F-Secure Internet Security 2013

Contenido

Capítulo 1: Instalación.....5

Antes de instalar por primera vez.....6
Instalación del producto por primera vez.....6
Instalación y actualización de las aplicaciones.....6
Ayuda y soporte.....7

Capítulo 2: Empezando.....9

Cómo usar las actualizaciones automáticas.....10
Revisar el estado de actualizaciones.....10
Cambiar la configuración de mi conexión a Internet.....10
Compruebe el estado de la Red de protección en tiempo real.....11
¿Cómo puedo saber qué ha hecho el producto?.....11
Ver historial de notificaciones.....11
Cambie las configuraciones de notificación.....11
Real-time Protection Network.....12
Definición de Real-time Protection Network.....12
Beneficios de Real-time Protection Network.....12
Qué datos puede aportar usted.....13
Cómo protegemos su privacidad.....14
Aportar a Real-time Protection Network.....14
Preguntas sobre Real-time Protection Network.....15
¿Cómo sé que mi suscripción es válida?.....15
Centro de acción.....15
Activar una suscripción.....16

Capítulo 3: Introducción.....17

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

Capítulo 4: Proteger mi equipo contra malware.....23

Cómo analizar mi equipo.....24
Analizar archivos automáticamente.....24
Analizar archivos manualmente.....26
Analizar mensajes de correo electrónico.....29
Ver resultados del análisis.....30
Cómo excluir archivos del análisis.....30
Excluir tipos de archivos.....30
Excluir archivos por ubicación.....31
Ver aplicaciones excluídas.....32
¿Cómo usar el almacén de cuarentena?.....32
Ver elementos en cuarentena.....33
Restaurar elementos en cuarentena.....33
¿Qué es DeepGuard?.....33
Activar o desactivar DeepGuard.....34
Permitir aplicaciones que DeepGuard ha bloqueado.....34
Use DeepGuard en el modo de compatibilidad.....34
Qué hacer con las advertencias sobre comportamiento sospechoso.....35
¿Qué es un cortafuegos?.....35
Activar o desactivar el cortafuegos.....36
Cambiar la configuración del cortafuegos.....36
Impida que aplicaciones descarguen archivos dañinos.....36
Bloquear el spam.....37
Activar o desactivar el filtro de spam y phishing.....37
Protección contra intentos de phishing.....37
Configurar mis programas de correo electrónico para que filtren spam.....37

Capítulo 5: Uso seguro de Internet.....41

¿Cómo ejecutar tareas comunes?.....42
Cómo proteger las distintas cuentas de usuario.....42
Crear y editar cuentas de usuario de Windows.....42
¿Qué es la protección de navegación?.....42
Cómo activar o desactivar la protección de navegación.....42
Clasificación de seguridad de la protección de navegación.....43
Protección contra contenido dañino.....44
Qué hacer cuando se bloquea un sitio web.....44
Resumen de seguridad de un sitio web.....44
Navegación segura.....45
Limitar el acceso al contenido web.....45
Cómo programar el tiempo de navegación.....46
Restringir el tiempo diario de navegación en Internet.....47
Ver estadísticas.....47

Capítulo

1

Instalación

Temas:

- *Antes de instalar por primera vez*
- *Instalación del producto por primera vez*
- *Instalación y actualización de las aplicaciones*
- *Ayuda y soporte*

Antes de instalar por primera vez

Gracias por elegir F-Secure.

Para instalar el producto, necesitará lo siguiente:

- El CD de instalación o un paquete de instalación. Si está usando una netbook sin una unidad de CD, puede descargar el paquete de instalación en *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 eliminarlo automáticamente. Si esto no ocurre, elimínelo manualmente.

Nota: Si tiene más de una cuenta en la computadora, inicie sesión con los privilegios de administrador cuando haga 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 descargó.

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

2. Siga las instrucciones en la pantalla.

   - Si compró el producto en un CD de una tienda, puede encontrar la clave de suscripción en la cubierta de la Guía de instalación rápida.
   - Si descargó el producto de una tienda en línea de F-Secure, la clave de suscripción se incluye en el correo electrónico de confirmación de la orden de compra.

   Es posible que su computadora deba reiniciarse antes de validar su suscripción y descargar las actualizaciones más recientes de Internet. Si está instalando desde un CD, recuerde retirar el CD de instalación antes de reiniciar su computadora.

Instalación y actualización de las aplicaciones

Instrucciones para activar su suscripción nueva.

Siga estas instrucciones para activar su nueva suscripción o para instalar una aplicación nueva usando la plataforma de lanzamiento:

Nota: Puede encontrar el icono de la plataforma de lanzamiento en la bandeja del sistema de Windows.

1. En la plataforma de lanzamiento, haga clic derecho en el icono del extremo derecho.
   Se abre un menú emergente.
2. Seleccione **Ver mis suscripciones**
3. En **Mis suscripciones**, vaya a la página **Estado de la suscripción** y haga clic en **Activar suscripción**.
   Se abre la ventana **Activar suscripción**.

4. Ingrese su clave de suscripción para la aplicación y haga clic en **Aceptar**.
5. Después de validar y activar su suscripción, haga clic en **Cerrar**.
6. En **Mis suscripciones**, vaya a la página **Estado de la instalación**. Si la instalación no inicia automáticamente, siga estas instrucciones:
   a) Haga clic en **Instalar**.
   Se abre la ventana de instalación.
   b) Haga clic en **Siguiente**.
   La aplicación se descarga e inicia la instalación.
   c) Cuando termine la instalación, haga clic en **Cerrar**.

La suscripción nueva se ha activado.

Ayuda y soporte

Puede acceder a la ayuda del producto en línea haciendo clic en el icono de Ayuda o presionando F1 en cualquier pantalla del producto.

Después de registrar su licencia, usted tiene el derecho a servicios adicionales como actualizaciones gratis del producto y soporte del producto. Puede registrarse en *www.f-secure.com/register*.

Capítulo

2

Empezando

Temas:

- *Cómo usar las actualizaciones automáticas*
- *¿Cómo puedo saber qué ha hecho el producto?*
- *Real-time Protection Network*
- *¿Cómo sé que mi suscripción es válida?*

Información sobre los pasos iniciales del producto.

Esta sección describe cómo cambiar las configuraciones comunes y administrar sus suscripciones a través de la pantalla de inicio.

Las configuraciones comunes de la pantalla de inicio se aplican a todos los programas instalados en la pantalla de inicio. En lugar de cambiar las configuraciones de cada programa por separado, puede sencillamente editar las configuraciones comunes, que luego son utilizadas por todos los programas instalados.

Las configuraciones comunes de la pantalla de inicio incluyen:

- Descargas: donde puede ver la información sobre las actualizaciones que se han descargado y verificar de forma manual si existen actualizaciones nuevas disponibles.
- Configuración de la conexión: donde puede cambiar la manera en que su computadora se conecta a Internet.
- Notificaciones: donde puede ver notificaciones anteriores y establecer la clase de notificaciones que desea ver.
- Configuración de privacidad: donde puede seleccionar si su computadora se puede o no conectar a la Red de protección en tiempo real.

También puede administrar sus suscripciones para los programas instalados a través de la pantalla de inicio.

Cómo usar las actualizaciones automáticas

Las actualizaciones automáticas mantienen actualizada la protección de su equipo.

El producto obtiene e instala las actualizaciones más recientes en su equipo cuando está conectado a Internet. Detecta el tráfico de red y no interrumpe el uso de Internet aún cuando tiene una conexión a Internet lenta.

Revisar el estado de actualizaciones

Ver la fecha y la hora de la última actualización.

Cuando las actualizaciones automáticas se activan, el producto recibe las actualizaciones más recientes de manera automática cuando se conecta a Internet.

Para asegurarse de que dispone de las actualizaciones más recientes:

1. En la plataforma de lanzamiento, haga clic derecho en el icono del extremo derecho.
   Aparecerá un menú emergente.
2. Seleccione **Abrir configuraciones comunes**.
3. Seleccione **Actualizaciones automáticas** > **Descargar**.
4. Haga clic en **Comprobar ahora**.
   El producto se conecta a Internet y busca 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 la configuración de mi conexión a Internet

Generalmente no hay necesidad de cambiar la configuración predeterminada, sin embargo puede configurar cómo se conecta el servidor a Internet de manera que pueda recibir actualizaciones automáticamente.

Para cambiar la configuración de su conexión a Internet:

1. En la plataforma de lanzamiento, haga clic derecho en el icono del extremo derecho.
   Aparecerá un menú emergente.
2. Seleccione **Abrir configuraciones comunes**.
3. Seleccione **Actualizaciones automáticas** > **Conexión**.
4. En la lista de **Conexión a Internet**, seleccione cómo su equipo se conecta 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 recuperar las actualizaciones sólo si el producto detecta otro tráfico de red.

     Consejo: Si dispone de una configuración de hardware poco común en la que el parámetro de configuración **Detectar conexión** se utiliza para detectar una conexión de red activa incluso cuando no hay ninguna, seleccione **Detectar tráfico** en su lugar.
5. En **proxy de HTTP**, seleccione si su computadora usa un *servidor proxy* para conectarse a Internet.

- Seleccione **Sin proxy de HTTP** si su computadora está conectada a Internet directamente.
- Seleccione **Configurar manualmente el proxy HTTP** para configurar el parámetro de configuración *Proxy HTTP*.
- Seleccione **Usar el proxy HTTP del navegador**para utilizar los mismos parámetros del *proxy HTTP* que haya configurado en su navegador web.

Compruebe el estado de la Red de protección en tiempo real

Para funcionar adecuadamente, muchas funciones del producto dependen de la conectividad de la red de protección en tiempo real.

Si hay problemas con la red o si su cortafuegos bloquea el tráfico de la red de protección en tiempo real, el estado está 'desconectado'. Si no ha instalado funciones del producto que requieren acceso a la red de protección en tiempo real, el estado es 'no está en uso'.

