F-Secure Anti-Virus 2013

Contents

Capítulo 1: Instalación.....5

Antes de que realice la instalación por primera vez.....6
Instalación del producto por primera vez.....6
Cómo instalar y actualizar aplicaciones.....6
Ayuda y Asistencia técnica.....7

Capítulo 2: Procedimientos iniciales.....9

Cómo utilizar las actualizaciones automáticas.....10
Comprobar el estado de actualización.....10
Cambiar las opciones de conexión a Internet.....10
Compruebe el estado de la red de protección en tiempo real.....11
Cómo ver las acciones que ha llevado a cabo el producto.....11
Ver historial de notificaciones.....11
Cambiar la configuración de las notificaciones.....11
Red de protección en tiempo real.....12
Qué es la red de protección en tiempo real.....12
Ventajas de la red de protección en tiempo real.....12
Datos con los que puede colaborar.....13
Cómo protegemos su privacidad.....14
Cómo ser colaborador de la red de protección en tiempo real.....14
Preguntas sobre la red de protección en tiempo real.....15
Cómo puedo saber si mi suscripción es válida.....15
Centro de actividades.....15
Activar una suscripción.....16

Capítulo 3: Introducción.....17

Ver el estado general de mi protección.....18
Ver las estadísticas del producto.....18
Gestionar las actualizaciones del producto.....19
Ver versiones de la base de datos.....19
Cambiar la configuración de banda ancha móvil.....19
Qué son los virus y otros programas de malware.....20
Virus.....20
Spyware.....21
Rootkits.....21
Riskware.....21

Capítulo 4: Protección de su equipo frente a malware.....23
Cómo analizar mi equipo.....24
Analizar archivos automáticamente.....24
Analizar archivos manualmente.....26
Analizar correos electrónicos.....29
Ver los resultados del análisis.....30
Cómo excluir archivos del análisis.....30
Excluir tipos de archivos.....30
Excluir archivos por ubicación.....31
Ver las aplicaciones excluidas.....32
Cómo utilizar la función de cuarentena.....32
Ver elementos en cuarentena.....33
Restaurar elementos en cuarentena.....33
Qué es DeepGuard.....33
Activar o desactivar DeepGuard.....34
Permitir aplicaciones bloqueadas por DeepGuard.....34
Utilice DeepGuard en el modo de compatibilidad.....35
Cómo actuar con las advertencias de comportamiento sospechoso.....35

Capítulo

1

Instalación

Temas:

- *Antes de que realice la instalación por primera vez*
- *Instalación del producto por primera vez*
- *Cómo instalar y actualizar aplicaciones*
- *Ayuda y Asistencia técnica*

Antes de que realice la instalación por primera vez

Gracias por elegir F-Secure.

Para instalar el producto, deberá realizar los siguientes pasos:

- El CD de instalación o un paquete de instalación, Si va a utilizar un equipo ultraportátil sin unidad de CD, puede descargar el paquete de instalación de la página *www.f-secure.com/netbook*.
- Su clave de suscripción.
- Una conexión a Internet.

Si tiene un producto de seguridad de otro proveedor, el instalador intentará quitarlo automáticamente. Si esto no sucede, quítelo de forma manual.

Nota: Si tiene más de una cuenta en el equipo, inicie sesión con los privilegios del administrador durante la instalación.

Instalación del producto por primera vez

Instrucciones para instalar el producto.

Siga estas instrucciones para instalar el producto:

1. Inserte el CD o haga doble clic en el instalador que se ha descargado.

   Si el CD no se inicia automáticamente, acceda al Explorador de Windows, haga doble clic en el icono de CD-ROM y, a continuación, en el archivo de instalación para iniciar la instalación.

2. Siga las instrucciones descritas en la pantalla.

   - Si ha adquirido el CD del producto en un establecimiento, encontrará la clave de suscripción en la cubierta de la Guía de instalación rápida.
   - Si ha descargado el producto de la tienda electrónica de F-Secure, la clave de suscripción se incluirá en el mensaje de correo de confirmación de la orden de compra.

   Es posible que deba reiniciar su equipo antes de validar su suscripción y descargar las últimas actualizaciones de Internet. Si va a realizar la instalación desde el CD, recuerde que debe retirar el CD de instalación antes de reiniciar el equipo.

Cómo instalar y actualizar aplicaciones

Instrucciones para activar su nueva suscripción.

Siga estas instrucciones para activar su nueva suscripción o instale una nueva aplicación mediante el panel de inicio:

Nota: Puede encontrar el icono del panel de inicio en la bandeja del sistema de Windows.

1. En la barra de inicio, haga clic con el botón derecho en el icono situado más a la derecha.
   Se abrirá un menú emergente.
2. Seleccione **Ver mis suscripciones**
3. En **Mis suscripciones**, acceda a la página **Estado de suscripción** y haga clic en **Activar suscripción**.
   Se abrirá la ventana **Activar suscripción**.

4. Introduzca su clave de suscripción para la aplicación y haga clic en **Aceptar**.
5. Una vez que se ha validado y activado su sucripción, haga clic en **Cerrar**.
6. En **Mis suscripciones**, acceda a la página **Estado de la instalación**. Si la instalación no se inicia automáticamente, siga estas instrucciones:
   a) Haga clic en **Instalar**.
   Se abrirá la ventana de instalación.
   b) Haga clic en **Siguiente**.
   Se descargará la aplicación y se iniciará la instalación.
   c) Cuando se haya completado la instalación, haga clic en **Cerrar**.

Se ha activado la nueva suscripción.

Ayuda y Asistencia técnica

Puede acceder a la ayuda del producto online haciendo clic en el icono de Ayuda o pulsando el botón F1 de cualquier pantalla del producto.

Una vez que haya registrado su licencia, puede disponer de servicios adicionales como, por ejemplo, actualizaciones gratuitos de productos y asistencia técnica de productos. Puede registrarse en la página *www.f-secure.com/register*.

Capítulo

2

Procedimientos iniciales

Temas:

- *Cómo utilizar las actualizaciones automáticas*
- *Cómo ver las acciones que ha llevado a cabo el producto*
- *Red de protección en tiempo real*
- *Cómo puedo saber si mi suscripción es válida*

Información sobre cómo comenzar a utilizar el producto.

En esta sección se describe cómo cambiar la configuración común y cómo gestionar las suscripciones a través de la barra de inicio.

La configuración común de la barra de inicio se aplica a todos los programas instalados en la misma. En lugar de realizar cambios independientes de configuración en cada programa, puede simplemente editar la configuración común que se utilizará en todos los programas instalados.

La configuración común de la barra de inicio incluye las siguientes funciones:

- Descargas: puede encontrar información sobre las actualizaciones que se han descargado y comprobar de forma manual si hay nuevas actualizaciones disponibles.
- Configuración de la conexión: puede modificar el modo de conexión a Internet de su equipo.
- Notificaciones: puede consultar las notificaciones antiguas y configurar el tipo de notificación que desea ver.
- Configuración de privacidad: puede seleccionar si desea o no que su equipo se conecte a la red de protección en tiempo real.

Además, a través de la barra de inicio, puede administrar sus suscripciones para los programas instalados.

Cómo utilizar las actualizaciones automáticas

Las actualizaciones automáticas mantienen actualizada la protección del equipo.

El producto recupera las actualizaciones más recientes para su equipo cuando está conectado a Internet. Detecta el tráfico de red y no interfiere con el resto de usos de Internet, aunque la conexión de red sea lenta.

Comprobar el estado de actualización

Ver la fecha y la hora de la última actualización.

Al activar las actualizaciones automáticas, el producto recibe las actualizaciones más recientes automáticamente cuando el equipo se conecte a Internet.

Para asegurarse de que dispone de las actualizaciones más recientes:

1. En la barra de inicio, haga clic con el botón derecho en el icono situado más a la derecha. Aparecerá un menú desplegable.
2. Seleccione **Abrir configuración común**.
3. Seleccione **Actualizaciones automáticas** > **Descargas**.
4. Haga clic en **Comprobar ahora**.
   El producto se conecta a Internet y comprueba las actualizaciones más recientes. Si la protección no está actualizada, recuperará las actualizaciones más recientes.

   Nota: Si va a utilizar un módem o dispone de una conexión RDSI a Internet, la conexión deberá estar activa para buscar actualizaciones.

