McAfee®

Internet Security Suite 2008

Guía del usuario

Contenido

CAPÍTULO 1

McAfee Internet Security

McAfee Internet Security Suite con SiteAdvisor es un paquete de seguridad siempre actualizado 10 en 1 que protege lo que tiene valor, la identidad personal y el equipo frente a virus, software espía, fraudes por correo electrónico y mensajería instantánea, piratas informáticos y depredadores en línea, y proporciona copia de seguridad automática de los archivos importantes. Navegue por Internet, compre, realice gestiones bancarias, utilice el correo electrónico y la mensajería instantánea, y descargue archivos con confianza. McAfee SiteAdvisor y el controles parental le ayudarán a usted y a su familia a evitar los sitios Web no seguros. El servicio de seguridad de McAfee proporciona de manera continuada y automática las funciones, mejoras e información sobre amenazas más actualizadas. Además, la puesta a punto automática del equipo elimina archivos innecesarios para obtener el máximo rendimiento del equipo.

En este capítulo

CAPÍTULO 2

McAfee SecurityCenter

McAfee SecurityCenter le permite supervisar el estado de la configuración de seguridad de su equipo, saber al instante si los servicios de protección de virus, programas espía, correo electrónico y cortafuegos de su equipo están actualizados y actuar en vulnerabilidades potenciales de la seguridad. Ofrece las herramientas y controles de navegación necesarios para coordinar y gestionar todas las áreas de protección de su equipo.

Antes de comenzar a configurar y gestionar la protección de su equipo, revise la interfaz de SecurityCenter y asegúrese de que comprende la diferencia entre estado de protección, categorías de protección y servicios de protección. A continuación, actualice SecurityCenter para asegurarse de que dispone de la protección más reciente disponible de McAfee.

Después de finalizar las tareas de configuración iniciales, puede utilizar SecurityCenter para supervisar el estado de protección de su equipo. Si SecurityCenter detecta un problema de protección, le avisará, de modo que pueda solucionar u omitir el problema (según su gravedad). Además, en el registro de eventos puede revisar los eventos de SecurityCenter, como cambios de configuración en el análisis de virus.

Nota: SecurityCenter informa de los problemas de protección críticos y no críticos tan pronto como los detecta. Si necesita ayuda para diagnosticar sus problemas de protección, puede ejecutar McAfee Virtual Technician.

En este capítulo

Funciones de SecurityCenter

SecurityCenter ofrece las funciones siguientes:

Estado de protección simplificado

Facilita la comprobación del estado de protección de su equipo, la verificación de actualizaciones y la solución de problemas de protección potenciales.

Actualizaciones y mejoras automatizadas

Descarga e instala de manera automática las actualizaciones de sus programas registrados. Cuando una nueva versión de un programa registrado de McAfee está disponible, se obtiene sin cargo durante el período en el que la suscripción tenga validez, garantizando así que siempre tenga una protección actualizada.

Alertas en tiempo real

Las alertas de seguridad indican la aparición de emergencias de virus y amenazas contra la seguridad y ofrecen opciones para eliminar la amenaza, neutralizarla u obtener más información sobre ella.

CAPÍTULO 3

Uso de SecurityCenter

Antes de comenzar a utilizar SecurityCenter, revise los componentes y las áreas de configuración que se utilizarán para gestionar el estado de protección de su equipo. Si desea obtener más información sobre la terminología utilizada en esta imagen, consulte Descripción del estado de protección (página 8) y Descripción de las categorías de protección (página 9). A continuación, puede revisar la información de su cuenta de McAfee y verificar la validez de su suscripción.

En este capítulo

Descripción del estado de protección

El estado de protección de su equipo se muestra en la zona de estado de protección en el panel Inicio de SecurityCenter. Indica si su equipo está totalmente protegido contra las últimas amenazas de seguridad y puede verse influido por ataques externos contra la seguridad, otros programas de seguridad y los programas que tienen acceso a Internet.

El estado de protección de su equipo puede ser de color rojo, amarillo o verde.

Estado de protección	Descripción
Roja	Su equipo no está protegido. La zona de estado de protección del panel Inicio de SecurityCenter tiene color rojo e indica que no está protegido. SecurityCenter informa sobre, al menos, un problema de seguridad crítico. Para contar con una protección completa, debe solucionar todos los problemas de seguridad críticos de cada categoría de protección (en el estado de la categoría de problema se indica **Acción necesaria**, también en rojo). Para obtener más información sobre cómo solucionar problemas de protección, consulte Solución de problemas de protección (página 18).
Amarilla	Su equipo está parcialmente protegido. La zona de estado de protección del panel Inicio de SecurityCenter tiene color amarillo e indica que no está protegido. SecurityCenter informa sobre, al menos, un problema de seguridad no crítico. Para contar con una protección completa, debe solucionar u omitir los problemas de seguridad no críticos asociados con cada categoría de protección. Para obtener más información sobre cómo solucionar u omitir problemas de protección, consulte Solucionar u omitir problemas de protección (página 17).
Verde	Su equipo está totalmente protegido. La zona de estado de protección del panel Inicio de SecurityCenter tiene color verde e indica que está protegido. SecurityCenter no informa sobre problemas de seguridad críticos o no críticos. Cada categoría de protección muestra los servicios que protegen su equipo.

Descripción de las categorías de protección

Los servicios de protección de SecurityCenter se dividen en cuatro categorías: Equipo y archivos, Internet y redes, correo electrónico y MI y control parental. Estas categorías le ayudan a explorar y configurar los servicios de seguridad que protegen su equipo.

Debe hacer clic en un nombre de categoría para configurar sus servicios de protección y visualizar cualquier problema de seguridad detectado en esos servicios. Si el estado de protección de su equipo es de color rojo o amarillo, una o varias categorías muestran un mensaje de *Acción necesaria* o *Atención*, quiere decir que SecurityCenter ha detectado un problema en la categoría. Si desea obtener más información sobre estados de protección, consulte Descripción del estado de protección (página 8).

Categoría de protección	Descripción
Equipo y archivos	La categoría Equipo y archivos le permite configurar los siguientes servicios de protección: ▪ Protección contra virus ▪ Protección contra programas potencialmente no deseados (PUP) ▪ Monitores del sistema ▪ Protección de Windows
Internet y redes	La categoría Internet y redes le permite configurar los siguientes servicios de protección: ▪ Protección por cortafuegos ▪ Protección de la identidad
Correo electrónico y MI	La categoría Correo electrónico y MI le permite configurar los siguientes servicios de protección: ▪ Protección de correo electrónico ▪ Protección contra spam
Control parental	La categoría Control Parental le permite configurar los siguientes servicios de protección: ▪ Bloqueo de contenido

Descripción de los servicios de protección

Los servicios de protección son los componentes principales de SecurityCenter que se configuran para proteger a los equipos. Los servicios de protección se corresponden directamente con los programas de McAfee. Por ejemplo, cuando se instala VirusScan, están disponibles los siguientes servicios de protección: Protección antivirus, Protección contra programas potencialmente no deseados (PUP), Monitores del sistema y Protección de Windows. Si desea obtener información más detallada acerca de estos servicios de protección en particular, consulte la ayuda de VirusScan.