Para comprobar el estado:

1. En la plataforma de lanzamiento, haga clic derecho en el icono del extremo derecho.
   Aparecerá un menú emergente.
2. Seleccione **Abrir configuraciones comunes**.
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 puedo saber qué ha hecho el producto?

Puede ver las acciones que el producto ha realizado para proteger su computadora en la página de **Notificaciones**.

El producto mostrará una notificación cuando realiza una acción, por ejemplo, cuando encuentra un virus que bloquea. Es posible que su proveedor de servicios también envíe algunas notificaciones, por ejemplo, para permitirle conocer sobre servicios nuevos que están disponibles.

Ver historial de notificaciones

Puede ver las notificaciones que se han mostrado en el historial de notificaciones

Para ver el historial de notificaciones:

1. En la plataforma de lanzamiento, haga clic derecho en el icono del extremo derecho.
   Aparecerá un menú emergente.
2. Seleccione **Abrir configuraciones comunes**.
3. Seleccione **Otras** > **notificaciones**.
4. Haga clic en **Mostrar historial de notificaciones**.
   Se abre el historial de notificaciones,

Cambie las configuraciones de notificación

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

Para cambiar las configuraciones de notificación:

1. En la plataforma de lanzamiento, haga clic derecho en el icono del extremo derecho.
   Aparecerá un menú emergente.

2. Seleccione **Abrir configuraciones comunes**.
3. Seleccione **Otras** > **notificaciones**.
4. Seleccione o elimine **Permitir mensajes del programa** para activar o desactivar los mensajes del programa.

   Cuando se conecta esta configuración, el producto mostrará notificaciones desde los programas instalados.
5. Seleccione o elimine **Permitir mensajes de promoción** para activar o desactivar los mensajes de promoción.
6. Haga clic en **Aceptar**.

Real-time Protection Network

El presente documento brinda una descripción de Real-time Protection Network, servicio en línea de F-Secure Corporation que identifica las aplicaciones y los sitios web limpios, y ofrece protección contra el malware y las amenazas de sitios web.

Definición de Real-time Protection Network

Real-time Protection Network es un servicio en línea que ofrece una respuesta rápida ante las amenazas web más recientes.

Al aportar a Real-time Protection Network, puede ayudarnos a fortalecer la protección contra las nuevas amenazas y las amenazas emergentes. Esta red recopila datos estadísticos sobre determinadas aplicaciones desconocidas, dañinas o sospechosas, y sobre el efecto que tienen en los dispositivos. Esta información es anónima y se envía a F-Secure Corporation para que se lleve a cabo un análisis de datos combinados. Usamos la información analizada para mejorar la seguridad de su dispositivo frente a las amenazas más recientes y archivos dañinos.

Cómo funciona Real-time Protection Network

Al aportar a Real-time Protection Network, puede brindar información sobre sitios web y aplicaciones desconocidas, así como también sobre aplicaciones dañinas y ataques a la seguridad en sitios web. Esta red no realiza seguimiento alguno de su actividad web ni recopila información sobre los sitios web que ya se analizaron, ni tampoco recopila información sobre aplicaciones limpias que se encuentren instaladas en su equipo.

Si no desea aportar estos datos, Real-Time Protection Network no recopila información sobre aplicaciones instaladas ni sitios web visitados. No obstante, el producto necesita consultar a los servidores de F-Secure para conocer la reputación de las aplicaciones, los sitios web, los mensajes y demás objetos. La consulta se lleva a cabo mediante una suma de comprobación criptográfica, en la que el objeto consultado en sí no se envía a F-Secure. No realizamos seguimientos de los datos por usuario. Solo se aumenta el contador de coincidencias del archivo o del sitio web.

No es posible interrumpir completamente todo el tráfico de red de Real-time Protection Network, ya que éste es una parte integral de la protección suministrada con el producto.

Beneficios de Real-time Protection Network

Con Real-time Protection Network, tendrá una protección más rápida y precisa contra las amenazas más recientes y no recibirá alertas innecesarias de aplicaciones sospechosas que no son maliciosas.

Al aportar a Real-time Protection Network, puede ayudarnos a encontrar malware nuevo y no detectado, y eliminar los posibles falsos positivos de nuestra base de datos de definiciones de virus.

Todos los participantes de Real-time Protection Network se ayudan entre sí. Cuando Real-time Protection Network detecta una aplicación sospechosa en su dispositivo, usted se beneficia con los resultados del

análisis cuando la misma aplicación ya se detectó con anterioridad en otros dispositivos. Real-time Protection Network mejora el rendimiento general de su dispositivo, porque el producto de seguridad instalado no necesita volver a escanear las aplicaciones que Real-time Protection Network ya analizó y encontró limpias. De forma similar, la información sobre los sitios web maliciosos y el correo masivo no solicitado se comparte en Real-time Protection Network y podemos ofrecerle una protección más precisa contra las amenazas de los sitios web y el correo no deseado.

Mientras más personas brinden aportes a Real-time Protection Network, más protegidos estarán los participantes individuales.

Qué datos puede aportar usted

Al aportar a Real-time Protection Network, puede proporcionar información sobre aplicaciones almacenadas en su dispositivo y los sitios web que visita, de modo que esta red, a su vez, pueda ofrecer protección contra las aplicaciones dañinas más recientes y sitios web sospechosos.

Análisis de la reputación de los archivos

Real-time Protection Network solamente recopila información de aplicaciones sin una reputación conocida y de archivos sospechosos o que se sabe que son malware.

Real-time Protection Network recopila información anónima de aplicaciones limpias y sospechosas en su dispositivo. Real-time Protection Network recopila información de archivos ejecutables solamente (como archivos ejecutables portátiles en la plataforma de Windows, que tienen extensiones .cpl, .exe, .dll, .ocx, .sys, .scr, y .drv).

La información recopilada comprende:

- la ruta de acceso de la aplicación en su dispositivo,
- el tamaño del archivo y la fecha y hora de creación o modificación,
- atributos y privilegios de archivos,
- información de la firma del archivo,
- la versión actual del archivo y la empresa que lo creó,
- el origen del archivo o la dirección URL de descarga, y
- resultados de análisis de F-Secure DeepGuard y de antivirus de los archivos analizados y
- otros datos similares.

Real-time Protection Network nunca recopila información de sus documentos personales, a menos que se encuentren infectados. Para cualquier tipo de archivo malicioso, recopila el nombre de la infección y el estado de desinfección del archivo.

Con Real-time Protection Network, también puede enviar aplicaciones sospechosas para su análisis. Las aplicaciones que pueden enviar solamente incluyen archivos ejecutables portátiles. Real-time Protection Network nunca recopila ninguna información de sus documentos personales y éstos nunca se cargan automáticamente para su análisis.

Envío de archivos para su análisis

Con la Red de protección en tiempo real, también puede enviar aplicaciones sospechosas para analizarlas.

Puede enviar manualmente las aplicaciones sospechas individuales cuando el producto le pide que lo haga. Solo puede enviar archivos ejecutables portátiles. La Red de protección en tiempo real nunca descarga sus documentos personales.

Análisis de la reputación de los sitios web

Real-time Protection Network no hace un seguimiento de su actividad web ni recopila información de sitios web que ya han sido analizados. Garantiza que los sitios web visitados son seguros cuando usted navega

por Internet. Cuando visita un sitio web, Real-time Protection Network comprueba si es seguro y lo notifica si el sitio está calificado como sospechoso o dañino.

Si el sitio web que visita tiene contenido malicioso o sospechoso, o una amenaza conocida, Real-time Protection Network recopila la dirección URL completa del sitio para que la página web pueda ser analizada.

Si visita un sitio que aún no ha sido calificado, Real-time Protection Network recopila los nombres de dominio y subdominio, y en algunos casos la ruta a la página visitada , para que el sitio pueda analizarse y calificarse. Todos los parámetros de la dirección URL con información que pudiera vincularse con sus datos personales se eliminan para proteger su privacidad.

Nota: Real-time Protection Network no califica ni analiza sitios web de redes privadas, por lo que nunca recopila ninguna información de direcciones de red IP privadas (como Intranets corporativas).

Análisis de la información del sistema

Real-time Protection Network recopila el nombre y la versión de su sistema operativo, información sobre la conexión a Internet y las estadísticas de uso de Real-time Protection Network (por ejemplo, la cantidad de veces que se consultó la reputación de un sitio web y la cantidad promedio en que una consulta produjo un resultado) para que podamos hacer un seguimiento del servicio y mejorarlo.

Cómo protegemos su privacidad

Transferimos la información de forma segura y quitamos automáticamente toda la información personal que puedan contener los datos.

Real-time Protection Network elimina la necesidad de identificar datos antes de enviarlos a F-Secure y cifra toda la información recopilada durante la transferencia para protegerla de accesos no autorizados. La información recopilada no se procesa de forma individual, sino que se agrupa con información de otros contribuyentes de la Real-time Protection Network. Todos los datos se analizan estadísticamente y de forma anónima, por lo que ninguno de ellos se vinculará con usted en absoluto.

Los datos recopilados no incluyen ninguna información con la que pudieran identificarlo personalmente. Real-time Protection Network no recopila direcciones IP privadas ni información personal como direcciones de correo electrónico, nombres de usuario o contraseñas. Aunque hacemos todo lo que está a nuestro alcance para quitar todos los datos identificatorios, es posible algunos de estos datos permanezcan en la información recopilada. En tales casos, no procuraremos usar tales datos recopilados involuntariamente para identificarlo.

Aplicamos estrictas medidas de seguridad y salvaguardas físicas, administrativas y técnicas para proteger la información recopilada cuando ésta se transfiere, almacena y procesa. La información se guarda en lugares protegidos y en servidores bajo nuestro control, ubicados en nuestras oficinas o en las oficinas de nuestros subcontratistas. Sólo personal autorizado puede obtener acceso a la información recopilada.

F-Secure puede compartir los datos recopilados con sus filiales, subcontratistas, distribuidores y socios, pero siempre de forma anónima y no identificable.