Cambiar las opciones de conexión a Internet

Normalmente no es necesario cambiar la configuración predeterminada, pero puede configurar la forma en la que el servidor se conecta a Internet para poder recibir las actualizaciones automáticamente.

Para cambiar las opciones de conexión a Internet:

1. En la barra de inicio, haga clic con el botón derecho en el icono situado más a la derecha. Aparecerá un menú desplegable.
2. Seleccione **Abrir configuración común**.
3. Seleccione **Actualizaciones automáticas** > **Conexión**.
4. En la lista **Conexión a Internet**, seleccione el método de conexión de su equipo a Internet.
   - Seleccione **Suponer que siempre hay conexión** si dispone de una conexión de red permanente.

     Nota: Si el equipo no dispone de una conexión de red permanente y se configura para el marcado a petición, la selección del parámetro **Suponer que siempre hay conexión** puede provocar que se realicen varios marcados.
   - Seleccione **Detectar conexión** para obtener las actualizaciones sólo si el producto detecta una conexión de red activa.
   - Seleccione **Detectar tráfico** para obtener las actualizaciones sólo si el producto detecta otro tráfico de red.

     Sugerencia: Si dispone de una configuración de hardware poco común en la que el parámetro de configuración **Detectar conexión** se utilice para detectar una conexión de red activa incluso cuando no haya ninguna, seleccione **Detectar tráfico** en su lugar.

5. En la lista **Proxy HTTP**, seleccione si desea que su equipo utilice un *servidor proxy* para conectarse a Internet.
   - Seleccione **No usar proxy HTTP** si su equipo está conectado a Internet directamente.
   - Seleccione **Configurar manualmente el proxy HTTP** para configurar el parámetro de configuración *Proxy HTTP*.
   - Seleccione **Usar el proxy HTTP de mi navegador** para utilizar la misma configuración de *proxy HTTP* que se configuró en su navegador web.

Compruebe el estado de la red de protección en tiempo real

Muchos componentes del producto dependen de la conectividad de la red de protección en tiempo real para su correcto funcionamiento.

Si hay problemas de red o si su cortafuegos bloquea el tráfico de la red de protección en tiempo real, el estado será 'desconectada'. Si no hay ningún componente instalado que requiera acceso a la red de protección en tiempo real, el estado será 'no en uso'.

Para comprobar el estado:

1. En la barra de inicio, haga clic con el botón derecho en el icono situado más a la derecha.
   Aparecerá un menú desplegable.
2. Seleccione **Abrir configuración común**.
3. Seleccione **Actualizaciones automáticas** > **Conexión**.

En **Red de protección en tiempo real**, puede ver el estado actual de la red de protección en tiempo real.

Cómo ver las acciones que ha llevado a cabo el producto

En la página **Notificaciones**, puede ver qué acciones ha llevado a cabo el producto para proteger su equipo.

El producto mostrará una notificación cuando se lleve a cabo una acción, por ejemplo, cuando se detecte un virus para bloquear. Su proveedor de servicios también puede enviar algunas notificaciones, por ejemplo para informarle sobre los nuevos servicios.

Ver historial de notificaciones

Puede ver qué notificaciones se han mostrado en el historial de notificaciones

Para ver el historial de notificación:

1. En la barra de inicio, haga clic con el botón derecho en el icono situado más a la derecha.
   Aparecerá un menú desplegable.
2. Seleccione **Abrir configuración común**.
3. Seleccione **Otros** > **Notificaciones**.
4. Haga clic en **Mostrar historial de notificaciones**.
   Se abre la lista del historial de notificaciones.

Cambiar la configuración de las notificaciones

Puede seleccionar qué tipo de notificaciones desea que muestre el producto.

Para cambiar la configuración de notificación:

1. En la barra de inicio, haga clic con el botón derecho en el icono situado más a la derecha.

Aparecerá un menú desplegable.

2. Seleccione **Abrir configuración común**.
3. Seleccione **Otros** > **Notificaciones**.
4. Seleccione o desactive **Permitir mensajes de programa** para activar o desactivar mensajes de programa.

   Cuando esta configuración esté activada, el producto mostrará las notificaciones desde los programas instalados.
5. Seleccione o desactive **Permitir mensajes promocionales** para activar o desactivar los mensajes promocionales.
6. Haga clic en **Aceptar**.

Red de protección en tiempo real

En este documento, se describe la red de protección en tiempo real, un servicio online de F-Secure Corporation que identifica los sitios web y aplicaciones limpias a la vez que proporciona protección frente a malware y vulnerabilidades de sitios web.

Qué es la red de protección en tiempo real

La red de protección en tiempo real es un servicio en línea que ofrece respuesta rápida frente a las últimas amenazas basadas en Internet.

Como colaborador de la red de protección en tiempo real, puede ayudarnos a fortalecer la protección frente a amenazas nuevas y emergentes. La red de protección en tiempo real recopila datos estadísticos de algunas aplicaciones desconocidas, malintencionadas y sospechosas, así como su función dentro de su dispositivo. Esta información es anónima y se envía a F-Secure Corporation para realizar análisis de datos combinados. Utilizamos la información analizada para mejorar la seguridad de su dispositivo frente a las últimas amenazas y archivos que contienen código malintencionado.

Funcionamiento de la red de protección en tiempo real

Como colaborador de la red de protección en tiempo real, puede proporcionar información sobre sitios web y aplicaciones desconocidos y sobre vulnerabilidades de seguridad en sitios web. La red de protección en tiempo real no realiza un seguimiento de su actividad web ni recopila información sobre sitios web que ya han sido analizados, así como tampoco recopila información sobre aplicaciones limpias que han sido instaladas en su equipo.

Si no desea proporcionar estos datos, la red de protección en tiempo real no recopila información de sitios web visitados ni aplicaciones instaladas. No obstante, el producto necesita consultar a los servidores de F-Secure para conocer la reputación de aplicaciones, sitios web, mensajes y otros objetos. La consulta se realiza mediante una suma de comprobación criptográfica donde el objeto consultado en sí no se envía a F-Secure. No realizamos un seguimiento por cada usuario; sólo aumenta el contador de visitas del archivo o sitio web.

No es posible detener por completo todo el tráfico de red en la red de protección en tiempo real, ya que ésta supone una parte integral de la protección ofrecida por el producto.

Ventajas de la red de protección en tiempo real

Con la red de protección en tiempo real, tendrá una protección más precisa y rápida frente a las últimas amenazas y no recibirá alertas innecesarias sobre aplicaciones sospechosas que no sean dañinas.

Como colaborador de la red de protección en tiempo real, puede ayudarnos a encontrar malware nuevo y sin detectar y eliminar falsos positivos de nuestra base de datos de definición de virus.

Todos los participantes en la red de protección en tiempo real se ayudan mutuamente. Cuando la red de protección en tiempo real localiza una aplicación sospechosa en su dispositivo, se beneficia de los resultados de análisis cuando la misma aplicación ya se ha detectado. La red de protección en tiempo real mejora el rendimiento general de su dispositivo, dado que el producto de seguridad instalado no necesita analizar aplicaciones que han sido analizadas y clasificadas como limpias por la red de protección en tiempo real. Del mismo modo, la información sobre sitios web malintencionados y mensajes masivos no solicitados se comparten mediante la red de protección en tiempo real y podemos ofrecerle una protección más precisa frente a vulnerabilidades de sitios web y mensajes de correo no deseado.

Mientras más personas colaboren en la red de protección en tiempo real, mejor estarán protegidos los participantes individuales.

Datos con los que puede colaborar

Como colaborador de la red de protección en tiempo real, proporciona información sobre las aplicaciones almacenadas en su dispositivo y los sitios web que visita para que la red de protección en tiempo real pueda proporcionarle protección frente a las últimas aplicaciones malintencionadas y sitios web sospechosos.

Cómo analizar la reputación de los archivos

La red de protección en tiempo real recopila información únicamente de las aplicaciones que no tienen reputación conocida y de los archivos que pudieran ser malware.

La red de protección en tiempo real recopila información anónima de aplicaciones limpias y sospechosas que se encuentran en su dispositivo. La red de protección en tiempo real únicamente obtiene información de archivos ejecutables (como archivos portables ejecutables de la plataforma Windows, que poseen extensiones .cpl, .exe, .dll, .ocx, .sys, .scr, y .drv).

