menú contextual están deshabilitadas. No se ejecutará egui.exe. Adecuado únicamente para la administración desde el ESET PROTECT Cloud .
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 Security instalado en sus estaciones de trabajo, siga estos pasos:

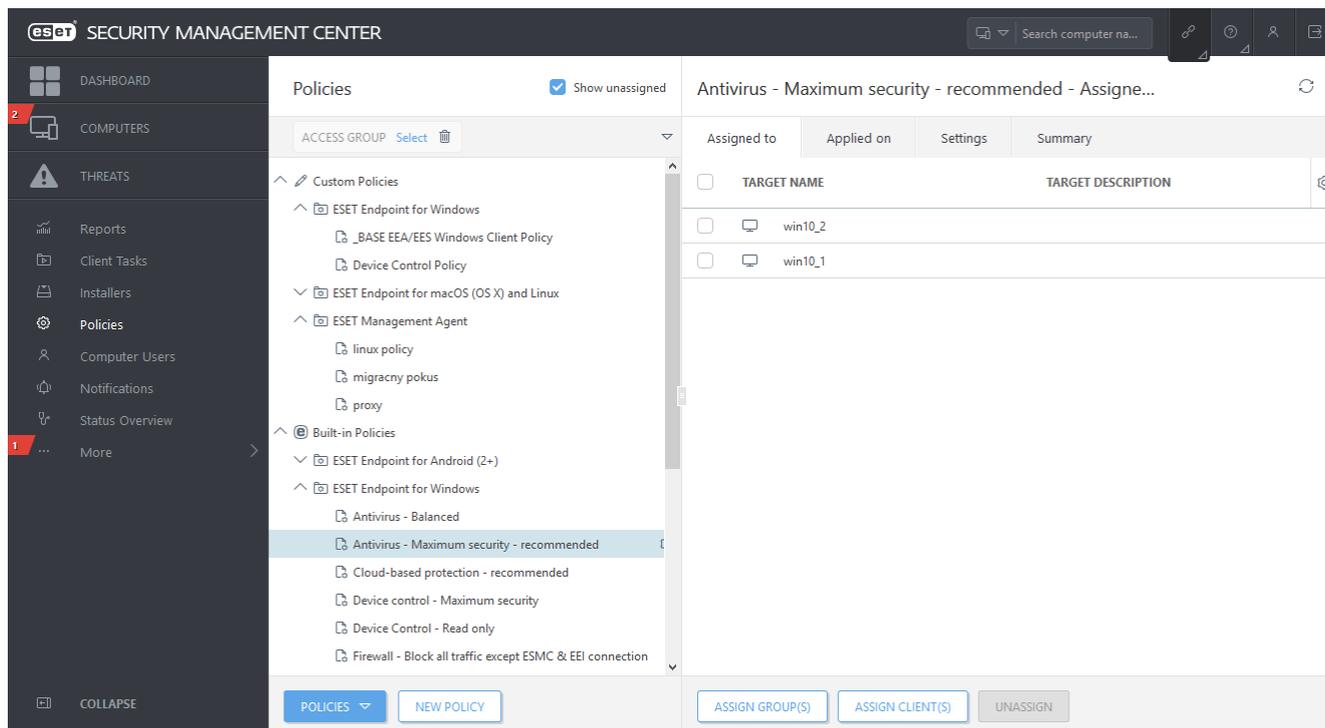
i Los siguientes artículos de la base de conocimiento de ESET pueden estar disponibles solo en inglés:

- [Aplique una política recomendada o predefinida para ESET Endpoint Security mediante ESMC](#)

1. Abra la consola web de ESMC.
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.



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 ESMC](#)

Cómo configurar un servidor reflejado

ESET Endpoint Security 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 Security o ESET Endpoint Antivirus.

Configuración de ESET Endpoint Security 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 [Actualizar reflejo](#).

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.

i Si no desea realizar la actualización de módulos mediante el servidor HTTP interno, desactive **Crear reflejo de actualización**.

Cómo actualizo a Windows 10 con ESET Endpoint Security



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.