De manera predeterminada, todos los servicios de protección asociados con un programa se activan al instalarlo; sin embargo, los servicios de protección se pueden desactivar en cualquier momento. Por ejemplo, si se instala Privacy Service, se activan los servicios Bloqueo de contenido y Protección de la identidad. Si no tiene intención de utilizar el servicio de protección Bloqueo de contenido, puede desactivarlo por completo. También es posible desactivar un servicio de protección de manera temporal, mientras se realizan tareas de mantenimiento o configuración.

Gestión de su cuenta de McAfee

Desde SecurityCenter puede gestionar su cuenta de McAfee y acceder de forma sencilla a la información de su cuenta y revisarla, además de verificar el estado actual de su suscripción.

Nota: si instaló sus programas de McAfee desde un CD, debe registrarlos primero en el sitio Web de McAfee para poder configurar o actualizar su cuenta de McAfee. Será sólo entonces cuando tendrá derecho a recibir las actualizaciones automáticas y regulares de los programas.

Gestione su cuenta de McAfee

Desde SecurityServer puede acceder fácilmente a la información de su cuenta de McAfee (Mi cuenta).

1. En **Tareas comunes**, haga clic en **Mi cuenta**.
2. Inicie sesión en su cuenta de McAfee.

Comprobación de su suscripción

Ha de comprobar su suscripción para asegurarse de que aún no ha caducado.

- Haga clic con el botón derecho del ratón en el icono de SecurityCenter que aparece en el área de notificación de Windows en el extremo derecho de la barra de tareas y, a continuación, haga clic en **Verificar suscripción**.

CAPÍTULO 4

Actualización de SecurityCenter

SecurityCenter asegura que sus programas registrados de McAfee están actualizados buscando e instalando actualizaciones en línea cada cuatro horas. En función de los programas que tenga instalados y registrados, las actualizaciones en línea pueden incluir las definiciones de virus más recientes y actualizaciones para la protección contra piratas informáticos, spam, programas espía o para la privacidad. Si desea buscar actualizaciones antes del período predeterminado de cuatro horas, puede hacerlo en cualquier momento. Mientras SecurityCenter comprueba si hay actualizaciones, puede seguir realizando otras tareas.

Aunque no es recomendable, puede modificar la forma en la que SecurityCenter busca e instala actualizaciones. Por ejemplo, puede configurar SecurityCenter para descargar las actualizaciones pero no para instalarlas o para notificarle antes de descargar o instalar las actualizaciones. También es posible desactivar las actualizaciones automáticas.

Nota: si instaló sus programas de McAfee desde un CD, no podrá recibir las actualizaciones automáticas y regulares para sus programas hasta que no los registre en el sitio Web de McAfee.

En este capítulo

Comprobar actualizaciones

De manera predeterminada, SecurityCenter comprueba automáticamente si hay actualizaciones cada cuatro horas si su equipo está conectado a Internet; sin embargo, si desea buscar actualizaciones antes del período predeterminado de cuatro horas, puede hacerlo. Si ha desactivado las actualizaciones automáticas, es su responsabilidad comprobar las actualizaciones de manera periódica.

- En el panel Inicio de SecurityCenter, haga clic en **Actualizar**.

Sugerencia: también puede comprobar si hay actualizaciones sin ejecutar SecurityCenter haciendo clic con el botón derecho en el icono de SecurityCenter en el área de notificación, situada en el extremo derecho de la barra de tareas y haciendo clic a continuación en **Actualizaciones**.

Configurar actualizaciones automáticas

De forma predeterminada, SecurityCenter comprueba e instala cada cuatro horas cuando su equipo está conectado a Internet. Si desea modificar este hábito predeterminado, puede configurar SecurityCenter para descargar las actualizaciones de manera automática y notificarle cuando las notificaciones estén listas para ser instaladas o notificarle antes de descargarlas.

Nota: SecurityCenter le notifica mediante alertas cuando hay actualizaciones listas para ser descargadas o instaladas. Desde las alertas puede descargar o instalar las actualizaciones o posponerlas. Cuando se actualiza un programa desde una alerta, es posible que se le solicite verificar su suscripción antes de descargarla e instalarla. Para obtener más información, consulte Trabajar con alertas (página 23).

1. Abrir el panel de Configuración de SecurityCenter.

   ¿Cómo?

   1. En **Tareas comunes**, haga clic en **Inicio**.
   2. En el panel de la derecha, en **Información de SecurityCenter**, haga clic en **Configurar**.

2. En el panel Configuración de SecurityCenter, bajo **Actualizaciones automáticas desactivadas**, haga clic en **Activar** y, a continuación, haga clic en **Opciones avanzadas**.
3. Haga clic en uno de los botones siguientes:
   - **Instalar actualizaciones automáticamente y notificarme cuando mis servicios estén actualizados (recomendado)**
   - **Descargar actualizaciones automáticamente y notificarme cuando estén listas para su instalación**
   - **Notificarme antes de descargar cualquier actualización**
4. Haga clic en **Aceptar**.

Desactivar las actualizaciones automáticas

Si desactiva las actualizaciones automáticas, es su responsabilidad comprobar las actualizaciones de manera periódica; de lo contrario, su equipo no dispondrá de la protección de seguridad más actualizada. Para obtener información sobre cómo buscar actualizaciones de manera manual, consulte Comprobar actualizaciones (página 13).

1. Abrir el panel de Configuración de SecurityCenter.

   ¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel de la derecha, en **Información de SecurityCenter**, haga clic en **Configurar**.

2 En el panel Configuración de SecurityCenter, bajo **Actualizaciones automáticas activadas**, haga clic en **Desactivar**.

Sugerencia: Las actualizaciones automáticas se activan haciendo clic en el botón **Activar** o desactivando la opción **Desactivar la actualización automática y permitirme comprobar manualmente las actualizaciones** del panel Opciones de actualización.

CAPÍTULO 5

Solucionar u omitir problemas de protección

SecurityCenter informa de los problemas de protección críticos y no críticos tan pronto como los detecta. Los problemas de protección críticos requieren una acción inmediata y ponen en peligro su estado de protección (el color cambia a rojo). Los problemas de protección no críticos no requieren acciones inmediatas y pueden poner en peligro o no su estado de protección (dependiendo del tipo de problema). Para conseguir un estado de protección de color verde, debe solucionar todos los problemas críticos y solucionar u omitir todos los problemas que no sean críticos. Si necesita ayuda para diagnosticar sus problemas de protección, puede ejecutar McAfee Virtual Technician. Si desea obtener más información sobre McAfee Virtual Technician, consulte la ayuda de McAfee Virtual Technician.

En este capítulo

Solución de problemas de protección

La mayoría de problemas de seguridad pueden solucionarse de manera automática; sin embargo, algunos problemas requieren que tome medidas. Por ejemplo, si la Protección del cortafuegos está desactivada, SecurityCenter puede activarla de manera automática; sin embargo, si la Protección del cortafuegos no está instalada, debe instalarla. La siguiente tabla indica algunas de las acciones posibles que puede tener que realizar a la hora de solucionar problemas de protección de manera manual:

Problema	Acción
No se ha realizado un análisis completo del equipo en los últimos 30 días.	Analizar el equipo manualmente. Para obtener más información, consulte la ayuda de VirusScan.
Los archivos de definiciones (DAT) no están actualizados.	Actualice la protección de manera manual. Para obtener más información, consulte la ayuda de VirusScan.
No está instalado un programa.	Instale el programa desde el sitio Web o el CD de McAfee.
Le faltan componentes a un programa.	Reinstale el programa desde el sitio Web o el CD de McAfee.
Un programa no está registrado y no puede recibir protección total.	Registre el programa en el sitio Web de McAfee.
Un programa ha caducado.	Compruebe el estado de su cuenta en el sitio Web de McAfee.