La información recopilada incluye:

- la ruta del archivo en la que se encuentra la aplicación dentro de su dispositivo,
- el tamaño del archivo y la fecha en la que se creó o se modificó,
- los atributos de archivo y los privilegios,
- la información de la firma del archivo,
- la versión actual del archivo y la empresa que lo creó,
- el origen del archivo y su URL de descarga, y
- los resultados del análisis de archivos realizado por el antivirus y por F-Secure DeepGuard, así como
- otra información similar.

La red de protección en tiempo real nunca recopila información sobre documentos personales, a menos que se encuentren infectados. Recopila el nombre de la infección de cualquier tipo de archivo dañino y el estado de desinfección de dicho archivo.

Con la red de protección en tiempo real, también puede enviar las aplicaciones sospechosas a analizar. Las aplicaciones que envíe deben contener sólo archivos portables ejecutables. La red de protección en tiempo real nunca recopila información de sus documentos personales ni los carga automáticamente para analizar.

Cómo enviar archivos para analizar

Con la red de protección en tiempo real, también puede enviar las aplicaciones sospechosas para análisis.

Puede enviar aplicaciones sospechosas individuales de forma manual cuando el producto le avise de que puede hacerlo. Sólo podrá enviar archivos ejecutables portátiles. La red de protección en tiempo real nunca sube sus documentos personales.

Cómo analizar la reputación de un sitio web

La red de protección en tiempo real no rastrea la actividad de su web ni recopila información de los sitios web que ya se han analizado. De este modo, queda garantizado que los sitios web visitados durante su

navegación web son seguros. Cuando visite un sitio web, la red de protección en tiempo real comprueba su seguridad y le informa sobre si el sitio ha sido clasificado como sospechoso o perjudicial.

Si el sitio web que visita contiene contenido sospechoso o malintencionado o alguna vulnerabilidad de seguridad conocida, la red de protección en tiempo real recopila la URL del sitio para que el contenido de la página web se pueda analizar.

Si visita un sitio que aún no ha sido clasificado, la red de protección en tiempo real recopila los nombres de dominio y subdominio y, en algunos casos, la ruta a la página visitada, para que el sitio se pueda analizar y clasificar. Se eliminarán todos los parámetros de URL que pudieran contener información relacionada con usted en un formato identificable de forma personal, para así proteger su privacidad.

Nota: La red de protección en tiempo real no clasifica ni analiza páginas web en redes privadas, por lo que nunca recopila información sobre direcciones IP de redes privadas (por ejemplo, intranets corporativas).

Cómo analizar información de sistema

La red de protección en tiempo real recopila el nombre y la versión de su sistema operativo, información sobre la conexión a Internet y estadísticas de uso de la red de protección en tiempo real (por ejemplo, el número de veces que se ha consultado la reputación del sitio web y el tiempo medio necesario para que la consulta devuelva un resultado) para que podamos supervisar y mejorar el servicio.

Cómo protegemos su privacidad

Transferimos la información de forma segura y eliminamos automáticamente cualquier información personal que los datos puedan contener.

La red de protección en tiempo real elimina la identificación de datos antes de enviarlos a F-Secure y, de este modo, cifra toda la información recopilada durante la transferencia para protegerlos del acceso no autorizado. La información recopilada no se procesa de manera individual; se agrupa con información de otros colaboradores de la red de protección en tiempo real. Todos los datos se analizan estadísticamente y de forma anónima, lo que significa que ningún dato se relacionará con usted de modo alguno.

En los datos recopilados no se incluye ninguna información que pueda identificarle personalmente. La red de protección en tiempo real no recopila información ni direcciones IP privadas, como direcciones de correo electrónico, nombres de usuario y contraseñas. Aunque estamos haciendo todo lo posible por eliminar todos los datos personalmente identificables, es posible que algunos permanezcan en la información obtenida. En estos casos, puede estar seguro de que no utilizaremos dicha información para identificarle.

Aplicamos estrictas medidas de seguridad y dispositivos de protección física, administrativa y técnica para proteger la información recopilada al transferirla, almacenarla y procesarla. La información se almacena en ubicaciones seguras y en servidores que controla F-Secure, ubicados en nuestras oficinas o en las oficinas de nuestros subcontratistas. Solo el personal autorizado puede acceder a la información recopilada.

F-Secure puede compartir los datos recopilados con sus filiales, subcontratistas, distribuidores y socios, pero siempre con un formato anónimo y sin identificar.

Cómo ser colaborador de la red de protección en tiempo real

Nos ayuda a mejorar la protección ofrecida por la red de protección en tiempo real al colaborar con información sobre sitios web y programas malintencionados.

Puede seleccionar si desea participar en la red de protección en tiempo real durante la instalación. Con la configuración de instalación predeterminada, puede aportar datos a la red de protección en tiempo real. Puede modificar esta configuración más tarde en el producto.

Siga estas instrucciones para cambiar la configuración de la red de protección en tiempo real:

1. En la barra de inicio, haga clic con el botón derecho en el icono situado más a la derecha. Aparecerá un menú desplegable.

2. Seleccione **Abrir configuración común**.
3. Seleccione **Otros** > **Privacidad**.
4. Marque la casilla de verificación de participación para ser un colaborador de la red de protección en tiempo real.

Preguntas sobre la red de protección en tiempo real

Información de contacto para realizar preguntas sobre la red de protección en tiempo real.

Si tiene cualquier pregunta sobre la red de protección en tiempo real, póngase en contacto con:

F-Secure Corporation

Tammasaarenkatu 7

PL 24

00181 Helsinki

Finlandia

http://www.f-secure.com/en/web/home_global/support/contact

La última versión de esta política siempre está disponible en nuestro sitio web.

Cómo puedo saber si mi suscripción es válida

El estado y tipo de suscripción se muestran en la página **Estado de suscripción**.

Cuando la suscripción está a punto de vencer o si ya ha vencido, cambiará el estado de protección total del programa en el icono de barra de inicio correspondiente.

Para comprobar la validez de su suscripción:

1. En la barra de inicio, haga clic con el botón derecho en el icono situado más a la derecha. Aparecerá un menú desplegable.
2. Seleccione **Ver mis suscripciones**.
3. Seleccione **Estado de suscripción** para ver información sobre sus suscripciones para los programas instalados.
4. Seleccione **Estado de instalación** para ver los programas que están disponibles para instalar.

El estado de su suscripción y la fecha de vencimiento también aparecen en la página **Estadísticas** del programa. Si su suscripción ha vencido, debe renovarla para seguir recibiendo actualizaciones y utilizando el producto.

Nota: Cuando su suscripción haya vencido, el icono de estado del producto parpadeará en su bandeja del sistema.

Centro de actividades

El centro de actividades le muestra cualquier notificación importante que requiera su atención.

Si su suscripción ha expirado o está a punto de expirar, su centro de actividades le informará de ello. El color del fondo y el contenido del mensaje del centro de actividades dependerán de su tipo de suscripción y del estado:

- Si su suscripción está a punto de expirar y hay suscripciones gratuitas disponibles, el mensaje mostrará un fondo de color blanco e incluirá un botón **Activar**.
- Si su suscripción está a punto de expirar y no hay suscripciones gratuitas disponibles, el mensaje mostrará un fondo de color amarillo e incluirá los botones **Comprar** e **Introducir clave**. Si ya ha comprado una nueva suscripción, puede hacer clic en **Introducir clave** para proporcionar la clave de suscripción y activar su nueva suscripción.
- Si su suscripción ha vencido y hay suscripciones gratuitas disponibles, el mensaje mostrará un fondo de color rojo e incluirá el botón **Activar**.
- Si su suscripción ha vencido y no hay suscripciones gratuitas disponibles, el mensaje mostrará un fondo de color rojo e incluirá los botones **Comprar** e **Introducir clave**. Si ya ha comprado una nueva suscripción, puede hacer clic en **Introducir clave** para proporcionar la clave de suscripción y activar su nueva suscripción.

Nota: El enlace **Mostrar historial de notificación** del centro de actividades muestra una lista de mensajes de notificación de productos y no los mensajes anteriores del centro de actividades.

Activar una suscripción

Cuando tiene una nueva clave de suscripción o código de campaña para un producto, debe activarlo.

Para activar una suscripción:

1. En la barra de inicio, haga clic con el botón derecho en el icono situado más a la derecha. Aparecerá un menú desplegable.
2. Seleccione **Ver mis suscripciones**.
3. Elija una de las opciones siguientes:
   - Haga clic en **Activar suscripción**.
   - Haga clic en **Activar código de campaña**.
4. En el cuadro de diálogo que se abre, introduzca la nueva clave de suscripción o código de campaña y haga clic en **Aceptar**.