Aportar a Real-time Protection Network

Cuando aporta información sobre sitios web y programas maliciosos, nos ayuda a mejorar Real-time Protection Network.

Puede elegir participar en Real-Time Protection Network durante la instalación. Mediante la configuración de instalación predeterminada, puede aportar datos a la red. Posteriormente puede cambiar esta configuración en el producto.

Siga estas instrucciones para cambiar la configuración de Real-Time Protection Network:

1. En la plataforma de lanzamiento, haga clic derecho en el icono del extremo derecho. Aparecerá un menú emergente.
2. Seleccione **Abrir configuraciones comunes**.

3. Seleccione**Otra** > **privacidad**.
4. Marque la casilla de verificación de participación para aportar a Real-Time Protection Network.

Preguntas sobre Real-time Protection Network

Información de contacto por cualquier inquietud acerca de Real-time Protection Network.

Ante cualquier otra duda sobre Real-time Protection Network, comuníquese 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 está siempre disponible en nuestro sitio web.

¿Cómo sé que mi suscripción es válida?

El tipo y el estado de su suscripción se mostrarán en la página de **Estado de suscripción**.

Cuando la suscripción esté a punto de caducar o si ya ha caducado, el estado de protección general del programa en el icono de la pantalla de inicio correspondiente cambiará.

Para comprobar la validez de su suscripción:

1. En la plataforma de lanzamiento, haga clic derecho en el icono del extremo derecho. Aparecerá un menú emergente.
2. Seleccione **Ver mis suscripciones**.
3. Seleccione **Estado de la suscripción** para ver la información sobre las suscripciones para los programas instalados.
4. Seleccione **Estado de la instalación** para ver los programas disponibles a instalar.

El estado de la suscripción y la fecha de caducidad también se muestran en la página de **Estadística** del programa. Si la suscripción ha caducado, necesitará renovar la suscripción para continuar recibiendo actualizaciones e utilizando el producto.

Nota: Cuando su suscripción haya caducado, el icono de estado del producto destellará en la bandeja del sistema.

Centro de acción

El centro de acción muestra todas las notificaciones importantes que requieren su atención.

Si su suscripción ha caducado y está por caducar, el centro de acción le notifica esto. El color de fondo y el contenido del mensaje del centro de acción depende de su tipo de suscripción y estado:

- Si su suscripción está por caducar y hay suscripciones gratis disponibles, el mensaje tiene un fondo blanco y un botón de **Activar**.

- Si su suscripción está por caducar y no hay suscripciones gratis disponibles, el mensaje tiene un fondo amarillo y los botones **Comprar** e **Ingresar clave**. Si ya compró una suscripción nueva, puede hacer clic en **Ingresar clave** para proporcionar la clave de suscripción y activar su suscripción nueva.
- Si su suscripción ha caducado y hay suscripciones gratis disponbiles, el mensaje tiene un fondo rojo y un botón de **Activar**.
- Si su suscripción ha caducado y no hay suscripciones gratis disponibles, el mensaje tiene un fondo rojo y los botónes **Comprar** e **Ingresar clave**. Si ya compró una suscripción nueva, puede hacer clic en **Ingresar clave** para proporcionar la clave de suscripción y activar su suscripción nueva.

Nota: El enlace de **Mostrar historial de notificaciones** en el centro de acción muestra una lista de mensajes de notificación del producto y no los mensajes del centro de acción anteriores.

Activar una suscripción

Cuando tenga una clave de suscripción nueva o un código de campaña para un producto, necesitará activarlo.

Para activar una suscripción:

1. En la plataforma de lanzamiento, haga clic derecho en el icono del extremo derecho. Aparecerá un menú emergente.
2. Seleccione **Ver mis suscripciones**.
3. Seleccione uno de los siguientes pasos:
   - Haga clic en **Activar suscripción**.
   - Haga clic en **Activar código de campaña**.
4. En el cuadro de diálogo que se abre, ingrese la clave de suscripción nueva o código de campaña y haga clic en **Aceptar**.

   Consejo: Si recibió su clave de suscripción por correo electrónico, puede copiar la clave en el mensaje de correo electrónico y pegarlo en el campo.

Después de ingresar la clave de suscripción nueva, la fecha de validez de la suscripción nueva se muestra en la página **Estado de suscripción**.

Capítulo

3

Introducción

Temas:

- *Ver el estado general de mi protección*
- *Ver las estadísticas del producto*
- *Manejar las actualizaciones del producto*
- *¿Qué son los virus y otro malware?*

Este producto protege a su computadora frente a virus y otras aplicaciones dañinas

El producto analiza archivos, analiza aplicaciones y realiza actualizaciones automáticamente. No requiere de niguna acción de su parte.

Ver el estado general de mi protección

La página de **Estado** muestra un resumen breve de las funciones del producto instalado y sus estados actuales.

Para abrir la página de **Estado**:

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

La página de **Estado** se abrirá.

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

Icono de estado	Nombre del estado	Descripción
	Aceptar	Su equipo está protegido. La función está activada y funciona correctamente.
	Información	El producto le informa sobre el estado especial de una función. Por ejemplo, la función se está actualizando.
	Advertencia	Su equipo no está totalmente protegido. Por ejemplo, el producto no ha recibido actualizaciones en mucho tiempo o el estado de una función requiere de su atención.
	Error	Su equipo no está protegido. Por ejemplo, su suscripción ha caducado o una función crítica está desactivada.
	Desactivado	Una función no crítica está desactivada.

Ver las estadísticas del producto

Puede ver qué ha hecho el producto desde su instalación en la página de **Estadísticas**.

Para abrir la página de **Estadísticas**:

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

Se abrirá la página de **Estadísticas**.

- **Comprobación de la última actualización exitosa** muestra la hora de la actualización más reciente.

- **Análisis de virus y spyware** muestra cuántos archivos ha analizado y limpiado el producto desde su instalación.
- **Aplicaciones** muestra cuántos programas DeepGuard ha permitido o bloqueado desde la instalción.
- **Conexiones del cortafuegos** muestra el número de conexiones permitidas y bloqueadas desde la instalación.
- **Filtro de spam y phishing** muestra cuántos mensajes de correo electrónico ha detectado el producto como mensajes de correo electrónico válidos y como mensajes de spam.

Manejar las actualizaciones del producto

El producto actualiza automáticamente la protección.

Ver versiones de base de datos

Puede consultar la hora y los números de versiones de las actualizaciones en la página de **Actualizaciones de base de datos**.

Para abrir la página de **Actualizaciones de base de datos**:

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

   Nota: Necesita derechos de administrador para cambiar la configuración.

2. Seleccione **Otras configuraciones** > **Versiones de base de datos**.

La página de **Versiones de base de datos** muestra la fecha más reciente de la actualización de las definiciones de virus y spyware, DeepGuard y filtro de span y phishing así como sus números de versiones.

Cambiar la configuración de la banda ancha móvil

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

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

De manera predeterminada, las actualizaciones de seguridad siempre se descargan cuando está en su red de operador doméstica. Sin embargo, las actualizaciones se suspenden cuando visita la red de otro operador. Esto se debe a que los precios de las conexiones pueden variar entre los operadores, por ejemplo, en diferentes países. Podría considerar conservar esta configuración sin cambios, si desea ahorrar ancho de banda y, posiblemente, también costos durante su visita.

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

Para cambiar la configuración:

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

   Nota: Necesita derechos de administrador para cambiar la configuración.

2. Seleccione **Otras configuraciones** > **Banda ancha móvil** > **Descargar actualizaciones de seguridad**.
3. Seleccione la opción de actualización preferida para conexiones móviles.
   - **Únicamente en la red del operador doméstico**

     Las actualizaciones siempre se descargan en su red de operador doméstica. Cuando visita la red de otro operador, las actualizaciones se suspenden. Recomendamos que seleccione esta opción para mantener actualizada la seguridad del producto con los costos esperados.

- **Nunca**

  Las actualizaciones no se descargan cuando usa la banda ancha móvil.
- **Siempre**

  Las actualizaciones siempre se descargan, sin importar la red que use. Seleccione esta opción si desea asegurarse de que la seguridad de su equipo siempre esté actualizada sin importar el costo.

4. Si quiere decidir por separado cada vez que sale de la red del operador doméstico, seleccione **Preguntarme cada vez que abandono la red del operador doméstico**.

Actualizaciones de seguridad suspendidas

Las actualizaciones de seguridad pueden suspenderse cuando use banda ancha móvil fuera de su red del operador doméstica.

En este caso, puede ver el aviso de notificación de **Suspendido** en la esquina derecha inferior de su pantalla. Las actualizaciones se suspendieron debido a que los precios de las conexiones pueden variar entre los operadores, por ejemplo, en diferentes países. Puede considerar conservar sin cambios esta configuración, si desea ahorrar banda ancha y posiblemente, costos también, durante su visita. Sin embargo, si aún quiere cambiar la configuración, haga clic en enlace **Cambiar**.

Nota:

Esta función está disponible sólo en Microsoft Windows 7.

¿Qué son los virus y otro malware?

Los programas de malware son programas diseñados específicamente para provocar daños en su equipo y utilizan su equipo con fines ilícitos sin su conocimiento o para 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 su 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 un *malware* en su equipo si de pronto se vuelve muy lento y se bloquea con frecuencia.

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 manera que 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

Los spyware son programas que recopilan información personal.

El spyware puede recopilar información personal incluyendo:

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

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

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 el malware en su equipo.

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 dañar su equipo, pero puede dañarlo si se hace mal uso de él.

El riskware no es exactamente un malware. Los programas de riskware realizan algunas funciones útiles, pero potencialmente peligrosas.

Ejemplos de programas de riskware son 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, por ejemplo, VoIP (*Protocolo de voz en Internet*) .
- Software de acceso remoto como, por ejemplo, VNC,
- scareware, el cual puede intentar asustar o engañar a individuos para que compren software de seguridad falsos o
- software diseñado para evadir las verificaciones del CD o protecciones de copias.