Versión 7.x:

Haga clic en el enlace apropiado más abajo para descargar e instalar la última versión para prepararse para actualizar a Microsoft Windows 10:

[Descargar ESET Endpoint Security 7 32-bit](#) [Descargar ESET Endpoint Antivirus 7 32-bit](#)

[Descargar ESET Endpoint Security 7 64-bit](#) [Descargar ESET Endpoint Antivirus 7 64-bit](#)

Versión 5.x:



Los productos de ESET Endpoint de la versión 5 se encuentran en este momento en el [Fin de su vida útil](#). Esto significa que las versiones ya no están disponibles a nivel público para la descarga. Recomendamos actualizar a la [versión más reciente de los productos de ESET Endpoint](#).

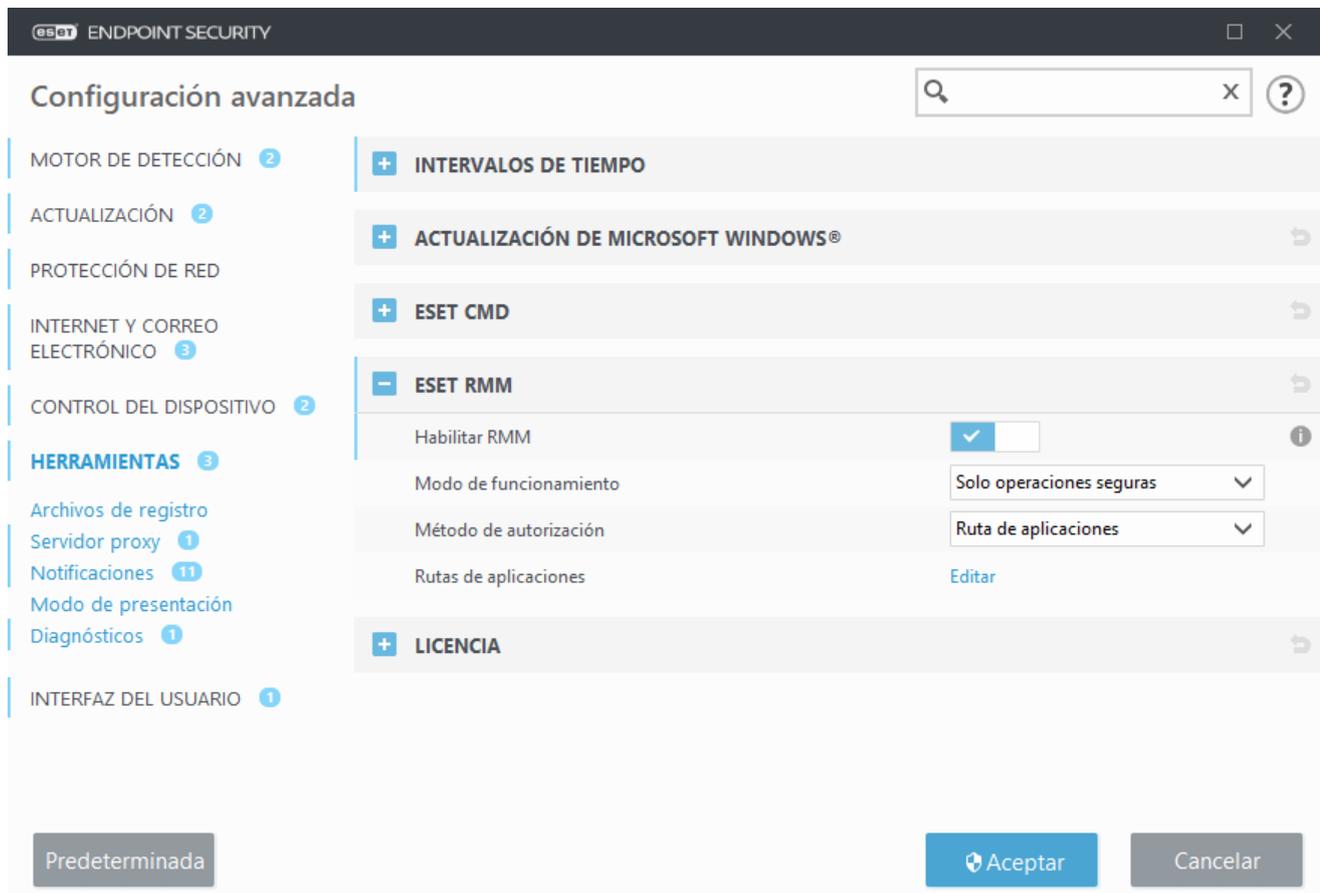
Versiones en otros idiomas:

