

The Bitdefender logo is displayed in a white, bold, sans-serif font. The background of the entire page is a dark, abstract digital landscape with glowing blue and cyan light trails, circular patterns, and a grid-like structure, suggesting a high-tech or cybersecurity environment.

# Bitdefender®

**Bitdefender Endpoint  
Security Tools for  
Windows**

**GUÍA DE USUARIO**

## Bitdefender Endpoint Security Tools for Windows Guía de Usuario

fecha de publicación 2019.11.29

Copyright© 2019 Bitdefender

### Advertencia legal

**Todos los derechos reservados.** Ninguna parte de este libro puede ser reproducida o transmitida de forma alguna, ni por ningún medio, electrónico o mecánico, incluyendo fotocopia, grabación o mediante un sistema de almacenamiento y recuperación, sin la autorización previa por escrito de un representante de Bitdefender. La inclusión de breves citas de reseñas se puede hacer sólo con la mención de la fuente citada. El contenido no puede ser modificado en forma alguna.

**Advertencia y Renuncia de Responsabilidad.** Este producto y su documentación están protegidos por los derechos de autor. La información en este documento se proporciona "tal cual", sin garantía. Aunque se han tomado todas las precauciones durante la preparación de este documento, los autores no tendrán responsabilidad alguna ante ninguna persona o entidad con respecto a cualquier pérdida o daño causado o presuntamente causado directa o indirectamente por la información contenida en el mismo.

Este documento contiene enlaces a sitios web de terceros que no están bajo el control de Bitdefender, por lo que Bitdefender no se hace responsable por el contenido de ningún sitio enlazado. Si usted accede a sitios web de terceros listados en este documento, lo hará bajo su responsabilidad. Bitdefender proporciona estos vínculos solamente para su conveniencia, y la inclusión del enlace no implica la aprobación por parte de Bitdefender o aceptar responsabilidad alguna sobre el contenido del sitio de terceros.

**Marcas Registradas.** En este documento pueden aparecer nombres de marcas registradas. Todas las marcas registradas y no registradas, en este documento, son propiedad exclusiva de sus respectivos propietarios, y respectivamente reconocidas.

## Tabla de contenidos

Prólogo .....	iv
1. Propósito y público al que va dirigida .....	iv
2. Cómo usar esta guía .....	iv
3. Convenciones utilizadas en esta guía .....	iv
4. Petición de Comentarios .....	v
1. Iniciando .....	1
1.1. Icono del área de notificación .....	1
1.2. La ventana principal .....	2
1.2.1. El área de estado .....	3
1.2.2. Cronología de eventos .....	4
1.3. La ventana de módulos .....	5
1.4. Menú Acciones .....	11
2. Analizando en busca de Malware .....	13
2.1. Analizar un archivo o carpeta .....	13
2.2. Ejecución de un análisis Quick Scan .....	13
2.3. Ejecución de un análisis completo .....	14
2.4. Configurar y ejecutar un análisis personalizado .....	15
2.4.1. Tipos archivo .....	16
2.4.2. Qué analizar? .....	17
2.4.3. ¿Qué hacer? .....	18
2.5. Comprobando Logs de Análisis .....	19
3. Uso del Cifrado de volúmenes .....	20
3.1. Cifrado de su sistema .....	20
3.2. Descifrado de su sistema .....	22
3.3. Comprobación del estado del cifrado .....	22
3.4. Cambio del PIN o contraseña de cifrado .....	22
4. Actualizaciones .....	24
4.1. Tipos de actualizaciones .....	24
4.2. Comprobar si su protección está actualizada .....	24
4.3. Realizando Actualización .....	25
5. Eventos .....	26
6. Uso de la interfaz de línea de comandos .....	28
6.1. Comandos compatibles .....	29
6.2. Códigos de error de la línea de comandos .....	38
7. Obtener Ayuda .....	40
Glosario .....	41

## Prólogo

### 1. Propósito y público al que va dirigida

Esta documentación se dirige a los usuarios finales de **Bitdefender Endpoint Security Tools**, el software cliente Security for Endpoints instalado en equipos y servidores para protegerlos frente al malware y otras amenazas de Internet y para hacer cumplir las políticas de control de usuarios.

La información aquí presentada debe ser fácilmente comprensible para cualquier persona que sepa trabajar en Windows.

### 2. Cómo usar esta guía

Esta guía está organizada de tal forma que sea sencillo encontrar la información que necesita.

[“Iniciando” \(p. 1\)](#)

Familiarícese con la interfaz de usuario de Bitdefender Endpoint Security Tools.

[“Analizando en busca de Malware” \(p. 13\)](#)

Descubra cómo ejecutar análisis en busca de malware.

[“Actualizaciones” \(p. 24\)](#)

Conozca más sobre las actualizaciones de Bitdefender Endpoint Security Tools.

[“Eventos” \(p. 26\)](#)

Compruebe la actividad de Bitdefender Endpoint Security Tools.

[“Obtener Ayuda” \(p. 40\)](#)

Dónde consultar y dónde pedir ayuda si se produce una situación inesperada.

### 3. Convenciones utilizadas en esta guía

#### Convenciones Tipográficas

En este manual se utilizan distintos estilos de texto con el fin de mejorar su lectura. Su aspecto y significado se indica en la tabla que aparece continuación.

Apariencia	Descripción
<a href="mailto:business-docs@bitdefender.com">business-docs@bitdefender.com</a>	Las direcciones de e-mail se incluyen en el texto como información de contacto.
“Prólogo” (p. iv)	Este es un enlace interno, hacia alguna localización dentro del documento.
nombre de archivo	Los archivos y carpetas se muestran usando una fuente monoespaciada.
opción	Todas las opciones del producto se muestran utilizando caracteres en <b>negrita</b> .
palabra clave	La palabras o frase más importantes se destacan utilizando caracteres en <b>negrita</b> .

## Admoniciones

Las advertencias son notas dentro del texto, marcadas gráficamente, que le facilitan información adicional relacionada con el párrafo que está leyendo.



### Nota

La nota es una pequeña observación. Aunque puede omitirla, las notas pueden proporcionar información valiosa, como características específicas o enlaces hacia temas relacionados.



### Importante

Esta requiere su atención y no es recomendable saltársela. Normalmente proporciona información importante aunque no extremadamente crítica.

## 4. Petición de Comentarios

Por favor, escríbanos para decirnos cómo cree que podría mejorarse esta guía y ayúdenos a proporcionarle la mejor documentación posible.

Díganoslo enviando un mensaje de correo electrónico a [business-docs@bitdefender.com](mailto:business-docs@bitdefender.com).

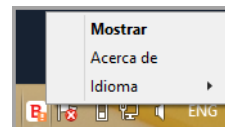
## 1. INICIANDO

Bitdefender Endpoint Security Tools es un programa de seguridad informática totalmente automatizado, gestionado de forma remota por su administrador de red. Una vez instalado, le protege frente a todo tipo de malware (como virus, spyware y troyanos), ataques de red, phishing y robo de datos. También puede utilizarse para hacer cumplir las políticas de uso de Internet y de equipos en su organización. Bitdefender Endpoint Security Tools tomará por usted la mayoría de las decisiones relacionadas con la seguridad y rara vez se mostrarán alertas emergentes. Los detalles sobre las acciones adoptadas y la información sobre las operaciones del programa están disponibles en la línea de tiempo de **Eventos**.

### 1.1. Icono del área de notificación

En el momento de la instalación, Bitdefender Endpoint Security Tools coloca un icono **B** en el área de notificación. Si hace doble clic en este icono, se abrirá la ventana principal. Si hace clic con el botón derecho sobre el icono se mostrará un menú contextual con algunas opciones útiles.

- **Mostrar** - abre la ventana principal de Bitdefender Endpoint Security Tools.
- **Acerca de** - abre una ventana con información sobre Bitdefender Endpoint Security Tools y le indica dónde buscar ayuda en caso de que surjan problemas inesperados. Esta ventana también incluye un enlace a la política de privacidad de Bitdefender.
- **Idioma** - le permite cambiar el idioma de la interfaz de usuario.
- **Usuario avanzado** - le permite acceder a los ajustes de seguridad y modificarlos después de proporcionar la contraseña en la ventana de inicio de sesión. Control Center recibe una notificación cuando un endpoint está en modo de Usuario avanzado y el administrador de Control Center siempre puede sobrescribir los ajustes de seguridad locales.



Icono Bandeja de sistema





#### Importante

Esta opción solo está disponible si el administrador de la red lo ha permitido mediante los ajustes de políticas.

Esta opción no está disponible para Bitdefender Endpoint Security Tools for Windows Legacy.

El icono Bitdefender Endpoint Security Tools del área de notificación le informa, cambiando de aspecto, sobre cuándo se producen incidencias que afectan a su equipo:

-  Critical issues affect the security of the system.
-  Some issues affect the security of the system.




### Nota

El administrador de red puede elegir ocultar el icono del área de notificación.

## 1.2. La ventana principal

La ventana principal de Bitdefender Endpoint Security Tools le permite consultar el estado de protección y ejecutar tareas de análisis. Todo se encuentra a tan sólo unos clics. La administración y configuración de la protección la realiza de forma remota el administrador de red.