   Sugerencia: Si recibió su clave de suscripción a través de correo electrónico, puede copiar la clave del mensaje de correo electrónico y pegarla en el campo.

Una vez que haya introducido la nueva clave de suscripción, se mostrará la fecha de validez de la nueva suscripción en la página **Estado de suscripción**.

Capítulo

3

Introducción

Temas:

- *Ver el estado general de mi protección*
- *Ver las estadísticas del producto*
- *Gestionar las actualizaciones del producto*
- *Qué son los virus y otros programas de malware*

Este producto protege su equipo frente a virus y otras aplicaciones dañinas.

El producto analiza archivos, aplicaciones y actualizaciones de forma automática. No necesita que realice ninguna acción.

Ver el estado general de mi protección

En la página **Estado** aparece una breve descripción general de las características del producto instaladas y su estado actual.

Para abrir la página **Estado**:

En la página principal, haga clic en **Estado**.

Se abrirá la página **Estado**.

Los iconos muestran el estado del programa y sus funciones de seguridad.

Icono de estado	Nombre de estado	Descripción
	Aceptar	Su equipo está protegido. La función está activada y funciona correctamente.
	Información	El producto informa sobre un estado especial de una función. Por ejemplo, la función se va a actualizar,
	Advertencia	Su equipo no está totalmente protegido. Por ejemplo, el producto no ha recibido actualizaciones desde hace tiempo o el estado de una función debe revisarse.
	Error	Su equipo no está protegido Por ejemplo, su suscripción ha vencido o una función importante está desactivada.
	Desactivado	Una función que no es importante se encuentra desactivada.

Ver las estadísticas del producto

Puede ver las acciones que ha realizado el producto desde su instalación en la página **Estadísticas**.

Para abrir la página **Estadísticas**:

En la página principal, haga clic en **Estadísticas**.

Se abrirá la página **Estadísticas**.

- En **Última comprobación de actualizaciones correcta** aparecerá la hora de la última actualización.

- En **Análisis de virus y spyware** aparecerá la cantidad de archivos que el producto ha analizado y limpiado desde su instalación.
- La opción **Aplicaciones** muestra cuántos programas ha permitido o bloqueado DeepGuard desde su instalación.
- La función **Conexiones del cortafuegos** muestra el número de conexiones permitidas y bloqueadas desde el momento de la instalación.
- La función **Filtrado de spam y phishing** muestra el número de mensajes de correo electrónico que el producto ha detectado como mensajes de correo electrónico válidos y mensajes de spam.

Gestionar las actualizaciones del producto

El producto mantiene actualizada la protección de forma automática.

Ver versiones de la base de datos

Puede ver los números de versión y las fechas de actualización más recientes en la página **Actualización de la base de datos**.

Para abrir la página **Actualizaciones de la base de datos**, siga los siguientes pasos:

1. En la página principal, haga clic en **Configuración**.

   Nota: Necesita derechos administrativos para cambiar la configuración.

2. Seleccione **Otra configuración** > **Versiones de la base de datos**.

La página **Versiones de la base de datos** muestra la última fecha en la que se actualizaron las definiciones de virus y spyware, DeepGuard y el filtrado de spam y phishing, así como sus números de versión.

Cambiar la configuración de banda ancha móvil

Seleccione si desea descargar las actualizaciones de seguridad cuando utilice banda ancha móvil.

Nota: Esta función sólo está disponible en Microsoft Windows 7.

De manera predeterminada, las actualizaciones de seguridad siempre se descargan cuando utiliza la red doméstica de su operador. Sin embargo, las actualizaciones se suspenderán cuando visite otra red del operador. Esto se debe a que los precios de las conexiones varían según el operador, por ejemplo, en función del país. Quizá deba considerar no modificar esta configuración si desea ahorrar ancho de banda y, posiblemente, también costes durante su visita.

Nota: Esta configuración se aplica exclusivamente a las conexiones de banda ancha móvil. Cuando el equipo esté conectado a una red inalámbrica o fija, el producto se actualizará automáticamente.

Para modificar la configuración:

1. En la página principal, haga clic en **Configuración**.

   Nota: Necesita derechos administrativos para cambiar la configuración.

2. Seleccione **Otra configuración** > **Banda ancha móvil** > **Descargar actualizaciones de seguridad**.
3. Seleccione la opción de actualización deseada para las conexiones móviles:
   - **Solo en la red doméstica de mi operador**

Las actualizaciones se descargan siempre en la red doméstica de su operador. Cuando visite otra red del operador, se suspenderán las actualizaciones. Le recomendamos que seleccione esta opción para mantener su producto de seguridad actualizado con los costes estimados.

- **Nunca**

  Las actualizaciones no se podrán descargar cuando utilice banda ancha móvil.

- **Siempre**

  Las actualizaciones se descargan siempre, con independencia de la red que utilice. Seleccione esta opción si desea tener la certeza de que la seguridad de su equipo estará siempre actualizada independientemente de los costes.

4. Si quiere decidir de forma independiente cada vez que salga de la red doméstica de su operador, seleccione la opción **Preguntarme cada vez que salga de la red doméstica de mi operador**.

Se han suspendido las actualizaciones de seguridad

Las actualizaciones de seguridad se pueden suspender cuando utilice banda ancha móvil fuera de la red doméstica del operador.

En este caso, puede ver el aviso de notificación de **suspensión** en la esquina inferior derecha de la pantalla. Las actualizaciones se han suspendido porque los precios de las conexiones pueden variar según el operador, por ejemplo, según el país. No modifique esta opción para ahorrar ancho de banda y, posiblemente, para reducir costes durante su visita. Sin embargo, si desea cambiar la configuración, haga clic en el enlace **Cambiar**.

Nota:

Esta función sólo está disponible en Microsoft Windows 7.

Qué son los virus y otros programas de malware

Los programas de malware son programas diseñados específicamente para provocar daños en su equipo, utilizar su equipo con fines ilícitos sin su conocimiento o robar información de su equipo.

El malware puede:

- tomar el control de su navegador Web,
- redirigir sus búsquedas,
- mostrar publicidad no deseada,
- realizar un seguimiento de los sitios Web que visite,
- robar información personal como, por ejemplo información bancaria,
- utilizar su equipo para enviar spam y
- utilizar su equipo para atacar a otros equipos.

El malware también puede hacer que su equipo se vuelva lento e inestable. Es posible que tenga *malware* en su equipo si se vuelve muy lento de repente y se bloquea a menudo.

Virus

Por lo general, un virus es un programa que se puede adjuntar a archivos y reproducirse repetitivamente; puede alterar y sustituir los contenidos de otros archivos de forma que se provoquen daños en su equipo.

Un *virus* es un programa que, por lo general, se instala sin su conocimiento en su equipo. Una vez instalado, el virus intenta reproducirse. El virus:

- utiliza algunos de los recursos del sistema de su equipo,

- puede alterar o provocar daños en archivos de su equipo,
- probablemente intente utilizar su equipo para infectar otros equipos,
- puede permitir que su equipo se utilice con fines ilícitos

Spyware

El spyware son programas que recopilan información personal.

El spyware puede recopilar información personal, entre la que se incluye:

- sitios de Internet a los que haya accedido,
- direcciones de correo electrónico de su equipo,
- contraseñas o
- números de tarjeta de crédito.

El spyware casi siempre se instala sin su permiso explícito. El spyware se puede instalar junto con un programa útil o engañándole para que haga clic en una opción en una ventana emergente engañosa.

Rootkits

Los rootkits son programas que dificultan la búsqueda de otros programas de *malware*.

Los rootkits ocultan archivos y procesos. Por lo general, lo hacen para ocultar actividades dañinas en su equipo. Cuando un rootkit está ocultando *malware*, no se puede descubrir fácilmente que su equipo contenga malware.

Este producto incluye un explorador de rootkits que realiza un análisis específico para detectar rootkits, por lo que los programas de *malware* no se pueden ocultar fácilmente.

Riskware

El riskware no está diseñado específicamente para provocar daños en su equipo, pero puede provocar daños en él si se utiliza de forma incorrecta.

El riskware no es malware en sentido estricto. Los programas de riskware realizan algunas funciones útiles pero potencialmente peligrosas.