Nota: a menudo, un único problema de protección afecta a más de una categoría de protección. En este caso, solucionar el problema en una categoría lo borra del resto de categorías de protección.

Solucionar problemas de protección automáticamente

SecurityCenter puede solucionar la mayoría de problemas de protección automáticamente. Los cambios de configuración que SecurityCenter realiza al solucionar de manera automática los problemas de protección no se guardan en el registro de eventos. Si desea obtener más información sobre los eventos, consulte Visualización de eventos (página 29).

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel Inicio de SecurityCenter, en la zona de estado de protección, haga clic en **Solucionar**.

Solucionar problemas de protección manualmente

Si uno o más problemas persisten después de haber intentado solucionarlos de manera automática, puede solucionarlos manualmente.

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel Inicio de SecurityCenter, haga clic en la categoría de protección en la que SecurityCenter ha clasificado el problema.
3. Haga clic en el enlace que sigue a la descripción del problema.

Omitir problemas de protección

Si SecurityCenter detecta un problema no crítico, puede solucionarlo u omitirlo. Otros problemas no críticos (por ejemplo, si los servicios Anticorreo basura o Privacy Service no están instalados) se omiten de manera automática. Los problemas omitidos no se muestran en la zona de información de la categoría de protección del panel Inicio de SecurityCenter a menos que el estado de protección del equipo tenga color verde. Si un problema se omite, pero más tarde desea que aparezca en la zona de información de la categoría de protección incluso si el estado de protección de su equipo no tiene color verde, puede mostrar el problema omitido.

Omitir un problema de protección

Si SecurityCenter detecta un problema no crítico que no tiene intención de solucionar, puede omitirlo. Al omitirlo, el problema desaparece de la zona de información de la categoría de protección de SecurityCenter.

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel Inicio de SecurityCenter, haga clic en la categoría de protección en la que el problema ha sido clasificado.
3. Haga clic en el enlace **Omitir** que se encuentra junto al problema de protección.

Mostrar u ocultar problemas omitidos

Dependiendo de su gravedad, los problemas de protección omitidos pueden mostrarse u ocultarse.

1. Abra el panel Opciones de alerta.

   ¿Cómo?

   1. En **Tareas comunes**, haga clic en **Inicio**.
   2. En el panel de la derecha, en **Información de SecurityCenter**, haga clic en **Configurar**.
   3. En **Alertas**, haga clic en **Opciones avanzadas**.
2. En el panel Configuración de SecurityCenter, haga clic en **Problemas omitidos**.
3. En el panel Problemas omitidos, haga lo siguiente:
   - Para ignorar un problema, marque su casilla de verificación.
   - Para notificar sobre la existencia de un problema en la zona de información de la categoría de protección, desactive esta casilla de verificación.

4 Haga clic en **Aceptar**.

Sugerencia: además, también puede omitir un problema haciendo clic en el enlace **Omitir** que se encuentra junto al problema notificado en la zona de información de la categoría de protección.

CAPÍTULO 6

Trabajar con alertas

Las alertas son pequeños cuadros de diálogo emergentes que aparecen en la esquina inferior derecha de la pantalla cuando se producen determinados eventos de SecurityCenter. Una alerta proporciona información detallada acerca de un evento así como recomendaciones y opciones para resolver problemas que pueden estar asociados al evento. Algunas alertas también contienen enlaces a información adicional sobre el evento. Estos enlaces le permiten abrir el sitio Web global de McAfee o enviar información a McAfee para resolver problemas.

Hay tres tipos de alertas: roja, amarilla y verde.

Tipo de alerta	Descripción
Roja	Una alerta roja es una notificación crítica que requiere una respuesta del usuario. Las alertas rojas se producen cuando SecurityCenter no puede determinar automáticamente cómo solucionar un problema de protección.
Amarilla	Una alerta amarilla es una notificación no crítica que normalmente requiere una respuesta del usuario.
Verde	Una alerta verde es una notificación no crítica que no requiere una respuesta del usuario. Las alertas verdes proporcionan información básica sobre un evento.

Debido a que las alertas juegan un papel muy importante en la supervisión y gestión de su estado de protección, no es posible desactivarlas. Sin embargo, puede controlar cuando pueden aparecer determinados tipos de alertas informativas y configurar otras opciones de alerta (como, por ejemplo, si SecurityCenter debe emitir un sonido cuando emite una alerta o si se debe mostrar la pantalla de bienvenida de McAfee al iniciar).

En este capítulo

Mostrar y ocultar alertas informativas

Las alertas informativas le indican cuando se producen eventos que no suponen amenazas para la seguridad de su equipo. Por ejemplo, si ha configurado la Protección del cortafuegos, aparecerá una alerta informativa de manera predeterminada cuando a un programa de su equipo se le haya permitido acceder a Internet. Si no desea que aparezca un determinado tipo de alerta informativa, puede ocultarla. Si no desea que aparezca ninguna alerta informativa, puede ocultarlas todas. También puede ocultar todas las alertas informativas cuando está jugando a pantalla completa en su equipo. Al finalizar el juego y salir del modo de pantalla completa, SecurityCenter comienza a mostrar de nuevo las alertas informativas.

Si por error oculta una alerta informativa, puede mostrarla de nuevo en cualquier momento. De manera predeterminada, SecurityCenter muestra todas las alertas informativas.

Muestre u oculte alertas informativas

Puede configurar SecurityCenter para que muestre algunas alertas informativas y que oculte otras o para ocultar todas las alertas informativas.

1. Abra el panel Opciones de alerta.

   ¿Cómo?

   1. En **Tareas comunes**, haga clic en **Inicio**.
   2. En el panel de la derecha, en **Información de SecurityCenter**, haga clic en **Configurar**.
   3. En **Alertas**, haga clic en **Opciones avanzadas**.

2. En el panel Configuración de SecurityCenter, haga clic en **Alertas informativas**.
3. En el panel Alertas informativas, haga lo siguiente:
   - Para mostrar una alerta informativa, desactive su casilla de verificación.
   - Para ocultar una alerta informativa, marque su casilla de verificación.
   - Para ocultar todas las alertas informativas, seleccione la casilla de verificación **No mostrar alertas informativas**.
4. Haga clic en **Aceptar**.

Sugerencia: también puede ocultar una alerta informativa al seleccionar la casilla de verificación **No volver a mostrar esta alerta** en la misma alerta. Si lo hace, puede mostrar de nuevo la alerta informativa desactivando la casilla de verificación apropiada en el panel Alertas informativas.

Muestre u oculte alertas informativas al jugar

También puede ocultar las alertas informativas cuando está jugando a pantalla completa en su equipo. Al finalizar el juego y salir del modo de pantalla completa, SecurityCenter comienza a mostrar de nuevo las alertas informativas.

1 Abra el panel Opciones de alerta.

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel de la derecha, en **Información de SecurityCenter**, haga clic en **Configurar**.
3. En **Alertas**, haga clic en **Opciones avanzadas**.