Para acceder a la interfaz principal de Bitdefender Endpoint Security Tools, navegue desde el menú Inicio de Windows, siguiendo la ruta **Inicio** → **Todos los programas** → **Bitdefender Endpoint Security Tools** → **Abrir Consola de seguridad** o, de una manera más rápida, haga doble clic en el icono de Bitdefender Endpoint Security Tools  en la bandeja del sistema.



Ventana principal

La ventana está organizada en dos áreas principales:

- [Área de Estado](#)
- [Cronología de eventos](#)

### 1.2.1. El área de estado

El área de **estado** ofrece información útil relativa a la seguridad del sistema.



Área de Estado



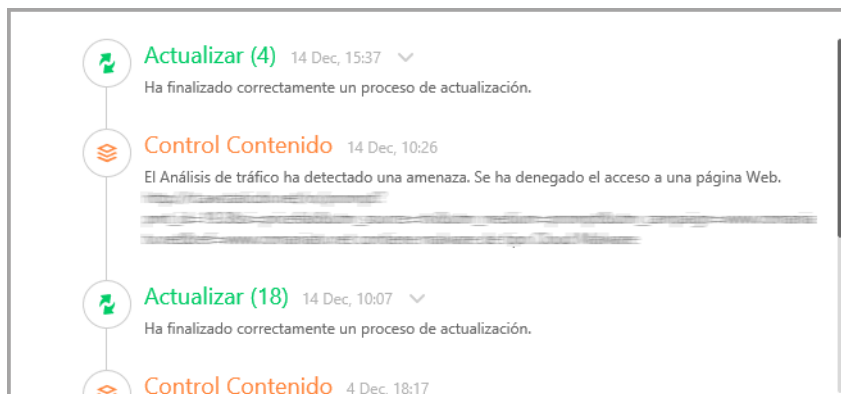
Puede identificar fácilmente el estado actual de seguridad gracias al símbolo que aparece a la izquierda del área de estado:

- **Marca de verificación verde.** No existen problemas que solucionar. Su equipo y sus datos están protegidos.
- **Marca de verificación amarilla.** Hay incidencias que afectan a la seguridad de su sistema, aunque no son críticas.
- **Aspa roja.** Hay incidencias críticas que afectan a la seguridad de su sistema.

Además del símbolo de estado, a la derecha del área de estado se muestra un mensaje detallado del estado de la seguridad. Puede ver las incidencias de seguridad detectadas haciendo clic en cualquier punto del área de estado. Las incidencias existentes las reparará su administrador de red.

## 1.2.2. Cronología de eventos


Bitdefender Endpoint Security Tools mantiene un registro detallado de los eventos relacionados con la actividad en su equipo (incluyendo también las actividades supervisadas por el Control de contenido).

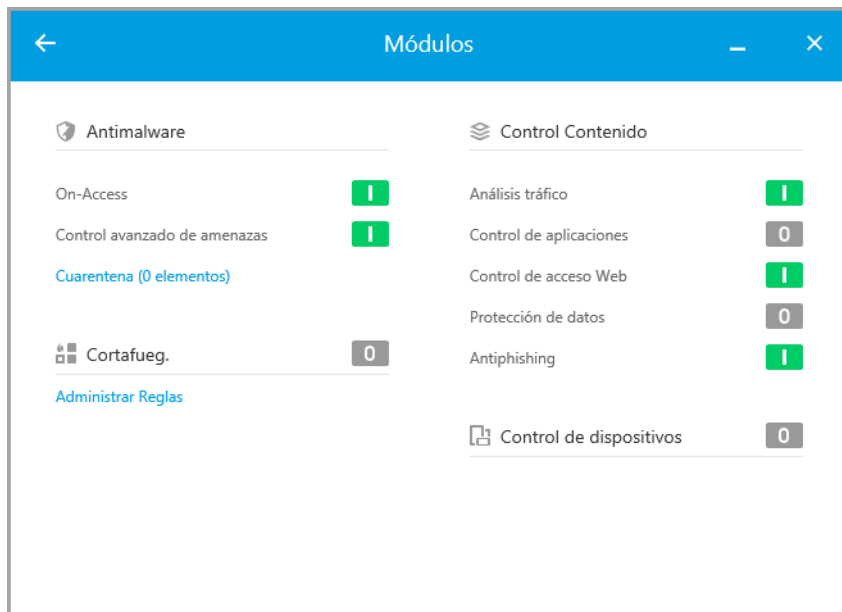


Cronología de eventos

La línea de tiempo de **eventos** es una herramienta muy importante para la supervisión de su protección de Bitdefender. Por ejemplo, puede comprobar fácilmente si una actualización se realizó correctamente o si se encontró malware en su equipo.

## 1.3. La ventana de módulos

La ventana de **módulos** muestra información útil sobre el estado y la actividad de los módulos de protección instalados. Para abrir la ventana de **módulos**, haga clic en el botón **Módulos**  de la ventana principal de Bitdefender Endpoint Security Tools.



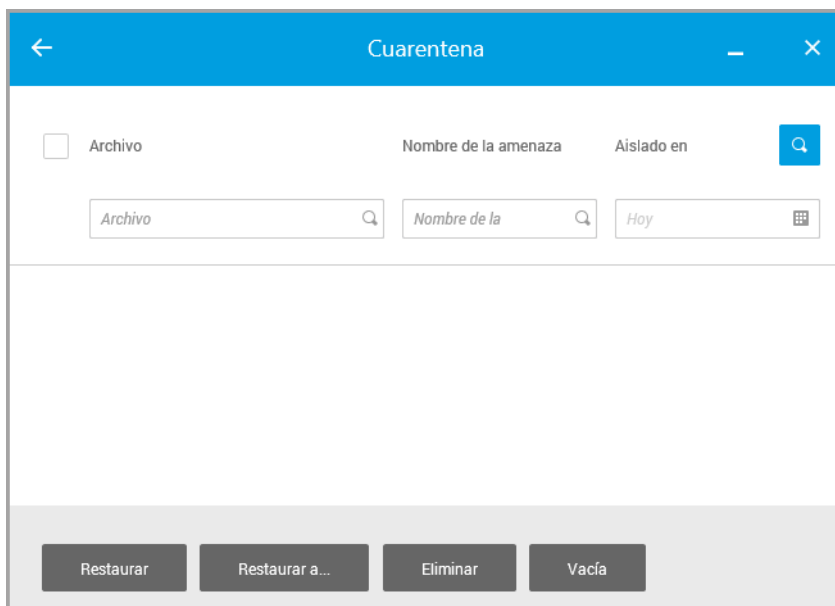
Ventana de módulos

### Antimalware

La protección antimalware es la base de su seguridad. Bitdefender Endpoint Security Tools le protege en tiempo real y bajo demanda contra todo tipo de malware, como virus, troyanos, spyware, adware, etc.

- **On-Access.** El análisis on-access evita que entren en el sistema nuevas amenazas de malware gracias al análisis de los archivos locales y de red cuando se accede a ellos (al abrirlos, moverlos, copiarlos o ejecutarlos), al análisis de los sectores de arranque y al de las aplicaciones potencialmente no deseadas (APND).

- **HyperDetect.** HyperDetect desvela ataques avanzados y actividades sospechosas en la etapa previa a su ejecución. Esta capa de seguridad contiene modelos de aprendizaje automático y tecnología de detección de ataques sigilosos.
- **Advanced Threat Control.** Monitoriza continuamente las aplicaciones que se están ejecutando en el endpoint, en busca de acciones indicativas de malware. Advanced Threat Control tratará automáticamente de desinfectar el archivo detectado.
- La **cuarentena** muestra la lista de archivos en cuarentena, su ruta original, la fecha y hora de su puesta en cuarentena y su estado de seguridad. Utilice los botones de abajo para eliminar o restaurar los archivos que desee. Si desea eliminar todos los archivos de la cuarentena, haga clic en el botón **Vaciar**.



Cuarentena

## Control Contenido

El módulo de control de contenido le protege mientras navega por Internet contra ataques de phishing, intentos de fraude, filtraciones de datos privados

y contenido Web inapropiado. También incluye un amplio conjunto de controles de usuario que ayudan al administrador de la red a hacer cumplir las políticas de uso de los equipos y de Internet.

- **Análisis de tráfico.** Gracias al análisis de los correos electrónicos entrantes y del tráfico web en tiempo real, este componente evita que se descargue malware en el endpoint. Los mensajes de correo salientes se analizan para evitar que el malware infecte otros endpoints.
- **Lista negra de aplicaciones.** Este componente impide el acceso a las aplicaciones no autorizadas en su empresa. El administrador es el responsable de crear las reglas para las aplicaciones permitidas en la organización.
- **Control de acceso Web.** Este componente le protege de acceder a sitios Web peligrosos en función de las reglas definidas por el administrador.
- **Protección de datos.** Este componente evita la divulgación no autorizada de información sensible basándose en las reglas definidas por el administrador.
- **Protección Antiphishing.** Este componente bloquea automáticamente las páginas Web de phishing conocidas para evitar que los usuarios puedan revelar sin darse cuenta información privada o confidencial a impostores online.
- **Network Attack Defense.** Network Attack Defense detecta técnicas de ataque a la red empleadas para obtener acceso a endpoints concretos, como ataques de fuerza bruta, exploits de red o ladrones de contraseñas.