Si ha instalado expresamente el programa y lo ha configurado correctamente, hay menos probabilidades de 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

Proteger mi equipo contra malware

Temas:

- *Cómo analizar mi equipo*
- *Cómo excluir archivos del análisis*
- *¿Cómo usar el almacén de cuarentena?*
- *¿Qué es DeepGuard?*
- *¿Qué es un cortafuegos?*
- *Bloquear el spam*

El análisis de virus y spyware protege a su equipo de programas que pueden robar su información personal, dañar el servidor o usarlo para propósitos ilegales.

De forma predeterminada, todos los tipos de malware se manejan de inmediato cuando se detectan de manera que no pueden provocar daños.

De manera predeterminada, los análisis para buscar virus y spyware en los discos duros lcales, discos extraíbles (como discos portátiles o discos compactos) y contenido descargado automáticamente. Además puede configurar que se analicen sus correos electrónicos automáticamente.

El análisis de virus y spyware también vigila de que no haya cambios en su equipo que puedan indicar *malware*. Si se detecta que cualquier sistema peligroso cambia, por ejemplo, la configuración del sistema o intenta cambiar procesos del sistema importantes, DeepGuard impide que este programa se ejecute pues es probable que sea un *malware*.

Cómo analizar mi equipo

Cuando el análisis de virus y spyware esté activado, éste analiza automáticamente su computadora para buscar archivos dañinos. También puede analizar archivos manualmente y configurar análisis programados.

Le recomendamos que mantenga el análisis de virus y spyware activado en todo momento. Analice sus archivos manualmente cuando desee asegurarse de que no hay archivos dañinos en su computadora o si desea analizar archivos que ha excluido del análisis en tiempo real.

Al configurar un análisis programado, el análisis de virus y spyware retira los archivos dañinos de su computadora en horas específicas.

Analizar archivos automáticamente

El análisis en tiempo real protege a su equipo mediante el análisis de todos los archivos cuando se accede a ellos y mediante el bloqueo al acceso de los archivos que contienen *malware*.

Cuando su computadora intenta acceder a un archivo, el análisis en tiempo real analiza el archivo para buscar malware antes de permitirle a su computadora el acceso al archivo. Si el análisis en tiempo real detecta cualquier contenido dañino, lo pone bajo cuarentena antes de que cause algún daño.

¿El análisis en tiempo real afecta el rendimiento de mi computadora?

Por lo general, 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.

Los archivos que tardan más tiempo en analizarse son los siguientes:

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

  Nota: De manera predeterminada, los archivos comprimidosno se analizan.

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

- tiene una computadora que no reúne los requisitos del sistema, o bien
- accede a muchos archivos al mismo tiempo. Por ejemplo, cuando abre un directorio que contiene muchos archivos que necesitan analizarse.

Activar o desactivar el análisis en tiempo real

Mantenga activado el análisis en tiempo real para detener el *malware* antes de que haga daño a su computadora.

Para activar o desactivar el análisis en tiempo real:

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

   Nota: Debe tener derechos administrativos para desactivar las funciones de seguridad.

3. Activar o desactivar el **Análisis de virus y spyware**.
4. Haga clic en **Cerrar**.

Procesar archivos dañinos automáticamente

El análisis en tiempo real puede procesar archivos dañinos automáticamente sin hacerle preguntas.

Para dejar que el análisis en tiempo real procese los archivos dañinos automáticamente:

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

   Nota: Necesita derechos de administrador para cambiar la configuración.

2. Seleccione **Seguridad del equipo** > **Análisis de virus y spyware**.
3. Seleccione **Procesar archivos dañinos automáticamente**.

Si usted selecciona no procesar archivos dañinos automáticamente, el análisis en tiempo real le pregunta qué desea hacer con el archivo dañino cuando se detecta.

Procesar el spyware

El análisis de virus y spyware bloquea el spyware inmediatamente cuando intenta iniciarse.

Antes de que una aplicación de spyware pueda iniciarse, el producto la bloquea y permite que usted decida qué desea hacer con ella.

Seleccione una de las siguientes acciones cuando se detecte un spyware:

Acción a realizar	Qué ocurre con el spyware
Procesar automáticamente	Dejar que el producto decida la mejor acción a realizar en base al spyware que se detectó.
Poner spyware bajo cuarentena	Mover el spyware a cuarentena donde no pueda hacer daño a su computadora.
Borrar el spyware	Retirar de su computadora todos los archivos relacionados con spyware.
Solo bloquear el spyware	Bloquear el acceso al spyware pero dejarlo en su computadora.
Excluir el spyware del análisis	Permitir que spyware se ejecute y excluir del análisis en el futuro.

Procesar el riskware

El análisis de virus y spyware bloquea el riskware inmediatamente cuando intenta iniciarse.

Antes de que una aplicación de riskware pueda iniciarse, el producto la bloquea y deja que usted decida qué desea hacer con ella.

Seleccione una de las siguientes acciones a realizar cuando se detecte un riskware:

Acción a realizar	Qué ocurre con el riskware
Solo bloquear el riskware	Bloquear el acceso al riskware pero dejarlo en su computadora.
Poner el riskware bajo cuarentena	Mover el riskware a la cuarentena donde no pueda hacer daño a su computadora.
Borrar el riskware	Retirar de su computadora todos los archivos relacionados con riskware.
Excluir el riskware del análisis	Permitir que el riskware se ejecute y excluirlo del análisis en el futuro.

Retirar las cookies de rastreo automáticamente.

Al retirar las cookies de rastreo, evita que los sitios web puedan rastrear los sitios que usted visita en Internet.

Las cookies de rastreo son archivos pequeños que permiten a los sitios web registrar sitios en Internet que usted visita. Siga estas instrucciones para mantener su computadora libre de cookies de rastreo.

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

   Nota: Necesita derechos de administrador para cambiar la configuración.

2. Seleccione **Seguridad del equipo** > **Análisis de virus y spyware**.
3. Seleccione **Retirar cookies de rastreo**.
4. Haga clic en **Aceptar**.

Analizar archivos manualmente

Puede analizar sus archivos manualmente, por ejemplo, cuando conecta un dispositivo externo a su computadora, para asegurarse de que no contiene ningún malware.

Iniciando el 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 completo de su equipo.

Para comenzar a analizar manualmente su equipo:

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

   Después se mostrarán las opciones de análisis.

2. Seleccione el tipo de análisis

   Seleccione **Cambiar configuración del análisis** para optimizar la manera en que el análisis manual analiza la computadora para buscar virus y otras aplicaciones dañinas.

3. Si seleccionó **Elegir qué analizar**, se abrirá una ventana donde podrá seleccionar qué ubicación 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.

Los siguientes son los diferentes tipos de análisis:

Tipo de análisis	Qué se analiza	Cuando usar este tipo
Buscar virus y spyware	Analiza partes de su equipo para buscar spyware y riskware.	Este tipo de análisis es más rápido que un análisis completo. Busca sólo en partes del sistema que contienen archivos de programa instalados. Este tipo de análisis se recomienda si desea comprobar que su equipo está limpio, ya que es capaz de detectar y eliminar eficientemente todo el malware activo en su equipo.
Análisis completo del equipo	Se analiza todo su equipo (incluyendo los discos duros internos y externos) para buscar virus, spyware y riskware.	Cuando desee estar completamente seguro de que no exista malware ni riskware en su equipo. Este tipo de análisis toma más tiempo en terminar. Combina el análisis de malware rápido y el análisis del disco duro. También revisa los elementos que posiblemente estén ocultos por un rootkit.

Tipo de análisis	Qué se analiza	Cuando usar este tipo
Seleccione qué desea analizar	Analiza un archivo, carpeta o unidad específica para buscar virus, spyware y riskware.	Cuando sospeche que una ubicación específica de su equipo contenga malware, por ejemplo, la ubicación contiene descargas de fuentes potencialmente peligrosas, tales como redes de uso compartido de archivos entre pares. El tiempo que tarda un análisis depende del tamaño del destino que desea analizar. El análisis termina rápido si, por ejemplo, analiza una carpeta que contiene sólo algunos archivos pequeños.
Análisis de rootkit	Ubicaciones de seguridad importantes donde un elemento sospechoso podría implicar un problema de seguridad. Analiza para buscar archivos, carpetas, unidades o procesos ocultos.	Cuando sospeche que puede tener un rootkit instalado en su equipo. Por ejemplo, si se detectó un malware recientemente en su equipo, y usted desea asegurarse de que no se instaló un rootkit.

Analizar en 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 derecho.
2. En el menú contextual, seleccione **Buscar virus en carpetas**. (El nombre de la opción dependerá de si analiza un disco, una carpeta o un archivo).
   Se abrirá ventana del **Asistente de análisis** y se iniciará el análisis.

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

Seleccionar archivos a analizar

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

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

   Nota: Necesita derechos de administrador para cambiar la configuración.

2. Seleccione **Otras configuraciones** > **Análisis manual**.
3. En **Opciones de análisis**, seleccione de las siguientes configuraciones:

Analizar únicamente los tipos de archivos conocidos	Para analizar sólo los tipos de archivos con mayores probabilidades de estar infectados, por ejemplo, los archivos ejecutables. Si selecciona esta opción, el análisis también será 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 dentro de archivos comprimidos	Para analizar archivos y carpetas comprimidas.

Usar heurística avanzada	Usar toda la heurística avanzada durante el análisis es mejor para detectar malware nuevo o desconocido. **Nota:** Si selecciona esta opción, el análisis toma más tiempo y puede resultar en más falsos positivos (archivos inofensivos se reportan como sospechosos).

4. Haga clic en **Aceptar**.

Nota: Los archivos excluidos en la lista de elementos excluidos no se analizan incluso si usted los seleccionó para analizarlos aquí.

Qué hacer cuando se detecten archivos dañinos

Seleccione cómo desea procesar los archivos dañinos cuando se detecten.