2 En el panel Opciones de alerta, seleccione o desactive la casilla de verificación **Mostrar alertas informativas cuando se detecte el modo de juegos**.

3 Haga clic en **Aceptar**.

Configuración de las opciones de alerta

SecurityCenter configura la apariencia y la frecuencia de las alertas; sin embargo, puede ajustar algunas opciones de alerta básicas. Por ejemplo, se puede emitir un sonido junto con las alertas u ocultar la pantalla de bienvenida cuando se inicia Windows. También puede ocultar las alertas que le informan sobre nuevos virus y otras amenazas de seguridad de la comunidad en línea.

Emitir un sonido junto con las alertas

Si desea recibir una indicación audible que le indique que ha aparecido una alerta, SecurityCenter puede configurarse para que emita un sonido con cada alerta.

1 Abra el panel Opciones de alerta.

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel de la derecha, en **Información de SecurityCenter**, haga clic en **Configurar**.
3. En **Alertas**, haga clic en **Opciones avanzadas**.

2 En el panel Opciones de alerta, bajo **Sonido**, seleccione la casilla de verificación **Reproducir un sonido cuando se produzca una alerta**.

Ocultar la pantalla de bienvenida al iniciar

De manera predeterminada, la pantalla de bienvenida de McAfee aparece brevemente cuando Windows se inicia, indicándole que SecurityCenter está protegiendo su equipo. Sin embargo, puede ocultar la pantalla de bienvenida si no desea que aparezca.

1 Abra el panel Opciones de alerta.

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel de la derecha, en **Información de SecurityCenter**, haga clic en **Configurar**.
3. En **Alertas**, haga clic en **Opciones avanzadas**.

2 En el panel Opciones de alerta, bajo **Pantalla de bienvenida**, desactive la casilla de verificación **Mostrar la pantalla de bienvenida de McAfee al iniciar Windows**.

Sugerencia: en cualquier momento puede mostrar la pantalla de bienvenida de nuevo seleccionando la casilla de verificación **Mostrar la pantalla de bienvenida de McAfee al iniciar Windows**.

Ocultar alertas de nuevos virus

Puede ocultar las alertas que le informan sobre nuevos virus y otras amenazas de seguridad de la comunidad en línea.

1 Abra el panel Opciones de alerta.

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel de la derecha, en **Información de SecurityCenter**, haga clic en **Configurar**.
3. En **Alertas**, haga clic en **Opciones avanzadas**.

2 En el panel Opciones de alerta, desactive la casilla de verificación **Avisarme cuando se produzca un brote de virus o una amenaza para la seguridad**.

Sugerencia: puede mostrar las alertas de brotes de virus en cualquier momento seleccionando la casilla de verificación **Avisarme cuando se produzca un brote de virus o una amenaza para la seguridad**.

CAPÍTULO 7

Visualización de eventos

Un evento es una acción o un cambio de configuración que se produce en una categoría de protección y en sus servicios de protección relacionados. Los diferentes servicios de protección registran diferentes tipos de eventos. Por ejemplo, SecurityCenter registra un evento si un servicio de protección está activado o desactivado; la Protección antivirus registra un evento cada vez que se detecta y elimina un virus; y la Protección del cortafuegos registra un evento cada vez que se bloquea un intento de conexión a Internet. Si desea obtener más información sobre categorías de protección, consulte Descripción de las categorías de protección (página 9).

Puede visualizar los eventos al resolver problemas de configuración y al revisar operaciones realizadas por otros usuarios. Muchos padres utilizan el registro de eventos para supervisar los hábitos de sus hijos en Internet. Puede visualizar los eventos recientes si desea examinar únicamente los últimos 30 eventos ocurridos. Puede visualizar todos los eventos si desea examinar una lista detallada de todos los eventos ocurridos. Al visualizar todos los eventos, SecurityCenter abre el registro de eventos, que muestra los eventos según la categoría de protección en la que se produjeron.

En este capítulo

Ver eventos recientes

Puede visualizar los eventos recientes si desea examinar únicamente los últimos 30 eventos ocurridos.

- Bajo **Tareas comunes,** haga clic en **Ver eventos recientes**.

Visualizar todos los eventos

Puede visualizar todos los eventos si desea examinar una lista detallada de todos los eventos ocurridos.

1. Bajo **Tareas comunes,** haga clic en **Ver eventos recientes**.
2. En el panel Eventos recientes, haga clic en **Ver registro**.
3. En el panel de la izquierda del registro de eventos, haga clic en el tipo de eventos que desea visualizar.

CAPÍTULO 8

McAfee VirusScan

Los servicios avanzados de detección y protección de VirusScan le defienden a usted y a su equipo de las últimas amenazas para la seguridad, tales como virus, troyanos, cookies de rastreo, software espía, software publicitario y otros programas potencialmente no deseados. La protección se amplía más allá de los archivos y carpetas de su equipo de sobremesa, centrándose en las amenazas desde diferentes puntos de entrada, tales como el correo electrónico, los mensajes instantáneos e Internet.

Con VirusScan, la protección de su equipo es inmediata y constante (no es necesario realizar tareas de administración tediosas). Al trabajar, jugar, navegar por Internet o comprobar su correo electrónico, se ejecuta en segundo plano, supervisando, analizando y detectando daños potenciales en tiempo real. Los análisis exhaustivos se realizan de manera programada y comprueban su equipo periódicamente utilizando un conjunto de opciones más sofisticado. VirusScan le ofrece la flexibilidad de personalizar este hábito si así lo desea; pero, en caso contrario, su equipo continúa protegido.

Con el uso normal del equipo, virus, gusanos y otras amenazas potenciales pueden infiltrarse en su equipo. Si esto ocurre, VirusScan le notifica la amenaza, pero normalmente la gestiona por usted: limpiando o poniendo en cuarentena los elementos infectados antes de que se produzca cualquier daño. Aunque no es muy común, en ocasiones puede ser necesario realizar acciones adicionales. En estos casos, VirusScan le permite decidir qué hacer (volver a analizar el equipo la próxima vez que se reinicie, guardar el elemento detectado o eliminarlo).

Nota: SecurityCenter informa de los problemas de protección críticos y no críticos tan pronto como los detecta. Si necesita ayuda para diagnosticar sus problemas de protección, puede ejecutar McAfee Virtual Technician.

En este capítulo

Funciones de VirusScan

VirusScan ofrece las funciones siguientes.

Protección antivirus más completa

Los servicios avanzados de detección y protección de VirusScan le defienden a usted y a su equipo de las últimas amenazas para la seguridad, tales como virus, troyanos, cookies de rastreo, software espía, software publicitario y otros programas potencialmente no deseados. La protección se amplía más allá de los archivos y carpetas y de su equipo de sobremesa, centrándose en las amenazas desde diferentes puntos de entrada, tales como el correo electrónico, los mensajes instantáneos e Internet. No es necesario realizar tareas de administración tediosas.

Opciones de análisis sensibles a los recursos

Si experimenta unas velocidades de análisis muy lentas, puede desactivar la opción que utiliza menos recursos del equipo, pero tenga en cuenta que se le asignará una mayor prioridad a la protección antivirus que a otras tareas. VirusScan le ofrece la flexibilidad de personalizar las opciones de análisis manual y en tiempo real si así lo desea; pero, en caso contrario, su equipo continúa protegido.