### Nota

Este módulo no está disponible para Bitdefender Endpoint Security Tools for Windows Legacy.

## Cortafuego

El cortafuego le protege mientras está conectado a las redes e Internet filtrando los intentos de conexión y bloqueando las conexiones sospechosas o con riesgo.



### Nota

Este módulo no está disponible para Bitdefender Endpoint Security Tools for Windows Legacy.

## Control de dispositivos

Evitar la fuga de datos confidenciales y las infecciones de malware a través de dispositivos externos conectados a los endpoints. Para ello, aplica políticas con reglas de bloqueo y exclusiones a una amplia gama de dispositivos. El administrador es responsable de gestionar los permisos para los siguientes tipos de dispositivos:

- Adaptadores de Bluetooth
- Dispositivos CDROM
- Unidades de disquete
- IEEE 1284.4
- IEEE 1394
- Dispositivos de imágenes
- Modems
- Unidades de cinta
- Windows Portable
- Puertos COM/LPT
- Raid SCSI
- Impresoras
- Adaptadores de Red
- Adaptadores de red inalámbrica
- Almacenamiento interno y externo



### Nota

Este módulo no está disponible para Bitdefender Endpoint Security Tools for Windows Legacy.

## Control de aplicaciones

El módulo de Control de aplicaciones bloquea la ejecución de aplicaciones y procesos no autorizados en el endpoint. El Control de aplicaciones disminuye la frecuencia y el impacto de los problemas de malware, al reducir la superficie de ataque y las vulnerabilidades mediante el control del número de aplicaciones no deseadas en la red.



### Nota

Este módulo no está disponible para Bitdefender Endpoint Security Tools for Windows Legacy.

## Sandbox Analyzer

El módulo Sandbox Analyzer proporciona una potente capa de protección contra amenazas avanzadas que realiza un análisis automático y en profundidad de los archivos sospechosos que aún carecen de firma en los motores antimalware de Bitdefender. En el espacio aislado de Sandbox Analyzer se emplea un amplio conjunto de tecnologías de desarrollo propio para ejecutar las posibles acciones destructivas en un entorno virtual contenido alojado por Bitdefender, analizar su comportamiento e informar de cualquier cambio sutil en el sistema que pueda indicar malas intenciones.



### Nota

Este módulo no está disponible para Bitdefender Endpoint Security Tools for Windows Legacy.

## Cifrado de volumen

El módulo de Cifrado de volumen le permite realizar el cifrado de disco completo basándose en BitLocker en los equipos con Windows. Puede cifrar y descifrar los volúmenes, ya sean de arranque o no, con un solo clic, mientras que GravityZone gestiona todo el proceso, con una mínima intervención de los usuarios. Además, GravityZone almacena las claves de recuperación necesarias para desbloquear los volúmenes cuando los usuarios olvidan sus contraseñas.



### Nota

Este módulo no está disponible para Bitdefender Endpoint Security Tools for Windows Legacy.

## Sensor EDR

El sensor EDR (Endpoint Detection and Response) recopila, maneja e informa sobre los datos de comportamiento de aplicaciones y endpoints. Parte de la información se procesa localmente, mientras que se informa de un conjunto más complejo de datos a un componente backend de GravityZone.

El uso de este módulo supone un escaso impacto en cuanto a ancho de banda de red y consumo de recursos de hardware.



### Nota

Este módulo no está disponible para Bitdefender Endpoint Security Tools for Windows Legacy.

## Administración de parches


La Administración de parches mantiene al día el sistema operativo y las aplicaciones de software. Este módulo incluye varias características, como análisis de parches bajo demanda o programados, aplicación manual o automática de parches o informes de los parches que faltan.

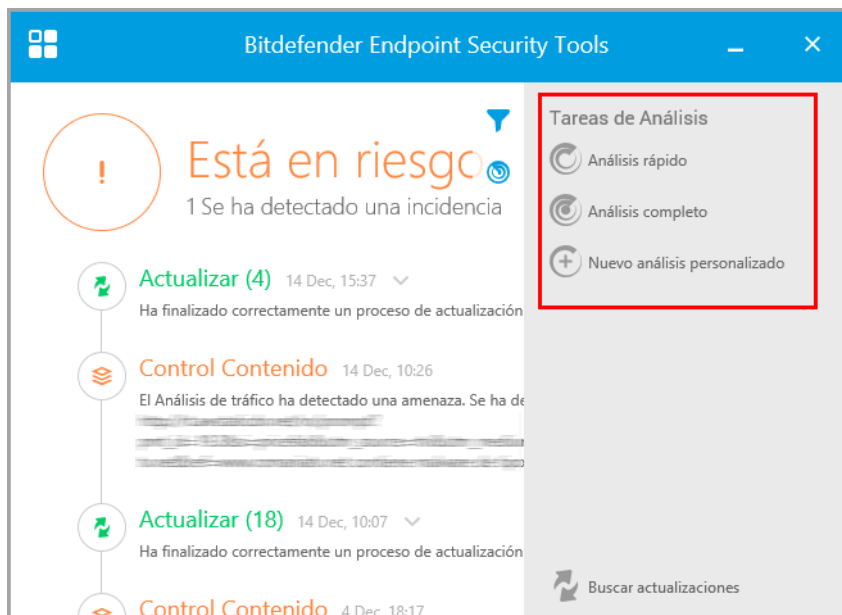


### Nota

Este módulo no está disponible para Bitdefender Endpoint Security Tools for Windows Legacy.

## 1.4. Menú Acciones

Para definir o ejecutar una tarea de análisis, haga clic en el botón **Acciones**  para abrir el menú de **Acciones**. Aquí puede comprobar también si hay actualizaciones.



Menú Acciones

### Análisis rápido

Utiliza el análisis en la nube para detectar malware ejecutándose en su sistema. Ejecutar un Análisis Rápido normalmente toma menos de un minuto y utiliza una fracción de los recursos del sistema que un análisis de virus regular.

### Análisis de sistema

Analiza el equipo por completo en busca de todo tipo de malware que pueda amenazar su seguridad, como virus, spyware, adware, rootkits y otros.

### Análisis personalizado

Le permite elegir las ubicaciones que desea analizar y configurar las opciones de análisis.





### Buscar actualizaciones

Dependiendo de los ajustes de actualización establecidos por su administrador de red, si se detecta una actualización, se le solicitará que la confirme o la actualización se realizará de forma automática.

## 2. ANALIZANDO EN BUSCA DE MALWARE

El objetivo principal de Bitdefender Endpoint Security Tools es mantener su equipo libre de malware. Esto lo consigue principalmente analizando en tiempo real los archivos a los que se accede, mensajes de correo y cualquier archivo nuevo descargado o copiado a su equipo. Además de la protección en tiempo real, también permite ejecutar análisis para detectar y eliminar malware de su equipo.

Puede analizar el equipo siempre que quiera ejecutando las tareas predeterminadas o sus propias tareas de análisis (tareas definidas por el usuario). Las tareas de análisis especifican las opciones de análisis y los objetos a analizar. Si desea analizar ubicaciones específicas en el equipo o configurar las opciones de análisis, configure y ejecute un análisis personalizado.

En cualquier momento durante el análisis puede ver el progreso de esta en la línea de tiempo de **eventos**.

### 2.1. Analizar un archivo o carpeta

Debe analizar archivos y carpetas que sospeche que puedan estar infectados. Haga clic derecho en el archivo o carpeta que desee analizar y seleccione la opción **Analizar con Bitdefender Endpoint Security Tools**. Dará comienzo el análisis y podrá supervisar el progreso en la línea de tiempo de **eventos**.

Al finalizar el análisis, podrá ver el resultado. Para obtener información detallada, haga clic **Ver registro**.

### 2.2. Ejecución de un análisis Quick Scan

**QuickScan** utiliza el análisis en la nube para detectar malware ejecutándose en su sistema. Ejecutar un Análisis Rápido normalmente toma menos de un minuto y utiliza una fracción de los recursos del sistema que un análisis de virus regular.

**Quick Scan** está preconfigurado para permitir el análisis:

- Procesos en ejecución, **sectores de arranque** y registro.
- Regiones de memoria críticas
- Archivos nuevos y modificados
- En busca de **rootkits**, **adware**, **spyware** y aplicaciones dialer en rutas críticas del sistema operativo como: %windir%\system32\, %temp%, /etc, /lib.

- En busca de aplicaciones potencialmente no deseadas (APND).

Para ejecutar un QuickScan, siga estos pasos:

1. Abra la ventana de Bitdefender Endpoint Security Tools.
2. Haga clic en el botón **Acciones** de la esquina superior derecha.
3. Haga clic en **Quick Scan**.
4. Espere a que se complete el análisis. Puede ver el progreso del análisis en la línea de tiempo. Una vez finalizado, haga clic en **Ver registro** para ver los resultados detallados.

## 2.3. Ejecución de un análisis completo

La tarea de **análisis completo** analiza todo el equipo en busca de todo tipo de malware que amenace su seguridad, como virus, spyware, adware, rootkits y otros.



### Nota

Ya que el **Análisis completo** realiza un análisis exhaustivo de todo el sistema, el análisis puede tomar cierto tiempo. Por lo tanto, se recomienda ejecutar esta tarea cuando no está utilizando su equipo.