Entre los ejemplos de programas de riskware se encuentran los siguientes:

- programas de mensajería instantánea como, por ejemplo, IRC (Internet Relay Chat),
- programas de transferencia de archivos a través de Internet de un equipo a otro,
- o programas de conexión telefónica por Internet (VoIP, *Protocolo de voz en Internet*),
- Software de acceso remoto como, por ejemplo, VNC,
- scareware que puede intentar asustar o estafar a personas para que compren un software de seguridad falso, o
- software diseñado para anular protecciones de copias o comprobaciones de CD.

Si ha instalado explícitamente el programa y lo ha configurado correctamente, es menos probable que sea dañino.

Si el riskware se ha instalado sin su conocimiento, lo más probable es que se haya instalado con fines dañinos, por lo que deberá eliminarlo.

Capítulo

4

Protección de su equipo frente a malware

Temas:

- *Cómo analizar mi equipo*
- *Cómo excluir archivos del análisis*
- *Cómo utilizar la función de cuarentena*
- *Qué es DeepGuard*

El análisis de virus y spyware protege el equipo de programas que pueden robar información personal, dañar el servidor o utilizarlo con fines ilegales.

De forma predeterminada, todos los tipos de malware se bloquean nada más detectarse para impedir que provoquen daños en el sistema.

De manera predeterminada, el análisis de virus y spyware examina automáticamente sus unidades de discos duros locales, cualquier unidad extraíble (tales como unidades portátiles o CD) y contenido descargado. Asimismo, puede configurar el producto para que analice sus mensajes de correo electrónico también de forma automática.

Además, el análisis de virus y spyware inspecciona su equipo para detectar cualquier cambio que indique la presencia de *malware*. Si se detectan cambios peligrosos en el sistema como, por ejemplo, en la configuración del sistema o intentos de modificación de procesos importantes del sistema, DeepGuard detiene la ejecución de este programa ante la posibilidad de que se trate de *malware*.

Cómo analizar mi equipo

Cuando la función Análisis de virus y spyware esté activada, esta analiza su equipo para detectar archivos perjudiciales de forma automática. También puede analizar archivos manualmente y configurar análisis programados.

Le recomendamos que mantenga la función Análisis de virus y spyware activada en todo momento. Analice sus archivos de forma manual si desea asegurarse de que no existen archivos perjudiciales en su equipo o si quiere analizar archivos que no haya incluido en el análisis en tiempo real.

Al configurar un análisis programado, la función Análisis de virus y spyware elimina los archivos perjudiciales de su equipo en la hora que usted especifique.

Analizar archivos automáticamente

Para proteger el equipo, el análisis en tiempo real analiza todos los archivos cuando se accede a ellos y bloquea el acceso a aquellos archivos que contienen *malware*.

Cuando su equipo intente acceder a un archivo, la función Análisis en tiempo real analizará el archivo en busca de malware antes de permitir que su equipo acceda a él. Si esta función encuentra contenido perjudicial, pondrá el archivo en cuarentena antes de que pueda causar cualquier daño.

¿El análisis en tiempo real afecta al rendimiento de mi equipo?

Por lo general, el usuario no se percata del proceso de análisis porque consume poco tiempo y recursos del sistema. La cantidad de tiempo y recursos del sistema consumidos por el análisis en tiempo real depende, por ejemplo, de los contenidos, la ubicación y el tipo de archivo.

Archivos que tardan más tiempo en analizarse:

- Archivos en unidades extraíbles, tales como CD, DVD y unidades USB portátiles.
- Los archivos comprimidos, tales como los archivos *.zip* archivos.

  Nota: Los archivos comprimidos no se analizan de forma predeterminada.

Es posible que el análisis en tiempo real ralentice su equipo si:

- tiene un equipo que no cumple los requisitos del sistema o
- accede a un gran número de archivos a la vez. Por ejemplo, cuando abra un directorio que incluye muchos archivos que se deben analizar.

Activar o desactivar el análisis en tiempo real

Mantenga el análisis en tiempo real activado para detener el *malware* antes de que pueda dañar su equipo.

Para activar o desactivar el análisis en tiempo real:

1. En la página principal, haga clic en **Estado**.
2. Haga clic en **Cambiar la configuración de esta página**.

   Nota: Necesita derechos administrativos para desactivar las funciones de seguridad.

3. Active o desactive el **Análisis de virus y spyware**.
4. Haga clic en **Cerrar**.

Administrar los archivos perjudiciales de forma automática

El análisis en tiempo real puede administrar los archivos perjudiciales de forma automática sin solicitarle ninguna información.

Para permitir que el análisis en tiempo real administre los archivos perjudiciales de forma automática:

1. En la página principal, haga clic en **Configuración**.

   Nota: Necesita derechos administrativos para cambiar la configuración.

2. Selecione **Seguridad de equipo** > **Análisis de virus y spyware**.
3. Seleccione la opción para **Administrar archivos perjudiciales de forma automática**.

Si prefiere no administrar los archivos perjudiciales de forma automática, el análisis en tiempo real le preguntará qué acción desea realizar con un archivo perjudicial cuando se detecte.

Controlar el spyware

El análisis de virus y spyware bloquea el spyware de forma inmediata cuando este intenta iniciarse.

Antes de que una aplicación de spyware pueda iniciarse, el producto la bloqueará y le permitirá decidir qué acción desea realizar con ella.

Cuando se detecte spyware, debe seleccionar una de las siguientes acciones:

Acción a realizar	Qué ocurre con el spyware
Administrar de forma automática	Permitir al producto decidir la mejor acción en función del spyware que se haya detectado.
Poner en cuarentena el spyware	Mover el spyware a cuarentena de tal forma que no pueda dañar su equipo.
Eliminar el spyware	Eliminar todos los archivos relacionados con el spyware de su equipo.
Sólo bloquear el spyware	Bloquear el acceso al spyware pero dejarlo en su equipo.
Excluir el spyware del análisis	Permitir que el spyware se ejecute y excluirlo del análisis en el futuro.

Controlar el riskware

El análisis de virus y spyware bloquea el riskware de forma inmediata cuando este intenta iniciarse.

Antes de que una aplicación de riskware pueda iniciarse, el producto la bloqueará y le permitirá decidir qué acción desea realizar con ella.

Cuando se detecte riskware, debe seleccionar una de las siguientes acciones:

Acción a realizar	Qué ocurre con el riskware
Sólo bloquear el riskware	Bloquear el acceso al riskware pero dejarlo en su equipo.
Poner en cuarentena el riskware	Mover el riskware a cuarentena de tal forma que no pueda dañar su equipo.
Eliminar el riskware	Eliminar todos los archivos relacionados con el riskware de su equipo.
Excluir el riskware del análisis	Permitir que el riskware se ejecute y excluirlo del análisis en el futuro.

Eliminar cookies de seguimiento de forma automática

Al eliminar las cookies de seguimiento, impide que los sitios web puedan rastrear las páginas que visite en Internet.

Las cookies de seguimiento son pequeños archivos que permiten a los sitios web registrar las páginas que visita. Siga estas instrucciones para desactivar las cookies de seguimiento en su equipo.

1. En la página principal, haga clic en **Configuración**.

   Nota: Necesita derechos administrativos para cambiar la configuración.

2. Selecione **Seguridad de equipo** > **Análisis de virus y spyware**.
3. Seleccione la opción para **eliminar cookies de seguimiento**.
4. Haga clic en **Aceptar**.

Analizar archivos manualmente

Puede analizar archivos manualmente, por ejemplo, cuando conecte un dispositivo externo a su equipo, para asegurarse de que no contiene malware.

Iniciar análisis manual

Puede analizar todo el equipo o realizar un análisis para detectar un tipo específico de *malware* o una ubicación específica.

Si sospecha que existe un determinado tipo de *malware* , puede realizar un análisis para detectar sólo ese tipo. Si sospecha de una determinada ubicación del equipo, puede analizar sólo esa sección. Estos análisis finalizarán mucho más rápido que un análisis de la totalidad de su equipo.

Para comenzar a analizar manualmente su equipo:

1. En la página principal, haga clic en la flecha situada debajo de **Analizar**.

   Aparecerán las opciones de análisis.

2. Seleccione el tipo de análisis.

   Seleccione **Cambiar configuración de análisis** para optimizar el modo en que el análisis manual analiza su equipo para detectar si hay virus u otras aplicaciones perjudiciales.