Si busca versiones en otros idiomas para su ESET endpoint product, [visite nuestro sitio de descarga](#).

i [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 Security 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, presione **F5** para acceder a Configuración avanzada, haga clic en **Herramientas**, expanda **ESET RMM** y active el interruptor que se encuentra 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.

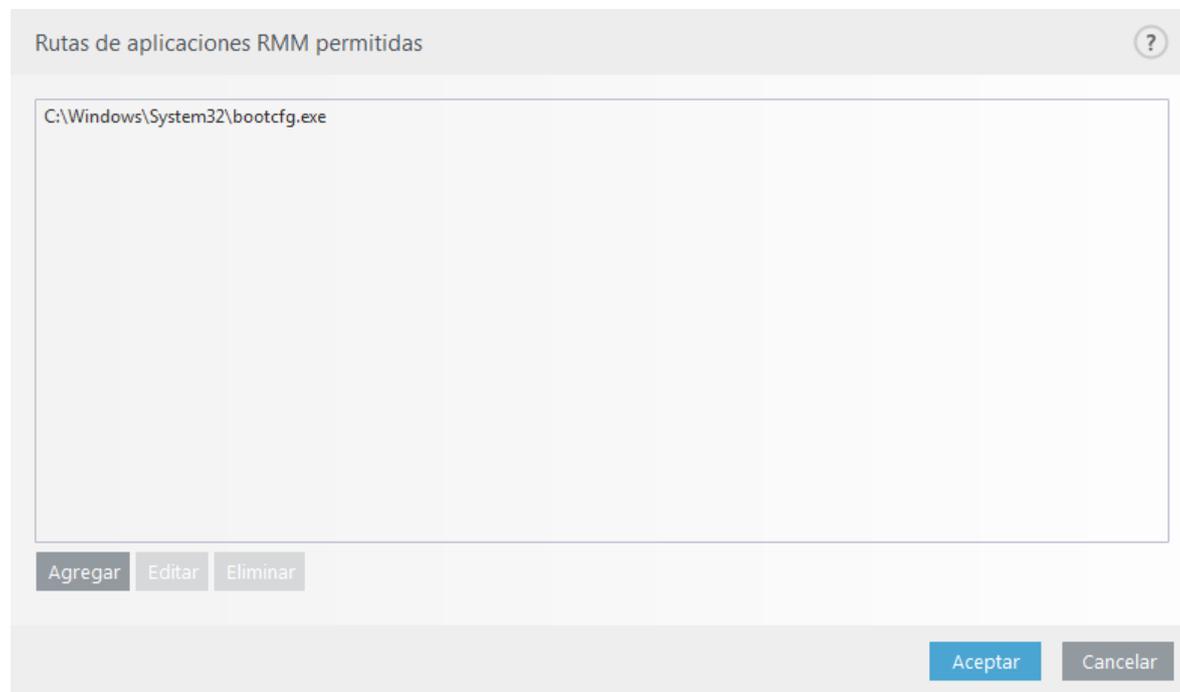
Operación	Modo Operaciones seguras únicamente	Modo Todas las operaciones
Obtener información de la aplicación	✓	✓
Obtener configuración	✓	✓
Obtener información de la licencia	✓	✓
Obtener registros	✓	✓
Obtener estado de protección	✓	✓
Obtener estado de actualización	✓	✓
Establecer configuración		✓
Comenzar 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.