Reparaciones automáticas

Si VirusScan detecta una amenaza para la seguridad al ejecutar un análisis manual o en tiempo real, intentará gestionar la amenaza de manera automática según el tipo de amenaza. De esta manera, es posible detectar y neutralizar la mayoría de amenazas sin la necesidad de su intervención. Aunque no es muy frecuente, es posible que VirusScan no pueda neutralizar una amenaza por su cuenta. En estos casos, VirusScan le permite decidir qué hacer (volver a analizar el equipo la próxima vez que se reinicie, guardar el elemento detectado o eliminarlo).

Detener tareas en modo de pantalla completa

al realizar actividades lúdicas como ver películas, jugar en el equipo o cualquier otra actividad que ocupe toda la pantalla, VirusScan detiene varias tareas, como las actualizaciones automáticas y los análisis manuales.

Inicio de la protección contra virus en tiempo real

VirusScan ofrece dos tipos de protección contra virus: en tiempo real y manual. La protección contra virus en tiempo real supervisa constantemente el equipo en busca de virus y analiza los archivos cada vez que usted o su equipo acceden a ellos. La protección manual contra virus le permite analizar los archivos libremente. Para asegurarse de que su equipo permanece protegido contra las amenazas de seguridad más recientes, active la protección contra virus en tiempo real y programe análisis manuales periódicos más exhaustivos. De manera predeterminada, VirusScan realiza un análisis programado una vez a la semana. Para obtener más información acerca del análisis en tiempo real y manual, consulte Analizar su equipo (página 57).

Aunque no es habitual, en ocasiones es posible que desee detener el análisis en tiempo real (por ejemplo, para cambiar algunas opciones del análisis o para resolver un problema de rendimiento). Cuando la protección contra virus en tiempo real está desactivada, su equipo no está protegido y su estado de protección en SecurityCenter es de color rojo. Para obtener más información sobre el estado de protección, consulte "Descripción del estado de protección" en la ayuda de SecurityCenter.

Inicie la protección contra virus en tiempo real

De manera predeterminada, la protección contra virus en tiempo real está activada y protege su equipo contra virus, troyanos y otras amenazas para la seguridad. Si desactiva la protección contra virus en tiempo real, debe activarla de nuevo para seguir protegido.

1 Abra el panel de Configuración de Equipo y archivos.

¿Cómo?

1. En el panel izquierdo, haga clic en **Menú Avanzado**.
2. Haga clic en **Configurar**.
3. En el panel Configurar, haga clic en **Equipo y Archivos**.

2 En **Protección antivirus**, haga clic en **Activado**.

Detener la protección contra virus en tiempo real

Es posible desactivar temporalmente la protección contra virus en tiempo real y, a continuación, indicar cuando se debe reanudar. Puede reanudar la protección de manera automática pasados 15, 30, 45 ó 60 minutos, cuando se reinicie el equipo o nunca.

1. Abra el panel de Configuración de Equipo y archivos.

   ¿Cómo?

   1. En el panel izquierdo, haga clic en **Menú Avanzado**.
   2. Haga clic en **Configurar**.
   3. En el panel Configurar, haga clic en **Equipo y Archivos**.

2. En **Protección antivirus**, haga clic en **Desactivado**.
3. En el cuadro de diálogo, seleccione cuando se debe reanudar el análisis en tiempo real.
4. Haga clic en **Aceptar**.

CAPÍTULO 9

Inicio de protección adicional

Además de la protección contra virus en tiempo real, VirusScan ofrece avanzada contra secuencias de comandos, programas espía y adjuntos de correos electrónicos y mensajes instantáneos potencialmente peligrosos. De manera predeterminada, están activados y protegen su equipo el análisis de secuencias de comandos y la protección contra programas espía, correo electrónico y mensajería instantánea.

Protección de análisis de secuencias de comandos

La protección de análisis de secuencias de comandos detecta las secuencias de comandos potencialmente peligrosas y evita que se ejecuten en su equipo. Supervisa su equipo en busca de actividades sospechosas en las secuencias de comandos, tales como una secuencia de comandos que crea, copia o elimina archivos o que abre el registro de Windows y, consecuentemente, le informa de ello antes de que se produzca cualquier daño.

Protección contra software espía

La protección contra software espía detecta software espía, software publicitario y otros programas potencialmente no deseados. Los programas espías son aplicaciones que se pueden instalar en su equipo de forma encubierta para supervisar sus hábitos, recopilar información personal e incluso interferir en el control de su equipo instalando programas adicionales o redirigiendo la actividad de los navegadores.

Protección de correo electrónico

La protección de correo electrónico detecta las actividades sospechosas en el correo electrónico y los archivos adjuntos enviados y recibidos.

Protección de mensajería instantánea

La protección de mensajería instantánea detecta potenciales amenazas contra la seguridad provenientes de adjuntos a mensajes instantáneos que se han recibido. Además, evita que los programas de mensajería instantánea compartan información personal.

En este capítulo

Inicie la protección de análisis de secuencias de comandos

Active la protección de análisis de secuencias de comandos para detectar las secuencias de comandos potencialmente peligrosas y evitar que se ejecuten en su equipo. La protección de análisis de secuencias de comandos le indica cuando una secuencia de comandos intenta crear archivos en su equipo, copiarlos o eliminarlos o cuando realiza cambios en el registro de Windows.

1 Abra el panel de Configuración de Equipo y archivos.

¿Cómo?

1. En el panel izquierdo, haga clic en **Menú Avanzado**.
2. Haga clic en **Configurar**.
3. En el panel Configurar, haga clic en **Equipo y Archivos**.

2 En **Protección de análisis de secuencias de comandos**, haga clic en **Activado**.

Nota: aunque en cualquier momento es posible desactivar la protección de análisis de secuencias de comandos, si lo hace deja a su equipo en una posición vulnerable ante secuencias de comandos dañinas.

Inicie la protección contra software espía

Active la protección contra software espía para detectar y eliminar software espía, software publicitario y otros programas potencialmente no deseados que recopilan y transmiten información sin su conocimiento o permiso.

1 Abra el panel de Configuración de Equipo y archivos.

¿Cómo?

1. En el panel izquierdo, haga clic en **Menú Avanzado**.
2. Haga clic en **Configurar**.
3. En el panel Configurar, haga clic en **Equipo y Archivos**.

2 En **Protección de análisis de secuencias de comandos**, haga clic en **Activado**.

Nota: aunque en cualquier momento es posible desactivar la protección contra software espía, si lo hace deja a su equipo en una posición vulnerable ante programas potencialmente no deseados.

Inicie la protección de correo electrónico

Active la protección de correo electrónico para detectar gusanos, así como otras amenazas peligrosas en los mensajes y adjuntos de correo electrónico salientes (SMTP) y entrantes (POP3).

1 Abrir el panel de configuración de Correo electrónico y MI.

¿Cómo?

1. En el panel izquierdo, haga clic en **Menú Avanzado**.
2. Haga clic en **Configurar**.
3. En el panel Configurar, haga clic en **Correo electrónico y MI**.

2 En **Protección de correo electrónico**, haga clic en **Activado**.

Nota: aunque en cualquier momento es posible desactivar la protección de correo electrónico, si lo hace deja a su equipo en una posición vulnerable ante amenazas de correo electrónico.