Si desea analizar ubicaciones específicas en su equipo o configurar las opciones de análisis, configure y ejecute un análisis personalizado. Para más información, por favor vea [“Configurar y ejecutar un análisis personalizado”](#) (p. 15).

Antes de ejecutar un análisis completo, asegúrese de que Bitdefender Endpoint Security Tools está actualizado con sus firmas de virus. Analizar su equipo con firmas antiguas puede impedir que Bitdefender Endpoint Security Tools detecte nuevo malware surgido después de la última actualización. Para más información, por favor vea [“Actualizaciones”](#) (p. 24).

El **análisis completo** está configurado para permitir el análisis:

- Procesos en ejecución, [sectores de arranque](#) y registro.
- Archivos de correo electrónico y archivos de red de todas las unidades, incluidas las extraíbles.
- En busca de [rootkits](#), [adware](#), [spyware](#), keylogger y aplicaciones dialer en todas las unidades, incluidas las extraíbles.
- En busca de aplicaciones potencialmente no deseadas (APND)
- Cookies del navegador

Para realizar un análisis completo, siga estos pasos:

1. Abra la ventana de Bitdefender Endpoint Security Tools.
2. Haga clic en el botón **Acciones** de la esquina superior derecha.
3. Haga clic en **Análisis completo**.
4. Espere a que se complete el análisis. Puede ver el progreso del análisis en la línea de tiempo. Haga clic en **Ver detalles** para ver los detalles del análisis en curso. También puede poner en pausa, posponer o detener definitivamente el análisis.
5. Bitdefender Endpoint Security Tools aplicará automáticamente las acciones recomendadas sobre los archivos detectados. Una vez finalizado, haga clic en **Ver registro** para ver los resultados detallados.

## 2.4. Configurar y ejecutar un análisis personalizado

Para configurar un análisis detallado en busca de malware y ejecutarlo a continuación, siga estos pasos:

1. Abra la ventana principal de Bitdefender Endpoint Security Tools.
2. Haga clic en el botón **Acciones** de la esquina superior derecha.
3. Haga clic en **Nuevo análisis personalizado**. Se abrirá la ventana de **Análisis personalizado**.
4. Configure las opciones de análisis: **Agresivo, Normal, Tolerante, Personalizado**. Utilice la descripción que hay debajo de la opción para determinar el nivel de análisis que mejor se adapta a sus necesidades.
5. Seleccione el objetivo del análisis en el panel lateral izquierdo.
6. También puede configurar el análisis para que ejecute la tarea con prioridad baja marcando la casilla de verificación correspondiente. Esto disminuye la prioridad de los procesos de análisis. De este modo los otros programas funcionarán más rápido, pero incrementará el tiempo necesario para realizar el análisis.

Después de configurar el análisis personalizado, puede guardarlo como favorito. Para ello, introduzca un nombre y haga clic en el botón **Favorito**.

Los usuarios avanzados podrían querer aprovechar las ventajas de las opciones de análisis que ofrece Bitdefender Endpoint Security Tools. Para configurar las opciones de análisis en detalle, haga clic en **Personalizado** y luego en **Ajustes**.

Como alternativa, puede configurar y ejecutar un análisis personalizado mediante la utilidad de línea de comandos del producto. Para obtener más información, consulte el capítulo [“Uso de la interfaz de línea de comandos”](#) (p. 28).

## 2.4.1. Tipos archivo

En la pestaña de **Tipos de archivos**, especifique qué tipos de archivos desea que sean analizados. Puede ajustar el agente de seguridad para analizar todos los archivos (con independencia de su extensión), solamente archivos de aplicación o extensiones de archivo específicas que considere peligrosas.

Analizando todos los archivos se proporciona una mejor protección, mientras que analizar solo aplicaciones puede ser utilizado solamente para realizar un análisis más rápido. Las aplicaciones (o archivos de programa) son mucho más vulnerables a ataques de malware que otro tipo de archivos. Esta categoría incluye las siguientes extensiones de archivo:

386; a6p; ac; accda; accddb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; lacddb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

### Opciones de análisis para archivos

Los archivos que contienen archivos infectados no son amenazas inmediatas para la seguridad de sus sistema. El malware puede afectar a su sistema su

el archivo infectado es extraído del archivo y ejecutado sin tener la protección en tiempo real activada. Sin embargo, recomendamos utilizar esta opción con el fin de detectar y eliminar cualquier amenaza potencial, incluso si esta no es una amenaza inmediata.

### **Analizar archivos de correo**

Seleccione esta opción si desea habilitar el análisis archivos de mensajes de correo y bases de datos de correo, incluyendo formatos de archivo tales como .eml, .msg, .pst, .dbx, .mbx, .tbb y otros.

## **2.4.2. Qué analizar?**

En la pestaña de **Análisis**, marque las casillas de verificación correspondientes para activar las opciones de análisis deseadas.

### **Analizar los sectores de arranque**

Puede configurar Bitdefender Endpoint Security Tools para que analice los sectores de arranque de su disco duro. Este sector del disco duro contiene el código del equipo necesario para iniciar el proceso de arranque. Cuando un virus infecta el sector de arranque, la unidad podría volverse inaccesible y ser incapaz de iniciar su sistema y acceder a sus datos.

### **Analizar en busca de Rootkits**

Seleccione esta opción para analizar en busca de **rootkits** y objetos ocultos que utilicen este tipo de software.

### **Analizar memoria**

Seleccione esta opción para analizar programas que se ejecuten en la memoria de su sistema.

### **Analizar registro**

Seleccione esta opción para analizar las claves de registro. El Registro de Windows es una base de datos que almacena los ajustes de configuración y opciones para los componentes del sistema operativo Windows, además de para las aplicaciones instaladas.

### **Analizar en busca de keyloggers**

Seleccione esta opción para analizar su sistema en busca de aplicaciones **keylogger**.

### **Analizar en busca de aplicaciones potencialmente no deseadas (APND)**

Una aplicación potencialmente no deseada (APND) es un programa que podría haberse instalado en el PC contra su voluntad y que a veces acompaña a

software freeware. Estos programas pueden instalarse sin el consentimiento del usuario (también llamados adware) o incluirse por defecto en el kit de instalación. Los efectos potenciales de estos programas incluyen la visualización de ventanas emergentes, la instalación de barras de herramientas no deseadas en el navegador por defecto o la ejecución de diversos procesos en segundo plano y la disminución del rendimiento del PC.

### **Analizar archivos nuevos y modificados**

Analizando solo archivos nuevos y cambiados, mejorará considerablemente el rendimiento general del sistema con una mínima compensación en seguridad.

### **Analizar cookies**

Seleccione esta opción para analizar las cookies almacenadas por los navegadores en su equipo.

## 2.4.3. ¿Qué hacer?

En la pestaña de **Acciones**, establezca la acción que desea realizar sobre los archivos detectados, en caso de que los haya.

### **Archivos infectados**

Los archivos detectados como infectados encajan con una firma de malware en la base de datos de firmas de malware de Bitdefender.

### **Archivos sospechosos**

Los archivos detectados como sospechosos por el análisis heurístico. Los archivos sospechosos no pueden ser desinfectados, porque no hay una rutina de desinfección disponible.

### **Rootkits**

Los rootkits representan un software especializado utilizado para ocultar archivos del sistema operativo. Aunque no son dañinos por su naturaleza, los rootkits se usan normalmente para ocultar malware o para encubrir la presencia de un intruso en el sistema.

## Tomar las medidas adecuadas

Dependiendo del tipo de archivos detectados, habrá disponibles una o varias de las siguientes opciones:

### **Eliminar**

Elimina los archivos detectados del disco.

Si se almacenan archivos infectados junto con archivos limpios en un mismo paquete, Bitdefender Endpoint Security Tools intentará limpiar los archivos infectados y reconstruir el paquete con los limpios. Si es imposible la reconstrucción del archivo empaquetado, se le informará de que no puede aplicarse ninguna acción para evitar perder archivos limpios.

### Omitir

No se realizará ninguna acción sobre los archivos detectados. Al finalizar el proceso de análisis, puede abrir el informe para ver información sobre estos archivos.

### Mover a cuarentena

Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado.

### Desinfectar

Elimina el código de malware del archivo infectado y reconstruye el archivo original.

## 2.5. Comprobando Logs de Análisis

Cada vez que realiza un análisis, se crea un registro de análisis. El informe de análisis detalla información sobre el proceso de análisis, como las opciones del análisis, el objetivo del análisis, las amenazas detectadas y las acciones realizadas.

Puede abrir el registro de análisis directamente desde la ventana principal, una vez finalizado el análisis, haciendo clic en **Ver registro**.

Para comprobar los registros de análisis más tarde, siga estos pasos:

1. Abra la ventana principal de Bitdefender Endpoint Security Tools.
2. Haga clic en el botón **Filtrar** para abrir el menú de **Filtros**.
3. Haga clic en el botón **Antimalware**. Aquí puede encontrar todos los eventos de análisis de malware, incluyendo amenazas detectadas por los análisis en tiempo real, análisis recientes, análisis iniciados por el usuario y cambios de estado para análisis automáticos.
4. Haga clic en un evento para ver más detalles sobre él.
5. Para abrir el registro de análisis, haga clic en **Ver registro**. Se mostrará el registro de análisis.