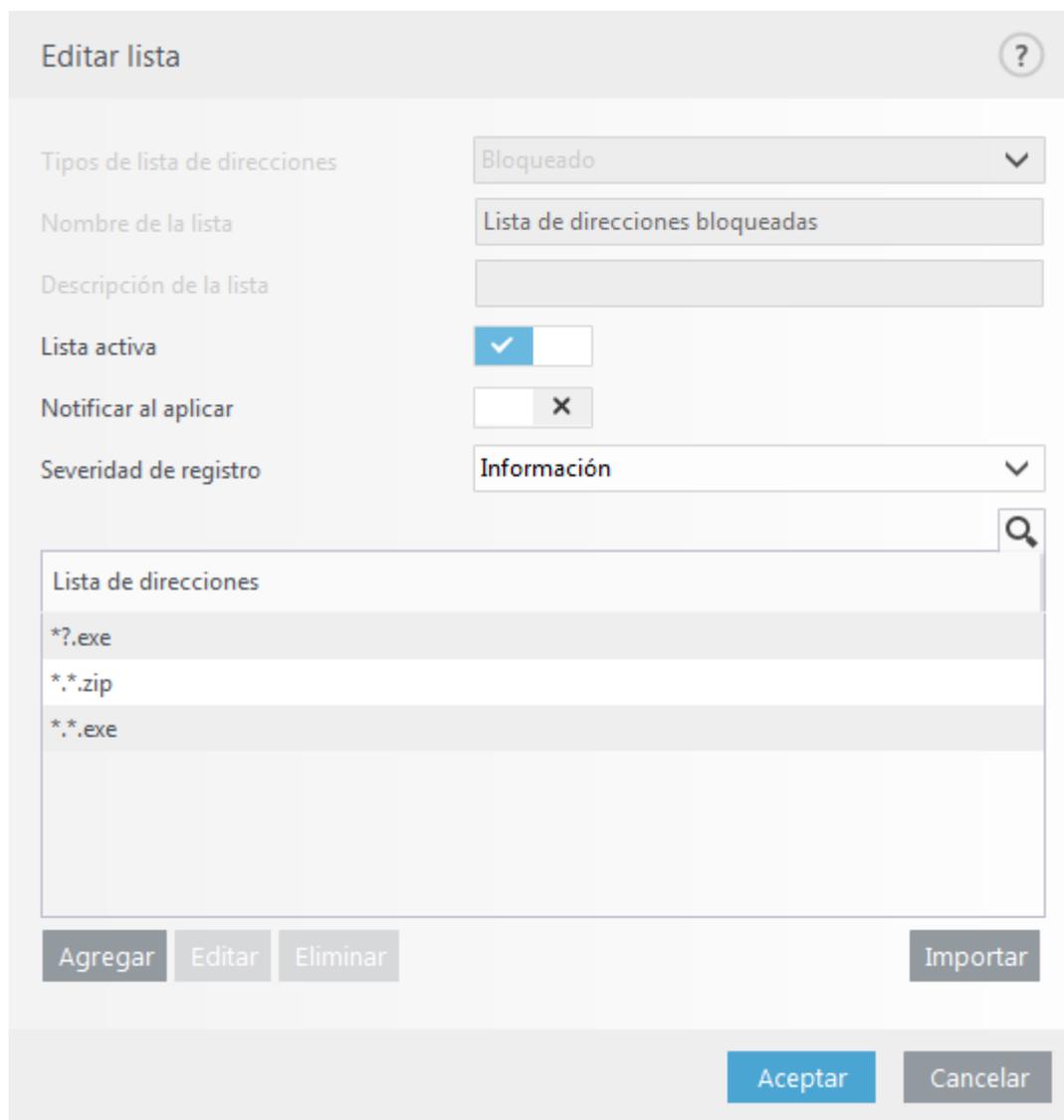
En la instalación predeterminada de ESET Endpoint Security, el archivo ermm.exe se encuentra en el directorio de la aplicación Endpoint (ruta predeterminada: *C:\Program Files\ESET\ESET Security*). Archivo ermm.exe intercambia información con el complemento RMM, que se comunica con el agente RMM, conectado 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 una nueva 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. El Administrador Remoto puede recopilar registros con la palabra **Advertencia**.



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

- *?.exe
- *. *.zip
- *. *.exe

Agregar Editar Eliminar Importar

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 todos los archivos comprimidos zip a descargar.

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 Security

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](#).