Inicie la protección de mensajería instantánea

Active la protección de mensajería instantánea para detectar amenazas contra la seguridad que puedan incluirse como adjuntos en los mensajes instantáneos entrantes.

1 Abrir el panel de configuración de Correo electrónico y MI.

¿Cómo?

1. En el panel izquierdo, haga clic en **Menú Avanzado**.
2. Haga clic en **Configurar**.
3. En el panel Configurar, haga clic en **Correo electrónico y MI**.

2 En **Protección de mensajería instantánea**, haga clic en **Activado**.

Nota: aunque en cualquier momento es posible desactivar la protección de mensajería instantánea, si lo hace deja a su equipo en una posición vulnerable ante los adjuntos dañinos de los mensajes instantáneos.

CAPÍTULO 10

Configurar la protección frente a virus

VirusScan ofrece dos tipos de protección contra virus: en tiempo real y manual. La protección frente a virus en tiempo real examina los archivos cada vez que el usuario o el equipo accede a ellos. La protección manual contra virus le permite analizar los archivos libremente. Puede definir opciones distintas para cada tipo de protección. Por ejemplo, debido a que la protección en tiempo real supervisa constantemente su equipo, puede seleccionar un grupo determinado de opciones de análisis básico, reservar un conjunto más exhaustivo de opciones de análisis para la protección manual, bajo demanda.

En este capítulo

Configuración de opciones de análisis en tiempo real

Al iniciar la protección contra virus en tiempo real, para analizar los archivos VirusScan utiliza un conjunto de opciones predeterminado; sin embargo, usted puede cambiar las opciones predeterminadas para ajustarlas a sus necesidades.

Para cambiar las opciones de análisis en tiempo real, debe decidir qué es lo que debe comprobar VirusScan durante un análisis, así como las ubicaciones y los tipos de archivo que debe analizar. Por ejemplo, puede determinar si VirusScan ha de buscar virus desconocidos o las cookies que los sitios Web pueden utilizar para realizar un seguimiento de tus hábitos y si analiza las unidades de red que están asignadas a su equipo o únicamente las unidades locales. También puede determinar qué tipo de archivos analiza (todos los archivos o únicamente los documentos y los archivos de programa, dado que es donde más virus se detectan).

Al cambiar las opciones de análisis en tiempo real, también debe decidir si es importante que su equipo cuente con protección contra desbordamiento de búfer. Un búfer es una porción de memoria utilizado para guardar datos informáticos de manera temporal. Los desbordamientos del búfer se pueden producir cuando la cantidad de programas o de procesos de información sospechosos almacenada en un búfer supera su capacidad. Cuando esto ocurre, su equipo se vuelve más vulnerable a los ataques contra la seguridad.

Configure las opciones de análisis en tiempo real

Debe configurar las opciones de análisis en tiempo real para personalizar lo que busca VirusScan durante un análisis en tiempo real, así como las ubicaciones y los tipos de archivo analizados. Las opciones incluyen el análisis en busca de virus desconocidos y cookies de rastreo, así como ofrecer protección contra desbordamiento de búfer. Además, también puede configurar el análisis en tiempo real para comprobar las unidades de red que están asignadas a su equipo.

1 Abra el panel de análisis en tiempo real.

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel Inicio de SecurityCenter, haga clic en **Equipo y archivos**.
3. En la zona información Equipo y archivos, haga clic en **Configurar**.
4. En el panel Configuración de Equipo y archivos, asegúrese de que la protección contra virus está activada y luego haga clic en **Avanzada**.

2 Especifique sus opciones de análisis en tiempo real y, a continuación, haga clic en **Aceptar**.

Para...	Hacer esto...
Detecte virus desconocidos y nuevas variantes de virus conocidos	Seleccione la casilla de verificación **Buscar virus nuevos desconocidos con la opción de heurística**.
Detecte las cookies	Seleccione la casilla de verificación **Analizar y eliminar las cookies de rastreo**.
Detecte virus y otras amenazas potenciales en las unidades que están conectadas en su red	Seleccione la casilla de verificación **Analizar unidades de red**.
Proteja su equipo de los desbordamientos del búfer	Seleccione la casilla de verificación **Activar protección contra desbordamiento de búfer**.
Especifique qué tipo de archivos desea analizar	Haga clic en **Todos los archivos (recomendado)** o en **Solamente archivos de programas y documentos**.

Configuración de las opciones de análisis manual

La protección manual contra virus le permite analizar los archivos libremente. Cuando se inicia un análisis manual, VirusScan comprueba su equipo en busca de virus y otros elementos potencialmente peligrosos utilizando un conjunto de opciones más exhaustivo. Para modificar las opciones de análisis manual, debe decidir qué es lo que debe comprobar VirusScan durante un análisis. Por ejemplo, puede determinar si VirusScan busca virus desconocidos, programas potencialmente no deseados, tales como programas espía o software publicitario; programas furtivos, tales como kits de raíz que pueden ofrecer acceso no autorizado a su equipo y las cookies utilizadas por los sitios Web para realizar un seguimiento de su hábitos. Además, debe decidir qué tipo de archivos se van a comprobar. Por ejemplo, puede determinar si VirusScan ha de comprobar todos los archivos o únicamente archivos y documentos (dado que es ahí donde se detecta la mayoría de virus). También puede determinar qué archivos de almacenamiento (por ejemplo, archivos .zip) se incluirán en el análisis.

De manera predeterminada, VirusScan comprueba todas las unidades y carpetas de su equipo cada vez que ejecuta un análisis manual; sin embargo, puede ajustar las ubicaciones predeterminadas a sus necesidades. Por ejemplo, puede analizar únicamente archivos de sistema importantes, elementos del escritorio o elementos de la carpeta Archivos de programa. A menos que se responsabilice usted mismo de iniciar cada análisis manual, puede establecer una programación periódica para realizar análisis. Los análisis programados siempre comprueban el equipo al completo mediante las opciones predeterminadas de análisis. De manera predeterminada, VirusScan realiza un análisis programado una vez a la semana.

Si cree que está experimentando unas velocidades de análisis muy lentas, considere la posibilidad de desactivar la opción que utiliza menos recursos del equipo, pero tenga en cuenta que se le asignará una mayor prioridad a la protección antivirus que a otras tareas.

Nota: al realizar actividades lúdicas como ver películas, jugar en el equipo o cualquier otra actividad que ocupe toda la pantalla, VirusScan detiene varias tareas, como las actualizaciones automáticas y los análisis manuales.

Configurar opciones de análisis manual

Debe configurar las opciones de análisis manual para personalizar lo que VirusScan busca durante un análisis manual, así como las ubicaciones y los tipos de archivo analizados. Las opciones incluyen el análisis en busca de virus desconocidos, archivos, programas espía y programas potencialmente no deseados, cookies de rastreo, kits de raíz y programas furtivos.

1 Abra el panel Análisis manual.

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel Inicio de SecurityCenter, haga clic en **Equipo y archivos**.
3. En la zona información Equipo y archivos, haga clic en **Configurar**.
4. En el panel Configuración de Equipo y archivos, asegúrese de que la protección contra virus está activada y haga clic en **Avanzada**.
5. Haga clic en **Análisis manual** en el panel Protección antivirus.