## 3. USO DEL CIFRADO DE VOLÚMENES

El módulo de Cifrado de volúmenes proporciona cifrado de disco completo en su sistema Windows mediante las políticas aplicadas por su administrador de seguridad.

### 3.1. Cifrado de su sistema

Cuando se aplica una política de cifrado a su sistema Windows:

1. Una ventana de configuración le solicita que introduzca una de las medidas de seguridad siguientes:
  - Un número de identificación personal (PIN) si el sistema tiene un chip de módulo de plataforma segura (TPM), como los portátiles más recientes.



#### **Nota**

Si su sistema tiene un TPM funcional, su administrador de seguridad puede configurar dicha política que cifra los volúmenes automáticamente, sin necesidad de PIN.

- Una contraseña si el sistema carece de un chip de módulo de plataforma segura (TPM). La contraseña también es necesaria cuando el TPM no está operativo o si Bitdefender Endpoint Security Tools no lo detecta.

**Cifrado de volumen**

### Fijar contraseña cifrado

Configure una contraseña con EN-US. La necesitará para arrancar el sistema operativo o para desbloquear el volumen.

El cifrado es un proceso que se realiza una sola vez y puede seguir trabajando como de costumbre.

Introduzca su contraseña de cifrado para el volumen C:. Necesitará esta contraseña para desbloquear el volumen.

**Elija una contraseña:**

**Repetir contraseña:**

**Requisitos de contraseña:**

- Ha de tener al menos 8 caracteres
- Debe contener mayúsculas y minúsculas
- Debe contener un número

[Descartar](#) [Guardar](#)

2. Haga clic en el botón **Guardar**. El proceso de cifrado comienza inmediatamente, empezando por el volumen de arranque.

Puede posponer el cifrado haciendo clic en **Descartar**. No obstante, la ventana volverá a aparecer pasado un tiempo pidiéndole que configure un PIN o contraseña de cifrado.

Necesita un solo PIN o contraseña para cifrar todos los volúmenes, tanto si son de arranque como si no, en discos fijos, en sistemas de escritorio y portátiles. No se cifran los discos extraíbles. Para obtener más información sobre la configuración del PIN o contraseña de cifrado, consulte [este artículo de la base de conocimientos](#).

Después del cifrado, es posible que deba ingresar el PIN o la contraseña cada vez que se inicie Windows, en una pantalla de autenticación previa al arranque, dependiendo de la política de seguridad aplicada en su sistema.



Si olvida el PIN o la contraseña de cifrado, póngase en contacto con su administrador de seguridad.

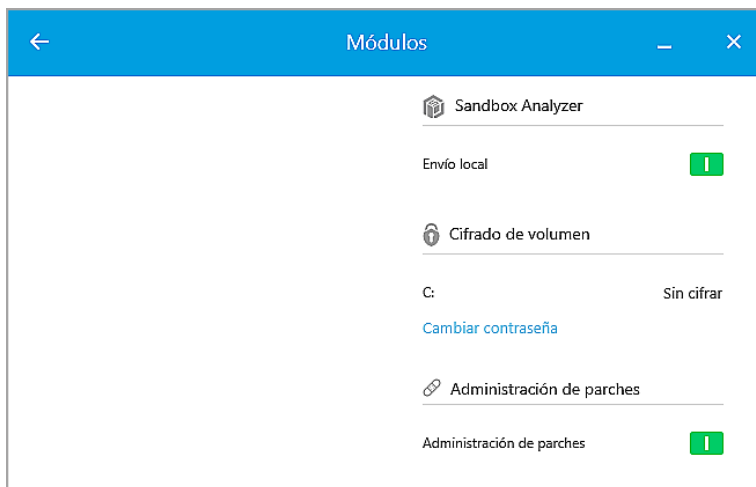
## 3.2. Descifrado de su sistema

Cuando se aplica una política de descifrado, los discos cifrados se descifran automáticamente, sin que sea preciso introducir nada. Sin embargo, no puede descifrar el sistema por su cuenta mientras exista una política de cifrado activa.

## 3.3. Comprobación del estado del cifrado

A continuación se indica cómo verificar el estado del cifrado en su sistema:

1. En la bandeja del sistema, haga doble clic en el icono  para acceder a la interfaz de usuario de Bitdefender Endpoint Security Tools.
2. En la esquina superior derecha, haga clic en el botón  para abrir la ventana de **Módulos**.
3. Acceda a la sección **Cifrado de volúmenes**, donde puede ver qué volúmenes están cifrados y cuáles no.



## 3.4. Cambio del PIN o contraseña de cifrado

El PIN o contraseña de cifrado se cambian así:

1. Haga clic en el nombre del disco cifrado en la ventana principal de la interfaz de usuario de Bitdefender Endpoint Security Tools.
2. Haga clic en la opción **Cambiar contraseña**.
3. En la ventana de configuración, introduzca el nuevo PIN o contraseña.
4. Haga clic en el botón **Guardar**.

## 4. ACTUALIZACIONES

En un mundo donde los cibercriminales tratan constantemente de encontrar nuevas formas de causar daño, es esencial disponer de un programa de seguridad al día si desea ir un paso por delante de ellos.

Si está conectado a Internet a través de una conexión de banda ancha o ADSL, Bitdefender Endpoint Security Tools se actualizará sólo. Por omisión, busca actualizaciones cuando enciende su equipo y cada **hora** a partir de ese momento.

### Nota

La frecuencia de actualización automática predeterminada la puede cambiar el administrador de la red.

El proceso de actualización se realiza al instante, actualizando o reemplazando los archivos antiguos progresivamente. De este modo, el proceso de actualización no afecta al rendimiento del producto a la vez que se evita cualquier riesgo.

Si está conectado a Internet a través de una conexión por módem analógico, es recomendable actualizar Bitdefender manualmente. Para más información, por favor vea [“Realizando Actualización”](#) (p. 25).

### 4.1. Tipos de actualizaciones

Las actualizaciones se presentan de las siguientes maneras:

- **Actualizaciones de las firmas de malware** - según aparecen nuevas amenazas, deben actualizarse las firmas de malware para garantizar una protección frente a ellas siempre al día
- **Actualizaciones del producto** - cuando aparece una nueva versión del producto, se introducen nuevas características y técnicas de análisis para mejorar el rendimiento del producto.

Un upgrade o mejora del producto es una nueva versión principal del producto.

### 4.2. Comprobar si su protección está actualizada

Para comprobar si la protección de está actualizada, siga estos pasos:

1. Haga clic con el botón derecho en el icono de Bitdefender Endpoint Security Tools en la bandeja del sistema y seleccione **Acerca de**.

2. Puede consultar el estado de actualización y la hora de la última comprobación e instalación de la actualización.

Para obtener información detallada sobre las últimas actualizaciones, compruebe los eventos de actualización:

1. En la ventana principal, haga clic en el botón **Filtrar** para abrir el menú de **Filtros**.
2. Haga clic en el botón **Actualizar**. Se mostrarán las últimas actualizaciones en la línea de tiempo de **eventos**.

Puede ver cuándo se iniciaron las actualizaciones, así como información acerca de estas: si tuvieron éxito o no, o si requieren un reinicio para terminar la instalación. Si es necesario, reinicie el sistema en cuanto pueda.

### 4.3. Realizando Actualización

Para poder hacer actualizaciones es necesaria una conexión a Internet.

Para iniciar una actualización:

- Haga doble clic en el icono de Bitdefender Endpoint Security Tools en la **bandeja del sistema**.
- Haga clic en el botón **Acciones** para abrir el menú de **Acciones**.
- Haga clic en **Buscar actualizaciones**. El módulo Actualizar conectará con el servidor de actualización de Bitdefender y comprobará la existencia de actualizaciones.
- Dependiendo de los ajustes de actualización establecidos por su administrador de red, si se detecta una actualización, se le solicitará que la confirme o la actualización se realizará de forma automática.



#### Importante

Si es necesario, reinicie el sistema en cuanto pueda. Le recomendamos que lo haga lo antes posible.




## 5. EVENTOS

Bitdefender Endpoint Security Tools muestra un registro detallado de los eventos relacionados con la actividad en su equipo, incluyendo las actividades del equipo supervisadas por el Control de contenidos y las aplicaciones bloqueadas por el Control de aplicaciones. La línea de tiempo de **eventos** es una herramienta muy importante para la monitorización de su protección de Bitdefender. Por ejemplo, puede comprobar fácilmente si una actualización se realizó correctamente, si se encontró malware en su equipo, etc. Para comprobar el registro de eventos, siga estos pasos:

1. Abra la ventana principal de Bitdefender Endpoint Security Tools.
2. Todos los eventos se muestran en la línea de tiempo de **eventos**.
3. Haga clic en el botón **Filtrar** para abrir el menú de **Filtros**.
4. Seleccione la categoría del evento desde el menú. Los eventos están agrupados en las siguientes categorías:
  - **Configuración general**
  - **Antimalware**
  - **Cortafuego**
  - **Actualizar**
  - **Control Contenido**
  - **Control de dispositivos**
  - **Control de aplicaciones**
  - **Sandbox Analyzer**
  - **Cifrado de volumen**

Cada evento incluye la siguiente información: una breve descripción, la acción que Bitdefender tomó cuando éste se produjo, y la fecha y hora de cuando ocurrió. Para ver información detallada sobre un evento de la lista en particular, haga clic en **Ver registro**.