Para seleccionar la acción a seguir cuando se detecta un contenido dañino durante el análisis manual:

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

   Nota: Necesita derechos de administrador para cambiar la configuración.

2. Seleccione **Otras configuraciones** > **Análisis manual**.
3. En **Cuando se detecta un virus o spyware**, seleccione una de las siguientes opciones:

Opción	Descripción
Preguntarme (predeterminado)	Puede seleccionar la acción a realizar para cada elemento que se detecte durante el análisis manual.
Limpiar los archivos	El producto intenta desinfectar automáticamente los archivos infectados que se detectan durante el análisis manual. **Nota:** Si el producto no puede limpiar el archivo infectado, éste se pone bajo cuarentena (excepto cuando se encuentra en una red o unidades extraíbles) para que así no haga daño a la computadora.
Poner los archivos bajo cuarentena	El producto pone cualquier archivo dañino que se detecte durante el análisis manual bajo cuarentena donde no puede hacer daño a la computadora.
Borrar los archivos	El producto borra cualquier archivo dañino que se detecte durante el análisis manual.
Sólo reportarlo	El produce deja cualquier archivo dañino que se detecte durante el análisis manual en su estado actual y registra la detección en el reporte del análisis. **Nota:** Si se desactiva el análisis en tiempo real, cualquier malware aún es capaz de dañar la computradora si selecciona esta opción.

Nota: Cuando se detectan archivos dañinos durante el análisis programado, estos se limpian automáticamente.

Programar un análisis

Configure su computadora para que analice y retire los virus y otras aplicaciones dañinas automáticamente cuando no la usa o configúrela para que ejecute una análisis periódicamente para asegurarse de que su computadora está limpia.

Para programar un análisis:

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

   Nota: Necesita derechos de administrador para cambiar la configuración.

2. Seleccione **Otras configuraciones** > **Análisis programado**.
3. Activar **Análisis programado**.
4. Seleccione cuándo le gustaría que iniciara el análisis.

Opción	Descripción
Diario	Analizar la computadora todos los días.
Semanal	Analizar la computadora en días seleccionados de la semana. Seleccione los días en la lista.
Mensual	Analizar la computadora en días seleccionados del mes. Para seleccionar los días: 1. Seleccione entre las opciones de **Día**. 2. Seleccione el día del mes en la lista situada junto al día seleccionado.

5. Seleccione cuándo desea iniciar el análisis en los días seleccionados.

Opción	Descripción
Inicio	Inicie el análisis en la hora especificada.
Tras un periodo de inactividad de	Inicie el análisis después de no haber usado la computadora por un periodo de tiempo especificado.

El análisis programado usa la configuración del análisis manual al analizar la computadora, excepto que analiza archivos en cada ocasión y limpia los archivos dañinos automáticamente.

Analizar mensajes de correo electrónico

El análisis de correo electrónico lo protege de recibir archivos dañinos en mensajes de correo electrónico que se le envían.

El análisis de virus y spyware debe activarse para analizar los mensajes de correo electrónico para buscar virus.

Para activar el análisis de correo electrónico:

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

   Nota: Necesita derechos de administrador para cambiar la configuración.

2. Seleccione **Seguridad del equipo** > **Análisis de virus y spyware**.
3. Seleccione **Retirar archivos adjuntos dañinos de correo electrónico**.
4. Haga clic en **Aceptar**.

¿Cuándo se analizan los mensajes de correo electrónico y los documentos adjuntos?

El análisis de virus y spyware puede quitar el contenido dañino de los correos electrónicos que reciba.

El análisis de virus y spyware retira los mensajes de correo electrónico dañinos que se reciben en programas de correo electrónico tales como Microsoft Outlook y Outlook Express, Microsoft Mail o Mozilla Thunderbird. Analiza los mensajes y archivos adjuntos de correo electrónico descodificados cada vez que su programa de correo electrónico los recibe de un servidor de correo que usa el protocolo POP3.

El análisis de virus y spyware no puede analizar mensajes de correo electrónico en correo web, el cual incluye aplicaciones de correo electrónico que se ejecutan en su navegador de Internet tales como Hotmail, Yahoo! mail o Gmail. Aún así está protegido contra *virus* incluso si no retira los archivos adjuntos dañinos o si está usando un correo web. Cuando abra los archivos adjuntos del correo electrónico, el análisis en tiempo real retira cualquier archivo adjunto dañino antes de que causen daños.

Nota: El análisis en tiempo real únicamente protege su computadora mas no a sus amigos. El análisis en tiempo real no analiza los archivos adjuntos a menos que usted los abra. Esto significa que si está usando un correo web y reenvió un mensaje antes de abrir el archivo adjunto, usted puede reenviar un mensaje correo electrónico infectado a sus amigos.

Ver resultados del análisis

El historial de virus y spyware muestra todos los archivos dañinos que el producto ha detectado.

Algunas veces, el producto no puede realizar la acción que ha seleccionado cuando se detecta un elemento dañino. Por ejemplo, si seleccionó limpiar los archivos y un archivo no puede limpiarse, el producto lo pone bajo 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 de administrador para cambiar la configuración.

2. Seleccione **Seguridad del equipo** > **Análisis de virus y spyware**.
3. Haga clic en **Ver historial de remoción**.

El historial de virus y spyware muestra la siguiente información:

- fecha y hora cuando se detectó el archivo dañino,
- el nombre del malware y su ubicación en la computadora y
- la acción realizada.

Cómo excluir archivos del análisis

Algunas veces puede desear excluir algunos archivos o aplicaciones del análisis. Los elementos excluidos no se analizan a menos que los retire de la lista de elementos excluidos.

Nota: Las listas de exclusión son elementos que no se incluyen en el análisis en tiempo real y manual. Por ejemplo, si excluye un archivo del análisis en tiempo real, éste se analiza durante el análisis manual a menos que lo excluya también del análisis manual.

Excluir tipos de archivos

Cuando excluya archivos por su tipo, los archivos con las extensiones especificadas no se analizarán para buscar contenido dañino.

Para añadir o retirar tipos de archivo que desee excluir:

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

   Nota: Necesita derechos de administrador para cambiar la configuración.

2. Seleccione si desea excluir el tipo de archivo del análisis en tiempo real o manual:

   - Seleccione **Seguridad del equipo** > **Análisis de virus y spyware** para excluir el tipo de archivo del análisis en tiempo real.

- Seleccione **Otras configuraciones** > **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 pestaña de **Tipos de archivos**.
   b) Seleccione **Excluir archivos con las extensiones**.
   c) Ingrese una extensión de archivo que identifica el tipo de archivos que desea excluir, en el campo situado a un lado del botón **Añadir**.

      Para especificar los archivos que no tienen extensión, escriba '.'. Puede usar el comodín '?' para representar cualquier carácter o '*' para representar cualquier número de caracteres.

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

Los tipos de archivos seleccionados se excluyen del análisis en el futuro.

Excluir archivos por ubicación

Cuando excluya archivos por ubicación, los archivos en unidades o carpetas especificadas no se analizan para buscar contenido dañino.

Para añadir o retirar ubicaciones de archivos que desea excluir:

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

   Nota: Necesita derechos de administrador para cambiar la configuración.

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

      Nota: Algunas unidades puede ser unidades extraíbles como por ejemplo un CD, DVD o unidades de 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 de virus.
6. Haga clic en **Aceptar** para cerrar el cuadro de diálogo de **Excluir del análisis**.
7. Haga clic en **Aceptar** para aplicar la nueva configuración.

Los archivos, unidades o carpetas seleccionadas se excluyen del análisis en el futuro.

Ver aplicaciones excluídas

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

Si el análisis en tiempo real o manual detecta una aplicación que se comporta como spyware o riskware pero usted sabe que es segura, puede excluirla del análisis a fin de que el producto no le advierta más sobre ella.

Nota: Si la aplicación se comporta como un virus u otro software dañino, no puede excluirse.

No puede excluir aplicaciones directamente. Las aplicaciones nuevas aparecen en la lista de exclusión únicamente si usted las excluye durante el análisis.

Para ver las aclicaciones que se excluyen del análisis:

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

   Nota: Necesita derechos de administrador para cambiar la configuración.

2. Seleccione si desea ver las aplicaciones que se han excluido del análisis en tiempo real o manual:
   - Seleccione **Computadora** > **Análisis de virus y spyware** para ver las aplicaciones que se han excluido del análisis en tiempo real.
   - Seleccione **Computadora** > **Análisis manual** para ver las aplicaciones que se han excluido del análisis manual.
3. Haga clic en **Excluir archivo del análisis**.
4. Seleccione la pestaña **Aplicaciones**.

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

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

¿Cómo usar el almacén de cuarentena?

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

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

Puede poner en cuarentena el *malware*, *spyware* y *riskware* para eliminar el riesgo de daños. Puede restaurar aplicaciones o archivos en cuarentena posteriormente si los necesita.

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 sobre los elementos en cuarentena:

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

   Nota: Necesita derechos de administrador para cambiar la configuración.

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

   Puede clasificar el contenido ya sea por nombre de malware o ruta de archivo.

   Una lista de los primeros 100 elementos se muestra con el tipo de los elementos en cuarentena, su nombre y la ruta donde se instalaron los archivos.
5. Para ver más información sobre un elemento bajo cuarentena, haga clic en el icono situado a un lado del elemento en 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 regresan a su ubicación original en el equipo.

Para restaurar los elementos en cuarentena:

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

   Nota: Necesita derechos de administrador para cambiar la configuración.

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

¿Qué es DeepGuard?

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

DeepGuard bloquea *virus*, *gusanos* y otras aplicaciones dañinas nuevas y desconocidas que intentan hacer cambios en su computadora e impide que aplicaciones sospechosas accedan a Internet.

Cuando DeepGuard detecta una aplicación nueva que intenta hacer cambios potencialmente dañinos al sistema, permite que la aplicación se ejecute en una zona segura. En la zona segura, la aplicación no puede dañar su computadora. DeepGuard analiza los cambios que intentó realizar la aplicación y en base a esto, la probabilidad de que la aplicación sea un *malware*. Si es muy probable que la aplicación es un *malware*, DeepGuard la bloquea.