2 Especifique sus opciones de análisis manual y, a continuación, haga clic en **Aceptar**.

Para...	Hacer esto...
Detecte virus desconocidos y nuevas variantes de virus conocidos	Seleccione la casilla de verificación **Buscar virus nuevos desconocidos con la opción de heurística**.
Detecte y elimine los virus de los archivos .zip y otros archivos de almacenamiento	Seleccione la casilla de verificación **Buscar en archivos .zip y otros archivos de almacenamiento**.
Detecte software espía, software publicitario y otros programas potencialmente no deseados	Seleccione la casilla de verificación **Buscar software espía y programas potencialmente no deseados**.
Detecte las cookies	Seleccione la casilla de verificación **Analizar y eliminar las cookies de rastreo**.
Detecte los kits de raíz y los programas furtivos que pueden alterar y obtener archivos de sistema de Windows	Seleccione la casilla de verificación **Buscar kits de raíz y otros programas furtivos**.

Para...	Hacer esto...
Utilice menos potencia del procesador durante el análisis y dé más prioridad a otras tareas (tales como navegar en Internet o abrir documentos)	Seleccione la casilla de verificación **Análisis utilizando mínimos recursos del equipo**.
Especifique qué tipo de archivos desea analizar	Haga clic en **Todos los archivos (recomendado)** o en **Solamente archivos de programas y documentos**.

Configurar ubicación de análisis manual

Usted configura la ubicación del análisis manual para determinar dónde va a realizar la búsqueda VirusScan de virus y otros elementos peligrosos durante un análisis manual. Es posible analizar todos los archivos, carpetas y unidades de su ordenador o puede restringir el análisis a determinadas carpetas y unidades.

1 Abra el panel Análisis manual.

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel Inicio de SecurityCenter, haga clic en **Equipo y archivos**.
3. En la zona información Equipo y archivos, haga clic en **Configurar**.
4. En el panel Configuración de Equipo y archivos, asegúrese de que la protección contra virus está activada y haga clic en **Avanzada**.
5. Haga clic en **Análisis manual** en el panel Protección antivirus.

2 Haga clic en **Ubicación predeterminada para el análisis**.

3 Especifique su ubicación de análisis manual y, a continuación, haga clic en **Aceptar**.

Para...	Hacer esto...
Analice todos los archivos y carpetas de su equipo	Seleccione la casilla de verificación **(Mi) Equipo**.
Analice archivos, carpetas y unidades determinadas de su equipo	Desactive la casilla de verificación **(Mi) Equipo** y seleccione una o más unidades o carpetas.

Para...	Hacer esto...
Analizar archivos de sistema importantes	Desactive la casilla de verificación **(Mi) Equipo** y, a continuación, seleccione la casilla de verificación **Archivos de sistema importantes**.

Planificar un análisis

Planifique análisis para comprobar a fondo su equipo en busca de virus y otras amenazas en cualquier momento de cualquier día de la semana. Los análisis programados siempre comprueban el equipo al completo mediante las opciones predeterminadas de análisis. De manera predeterminada, VirusScan realiza un análisis programado una vez a la semana. Si cree que está experimentando unas velocidades de análisis muy lentas, considere la posibilidad de desactivar la opción que utiliza menos recursos del equipo, pero tenga en cuenta que se le asignará una mayor prioridad a la protección antivirus que a otras tareas.

1 Abra el panel Análisis programado.

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel Inicio de SecurityCenter, haga clic en **Equipo y archivos**.
3. En la zona información Equipo y archivos, haga clic en **Configurar**.
4. En el panel Configuración de Equipo y archivos, asegúrese de que la protección contra virus está activada y haga clic en **Avanzada**.
5. Haga clic en **Análisis programado** en el panel Protección antivirus.

2 Seleccione **Activar análisis programado**.

3 Para reducir la cantidad de potencia del procesador que se utiliza normalmente para los análisis, seleccione **Análisis utilizando mínimos recursos del equipo**.

4 Seleccione uno o más días.

5 Especifique una hora de inicio.

6 Haga clic en **Aceptar**.

Sugerencia: puede restablecer la programación predeterminada haciendo clic en **Restablecer**.

Utilización de las opciones de Guardianes del sistema

Guardianes del sistema supervisa, registra y gestiona los cambios potencialmente no autorizados realizados en el registro de Windows o en archivos de sistema importantes en su equipo e informa sobre ellos. Los cambios no autorizados en el registro y en archivos pueden causar daños en el equipo, poner en riesgo la seguridad y dañar archivos importantes del sistema.

Los cambios en el registro y en los archivos son comunes y normalmente se producen en su equipo. Debido a que muchos son inofensivos, los ajustes predeterminados de Guardianes del sistema están configurados para ofrecer una protección fiable, inteligente y real contra los cambios no autorizados que supongan un gran potencial de peligrosidad. Por ejemplo, cuando Guardianes del sistema detecta los cambios no comunes y que presentan una amenaza potencialmente significativa, se informa sobre la actividad de manera inmediata y se añade al registro. Los cambios que sean más comunes, pero que aún impliquen algún potencial peligroso, sólo se incluyen en el registro. Sin embargo, la supervisión de los cambios estándar y de bajo riesgo está, de manera predeterminada, desactivada. La tecnología Guardianes del sistema puede configurarse para ampliar su protección a cualquier entorno que desee.

Hay tres tipos de Guardianes del sistema: Guardianes del sistema de programas, Guardianes del sistema de Windows y Guardianes del sistema de navegadores.

Guardianes del sistema de programas

Los Guardianes del sistema de programas detectan los cambios no autorizados potencialmente en el registro de su equipo y en otros archivos importantes esenciales para Windows. Estos importantes elementos y archivos del registro incluyen instalaciones de ActiveX, elementos de inicio, hooks de ejecución en shell de Windows y las cargas retrasadas de objeto de servicio de Shell. Al supervisarlos, la tecnología Guardianes del sistema de programas detiene los programas sospechosos con ActiveX (descargados de Internet), además de los programas espía y los programas potencialmente no deseados que se ejecutan de manera automática cuando Windows se inicia.

Guardianes del sistema de Windows

Los Guardianes del sistema de Windows también detectan los cambios no autorizados potencialmente en el registro de su equipo y en otros archivos importantes esenciales para Windows. Estos importantes elementos y archivos del registro incluyen identificadores de menús contextuales, applnit DLLs y el archivo hosts de Windows. Al supervisar estos elementos, la tecnología Guardianes del sistema ayuda a evitar que su equipo envíe y reciba información personal o no autorizada a través de Internet. También contribuye a detener los programas sospechosos que pueden traer cambios no deseados en relación con la apariencia y los hábitos de los programas que son importantes para usted y su familia.

Guardianes del sistema de navegadores

Al igual que los Guardianes del sistema de programa y de Windows, los Guardianes del sistema de navegadores detectan los cambios no autorizados potencialmente en el registro de su equipo y en otros archivos importantes esenciales para Windows. Sin embargo, los Guardianes del sistema de navegadores supervisan los cambios de elementos importantes del registro y de archivos como los complementos de Internet Explorer, las URL de Internet Explorar y las zonas de seguridad de Internet Explorer. Al supervisar este sistema, la tecnología de los Guardianes del sistema de navegadores ayuda a evitar la actividad no autorizada en los navegadores como la redirección a sitios Web sospechosos, cambios en los ajustes y en las opciones del navegador sin la formación adecuada y la confianza no autorizada en sitios Web sospechosos.