3. Si selecciona **Elija los elementos que desea analizar**, se abrirá una ventana en la que podrá seleccionar qué ubicaciones desea analizar.
   Se abrirá el **Asistente de análisis**.

Tipos de análisis

Puede analizar todo el equipo o realizar un análisis para detectar un tipo específico de malware o una ubicación específica.

A continuación se indican los distintos tipos de análisis:

Tipo de análisis	Elementos analizados	Cuándo utilizar este tipo
Análisis de virus y spyware	Partes de su equipo para detectar virus, spyware y riskware.	Este tipo de análisis es mucho más rápido que un análisis completo. Busca sólo en las partes de su sistema que contienen archivos de programa instalados. Este tipo de análisis se recomienda si desea comprobar rápidamente si su equipo está limpio, porque puede buscar y eliminar de forma eficaz todo malware activo en su equipo.
Análisis de equipo completo	El equipo en su totalidad (unidades de disco duro internas y externas) para detectar virus, spyware y riskware.	Cuando desee estar completamente seguro de que no exista malware ni riskware en su equipo.Este tipo de análisis es el que tarda más en completarse. Combina el análisis rápido para detectar malware con el análisis

Tipo de análisis	Elementos analizados	Cuándo utilizar este tipo
		del disco duro. También comprueba los elementos que posiblemente estén ocultos por un rootkit.
Elija los elementos que desee analizar	Una carpeta, una unidad o un archivo específicos para detectar virus, spyware y riskware.	Cuando sospeche que es posible que una ubicación específica de su equipo contenga malware , por ejemplo, si ha observado algo sospechoso en esa ubicación, o que quizá contenga descargas de fuentes potencialmente peligrosas, tales como redes de uso compartido de archivos peer-to-peer (P2P). El tiempo que tarda en realizarse el análisis depende del tamaño del destino analizado. El análisis se completa rápidamente si, por ejemplo, analiza una carpeta que sólo contiene unos pocos archivos.
Análisis de rootkits	Ubicaciones de seguridad importantes donde un elemento sospechoso podría implicar un problema de seguridad.Busca en procesos, unidades, carpetas y archivos ocultos	Cuando sospeche que pueda haber un rootkit instalado en su equipo. Por ejemplo, si se ha detectado malware recientemente en su equipo y desea asegurarse de que no instaló un rootkit.

Analizar el Explorador de Windows

Puede buscar *virus*, *spyware* y *riskware* en los discos, las carpetas y los archivos del Explorador de Windows.

Para analizar un disco, una carpeta o un archivo:

1. Coloque el puntero del ratón sobre el disco, la carpeta o el archivo que desee analizar y haga clic con el botón derecho.
2. En el menú contextual, seleccione **Analizar carpetas para detectar virus**. (El nombre de la opción dependerá de si va a analizar un disco, una carpeta o un archivo.)
   Se abrirá la ventana del **Asistente de análisis** y se iniciará el análisis.

Si se encuentra un *virus* o *spyware*, el **Asistente de análisis** le guiará durante las etapas de limpieza.

Seleccionar los archivos para analizar

Seleccione los tipos de archivo en los que desee buscar *virus* y *spyware* en análisis manuales y programados.

1. En la página principal, haga clic en **Configuración**.

   Nota: Necesita derechos administrativos para cambiar la configuración.

2. Seleccione **Otra configuración** > **Análisis manual**.
3. En **Opciones de análisis**, configure las siguientes opciones:

Analizar solo los tipos de archivos conocidos Para analizar únicamente los tipos de archivos que suelen infectarse con mayor frecuencia como, por ejemplo, los archivos ejecutables. Si selecciona esta opción, el análisis se realizará de un modo más rápido. Se analizarán los archivos con las siguientes extensiones: `.ani, .asp, .ax, .bat, .bin, .boo, .chm, .cmd, .com, .cpl, .dll, .doc, .dot, .drv, .eml, .exe, .hlp, .hta, .htm, .html, .htt, .inf, .ini, .job, .js, .jse, .lnk, .lsp, .mdb, .mht, .mpp, .mpt, .msg, .ocx, .pdf, .php, .pif, .pot, .ppt, .rtf, .scr, .shs, .swf, .sys, .td0, .vbe, .vbs, .vxd, .wbk, .wma, .wmv, .wmf, .wsc, .wsf,`

	`.wsh`, `.wri`, `.xls`, `.xlt`, `.xml`, `.zip`, `.jar`, `.arj`, `.lzh`, `.tar`, `.tgz`, `.gz`, `.cab`, `.rar`, `.bz2`, y `.hqx`.
Analizar archivos comprimidos	Para analizar carpetas y archivos comprimidos.
Utilizar heurística avanzada	Para utilizar toda la heurística disponible durante el análisis para mejorar la búsqueda de malware conocido o nuevo. **Nota:** Si selecciona esta opción, la duración del análisis será mayor, y se podrán producir más falsos positivos (archivos no dañinos que se notifican como sospechosos).

4. Haga clic en **Aceptar**.

Nota: Los archivos excluidos de la lista de elementos excluidos no se analizarán aunque los seleccione para analizar aquí.

Qué se debe hacer cuando se detectan archivos perjudiciales

Seleccione el modo en que quiere gestionar sus archivos perjudiciales cuando se detecten.

Para seleccionar la acción que se va a llevar a cabo cuando se detecta contenido perjudicial durante el análisis manual:

1. En la página principal, haga clic en **Configuración**.

   Nota: Necesita derechos administrativos para cambiar la configuración.

2. Seleccione **Otra configuración** > **Análisis manual**.
3. En la opción **Cuando se detecta virus o spyware**, seleccione una de las siguientes opciones:

Opción	Descripción
Preguntar mi opinión (opción predeterminada)	Puede seleccionar la acción que se va a llevar a cabo por cada elemento que se detecte durante el análisis manual:
Limpiar los archivos	El producto intentará desinfectar automáticamente los archivos infectados que se han detectado durante un análisis manual. **Nota:** Si el producto no puede limpiar el archivo infectado, se enviará a cuarentena (excepto cuando se haya detectado en unidades extraíbles o en la red), de tal forma que no pueda dañar el equipo.
Poner en cuarentena los archivos	El producto pondrá en cuarentena cualquier archivo perjudicial detectado durante el análisis manual para evitar que pueda dañar el equipo.
Eliminar los archivos	El producto eliminará cualquier archivo perjudicial detectado durante el análisis manual.
Sólo notificar	El producto dejará los archivos perjudiciales detectados durante el análisis manual tal cual y los registrará en el informe de análisis. **Nota:** Si el análisis en tiempo real está desactivado, todavía es posible que cualquier malware pueda dañar el equipo si selecciona esta opción.

Nota: Cuando los archivos perjudiciales se detectan durante el análisis programado, se limpiarán automáticamente.

Programar un análisis

Configure su equipo para que analice y elimine virus y otras aplicaciones perjudiciales de forma automática cuando no lo utilice, o configure el análisis de tal forma que se ejecute periódicamente para garantizar que su equipo esté en perfecto estado.

Para programar un análisis:

1. En la página principal, haga clic en **Configuración**.

   Nota: Necesita derechos administrativos para cambiar la configuración.

2. Seleccione **Otra configuración** > **Análisis programado**.
3. Active el **Análisis programado**.
4. Seleccione la fecha en la que le gustaría que se iniciara el análisis.

Opción	Descripción
Diario	Analice su equipo cada día.
Semanal	Analice su equipo los días seleccionados de la semana. Seleccione los días de la lista.
Mensual	Analice su equipo los días seleccionados del mes. Para seleccionar los días: 1. Seleccione una de las opciones de **Día**. 2. Seleccione el día del mes en la lista situada junto al día seleccionado.

5. Seleccione cuándo desea comenzar el análisis en los días seleccionados>.

Opción	Descripción
Inicio	Inicie el análisis en la hora indicada.
Tras un periodo de inactividad de	Inicie el análisis después de que haya transcurrido un período de tiempo específico durante el cual no haya utilizado su equipo.

El análisis programado utiliza la configuración del análisis manual para analizar su equipo, con la excepción de que el análisis programado analiza los archivos cada vez y elimina los archivos perjudiciales de forma automática.

Analizar correos electrónicos

El análisis de correo electrónico le protege frente a los archivos perjudiciales incluidos en los correos electrónicos que reciba.