Cómo resolver el mensaje de error "El navegador seguro no pudo redireccionarse a la página web solicitada"

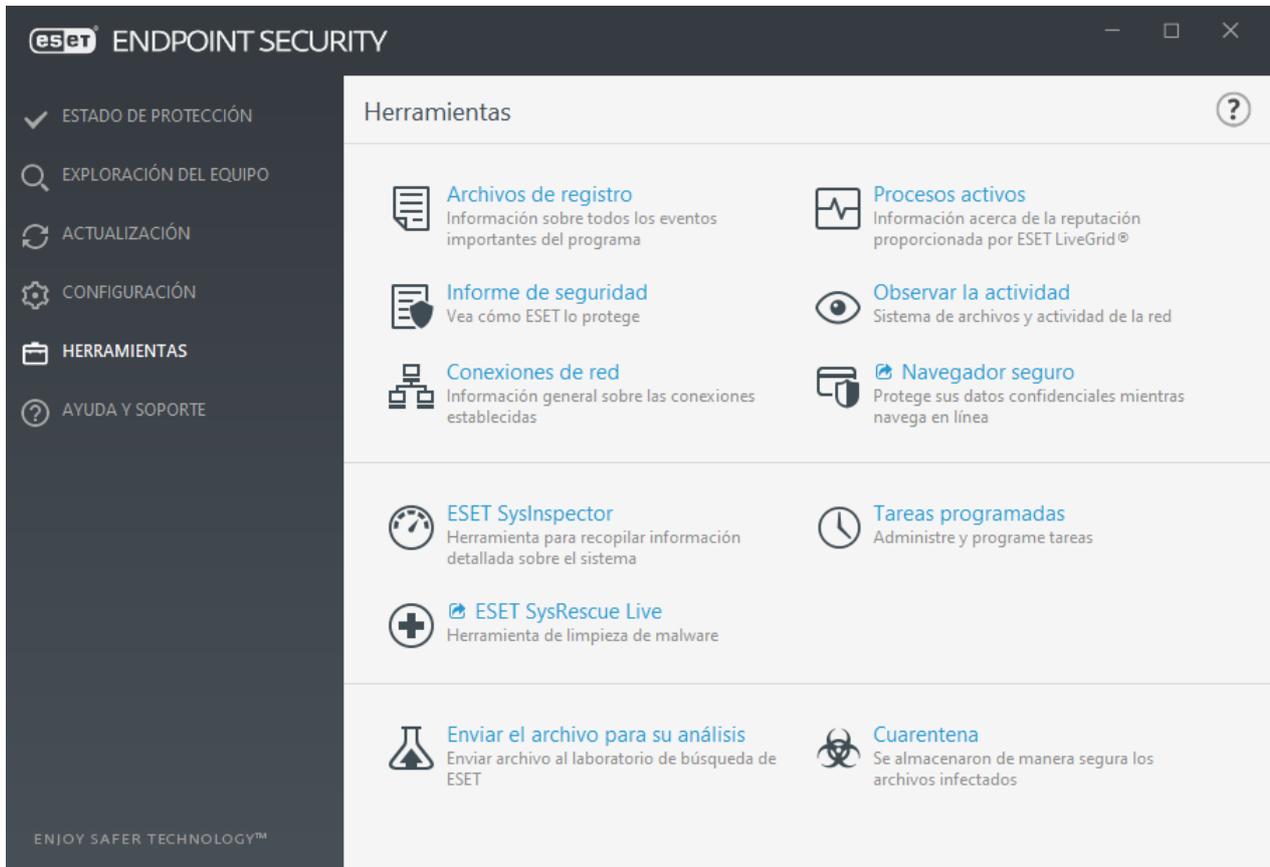
Para resolver este error, siga las instrucciones que se mencionan abajo:

Luego de completar cada uno de los pasos, verifique si el navegador seguro está funcionando.



Si la ventana del navegador sigue sin funcionar, complete el siguiente paso hasta que funcione nuevamente.

1. Abra la ventana principal del programa de su producto ESET.
2. Haga clic en **Herramientas > Navegador seguro**. Con la ventana Navegador seguro abierta, continúe al siguiente paso.