También puede filtrar los eventos según su importancia para el nivel de protección. Existen tres tipos de eventos:

-  indica operaciones realizadas correctamente.
-  indica incidencias que no son críticas.
-  indica incidencias críticas



Algunos de los problemas, críticos o no, mostrados en la línea de tiempo de **Eventos** van asociados a las acciones recomendadas para solucionarlos.



## 6. USO DE LA INTERFAZ DE LÍNEA DE COMANDOS

Bitdefender Endpoint Security Tools le permite ejecutar automáticamente las actualizaciones y tareas de análisis bajo demanda locales mediante la consola del producto, una interfaz de línea de comandos que se encuentra en la carpeta de instalación del producto en sus máquinas Windows.

La interfaz de línea de comandos de BEST tiene dos modos de funcionamiento:

- **Varios comandos a la vez.** Este modo utiliza la interfaz de línea de comandos propia y le permite introducir comandos y recibir resultados hasta que salga de ella.

Para acceder a este modo:

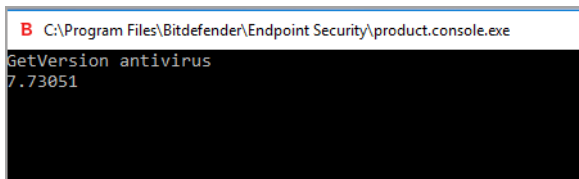
1. Diríjase a `c:\Program Files\Bitdefender\Endpoint Security 0` a la carpeta donde se instaló BEST.
2. Busque el ejecutable **product.console** y haga doble clic en él. Se abre la interfaz de línea de comandos.
3. Ejecute el comando deseado.

Ejemplo:

```
GetVersion antivirus
```

El resultado devuelto es el número de versión de las firmas antimalware.

4. Ejecute `exit` para cerrar la interfaz de línea de comandos.



```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
GetVersion antivirus
7.73051
```

- **Un comando a la vez.** Este modo utiliza el símbolo del sistema y vuelve a él después de ejecutar el comando.

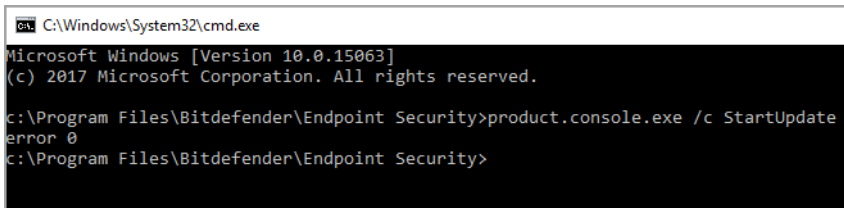
Para acceder a este modo:

1. Abra el símbolo del sistema (`cmd.exe`).
2. Utilice el comando `cd` para dirigirse a la carpeta de instalación de Bitdefender Endpoint Security Tools.
3. Ejecute el comando deseado.

Ejemplo:

```
C:\Program Files\Bitdefender\Endpoint Security>
product.console.exe /c StartUpdate
```

4. Si el comando se ejecuta correctamente el resultado devuelto es `error 0`.



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

c:\Program Files\Bitdefender\Endpoint Security>product.console.exe /c StartUpdate
error 0
c:\Program Files\Bitdefender\Endpoint Security>
```

## 6.1. Comandos compatibles

La interfaz de línea de comandos admite varios comandos, algunos de los cuales requieren parámetros para que devuelvan resultados válidos.

Todos los ejemplos de esta sección se proporcionan mediante la consola de producto de la carpeta de instalación de BEST.

**GetUpdateStatus** `product|antivirus`

Obtener información sobre las últimas actualizaciones.

Este comando requiere uno de los siguientes parámetros:

- `product`: se refiere a la versión de BEST.
- `antivirus`: se refiere a la versión de las firmas de antimalware.

Ejemplo:

```
C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
GetUpdateStatus product
lastSucceededTime: 1504513705
lastAttemptedTime: 1504513705
lastError: 0
GetUpdateStatus antivirus
lastSucceededTime: 1505739144
lastAttemptedTime: 1505739144
lastError: 0
```

### GetVersion product|antivirus

Obtener información sobre la versión actual del producto.

Este comando requiere uno de los siguientes parámetros:

- `product`: se refiere a la versión de BEST.
- `antivirus`: se refiere a la versión de las firmas de antimalware.

Ejemplo:

```
C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
GetVersion product
6.2.24.938
GetVersion antivirus
7.73205
```

### IsUpdateInProgress

Comprobar si hay una actualización de producto en curso.

Valores de salida:

- `true`: hay una actualización de producto en curso.
- `false`: no hay ninguna actualización de producto en curso.

Ejemplo:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
IsUpdateInProgress
false
```

### IsUpdateRestartNeeded

Comprobar si una máquina requiere reiniciar el sistema después de la actualización.

Valores de salida:

- `true`: la máquina requiere reiniciar el sistema después de la actualización.
- `false`: la máquina no requiere reiniciar el sistema después de la actualización.

Ejemplo:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
IsUpdateRestartNeeded
false
```

### StartUpdate

Iniciar una actualización y obtener el resultado sin esperar a que finalice la tarea.

Ejemplo:

```
StartUpdate
```

Formato de salida: `error 0` (el comando se ha ejecutado correctamente)

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
StartUpdate
error 0
```

**FileScan.OnDemand.RunScanTask** custom [opción]

Iniciar un análisis bajo demanda y mostrar la ruta al registro de análisis y el resumen de este.

Este comando requiere el parámetro `custom`, seguido, si es necesario, de una o más opciones. Por ejemplo:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1505742554_1_01.xml
Scanned items: 990886
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

Gracias a estas opciones puede personalizar una tarea de análisis. Dichas opciones no son obligatorias.

Cada opción tiene dos o más valores disponibles, pero solo puede utilizar uno. Cuando no se especifica ninguna opción para el comando `FileScan.OnDemand.RunScanTask`, el análisis personalizado toma en cuenta el valor por defecto de esa opción. Por ejemplo, si ejecuta este comando sin mencionar la opción `scanKeyloggers`, significa que Bitdefender Endpoint Security Tools seguirá analizando keyloggers de acuerdo con el valor por defecto de `scanKeyloggers` (`true`).



### Nota

No existen comandos específicos para **Quick scan** o **Análisis completo**. Sin embargo, puede configurar `FileScan.OnDemand.RunScanTask` para analizar solo la ubicación del SO o todo el sistema, con todas las opciones habilitadas según sea necesario.

## Opciones

path="<ruta>"

Introduzca la ruta de acceso de la ubicación de destino del análisis. Para varias rutas utilice: path="<ruta1>" path="<ruta2>".

Ejemplo:

```
FileScan.OnDemand.RunScanTask custom path="C:\Program Files"
```

```
FileScan.OnDemand.RunScanTask custom path="C:\Program Files"
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1505746495_1_01.xml
Scanned items: 74074
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

infectedAction1=ignore|disinfect|disinfectOnly|delete|quarantine

Seleccione la primera acción adoptada cuando se detecta un archivo infectado: ignorar, desinfectar, solo desinfectar, eliminar o poner en cuarentena. Puede utilizar esta acción junto con infectedAction2.

Valor por defecto: disinfect

Ejemplo:

```
FileScan.OnDemand.RunScanTask custom path="C:\Program Files\Common Files" infectedAction1=ignore
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1505813252_1_01.xml
Scanned items: 5542
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

infectedAction2=ignore|disinfect|disinfectOnly|delete|quarantine

Seleccione la segunda acción adoptada cuando se detecta un archivo infectado, en caso de que fracase la primera acción.

Valor por defecto: quarantine

Ejemplo:

```
FileScan.OnDemand.RunScanTask custom infectedAction1=disinfect infectedAction2=quarantine
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1505824102_1_01.xml
Scanned items: 500139
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

suspiciousAction1=ignore|delete|quarantine

Seleccione la primera acción adoptada cuando se detecta un archivo sospechoso. Puede utilizar esta acción junto con `suspiciousAction2`.

Valor por defecto: `ignore`

Ejemplo:

```
FileScan.OnDemand.RunScanTask custom path="C:\Program Files\Common Files" suspiciousAction1=quarantine
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1505824920_1_01.xml
Scanned items: 5542
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

suspiciousAction2=ignore|delete|quarantine

Seleccione la segunda acción adoptada cuando se detecta un archivo sospechoso, en caso de que fracase la primera acción.

Valor por defecto: `ignore`

Ejemplo:

```
FileScan.OnDemand.RunScanTask custom path="C:\Users" suspiciousAction1=delete suspiciousAction2=quarantine
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1505825170_1_01.xml
Scanned items: 54455
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

scanBootSectors=true|false

Analizar los sectores de arranque de las unidades disponibles.

Valor por defecto: `false`

Ejemplo:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom scanBootSectors=true
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506073447_1_01.xml
Scanned items: 416206
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

`scanRegistry=true|false`

Analizar las claves del registro en su máquina.

Valor por defecto: `false`

Ejemplo:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom scanRegistry=true
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506073099_1_01.xml
Scanned items: 419060
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

`scanMemory=true|false`

Analizar los programas que se ejecutan en la memoria del sistema.

Valor por defecto: `false`

Ejemplo:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom scanMemory=true
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506072517_1_01.xml
Scanned items: 427016
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0

FileScan.OnDemand.RunScanTask custom scanMemory=true
```

`smartScan=true|false`

Analizar solo los archivos nuevos o modificados.