El análisis de virus y spyware debe estar activado para analizar los correos electrónicos y detectar si incluyen virus.

Para activar el análisis de correo electrónico:

1. En la página principal, haga clic en **Configuración**.

   Nota: Necesita derechos administrativos para cambiar la configuración.

2. Selecione **Seguridad de equipo** > **Análisis de virus y spyware**.
3. Seleccione la opción para **Eliminar archivos adjuntos de correo electrónico perjudiciales**.
4. Haga clic en **Aceptar**.

Cuándo se analizan los mensajes de correo electrónico y los adjuntos

El análisis de virus y spyware puede eliminar el contenido perjudicial de los correos electrónicos que reciba.

El análisis de virus y spyware elimina mensajes de correo electrónico perjudiciales recibidos por otros programas de correo electrónico como, por ejemplo, Microsoft Outlook y Outlook Express, Microsoft Mail, Microsoft Mail o Mozilla Thunderbird. Analiza los archivos adjuntos y los mensajes de correo electrónico que no están cifrados cada vez que su programa de correo electrónico los recibe desde el servidor de correo mediante el protocolo POP3.

El análisis de virus y spyware no puede analizar mensajes de correo electrónico en el correo web, lo que incluye aplicaciones que se ejecuten en su navegador web como, por ejemplo, Hotmail, Yahoo! Mail o Gmail. Seguirá estando protegido frente a *virus*, incluso si no elimina los archivos adjuntos perjudiciales o si está utilizando correo web. Cuando abra archivos adjuntos de correo electrónico, el análisis en tiempo real eliminará cualquier archivo adjunto perjudicial antes de que pueda provocar daños.

Nota: El análisis en tiempo real solo protege su equipo, no el de sus amigos. El análisis en tiempo real no analiza archivos adjuntos a menos que los abra. Es decir, si está utilizando correo web y renvía un mensaje antes de abrir su archivo adjunto, es posible que esté renviando un mensaje de correo electrónico infectado a sus amigos.

Ver los resultados del análisis

El historial de virus y spyware muestra todos los archivos perjudiciales detectados por el producto.

En ocasiones, el producto no puede realizar la acción que ha seleccionado cuando se detecta contenido perjudicial. Por ejemplo, si selecciona que desea limpiar archivos y no se puede limpiar un archivo, el producto lo moverá a cuarentena. Puede ver esta información en el historial de virus y spyware.

Para ver el historial:

1. En la página principal, haga clic en **Configuración**.

   Nota: Necesita derechos administrativos para cambiar la configuración.

2. Selecione **Seguridad de equipo** > **Análisis de virus y spyware**.
3. Haga clic en **Ver historial de eliminación**.

El historial de virus y spyware mostrará la siguiente información:

- fecha y hora en las que se ha detectado el archivo perjudicial,
- el nombre del malware y la ubicación en su equipo, y
- la acción realizada.

Cómo excluir archivos del análisis

En ocasiones es posible que desee excluir algunos archivos o aplicaciones del análisis. Los elementos excluidos no se analizarán a menos que los elimine de la lista de elementos excluidos.

Nota: Las listas de exclusión para el análisis manual y el análisis en tiempo real son independientes. Por ejemplo, si excluye un archivo del análisis en tiempo real, se analizará durante el análisis manual a menos que también lo excluya de dicho análisis.

Excluir tipos de archivos

Cuando excluya archivos por tipo de archivo, los archivos con extensiones especificados no se analizarán para detectar si incluyen contenido perjudicial.

Para añadir o eliminar un tipo de archivo que desee excluir:

1. En la página principal, haga clic en **Configuración**.

   Nota: Necesita derechos administrativos para cambiar la configuración.

2. Seleccione si desea excluir el tipo de archivo del análisis manual o del análisis en tiempo real:
   - Seleccione **Seguridad de equipo** > **Análisis de virus y spyware** para excluir el tipo de archivo del análisis en tiempo real.
   - Seleccione **Otra configuración** > **Análisis manual** para excluir el tipo de archivo del análisis manual.
3. Haga clic en **Excluir archivos del análisis**.
4. Para excluir un tipo de archivo:
   a) Seleccione la ficha **Tipos de archivos**.
   b) Seleccione **Excluir archivos con las extensiones**.
   c) Introduzca una extensión de archivo que identifique el tipo de archivo que desee excluir en el campo junto al botón **Añadir**.

      Para especificar archivos sin extensión, escriba '.'. Puede utilizar el carácter comodín '?' para representar cualquier carácter único o '*' para representar cualquier número de caracteres.

      Por ejemplo, para excluir archivos ejecutables, introduzca `exe` en el campo.
   d) Haga clic en **Añadir**.
5. Repita el paso anterior para cualquier otra extensión que desee excluir del análisis para detectar virus.
6. Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Excluir del análisis**.
7. Haga clic en **Aceptar** para aplicar la nueva configuración.

Los tipos de archivos seleccionados se excluirán de futuros análisis.

Excluir archivos por ubicación

Cuando excluya archivos por ubicación, los archivos de carpetas o unidades determinadas no se analizarán para detectar si incluyen contenido perjudicial.

Para añadir o eliminar ubicaciones de archivos que desee excluir:

1. En la página principal, haga clic en **Configuración**.

   Nota: Necesita derechos administrativos para cambiar la configuración.

2. Seleccione si desea excluir la ubicación del análisis manual o del análisis en tiempo real:
   - Seleccione **Equipo** > **Análisis de virus y spyware** para excluir la ubicación del análisis en tiempo real.
   - Seleccione **Equipo** > **Análisis manual** para excluir la ubicación del análisis manual.
3. Haga clic en **Excluir archivos del análisis**.
4. Para excluir un archivo, una unidad o una carpeta:
   a) Seleccione la ficha **Objetos**.
   b) Seleccione **Excluir objetos (archivos, carpetas...)**.
   c) Haga clic en **Añadir**.
   d) Seleccione el archivo, la carpeta o la unidad que desee excluir del análisis para detectar virus.

      Nota: Es posible que algunas unidades sean extraíbles, tales como las unidades de CD, DVD o red. Las unidades de red y las unidades extraíbles vacías no se pueden excluir.

   e) Haga clic en **Aceptar**.

5. Repita el paso anterior para excluir otros archivos, unidades o carpetas del análisis para detectar virus.
6. Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Excluir del análisis**.
7. Haga clic en **Aceptar** para aplicar la nueva configuración.

Los archivos, unidades y carpetas seleccionados se excluirán de futuros análisis.

Ver las aplicaciones excluidas

Puede ver las aplicaciones que ha excluido del análisis y eliminarlas de la lista de elementos excluidos si desea analizarlas en el futuro.

Si el análisis manual o el análisis en tiempo real detecta una aplicación que se comporta como spyware o riskware pero usted sabe que es segura, puede excluirla del análisis para que el producto no vuelva a avisarle sobre esta aplicación nunca más.

Nota: Si la aplicación se comporta como un virus u otro tipo de software malintencionado, no es posible excluirla.

No es posible excluir las aplicaciones directamente. Las nuevas aplicaciones aparecerán en la lista de exclusión solo si las excluye durante el análisis.

Para ver las aplicaciones excluidas del análisis:

1. En la página principal, haga clic en **Configuración**.

   Nota: Necesita derechos administrativos para cambiar la configuración.

2. Seleccione si desea ver las aplicaciones que han sido excluidas del análisis manual o del análisis en tiempo real:
   - Seleccione **Equipo** > **Análisis de virus y spyware** para ver las aplicaciones que hayan sido excluidas del análisis en tiempo real.
   - Seleccione **Equipo** > **Análisis manual** para ver las aplicaciones que hayan sido excluidas del análisis manual
3. Haga clic en **Excluir archivos del análisis**.
4. Seleccione la ficha **Aplicaciones**.

   Nota: Sólo se pueden excluir las aplicaciones de spyware y riskware, no los virus.

5. Si desea volver a analizar la aplicación excluida:
   a) Seleccione la aplicación que desea incluir en el análisis.
   b) Haga clic en **Eliminar**.
6. Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Excluir del análisis**.
7. Haga clic en **Aceptar** para salir.

Cómo utilizar la función de cuarentena

El repositorio de cuarentena es un repositorio seguro para los archivos que pueden resultar dañinos.

Los archivos en cuarentena no se pueden propagar ni causar daño alguno en su equipo.