3. Limpie el caché del navegador. ¿Cómo [limpio el caché de Firefox](#) o de [Google Chrome en mi navegador](#)?
4. Asegúrese de estar usando la versión más reciente de su sistema operativo Windows y de su producto comercial Windows de ESET: [Consulte cuál es la versión más reciente de los productos comerciales de ESET.](#)
5. [Deshabilite el navegador seguro](#) y reinicie su equipo. Vuelva a habilitar el navegador seguro e intente abrir la ventana Navegador seguro.
6. Asegúrese de que su navegador predeterminado esté incluido en **Configuración avanzada > Web y correo electrónico > Filtrado de protocolos > Aplicaciones excluidas.**
7. Es posible que experimente un conflicto con su software o cortafuegos de seguridad de terceros. Analice la posibilidad de revisar y desinstalar este software de terceros en la ventana de programas Añadir/eliminar.
8. Si no actualizó su producto ESET en los pasos anteriores, [desinstale y vuelva a instalar el producto ESET.](#) Luego de reiniciar su equipo, deshabilite y vuelva a habilitar el Navegador seguro.

Navegador seguro en línea es una capa de protección adicional diseñada para proteger sus datos financieros durante las transacciones en línea.

En la mayoría de los casos, la protección de banca y pagos se ejecuta en su navegador predeterminado luego de visitar un sitio web de banca conocido. Para acceder directamente al navegador protegido, haga clic en

Herramientas en ESET Endpoint Security y, luego, haga clic en  **Navegador seguro.**

Para obtener más información sobre las funciones de Navegador seguro, lea los siguientes artículos de la base de conocimientos de ESET que están disponibles en inglés y otros idiomas:

- [¿Cómo uso el navegador seguro de ESET?](#)
 - [Habilitar o deshabilitar la Protección de banca y pagos en línea de ESET para un sitio web específico](#)
 - [Pausar o deshabilitar la protección de banca y pagos en línea en los productos de inicio de ESET Windows](#)
 - [Protección de banca y pagos en línea de ESET: errores frecuentes](#)
 - [Glosario de ESET | Protección de banca y pagos en línea](#)
-

Si todavía no puede resolver su problema, [envíe un correo electrónico a Soporte técnico de ESET](#).

Acuerdo de licencia de usuario final

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

Bajo los términos de este Acuerdo de licencia de usuario final (en adelante, el "Acuerdo") celebrado entre ESET, spol. s r. o., con domicilio social en Einsteinova 24, 851 01 Bratislava, Slovak Republic, inscrita en el Registro Mercantil y de Sociedades administrado por el Tribunal del Distrito I de Bratislava, Sección Sro, Asiento n.º 3586/B, Número de registro comercial 31333532 (en adelante, "ESET" o el "Proveedor") y Usted, persona física o jurídica (en adelante, "Usted" o el "Usuario final"), tiene derecho a utilizar el Software definido en el Artículo 1 del presente 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 la opción "Acepto" durante la instalación, la descarga, la copia o la utilización del Software, Usted acepta los términos y condiciones del presente Acuerdo. Si no acepta todas las disposiciones de este Acuerdo, haga clic en la opción "No acepto" de inmediato, cancele la instalación o la descarga, destruya o devuelva el Software, el soporte de instalación, la documentación adjunta y el recibo de compra al Proveedor o al punto de venta donde adquirió 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 (en adelante referido como "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 (en adelante, 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 (en adelante, "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 tiene el derecho de ingresar la clave de licencia para acceder al Software solo en la medida en que utilice el Software en conformidad con las limitaciones que surgen de la cantidad 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) **Business Edition.** Para usar el Software en servidores de correo, pasarelas de correo, puertas de correo o puertas de Internet, deberá adquirir la versión Business Edition del Software.

d) **Término de la Licencia.** El derecho a utilizar el Software tendrá un límite de tiempo.

e) **Software de OEM.** El Software de OEM estará limitado al equipo con el cual lo adquirió. 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 rescindiré 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 tendrá el derecho de lanzar actualizaciones del Software de cuando en cuando (en adelante, "Actualizaciones"), pero no tiene la obligación de suministrar actualizaciones. Esta función se encuentra habilitada en la configuración estándar del Software, por lo que las Actualizaciones se instalan en forma automática, a menos que el Usuario final haya deshabilitado la instalación automática de las Actualizaciones. A fin de que se suministren las Actualizaciones, es necesario llevar a cabo la verificación de la autenticidad de la Licencia, que incluye información relacionada con el equipo y/o con la plataforma en la que se instale el Software en conformidad con la Política de Privacidad.