Valor por defecto: `true`

Ejemplo:



```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom smartScan=false
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506070911_1_01.xml
Scanned items: 1614889
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

scanRootKits=true|false

Analizar rootkits y objetos ocultos mediante dicho software.

Valor por defecto: false

Ejemplo:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom scanRootKits=true
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506070601_1_01.xml
Scanned items: 416548
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

scanKeyloggers=true|false

Analizar en busca de software de keylogger.

Valor por defecto: true

Ejemplo:

```
FileScan.OnDemand.RunScanTask custom scanKeyloggers=false
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506069462_1_01.xml
Scanned items: 416845
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

scanPUA=true|false

Analizar en busca de aplicaciones potencialmente no deseadas (APND).

Valor por defecto: false

Ejemplo:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom scanPUA=true
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506068866_1_01.xml
Scanned items: 165522
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

`scanArchives=true|false`

Analizar en busca de archivos infectados dentro de archivos comprimidos.

Valor por defecto: `true`

Ejemplo:

```
FileScan.OnDemand.RunScanTask custom scanArchives=false
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506069462_1_01.xml
Scanned items: 416845
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

`extensionType=all|application|custom|none`

Analizar archivos en función de su extensión: todos los archivos, solo los ejecutables, solo archivos con las extensiones que desea, o no analizar ningún archivo.

Valor por defecto: `all`

Ejemplo:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom extensionType=application
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506068866_1_01.xml
Scanned items: 165522
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

`customExt="<string>"`

Esta opción le ayuda a analizar solo los archivos con las extensiones que desee. Requiere una cadena con cada extensión entre barras verticales

(por ejemplo: "|exe|ini|txt|"). Esta opción solo es válida junto con la opción `extensionType=custom`.

Ejemplo:

```
C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom path="c:\Program Files\WinRAR" extensionType=custom customExt="|dll|"
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0-0-0\1506351027_1_01.xml
Scanned items: 6
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0

FileScan.OnDemand.RunScanTask custom path="c:\Program Files\WinRAR" extensionType=custom customExt="|dll|dat|"
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0-0-0\1506351335_1_01.xml
Scanned items: 0
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

`lowPriority=true|false`

Ejecutar la tarea con prioridad baja.

Valor por defecto: `false`

Ejemplo:

```
C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom lowPriority=true
```

Estas opciones son una alternativa a las disponibles en la consola de BEST. Para obtener más información, consulte [“Configurar y ejecutar un análisis personalizado”](#) (p. 15).

## 6.2. Códigos de error de la línea de comandos

La utilidad de línea de comandos puede devolver los mensajes siguientes:

Código de error	Descripción
0	Comando ejecutado correctamente.



Código de error	Descripción
87	Parámetro no válido.
160	Argumentos erróneos.
1627	Error en la función: se ha producido un error al ejecutar el comando.



## 7. OBTENER AYUDA

Para cualquier problema o pregunta relativa a Bitdefender Endpoint Security Tools, contacte con su administrador de red.

Para encontrar la información de contacto y sobre los productos, haga clic con el botón derecho en el icono de Bitdefender Endpoint Security Tools en la bandeja del sistema y seleccione **Acerca de** para abrir la ventana **Acerca de**.

## Glosario

### Actualizar

Una nueva versión de un producto de software o hardware, diseñada para reemplazar una versión anterior del mismo producto. Además, durante la instalación se verifica si en su ordenador existe una versión anterior; si no se encuentra ninguna, no se instalará la actualización.

Bitdefender posee su propio módulo de actualización que le permite comprobar manualmente las actualizaciones, o actualizar automáticamente el producto.

### Adware

El adware habitualmente se combina con aplicaciones que son gratuitas a cambio de que el usuario acepte la instalación del componente adware. Puesto que las aplicaciones adware generalmente se instalan una vez el usuario acepta los términos de licencia que manifiestan el propósito de la aplicación, no se comete ningún delito.

Sin embargo, los pop-up de publicidad pueden resultar molestos, y en algunos casos afectar al rendimiento del sistema. Además, la información que recopilan algunas de estas aplicaciones puede causar problemas de privacidad a aquellos usuarios que no eran plenamente conscientes de los términos de la licencia.

### Archivo Comprimido

Disco, cinta o directorio conteniendo ficheros almacenados.

Fichero conteniendo uno o varios ficheros en formato comprimido.

### Archivo de informe

Es un fichero que lista las acciones ocurridas. Bitdefender mantiene un archivo de informe que incluye la ruta analizada, las carpetas, el número de archivos comprimidos y no comprimidos analizados, así como cuántos archivos infectados o sospechosos se encontraron.

### Archivos sospechosos y tráfico de red

Los archivos sospechosos son los que tienen una reputación dudosa. Esta clasificación se otorga en función de muchos factores, entre los cuales se cuentan la existencia de la firma digital, el número de ocurrencias en las redes informáticas, el empaquetador utilizado, etc. El tráfico de red se considera sospechoso cuando se desvía del patrón. Por ejemplo, una fuente no fiable,

peticiones de conexión a puertos inusuales, aumento del uso de ancho de banda, tiempos de conexión aleatorios, etc.

### **Área de notificación del Sistema**

Elemento introducido con el sistema Windows 95, la bandeja de sistema está ubicada en la barra de tareas de Windows (normalmente al lado del reloj) y contiene iconos en miniatura para acceder fácilmente a las funciones del sistema, como el fax, la impresora, el módem, el volumen etc. Al hacer doble clic o clic derecho en el icono correspondiente, verá y abrirá los detalles y los mandos de los programas.

### **Ataques personalizados**

Ataques informáticos que persiguen principalmente beneficios económicos o minar la reputación. El objetivo puede ser un individuo, una empresa, un software o un sistema que se ha estudiado concienzudamente antes de que el ataque tenga lugar. Estos ataques se desarrollan durante un largo período de tiempo y por etapas, aprovechando uno o más puntos de infiltración. Apenas se notan; la mayoría de las veces solo cuando el daño ya está hecho.

### **Backdoor**

Es una brecha de seguridad dejada intencionalmente por los diseñadores o los administradores. La motivación no es siempre maléfica; algunos sistemas operativos funcionan con unas cuentas privilegiadas, concebidas para el uso de los técnicos del service o para los responsables con el mantenimiento del producto, de parte del vendedor.

### **Bootkit**

Un bootkit es un programa malicioso que tiene la capacidad de infectar el registro de arranque maestro (MBR), el registro de arranque de volumen (VBR) o el sector de arranque. El bootkit permanece activo incluso después de un reinicio del sistema.

### **Cookie**

En la industria del Internet, las cookies se describen como pequeños ficheros conteniendo información sobre los ordenadores individuales que se pueden analizar y usar por los publicistas para determinar los intereses y los gustos online de los usuarios respectivos. En este ambiente, la tecnología de las cookies se desarrolla con la intención de construir reclamos y mensajes publicitarios correspondientes a los intereses declarados por usted. Es un

arma de doble filo para mucha gente porque, por un lado, es más eficiente y pertinente que usted vea publicidades relacionadas con sus intereses. Por otro lado, implica seguir cada paso suyo y cada clic que usted haga. Por consiguiente, es normal que haya resultado un debate sobre la privacidad y mucha gente se sintió ofendida por la idea de ser vista como "número de SKU" (el código de barras ubicado en la parte posterior de los paquetes analizados a la salida de los supermercados). Aunque esta perspectiva pueda parecer extremista, en algunos casos es cierta.

### **Downloader de Windows**

Es el nombre genérico que reciben los programas que tienen una funcionalidad primaria de descarga de contenidos con fines no deseados o maliciosos.

### **Eventos**

Una acción o acontecimiento detectado por un programa. Los eventos pueden ser acciones, como por ejemplo hacer clic con el ratón o pulsar una tecla, o también pueden ser acontecimientos (agotar el espacio de memoria).

### **Exploit**

Un exploit se refiere generalmente a cualquier método utilizado para obtener acceso no autorizado a equipos, o una vulnerabilidad en la seguridad de un sistema que lo expone a un ataque.

### **Explorador**

Es la abreviatura de Navegador Web, una aplicación que se utiliza para ubicar y visualizar páginas web.

### **Extensión de un archivo**

La última parte del nombre de un fichero, que aparece después del punto e indica el tipo de información almacenada.

Muchos sistemas operativos utilizan extensiones de nombres de archivo, por ejemplo, Unix, VMS y MS-DOS. Normalmente son de una a tres letras (algunos viejos SO no soportan más de tres). Por ejemplo "c" para código fuente C, "ps" para PostScript, o "txt" para texto plano.

### **Falso positivo**

Ocurre cuando un analizador identifica un fichero infectado, cuando de hecho éste no lo es.



## Firma malware

Las firmas de malware son fragmentos de código extraídos de muestras reales de malware. Los programas antivirus las utilizan para realizar el reconocimiento de patrones y la detección de malware. Las firmas también se utilizan para eliminar el código malware de los archivos infectados.