Los cambios potencialmente dañinos al sistema que detecta DeepGuard incluyen:

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

Activar o desactivar DeepGuard

Mantenga DeepGuard activado para evitar que aplicaciones sospechosas realicen cambios potencialmente dañinos al sistema de su computadora.

Si tiene Windows XP, asegúrese de que el Service Pack 2 esté instalado antes de activar DeepGuard.

Para activar o desactivar DeepGuard:

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

   Nota: Debe tener derechos administrativos para desactivar las funciones de seguridad.

3. Activar o desactivar **DeepGuard**.
4. Haga clic en **Cerrar**.

Permitir aplicaciones que DeepGuard ha bloqueado

Usted puede controlar qué aplicaciones desea que DeepGuard permita y bloquee.

Algunas veces DeepGuard puede bloquear una aplicación segura para evitar que ésta se ejecute, incluso si desea usar la aplicación y sabe que es segura. Esto ocurre debido a que la aplicación intenta realizar cambios al sistema que pudieran ser potencialmente dañinos. Es posible que también usted haya bloqueado accidentalmente la aplicación cuando aparece una ventana emergente de DeepGuard.

Para permitir la aplicación que DeepGuard ha bloqueado:

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

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

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

DeepGuard permite que la aplicación haga cambios al sistema de nuevo.

Use DeepGuard en el modo de compatibilidad

Para mayor protección, DeepGuard modifica temporalmente los programas en curso. Algunos programas revisan que no estén corruptos o modificados y pueden no ser compatibles con esta función. Por ejemplo, los juegos en línea con herramientas antitrampas revisan que estos no se hayan modificado de alguna manera cuando se ejecutan. 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 de administrador para cambiar la configuración.

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

Qué hacer con las advertencias sobre comportamiento sospechoso

DeepGuard monitorea las aplicaciones que no son de confianza. Si una aplicación monitoreada intenta acceder a Internet, intenta cambiar su sistema o tiene un comportamiento sospechoso, DeepGuard la bloquea.

Cuando seleccione **Mostrar advertencia sobre comportamiento sospechoso** en la configuración de DeepGuard, este le notifica cuando detecta una aplicación potencialmente dañina o cuando inicia una aplicación que tiene una reputación desconocida.

Para decidir qué desea hacer con la aplicación que DeepGuard ha bloqueado:

1. Haga clic en **Detalles** para obtener más información sobre el programa.
   La sección de detalles muestra:
   - la ubicación de la aplicación,
   - la reputación de la aplicación en la Red de protección en tiempo real y
   - qué tan común es la aplicación.
2. Decida si confía en la aplicación que DeepGuard ha bloqueado:
   - Seleccione **Confío en la aplicación. Dejar que continúe.** si no desea bloquear la aplicación.

     La aplicación muy probablemente es segura si:
     - DeepGuard bloqueó la aplicación como resultado de algo que usted hizo.
     - reconoce la aplicación, o bien
     - recibió la aplicación de una fuente segura.
   - Seleccione **No confió en la aplicación. Mantenerla bloqueada** si desea mantener bloqueada la aplicación.

     La aplicación muy probablamente es insegura si:
     - la aplicación es poco común,
     - la aplicación tiene una reputación desconocida, o bien
     - desconoce la aplicación.
3. Si desea enviar una aplicación sospechosa para analizarla:
   a) Haga clic en **Reportar la aplicación a F-Secure**.
   El producto muestra las condiciones del envío.
   b) Haga clic en **Aceptar** si acepta las condiciones y desea enviar una muestra.

   Le recomendamos que envíe una muestra cuando:
   - DeepGuard bloquea una aplicación que usted sabe es segura o bien
   - sospecha que la aplicación puede ser un *malware*.

¿Qué es un cortafuegos?

El *cortafuegos* impide que intrusos y aplicaciones dañinas ingresen a su computadora desde Internet.

El cortafuegos solo permite conexiones de Internet seguras de su computadora y bloquea intrusiones provenientes de Internet.

Activar o desactivar el cortafuegos

Mantenga activado el cortafuegos para impedir que intrusos tengan acceso a su computadora.

Para activar o desactivar el cortafuegos:

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

   Nota: Debe tener derechos administrativos para desactivar las funciones de seguridad.

3. Activar o desactivar el **Cortafuegos**.

   Nota: Su computadora no está completamente protegida cuando desactiva las funciones de seguridad.

4. Haga clic en **Cerrar**.

Le recomendamos que no tenga desactivado el *cortafuegos*. Si lo hace, su computadora será vulnerable a ataques de red. Si una aplicación deja de funcionar debido a que no puede conectarse a Internet, cambie la *configuración del cortafuegos* en vez de desactivar el *cortafuegos*.

Cambiar la configuración del cortafuegos

Cuando se active el cortafuegos, este restringe el acceso hacia y desde su computadora. Algunas aplicaciones pueden requerir que les permita pasar por el cortafuegos para poder funcionar adecuadamente.

El producto utiliza el cortafuegos de Windows para proteger su computadora.

Para cambiar la configuración del cortafuegos de Windows:

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

   Nota: Necesita derechos de administrador para cambiar la configuración.

2. Seleccione **Seguridad del equipo** > **Cortafuegos**.
3. Haga clic en la configuración de **Cambiar cortafuegos de Windows**.

   Nota: Necesita derechos administrativos para editar la configuración.

Para másí nformación sobre el cortafuegos de Windows, consulte la documentación de Microsoft Windows.

Impida que aplicaciones descarguen archivos dañinos

Puede impedir que las aplicaciones en su computadora descarguen archivos dañinos de Internet.

Algunos sitios web contienen ataques y otros archivos dañinos que pueden dañar su computadora. Con la protección de red avanzada, puede impedir que cualquier aplicación descargue archivos dañinos antes de que lleguen a su computadora.

Para impedir que cualquier aplicación descargue archivos dañinos:

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

   Nota: Necesita derechos de administrador para cambiar la configuración.

2. Seleccione **Seguridad del equipo** > **Cortafuegos**.
3. Seleccione **No permitir que aplicaciones descarguen archivos dañinos**.

Nota: Esta configuración es efectiva aún si desactiva el cortafuegos.

Bloquear el spam

El filtro de spam y phishing protege su computadora contra mensajes de correo electrónico de *spam* y *phishing*.

Un mensaje de correo electrónico se considera como *spam* si se envió como parte de una colección más grande mensajes, todos con contenido casi idéntico y si los destinatarios no han dado permiso comprobable para que se envíe el mensaje. Los mensajes de *spam* y *phishing* a menudo tienden a inundarlos mensajes de correo electrónico deseables.

Use el filtro de spam y phishing para detectar los mensajes de spam y phishing y enviarlos a la carpeta de *spam*.

Activar o desactivar el filtro de spam y phishing

Mantenga activado el filtro de spam y phishing para retirar los mensajes de spam y phishing de su bandeja de entrada.

Para activar o desactivar el filtro de spam y phishing:

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

   Nota: Debe tener derechos administrativos para desactivar las funciones de seguridad.

3. Activar o desactivar **Filtro de spam y phishing**.
4. Haga clic en **Cerrar**.

Protección contra intentos de phishing

El filtro de spam y phishing protege su computadora contra intentos de *phishing* que usan mensajes de correo electrónico falsos que parecen provenir de negocios legítimos, para así robar su información personal.

Estos mensajes que parecen auténticos están diseñados para engañarlo a que envíe sus datos personales, tales como números de cuenta bancaria, contraseñas y números de tarjetas de crédito y seguridad social. No confíe en el contenido de cualquiera de estos mensajes de correo electrónico que detecte el filtro de spam y phishing.

Cuando reciba un mensaje de correo electrónico que se identifique como un intento de *phishing*, éste se transfiere automáticamente a la carpeta de *spam*.

En Microsoft Outlook, Outlook Express y Windows Mail, las reglas de *phishing* se crean automáticamente. Si usa otro programa de correo electrónico, usted debe crear las reglas de filtrado manualmente.

Configurar mis programas de correo electrónico para que filtren spam

Puede crear una carpeta de *spam* y una de *phishing*, así como reglas de filtrado, en el programa de correo electrónico para filtrar el *spam*.

El filtro de correo electrónico automáticamente crea una carpeta de *spam* y una de *phishing* así como las reglas de filtrado en Microsoft Outlook, Microsoft Outlook Express y Windows Mail (en Windows Vista). Si utiliza otro programa de correo electrónico, deberá crear las carpetas y las reglas de filtrado manualmente. Si tiene varias cuentas de correo electrónico, deberá crear las reglas de filtrado en cada una de las cuentas de forma independiente.

Nota: El filtro de *Spam* y *phishing* es compatible únicamente con el protocolo POP3. Los programas de correo electrónico ubicados en la red u otros protocolos no son compatibles.

¿Cómo trabajan juntas mis propias reglas y las del filtro de correo electrónico?

El filtro de correo electrónico filtra los mensajes de correo en base a sus propias reglas de filtrado. No filtrará los mensajes de correo electrónico que cumplan con una regla que usted ha creado. Por ejemplo, si ha creado una regla que filtra todos los mensajes de correo de una tienda en línea a una carpeta llamada tiendas en línea, tanto los mensajes de confirmación y el material de publicidad de esa tienda en línea se moverán desde su bandeja de entrada hasta la carpeta de tiendas en línea.

Esta sección contiene instrucciones sobre cómo se puede crear la carpeta de spam y la regla de filtrado en los programas de correo electrónico de Microsoft, Netscape, Mozilla Thunderbird y Eudora. También puede utilizar estas instrucciones para crear reglas de filtrado similares en otros programas de correo electrónico.