b) **Envío de infiltraciones e información al Proveedor.** El Software contiene funciones que reúnen muestras de nuevos virus informáticos, otros programas informáticos dañinos y objetos sospechosos, problemáticos, potencialmente no deseados o potencialmente no seguros como archivos, URLs, paquetes de IP y marcos de Ethernet (en adelante denominados "Infiltraciones") y luego los envía al Proveedor, incluso, por ejemplo, la información sobre el proceso de instalación, el equipo o la plataforma en los cual se instala el Software, o la información sobre las operaciones y la funcionalidad del Software (en adelante referida como "Información"). La Información y las Infiltraciones pueden contener datos (incluidos datos personales obtenidos aleatoriamente o accidentalmente) sobre el Usuario Final u otros usuarios del equipo en el cual se encuentra instalado el Software, y archivos afectados por Infiltraciones con metadatos asociados.

La Información y las Infiltraciones pueden ser recopiladas por las siguientes funciones del Software:

i. La función Sistema de reputación de LiveGride incluye la recopilación y el envío de hashes de una vía relacionados a Infiltraciones al Proveedor. Esta función se activa con la configuración estándar del Software.

ii. La función del sistema de comentarios de LiveGrid es recopilar información acerca de las infiltraciones con metadatos relacionados para enviársela al Proveedor. El Usuario final debe activar esta función durante la instalación del Software.

El proveedor solo debe hacer uso de la información y de las infiltraciones que recibe para analizar y para investigar las infiltraciones, para mejorar el Software y el proceso de verificación de la autenticidad de la Licencia. Asimismo, debe tomar las medidas correspondientes para garantizar la seguridad de las infiltraciones y de la información que recibe. Si se activa esta función del Software, el Proveedor deberá recopilar y procesar las infiltraciones y la información tal como se especifica en la Política de Privacidad y en conformidad con las normas legales vigentes. Puede desactivar estas funciones en cualquier momento.

A los efectos de este Acuerdo, es necesario recopilar, procesar y almacenar información que permita al Proveedor identificarlo en conformidad con la Política de Privacidad. Por medio del presente, reconoce que el Proveedor utiliza sus propios medios para verificar si Usted hace uso del Software de acuerdo con las disposiciones del Acuerdo. Asimismo, reconoce que, a los efectos de este Acuerdo, es necesario que su información se transfiera durante las comunicaciones entre el Software y los sistemas informáticos del Proveedor o de sus socios comerciales como parte de la red de distribución y soporte del Proveedor a fin de garantizar la funcionalidad del Software, de autorizar el uso del Software y proteger los derechos del Proveedor.

Tras la finalización de este Acuerdo, el Proveedor o cualquiera de sus socios comerciales tendrán el derecho de transferir, procesar y almacenar datos esenciales que lo identifiquen, con el propósito de realizar la facturación y para la ejecución del presente Acuerdo y para transmitir notificaciones a su equipo. Por medio del presente, Usted acepta recibir notificaciones y mensajes que incluye, pero que no se limitan a, información relacionada con el marketing.

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 licenciatarios. 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 licenciatarios. 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. Más allá de la forma de rescisión de este Acuerdo, las disposiciones de los artículos 7, 8, 11, 13, 19 y 21 seguirán siendo aplicables por tiempo ilimitado.