El producto puede poner en cuarentena *malware*, *spyware* y *riskware* para evitar que se produzcan daños. Podrá restaurar las aplicaciones o los archivos en cuarentena más tarde si es necesario.

Puede eliminar los elementos en cuarentena que no sean necesarios. Al eliminar un elemento en cuarentena, se suprimirá permanentemente de su equipo.

- En general, puede eliminar *malware* en cuarentena.
- En la mayoría de los casos, puede eliminar *spyware* en cuarentena. Es posible que el *spyware* en cuarentena forme parte de un programa de software válido y que, al eliminarlo, el propio programa deje de funcionar correctamente. Si desea conservar el programa en un equipo, puede restaurar el *spyware* en cuarentena.
- Es posible que un programa de *riskware* en cuarentena sea un programa de software válido. Si usted mismo ha instalado y configurado el programa, podrá restaurarlo desde su estado en cuarentena. Si el *riskware* se instala sin su consentimiento, es muy probable que se haya instalado con fines dañinos, por lo que deberá eliminarlo.

Ver elementos en cuarentena

Puede ver información adicional sobre los elementos en estado de cuarentena.

Para ver información detallada sobre los elementos en estado de cuarentena:

1. En la página principal, haga clic en **Configuración**.

   Nota: Necesita derechos administrativos para cambiar la configuración.

2. Selecione **Seguridad de equipo** > **Análisis de virus y spyware**.
3. Haga clic en **Ver cuarentena**.
   La página **Cuarentena** muestra el número total de elementos almacenados en cuarentena.
4. Para ver información detallada sobre los elementos en cuarentena, haga clic en **Detalles**.

   Puede ordenar el contenido por nombre de malware o por ruta de archivo.

   Se muestra una lista de los 100 primeros elementos indicando el tipo de elemento en cuarentena, su nombre y la ruta donde se instalaron los archivos.
5. Si desea obtener más información sobre un elemento en cuarentena, haga clic en el icono situado cerca de la columna de **estado**.

Restaurar elementos en cuarentena

Puede restaurar los elementos en cuarentena que necesite.

Puede restaurar aplicaciones o archivos del estado de cuarentena si los necesita. No restaure ningún elemento del estado de cuarentena a menos que esté seguro de que los elementos no suponen ninguna amenaza. Los elementos restaurados se devuelven a su ubicación original en el equipo.

Restaurar elementos en cuarentena

1. En la página principal, haga clic en **Configuración**.

   Nota: Necesita derechos administrativos para cambiar la configuración.

2. Selecione **Seguridad de equipo** > **Análisis de virus y spyware**.
3. Haga clic en **Ver cuarentena**.
4. Seleccione los elementos en cuarentena que desee restaurar.
5. Haga clic en **Restaurar**.

Qué es DeepGuard

DeepGuard analiza el contenido de los archivos y el comportamiento de las aplicaciones y supervisa las aplicaciones que no son de confianza.

DeepGuard bloquea los *virus* y los *gusanos* tanto nuevos como sin detectar, así como otras aplicaciones perjudiciales que intenten realizar cambios en su equipo, y evita que las aplicaciones sospechosas accedan a Internet.

Cuando DeepGuard detecta un programa que intenta realizar cambios que puedan ser perjudiciales en el sistema, permite que el programa se ejecute en una zona segura. En la zona segura, la aplicación no puede dañar su equipo. DeepGuard analiza los cambios que la aplicación ha intentado realizar y, en base a ello, decide con qué probabilidad se trata de *malware*. Si existe una gran probabilidad de que la aplicación sea *malware*, DeepGuard la bloqueará.

Entre los cambios potencialmente perjudiciales para el sistema detectados por DeepGuard se incluyen:

- cambios de configuración del sistema (registro de Windows),
- intentos de desactivar programas del sistema importantes como, por ejemplo, programas de seguridad como este producto, e
- intentos de editar archivos de sistema importantes.

Activar o desactivar DeepGuard

Active DeepGuard para evitar que las aplicaciones sospechosas realicen cambios del sistema que pudieran ser perjudiciales en su equipo.

Si tiene Windows XP, asegúrese de haber instalado Service Pack 2 antes de activar DeepGuard.

Para activar o desactivar DeepGuard:

1. En la página principal, haga clic en **Estado**.
2. Haga clic en **Cambiar la configuración de esta página**.

   Nota: Necesita derechos administrativos para desactivar las funciones de seguridad.

3. Active o desactive **DeepGuard**.
4. Haga clic en **Cerrar**.

Permitir aplicaciones bloqueadas por DeepGuard

Puede controlar qué aplicaciones permite y bloquea DeepGuard.

En ocasiones DeepGuard puede impedir que una aplicación se ejecute, aunque usted desee utilizarla y sea consciente de que es segura. Esto se produce cuando la aplicación intenta realizar cambios del sistema que pudieran ser perjudiciales. Es posible que también haya bloqueado de forma involuntaria la aplicación cuando haya aparecido un elemento emergente de DeepGuard.

Para permitir la aplicación bloqueada por DeepGuard:

1. En la página principal, haga clic en **Herramientas**.
2. Haga clic en **Aplicaciones**.
   Se muestra la lista **Aplicaciones supervisadas**.
3. Busque la aplicación que desea permitir.

   Nota: Puede hacer clic en los encabezados de las columnas para ordenar la lista. Por ejemplo, haga clic en la columna **Permiso** para ordenar la lista en grupos de programas permitidos y denegados.

4. Seleccione **Permitir** en la columna **Permiso**.
5. Haga clic en **Cerrar**.

DeepGuard permite que la aplicación vuelva a realizar cambios del sistema.

Utilice DeepGuard en el modo de compatibilidad

Para obtener una protección máxima, DeepGuard modificará temporalmente los programas en ejecución. Algunos programas comprobarán que no han sufrido daños o modificaciones y es posible que no sean compatibles con esta función. Por ejemplo, los juegos en línea con herramientas a prueba de trampas comprobarán que no han sufrido ningún tipo de modificación mientras estaban en ejecución. En estos casos, puede activar el modo de compatibilidad.

Para activar el modo de compatibilidad:

1. En la página principal, haga clic en **Configuración**.

   Nota: Necesita derechos administrativos para cambiar la configuración.

2. Seleccione **Seguridad de equipo** > **DeepGuard**.
3. Seleccione **Usar el modo de compatibilidad**.
4. Haga clic en **Aceptar**.

Cómo actuar con las advertencias de comportamiento sospechoso

DeepGuard supervisa las aplicaciones que no son de confianza. Si una aplicación supervisada intenta acceder a Internet, realizar cambios en su sistema o se comporta de forma sospechosa, DeepGuard la bloqueará.

Cuando haya seleccionado la opción para **recibir información sobre comportamiento sospechoso** en la configuración de DeepGuard, DeepGuard le informará cuando detecte una aplicación posiblemente perjudicial o cuando inicie una aplicación que tenga una reputación desconocida.

Para decidir qué acción desea llevar a cabo con la aplicación bloqueada por DeepGuard:

1. Haga clic en **Detalles** para ver más información sobre el programa.
   La sección Detalles le mostrará:
   - la ubicación de la aplicación,
   - la reputación de la aplicación en la red de protección en tiempo real, y
   - si la aplicación es muy común.
2. Decida si confía en la aplicación bloqueada por DeepGuard:
   - Seleccione la opción **Confío en la aplicación. Continuar.** si no desea bloquear la aplicación.

     Es más probable que la aplicación sea segura si:
     - DeepGuard ha bloqueado la aplicación como resultado de una acción que realizó,
     - usted reconoce la aplicación, o
     - obtuvo la aplicación de una fuente fiable.
   - Seleccione **No confío en la aplicación. Continuar con el bloqueo.** si desea que la aplicación siga bloqueada.

     Es más probable que la aplicación no sea segura si:
     - la aplicación no es muy común,
     - la aplicación tiene una reputación desconocida, o
     - usted no conoce la aplicación.
3. Si desea enviar una aplicación sospechosa para su análisis:
   a) Haga clic en **Notificar la aplicación a F-Secure**.
   El producto muestra las condiciones de envío.

b) Haga clic en **Aceptar** si está de acuerdo con las condiciones y desea enviar la muestra.

Le recomendamos que envíe una muestra cuando:

- DeepGuard bloquea una aplicación que usted sabe que es segura o
- si sospecha que la aplicación puede tratarse de *malware*.