Programas de correo electrónico de Microsoft

El filtro de correo eléctrico crea carpetas para mensajes de correo electrónico de *spam* y *phishing* y filtra reglas automáticamente en Microsoft Outlook, Microsoft Outlook Express y Windows Mail.

Nota: El filtrado automático puede no funcionar con las cuentas de correo electrónico que se han creado usando la applet de Correo que se encuentra en el panel de control de Windows. Si recibe mensajes de spam y phishing después de activar el filtro de correo electrónico, use el asunto de mensaje `[SPAM]` para filtrar los mensajes de spam y phishing.

Bloquear spam en Mozilla Thunderbird y Eudora OSE

Título de búsqueda: Crear una regla de filtrado de spam en Mozilla Thunderbird y Eudora OSE.

Para filtrar los mensajes de correo electrónico de *spam* y phishing, debe crear una carpeta de spam y la regla de filtrado.

Para crear la regla de filtrado de *spam*:

1. Haga clic derecho en **Carpetas locales** y seleccione **Carpeta nueva**.
2. Ingrese `spam` como el nombre de la nueva carpeta.
3. Seleccione **Herramientas** > **Filtros de mensajes**.
4. Haga clic en **Nuevo**.
5. Ingrese `spam` como el **Nombre del filtro**.
6. Cree una regla de comparación para detectar mensajes de spam:
   a) En las opciones de filtrado asegúrese de seleccionar **Asunto** y **contiene**.
   b) Ingrese `[SPAM]` en el tercer filtro.
7. Cree una acción que mueva el spam a la carpeta de spam.
   a) En la primera lista, seleccione **Mover mensaje a**.
   b) Seleccione la carpeta de *spam* en la segunda lista desplegable.
8. Haga clic en **Aceptar** para guardar los cambios.
9. Cierre el diálogo de **Filtros de mensajes**.

Ahora ha creado la regla de filtrado de *spam*. A partir de este momento, los mensajes de correo electrónico de *spam* se filtrarán a la carpeta de *spam*.

Bloquear spam en Opera

Título de búsqueda: Crear una regla de filtrado de spam en Opera.

Para filtrar los mensajes de correo electrónico de *spam* y phishing, debe crear una carpeta de spam y la regla de filtrado.

Nota: Los pasos aquí explicados aplican a la versión 11 de Opera. Los pasos para otras versiones pueden variar un poco.

Para crear una regla de filtrado de *spam*:

1. Abra la vista **Opera Mail**.
2. Haga clic derecho en su carpeta de *Spam* predeterminada y seleccione **Propiedades**.
3. Haga clic en **Añadir regla**.
4. Cree una regla para mover un mensaje de correo electrónico al filtro de *spam*:
   a) En las opciones de filtrado asegúrese de seleccionar **Asunto** y **contiene**.
   b) Ingrese `[SPAM]` en el tercer campo.
5. Haga clic en **Cerrar** para confirmar la nueva regla de filtrado de *spam*.

Ahora ha creado la regla de filtrado de *spam*. A partir de este momento, los mensajes de correo electrónico de *spam* se filtrarán a la carpeta de *spam*.

Capítulo

5

Uso seguro de Internet

Temas:

- *¿Cómo ejecutar tareas comunes?*
- *Cómo proteger las distintas cuentas de usuario*
- *¿Qué es la protección de navegación?*
- *Navegación segura*
- *Cómo programar el tiempo de navegación*
- *Ver estadísticas*

Información sobre los pasos iniciales del producto.

Este producto le ayuda a explorar Internet con seguridad. Además de protegerlo de software y sitios web dañinos, también puede restringir el tipo de contenido que pueden ver las distintas cuentas de usuario.

El producto usa las cuentas de usuario de Windows para controlar la configuración de cada persona que usa la computadora. Solamente quienes poseen derechos de acceso de administración pueden cambiar la configuración del producto para las diferentes cuentas de usuario de Windows. Recomendamos que configure una cuenta de usuario de Windows independiente para cada persona que use su computadora. Por ejemplo, los usuarios invitados no deben tener derechos de acceso de administración para sus cuentas de usuario de Windows.

¿Cómo ejecutar tareas comunes?

Puede ver lo que puede hacer con el producto y ejecutar tareas comunes en la página de **Tareas**.

Para abrir la página de **Tareas**:

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

La página de **Tareas** se abrirá.

Cómo proteger las distintas cuentas de usuario

Para brindarle la mejor protección contra amenazas en línea, debe emplear cuentas de usuario de Windows independientes para las personas que usen su computadora.

El producto le permite usar diferentes configuraciones para cada cuenta de usuario de Windows que tenga configurada en su computadora. Solo los usuarios que tienen acceso de administrador pueden cambiar la configuración del producto para otras cuentas de usuarios. Otras personas, con excepción de los administradores, solo deben contar con derechos de acceso normal, por lo que no pueden cambiar la configuración que usted definió para ellas.

Crear y editar cuentas de usuario de Windows

Puede obtener acceso a la configuración de las cuentas de usuario de Windows desde el producto.

Para crear o editar cuentas de usuario de Windows:

1. En la página principal, haga clic en **Herramientas**.
2. Haga clic en **Crear cuenta nueva** o **Editar cuentas de usuario**.
   Esto abre la configuración de cuentas de usuario en Windows.
3. Complete la información necesaria para crear o editar la cuenta de usuario.

¿Qué es la protección de navegación?

La protección de navegación ayuda a evaluar la seguridad de los sitios web que visita y evita que acceda involuntariamente a sitios web dañinos.

La protección de navegación es un complemento del navegador que le muestra las clasificaciones de seguridad de los sitios web enumerados en los resultados del motor de búsqueda. Al ayudarle a evitar sitios web que contienen amenazas de seguridad, tales como malware (virus, gusanos, troyanos) y phishing, las clasificaciones de seguridad de la protección de navegación le ayudan a evitar las amenazas más recientes de Internet que aún no son reconocidas por los programas de antivirus tradicionales.

Hay cuatro clasificaciones de seguridad posibles para los sitios web: seguro, sospechoso, dañino y desconocido. Estas clasificaciones de seguridad se basan en información de varias fuentes, como socios de F-Secure, y clasificaciones aportadas por otros usuarios de la protección de navegación.

Cómo activar o desactivar la protección de navegación

Cuando la protección de navegación está activada se le bloqueará el acceso a sitios web peligrosos.

Para activar o desactivar la protección de navegación:

1. En la página principal, haga clic en **Usuarios**.
2. Seleccione la cuenta de usuario de Windows que desea editar y, a continuación, haga clic en el conmutador junto a **Protección de navegación**.
   La protección de navegación ahora estará activada o desactivada para este usuario, según la configuración anterior.
3. Si su navegador está abierto, vuelva a iniciarlo para aplicar la configuración modificada.

Clasificación de seguridad de la protección de navegación

La protección de navegación muestra las clasificaciones de seguridad de los sitios web en los resultados del motor de búsqueda.

Los iconos codificados con colores muestran la clasificación de seguridad del sitio actual (en la barra de herramientas). La clasificación de seguridad de cada enlace en los resultados del motor de búqueda también se muestra con los mismos iconos. Se usan cuatro diferentes iconos codificados con colores:

- Verde indica que la página es segura.
- Amarillo indica que la página es sospechosa. El análisis de seguridad de la página indica que es segura, no obstante, muchos usuarios le han dado una clasificación de seguridad baja.
- Rojo indica que la página es dañina.
- Gris indica que la página no se ha analizado y actualmente no hay información disponible para ella.

Las clasificaciones de seguridad están disponibles en los siguientes sitios de búsqueda:

- Google
- MSN Live
- Yahoo

Dependiendo de la configuración de la protección de navegación, es posible que pueda visitar los sitios web que se clasifican como peligrosos. Los sitios web se bloquean automáticamente o sólo se le notifica sobre un posible riesgo.

Mostrar clasificaciones de los enlaces web

La clasificación de la protección de navegación puede aparecer en los resultados del motor de búsqueda.

Para definir dónde mostrar las clasificaciones de la protección de navegación:

1. En la página principal, haga clic en **Usuarios**.
2. Seleccione la cuenta de usuario de Windows que desea editar y, a continuación, haga clic en **Configuración** junto a **Protección de navegación**.
   Se abre el cuadro de diálogo de configuración de **Protección de navegación**.
3. En **Mostrar clasificaciones**, seleccione o despeje **Resultados de motor de búsqueda (Google, Yahoo)**.
   Cuando selecciona esta opción, las clasificaciones de la protección de navegación se mostrarán en el listado de sitios de los motores de búsqueda (Google, Yahoo, etc.).
4. Haga clic en **Aceptar**.

Las clasificaciones de seguridad se mostrarán según la configuración que seleccionó.

Consejo: Haga clic en **Resumen de seguridad de este sitio web** en la ventana emergente de la clasificación de seguridad para ir al portal de la protección de navegación, donde encontrará más detalles sobre el sitio web y en qué se basa la clasificación de seguridad.

Cómo clasificar los sitios web

Puede clasificar cualquier sitio web al que accede como seguro o peligroso.

Para clasificar un sitio web:

1. Seleccione **Notificarme** del menú de protección de navegación del navegador.
   Esto abre el cuadro de diálogo **Notificarme**.
2. Seleccione una clasificación para dar su opinión sobre la seguridad del sitio web (**Es seguro de usar**, **Es dañino de usar** o bien **No tengo opinión**).
3. Haga clic en **Aceptar**.
   Esto abrirá el cuadro de diálogo para la confirmación de la clasificación.

   Consejo: Seleccione la opción **No mostrar este mensaje de nuevo** si no desea ver el cuadro de diálogo de confirmación cuando clasifique sitios web en el futuro.

4. Haga clic en **Aceptar**.

Su clasificación se ha enviado a la información de análisis y clasificación que se reúne para ese sitio.

Protección contra contenido dañino

La protección de navegación bloquea el acceso a sitios web peligrosos en base a la configuración seleccionada.