11. DECLARACIONES DEL USUARIO FINAL. COMO USUARIO FINAL, USTED RECONOCE QUE EL SOFTWARE SE SUMINISTRA EN UNA CONDICIÓN "TAL CUAL ES", SIN UNA GARANTÍA EXPRESA O IMPLÍCITA DE NINGÚN TIPO Y HASTA EL ALCANCE MÁXIMO PERMITIDO POR LAS LEYES APLICABLES. NI EL PROVEEDOR, SUS LICENCIATARIOS, SUS AFILIADOS NI LOS TITULARES DEL COPYRIGHT PUEDEN HACER NINGUNA REPRESENTACIÓN O GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, PERO SIN LIMITARSE A, LAS GARANTÍAS DE COMERCIABILIDAD O ADECUACIÓN PARA UN FIN ESPECÍFICO O GARANTÍAS DE QUE EL SOFTWARE NO INFRINGIRÁ UNA PATENTE, DERECHOS DE PROPIEDAD INTELECTUAL, MARCAS COMERCIALES U OTROS DERECHOS. NO EXISTE NINGUNA GARANTÍA DEL PROVEEDOR NI DE NINGUNA OTRA PARTE DE QUE LAS FUNCIONES CONTENIDAS EN EL SOFTWARE CUMPLIRÁN CON SUS REQUISITOS O DE QUE LA OPERACIÓN DEL SOFTWARE SERÁ ININTERRUMPIDA O ESTARÁ LIBRE DE ERRORES. USTED ASUME TODA LA RESPONSABILIDAD Y EL RIESGO POR LA ELECCIÓN DEL SOFTWARE PARA LOGRAR SUS RESULTADOS DESEADOS Y POR LA INSTALACIÓN, EL USO Y LOS RESULTADOS QUE OBTENGA DEL MISMO.

12. Sin más obligaciones. Este Acuerdo no crea obligaciones del lado del Proveedor y sus licenciatarios, excepto las obligaciones específicamente indicadas en este Acuerdo.

13. LIMITACIÓN DE RESPONSABILIDAD. HASTA EL ALCANCE MÁXIMO PERMITIDO POR LAS LEYES APLICABLES, EN NINGÚN CASO EL PROVEEDOR, SUS EMPLEADOS O SUS LICENCIATARIOS SERÁN RESPONSABLES DE PÉRDIDAS DE BENEFICIOS, INGRESOS O VENTAS O DE PÉRDIDAS DE DATOS O COSTES SOPORTADOS PARA OBTENER

PRODUCTOS O SERVICIOS DE SUSTITUCIÓN, DE DAÑOS A LA PROPIEDAD, DAÑOS PERSONALES, INTERRUPCIÓN DEL NEGOCIO, PÉRDIDA DE INFORMACIÓN COMERCIAL O DE DAÑOS ESPECIALES, DIRECTOS, INDIRECTOS, ACCIDENTALES, ECONÓMICOS, DE COBERTURA, CRIMINALES, ESPECIALES O SUCESIVOS CAUSADOS DE CUALQUIER MODO, YA SEA A CAUSA DE UN CONTRATO, AGRAVIO, NEGLIGENCIA U OTRO HECHO QUE ESTABLEZCA LA OCURRENCIA DE RESPONSABILIDAD, SOPORTADOS DEBIDO AL USO O A LA INCAPACIDAD DE USO DEL SOFTWARE, INCLUSO EN EL CASO DE QUE EL PROVEEDOR, SUS LICENCIATARIOS O SUS AFILIADOS HAYAN SIDO NOTIFICADOS SOBRE 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. 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 (en adelante, "Afiladas") 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 Afiladas operen o estén constituidas (en adelante, "Leyes de Control de Exportaciones") 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 Afiladas operen o estén constituidas (en adelante, "Normas sancionadoras").

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 Afiladas 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, la devolución del Software y la Documentación deben enviarse a: ESET, spol. s r. o., Einsteinova 24, 851 01 Bratislava, Slovak Republic.

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. En caso de existir diferencias entre las versiones idiomáticas de este Acuerdo, prevalecerá el texto en lengua inglesa. Las revisiones de este Acuerdo pueden realizarse únicamente por escrito y deberán estar firmadas ya sea por un representante autorizado por el Proveedor o por una persona expresamente autorizada para actuar en su nombre según lo establezcan las disposiciones de un poder notarial.

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.

EULA ID: BUS-STANDARD-20-01

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:

o 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;

o información sobre dispositivos de la red local, como el tipo, el proveedor, el modelo o el nombre del dispositivo;

o información relativa al uso de Internet, como dirección IP e información geográfica, paquetes IP, URL y marcos de Ethernet;

o 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