La Base de Datos de Firmas Malware de Bitdefender es una colección de firmas de malware actualizada cada hora por los investigadores de malware de Bitdefender.

## Grayware

Una clase de aplicaciones de software entre el software legítimo y el malware. A pesar de que no son tan dañinas como el malware que afecta a la integridad del sistema, su comportamiento sigue siendo inquietante, y conduce a situaciones no deseadas como el robo de datos y el uso no autorizado o la publicidad no deseada. Las aplicaciones de grayware más comunes son el [spyware](#) y el [adware](#).

## Gusano

Es un programa que se propaga a través de la red, reproduciéndose mientras avanza. No se puede añadir a otros programas.

## Heurístico

Un método basado en reglas para identificar nuevos virus. Este método de análisis no se basa en firmas de virus específicas. La ventaja de un análisis heurístico es que no le engaña una nueva variante de un virus existente. Sin embargo, puede que informe ocasionalmente de códigos sospechosos en programas normales, generando el llamado "falso positivo".

## IP

Internet Protocol - Protocolo enrutable dentro del protocolo TCP/IP y que es responsable del direccionamiento IP, el enrutamiento y la fragmentación y reensamblado de los paquetes IP.

## Keylogger

Un keylogger es una aplicación que registra todo lo que escribe.

Los keyloggers en su esencia no son maliciosos. Pueden ser utilizados para propósitos legítimos, como monitorizar la actividad de los empleados o niños. Sin embargo, son cada vez más utilizados por cibercriminales con fines

maliciosos (por ejemplo, para recoger datos privados, como credenciales y números de seguridad social).

### **Ladrón de contraseñas**

Un ladrón de contraseñas recopila datos que pueden ser nombres de cuentas y contraseñas asociadas a ellos. Estas credenciales robadas se utilizan con fines maliciosos, como por ejemplo apoderarse de las cuentas.

### **Línea de comando**

En una interfaz con línea de comando, el usuario puede introducir comandos en el espacio provisto directamente en la pantalla, usando un lenguaje de comando.

### **Malware**

Malware es el término genérico que define al software diseñado para causar daños - una contracción de 'malicious software'. Todavía no se usa de forma universal, pero su popularidad como término general para definir virus, troyanos, gusanos y código móvil malicioso está creciendo.

### **No Heurístico**

Este método de análisis se basa en firmas de virus específicas. La ventaja del análisis no heurístico es que no se le puede engañar con aplicaciones que pueden parecer un virus, y por consiguiente, no genera falsas alarmas.

### **Phishing**

El acto de enviar un email a un usuario simulando pertenecer a una empresa legítima e intentar estafar al usuario solicitándole información privada que después se utilizará para realizar el robo de identidad. El email conduce al usuario a visitar una página Web en la que se le solicita actualizar información personal, como contraseñas y números de tarjetas de crédito, de la seguridad social y números de cuentas corrientes, que en realidad ya posee la organización auténtica. La página Web, en cambio, es una réplica fraudulenta, creada sólo para robar la información de los usuarios.

### **Puerto**

Interfaz en un ordenador a la que se puede conectar un dispositivo. Los ordenadores personales tienen distintos tipos de puertos. Hay varios puertos internos para conectar las unidades de disco, las pantallas, los teclados.

Asimismo, los ordenadores personales tienen puertos externos para conectar módems, impresoras, ratones y otros dispositivos periféricos.

En las redes de tipo TCP/IP y UDP representa el endpoint de una conexión lógica. El número de puerto indica el tipo del dicho puerto. Por ejemplo, el puerto 80 se usa para el tráfico http.

### **Ransomware**

Un malware que le impide acceder a su equipo o bloquea su acceso a los archivos y aplicaciones. El ransomware le exigirá que pague una cantidad determinada (pago de un rescate) a cambio de una clave de descifrado que le permita recuperar el acceso a su equipo o a sus archivos.

### **Rootkit**

Un rootkit es un conjunto de herramientas de software que ofrecen acceso al sistema a nivel de administrador. El término empezó a usarse con los sistemas operativos UNIX y hacía referencia a herramientas recompiladas que proporcionaba a los intrusos de derechos de administrador, permitiéndoles ocultar su presencia para no ser visto por los administradores de sistema.

El papel principal de los rootkits es ocultar procesos, archivos, conexiones y logs. También pueden interceptar datos de terminales, conexiones de red o periférica, si éstos incorporan el software apropiado.

Rootkits no son de naturaleza mala. Por ejemplo, los sistemas y algunas aplicaciones esconden ficheros críticos usando rootkits. Sin embargo, normalmente se utilizan para esconder la presencia de malware o para encubrir la presencia de un intruso en el sistema. Cuando se combinan con malware, los rootkits representan una gran amenaza para la seguridad e integridad de su sistema. Pueden monitorizar el tráfico, crear puertas traseras en el sistema, alterar ficheros y logs y evitar su detección.

### **Script**

Es otro término para macro o fichero batch y se constituye de una lista de comandos que se pueden ejecutar sin la intervención del usuario.

### **Sector de arranque:**

Un sector al principio de cada disco y que identifica la arquitectura del disco (tamaño del sector, tamaño del cluster, etc). Para los discos de inicio, el sector de arranque también incluye un programa para cargar el sistema operativo.

## Spam

Correo basura o los posts basura en los grupos de noticias. Se conoce generalmente como correo no solicitado.

## Spyware

Se trata de cualquier software que, en secreto, recopile información del usuario a través de su conexión a Internet sin su consentimiento, generalmente con fines comerciales. Las aplicaciones Spyware son, generalmente, componentes ocultos de programas freeware o shareware que pueden descargarse por Internet; sin embargo, debe observarse que la gran mayoría de aplicaciones shareware y freeware no contienen spyware. Una vez instalado, el spyware monitoriza la actividad del usuario en Internet y, en segundo plano, envía esa información a una tercera persona. El spyware también puede recoger información sobre direcciones de correo, e incluso contraseñas y números de tarjetas de crédito.

El spyware es similar al troyano en el hecho que los usuarios los instalan inconscientemente cuando instalan otra aplicación. Una forma habitual de infectarse con spyware es descargando, a través de programas de intercambio de ficheros, un determinado archivo que intercambia el nombre de los productos compartidos.

A parte de las cuestiones de ética y privacidad, el spyware roba al usuario recursos de memoria y ancho de banda mientras envía la información al creador del spyware a través de la conexión de Internet del usuario. Puesto que el spyware utiliza memoria y recursos del sistema, las aplicaciones que se ejecutan en segundo plano pueden provocar errores del sistema o inestabilidad general del mismo.

## TCP/IP

Transmission Control Protocol/Internet Protocol - Es una gama de protocolos de red, extremadamente utilizados en Internet para proporcionar comunicaciones en las redes interconectadas, que incluyen ordenadores con distintas arquitecturas de hardware y varios sistemas operativos. TCP/IP ofrece estándares para el modo de comunicación entre ordenadores y convenciones para las redes interconectadas.

### **Tormentas de análisis antimalware**

Un uso intensivo de recursos del sistema que tiene lugar cuando el software antivirus analiza simultáneamente múltiples máquinas virtuales en un solo host físico.

### **Troyano**

Es un programa destructivo disfrazado como aplicación benigna. A diferencia de los virus, los caballos troyanos no se multiplican; sin embargo pueden ser igual de peligrosos. Unos de los tipos más insidiosos de troyano es un programa que pretende desinfectar su ordenador y que en realidad introduce virus.

El término viene de la historia de la Ilíada de Homero, en la cual Grecia entrega un caballo gigante hecho de madera a sus enemigos, los Troyanos, supuestamente como oferta de paz. Pero después de que los troyanos arrastraran el caballo dentro de las murallas de su ciudad, los soldados griegos salieron del vientre hueco del caballo y abrieron las puertas de la ciudad, permitiendo a sus compatriotas entrar y capturar Troya.

### **Virus**

Es un programa o una parte de un código cargado en su ordenador sin avisarle y en contra de su voluntad. La mayoría de los virus se pueden multiplicar. Todos los virus informáticos son artificiales, creados por una persona. Es muy simple producir un virus que se multiplique continuamente. Pero, aún así, sería muy peligroso porque dentro de poco tiempo estaría usando toda la memoria disponible y llevaría al bloqueo del sistema. Un tipo de virus todavía más peligroso es uno capaz de propagarse a través de redes y evitando los sistemas de seguridad.

### **Virus de boot**

Es un virus que infecta el sector de arranque hallado en un disco fijo o en una disquetera. Al intentar de relanzar el sistema desde un disco infectado con un virus de boot, el virus se instalará activo en la memoria. Cada vez que usted trate de relanzar el sistema desde este punto en adelante, tendrá el virus activo en la memoria.

### **Virus de macro**

Es un tipo de virus informático que se encuentra codificado como una macro incluida en un documento. Muchas aplicaciones, como Microsoft Word o Excel, soportan potentes lenguajes macro.

Estas aplicaciones permiten introducir un macro en un documento y también que el macro se ejecute cada vez que se abra el documento.

### **Virus Polimórfico**

Son virus que se modifican en cada fichero que infectan. Al no tener una secuencia binaria constante, son muy difíciles de identificar.