Para seleccionar cuándo bloquear el acceso a un sitio web:

1. En la página principal, haga clic en **Usuarios**.
2. Seleccione la cuenta de usuario de Windows que desea editar y, a continuación, haga clic en **Configuración** junto a **Protección de navegación**.
   Se abre el cuadro de diálogo de configuración de **Protección de navegación**.
3. Seleccione **Sitios web calificados como peligrosos** para bloquear el acceso a los sitios web calificados como peligrosos.
4. Haga clic en **Aceptar**.

La protección de navegación bloquea el acceso a los sitios web de acuerdo con la configuración seleccionada.

Qué hacer cuando se bloquea un sitio web

Una página de bloqueo de la protección de navegación aparece cuando intenta acceder a un sitio que se clasificó como peligroso.

Cuando aparece una página de bloqueo de la protección de navegación:

1. Haga clic en **Página principal** para ir a su página principal sin tener acceso al sito web peligroso.
   Le recomendamos ampliamente esta acción.

   Consejo: Haga clic en **Resumen de seguridad de este sitio web** para ir al portal de protección de navegación, donde encontrará más detalles sobre el sitio web y en qué se basa la clasificación de seguridad.

2. Si desea entrar al sitio web de todos modos, haga clic en **Entrar a sitio web**.

Resumen de seguridad de un sitio web

Un resumen sobre la clasificación de cualquier sitio web que tiene una clasificación disponible en el portal de protección de navegación.

El resumen de seguridad de un sitio web le ofrece más detalles acerca de en qué se basa la clasificación de seguridad. Por ejemplo, el resumen de seguridad puede mostrar si la clasificación de seguridad se basa en el malware detectado en el sitio, en clasificaciones bajas de otros usuarios o en ambos. El resumen de seguridad se puede acceder desde varios lugares:

- desde el menú de clasificación de seguridad en la barra de herramientas,
- desde la ventana emergente de seguridad con enlaces a sitios web y

- desde el enlace del resumen de seguridad en las páginas web bloqueada por la protección de navegación.

Cualquiera de estos enlaces lo llevará al portal de protección de navegación, donde verá los detalles de la clasificación de seguridad del sitio web.

Navegación segura

Puede protegerse de muchas amenazas de Internet controlando la navegación de todas las cuentas de usuario de Windows de su computadora.

Internet está lleno de sitios web interesantes, pero también existen muchos riesgos para quienes usen la Web. Muchos sitios web contienen material que podría considerar inadecuado. Las personas pueden estar expuestas a material inadecuado o pueden recibir mensajes acosadores por medio del correo electrónico o del chat. Pueden descargar archivos por error que contengan *virus* que podrían dañar la computadora.

Nota: La restricción del acceso a contenido en línea protege las cuentas de usuario de los programas de chat y correo electrónico que se ejecutan en el navegador web. Puede bloquear el acceso a otros programas de chat o correo electrónico usando el componente de seguridad Control de aplicaciones.

Puede restringir las páginas web que se pueden ver y programar el tiempo que les permitirá estar conectados. Estas restricciones se aplican a las cuentas de usuario de Windows, de modo que cuando alguien inicie sesión en su cuenta de usuario, se aplicarán las restricciones.

Limitar el acceso al contenido web

Puede seleccionar el tipo de filtro que desea usar para las distintas cuentas de usuario de Windows.

El filtro de páginas web bloquea el acceso a cualquier página web que no ha permitido o a cualquier página web que posea contenido que ha decidido bloquear.

Autorizar sitio web

Puede permitir el acceso solo a los sitios y las páginas web en los que confíe agregándolos a la lista de sitios web permitidos.

Para permitir el acceso a páginas web específicas:

1. En la página principal, haga clic en **Usuarios**.
2. Seleccione la cuenta de usuario de Windows que desea editar y, a continuación, haga clic en **Configuración** junto a **Filtro de páginas web**.
   Se abre el asistente de filtro web.
3. Haga clic en **Siguiente** en la primera página.
4. Seleccione **Permitir solamente sitios web seleccionados** y, a continuación, haga clic en **Siguiente**.
5. Haga clic en **Agregar** para agregar sitios web a la lista **Sitios web permitidos**.
6. Cuando haya seleccionado todos los tipos de sitios web que desea permitir, haga clic en **Siguiente**.
7. Haga clic en **Finalizar** para cerrar el Asistente para filtrado web.

Cuando haya iniciado sesión en su computadora, cualquier persona que emplee una cuenta de usuario de Windows que usted haya editado solo podrá tener acceso a los sitios web que agregó a la lista de sitios web permitidos.

Bloquear las páginas web por el tipo de contenido

El filtrado web le permite permitir, bloquear o simplemente registrar el acceso a los sitios y las páginas web.

Para seleccionar tipos de contenido web que desee permitir:

1. En la página principal, haga clic en **Usuarios**.
2. Seleccione la cuenta de usuario de Windows que desea editar y, a continuación, haga clic en **Configuración** junto a **Filtro de páginas web**.
   Se abre el asistente de filtro web.
3. Haga clic en **Siguiente** en la primera página.
4. Seleccione **Limitar navegación web por contenido** y, a continuación, haga clic en **Siguiente**.
5. En la página **Restringir contenido web**, seleccione los tipos de contenido que desea bloquear.
6. Cuando haya seleccionado todos los tipos de contenido que desea bloquear, haga clic en **Siguiente**.
7. Haga clic en **Finalizar** para cerrar el Asistente para filtrado web.

Cuando haya iniciado sesión en su computadora, las personas que empleen una cuenta de usuario de Windows que usted haya editado no podrán tener acceso a los sitios web que contienen un tipo de contenido que haya bloqueado.

Editar sitios web permitidos o bloqueados

Puede elegir permitir sitios web específicos que son bloqueados por el filtro web y también bloquear sitios web individuales que no están incluidos en ningún tipo de contenido del filtro web.

Por ejemplo, puede considerar que un sitio web es seguro, aun si desea bloquear otros sitios web con ese tipo de contenido. También cabe la posibilidad de que desee bloquear un sitio web específico, aun si están permitidos otros sitios web con ese tipo de contenido.

Para permitir o bloquear un sitio web:

1. En la página principal, haga clic en **Usuarios**.
2. Seleccione la cuenta de usuario de Windows que desea editar, luego haga clic en **Abrir lista de sitios web**.

   Si el sitio web que desea editar ya está en la lista como permitido o denegado y desea moverlo de una lista a la otra:

   a) Dependiendo de qué lista de sitios web desea editar, haga clic en la pestaña de **Permtir** o **Denegar**.
   b) Haga clic derecho en el sitio web de la lista y seleccione **Permitir** o **Denegar**.

   Si el sitio web no está incluido en ninguna lista:

   a) Haga clic en la pestaña de **Permitir** si desea agregar un sitio web o la pestaña de **Denegar** si desea bloquear un sitio web.
   b) Haga clic en **Añadir** para agregar un nuevo sitio web a la lista.
   c) En el cuadro de diálogo **Añadir sitio web**, ingrese la dirección del sitio web que desea agregar y luego haga clic en **Aceptar**.
3. Haga clic en **Cerrar** para regresar a la página principal.

Para cambiar la dirección de un sitio web permitido o bloqueado, haga clic derecho en el stio web en la lista y seleccione **Editar**.

Para eliminar un sitio web permitido o bloqueado de la lista, seleccione el sitio web y haga clic en **Quitar**.

Cómo programar el tiempo de navegación

Puede controlar el tiempo que se puede navegar por Internet en la computadora.

Puede configurar diferentes restricciones para cada cuenta de usuario de Windows del equipo. Puede controlar:

- Cuando una persona tiene permitido navegar por Internet; por ejemplo, puede permitir que se navegue solo antes de las 8 de la noche.

- Durante cuánto tiempo una persona tiene permitido navegar por Internet; por ejemplo, puede permitir que se navegue solo una hora por día.

Nota: Si quita las restricciones de tiempo, la navegación por Internet se permite sin ningún tipo de límite de tiempo.

Cuando las restricciones de tiempo de navegación bloquean la conexión a Internet, una página de bloqueo en el navegador web indica cuándo puede acceder a Internet de nuevo. Si la cuenta de usuario de Windows tiene derechos de acceso de administrador, puede ampliar el tiempo de navegación introduciendo la contraseña de su cuenta de usuario de Windows y programando más tiempo.

Restringir el tiempo diario de navegación en Internet

Puede usar límites de tiempo diarios para restringir el acceso a Internet.

Puede configurar diferentes límites de tiempo diarios para cada cuenta de usuario de Windows del equipo.

Para configurar los límites de tiempo:

1. En la página principal, haga clic en **Usuarios**.
2. Seleccione la cuenta de usuario que desea editar y, a continuación, haga clic en **Configuración** junto a **Límites de tiempo**.
   Se abre el Asistente para **limitar tiempos de navegación**.
3. Haga clic en **Siguiente** en la primera página.
4. En la tabla **Permitir navegación web durante estas horas**, seleccione las horas en las que se permite la navegación web para cada día de la semana.
5. Cuando haya configurado las horas de navegación permitidas, haga clic en **Siguiente**.
6. Seleccione cuántas horas de navegación se permiten los días de semana y los fines de semana, y luego haga clic en **Siguiente**.
7. Haga clic en **Finalizar** para cerrar el Asistente para horas de navegación.

Cuando haya iniciado sesión en su computadora, las personas que empleen una cuenta de usuario de Windows que usted haya editado solo podrán navegar por Internet durante las horas permitidas.

Ver estadísticas

Puede ver qué páginas web se han visto y bloqueado en la página de **Estadísticas**.

El programa reúne información sobre los sitios web visitados y bloqueados. Esta información es específico al usuario para cada cuenta de usuario de Windows.

Los sitios web bloqueados se dividen en sitio que son bloqueados por el filtro de páginas web y aquellos bloqueados por protección de navegación. Esto le muestra si un sitio bloqueado tiene contenido que ha bloqueado intencionalmente o si el producto lo identificó como un sitio potencialmente dañino.