Active la protección Guardianes del sistema

Activa la protección de Guardianes del sistema para detectar los cambios potencialmente no autorizados en el registro de Windows y en los archivos de su equipo e informarle de ellos. Los cambios no autorizados en el registro y en archivos pueden causar daños en el equipo, poner en riesgo la seguridad y dañar archivos importantes del sistema.

1 Abra el panel de Configuración de Equipo y archivos.

¿Cómo?

1. En el panel izquierdo, haga clic en **Menú Avanzado**.
2. Haga clic en **Configurar**.
3. En el panel Configurar, haga clic en **Equipo y Archivos**.

2 En **Protección del guardián del sistema**, haga clic en **Activado**.

Nota: es posible desactivar la protección de los Guardianes del sistema haciendo clic en **Desactivar**.

Configure las opciones de Guardianes del sistema

Utilice el panel Guardianes del sistema para configurar las opciones de protección, registro y alertas de los cambios de registro y de archivo no autorizados asociados con los archivos y programas de Windows e Internet Explorer. Los cambios no autorizados en el registro y en archivos pueden causar daños en el equipo, poner en riesgo la seguridad y dañar archivos importantes del sistema.

1 Abra el panel Guardianes del sistema.

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel Inicio de SecurityCenter, haga clic en **Equipo y archivos**.
3. En la zona información Equipo y archivos, haga clic en **Configurar**.
4. En el panel Configuración de Equipo y archivos, asegúrese de que la protección del Guardián del sistema está activada y haga clic en **Avanzada**.

2 Seleccione un tipo de Guardián del sistema de la lista.

- **Guardianes del sistema de programas**
- **Guardianes del sistema de Windows**
- **Guardianes del sistema de navegadores**

3 En **Deseo**, elija una de las siguientes opciones:

- Para detectar y registrar cambios no autorizados en el registro y archivos asociados con los Guardianes del sistema de programa, de Windows y de navegadores e informar sobre ellos, haga clic en **Mostrar alertas.**
- Para detectar y registrar cambios no autorizados en el registro y archivos asociados con los Guardianes del sistema de programa, de Windows y de navegadores, haga clic en **Sólo cambios de registro.**
- Para desactivar la detección de cambios no autorizados en el registro y archivos asociados con los Guardianes del sistema de programa, de Windows y de navegador, haga clic en **Desactivar el Guardián del sistema.**

Nota: para obtener más información sobre los tipos de Guardianes del sistema, consulte Acerca de los tipos de Guardianes del sistema (página 49).

Acerca de los tipos de Guardianes del sistema

Los Guardianes del sistema detectan los cambios no autorizados potencialmente en el registro de su equipo y en otros archivos importantes esenciales para Windows. Hay tres tipos de Guardianes del sistema: Guardianes del sistema de programas, Guardianes del sistema de Windows y Guardianes del sistema de navegadores

Guardianes del sistema de programas

La tecnología Guardianes del sistema de programas detiene los programas sospechosos con ActiveX (descargados de Internet), además de los programas espía y los programas potencialmente no deseados que se ejecutan de manera automática cuando Windows se inicia.

guardián del sistema	Detecta...
Instalaciones de ActiveX	Los cambios no autorizados en las instalaciones de ActiveX que pueden causar daños en el equipo, ponen en riesgo su seguridad y dañar archivos importantes del sistema.
Elementos de inicio	El software espía, el software publicitario y los programas potencialmente no deseados que pueden instalar cambios en archivos de los elementos de inicio, lo que permite que se ejecuten programas sospechosos al iniciar el equipo.
Hooks de ejecución en Shell de Windows	El software espía, el software publicitario y otros programas potencialmente no deseados que pueden instalar hooks de ejecución en shell de Windows para impedir que se inicien los programas de seguridad.
Carga retrasada de objeto de servicio de Shell	El software espía, el software publicitario y otros programas potencialmente no deseados que pueden realizar cambios en el registro para la carga retrasada de objeto de servicio de shell, lo que permite que se ejecuten archivos dañinos al iniciar el equipo.

Guardianes del sistema de Windows

La tecnología Guardianes del sistema ayuda a evitar que su equipo envíe y reciba información personal o no autorizada a través de Internet. También contribuye a detener los programas sospechosos que pueden traer cambios no deseados en relación con la apariencia y los hábitos de los programas que son importantes para usted y su familia.

guardián del sistema	Detecta...
Identificadores de menús contextuales	Los cambios no autorizados en el registro para identificadores de menús contextuales de Windows que pueden afectar a la apariencia y comportamiento de los menús de Windows. Los menús contextuales permiten realizar acciones en el equipo, tales como hacer clic con el botón derecho en los archivos.
AppInit DLLs	Los cambios no autorizados en el registro para appInit DLLs de Windows que pueden permitir en principio que se ejecuten archivos dañinos al iniciar el equipo.
Archivo Hosts de Windows	El software espía, el software publicitario y los programas potencialmente no deseados que pueden realizar cambios no autorizados en el archivo hosts de Windows, lo que permite redireccionar el navegador a sitios Web sospechosos y bloquear actualizaciones de software.
Shell Winlogon	El software espía, el software publicitario y otros programas potencialmente no deseados que pueden realizar cambios en el registro de shell de Winlogon, lo que permite que otros programas sustituyan a Windows Explorer.
Winlogon User Init	El software espía, el software publicitario y otros programas potencialmente no deseados que pueden realizar cambios en el registro de Winlogon user init, lo que permite que se ejecuten programas sospechosos al iniciar la sesión en Windows.
Protocolos Windows	El software espía, el software publicitario y otros programas potencialmente no deseados que pueden realizar cambios en el registro de protocolos de Windows, lo que afecta a la forma en la que el equipo envía y recibe información a través de Internet.
Proveedores de servicios por niveles de Winsock	El software espía, el software publicitario y otros programas potencialmente no deseados que pueden instalar cambios en el registro de proveedores de servicios por niveles (LSP) Winsock para interceptar y modificar la información que se envía y se recibe a través de Internet.

guardián del sistema	Detecta...
Comandos de apertura de Shell de Windows	Los cambios no autorizados a comandos de apertura de shell de Windows que pueden permitir que se ejecuten gusanos y otros programas dañinos en el equipo.
Planificador de tareas compartidas	El software espía, el software publicitario y otros programas potencialmente no deseados que pueden realizar cambios en los archivos y el registro del planificador de tareas compartidas, lo que permite que se ejecuten archivos potencialmente dañinos al iniciar el equipo.
Windows Messenger Service	El software espía, el software publicitario y otros programas potencialmente no deseados que pueden realizar cambios en el registro de Windows messenger service, lo que permite que haya anuncios no solicitados y programas de ejecución remota en el equipo.
Archivo Win.ini de Windows	El software espía, el software publicitario y los programas potencialmente no deseados que pueden realizar cambios en el archivo Win.ini, lo que permite que se ejecuten programas sospechosos al iniciar el equipo.

Guardianes del sistema de navegadores

La tecnología de los Guardianes del sistema de navegadores ayuda a evitar la actividad no autorizada en los navegadores como la redirección a sitios Web sospechosos, cambios en los ajustes y en las opciones del navegador sin la formación adecuada y la confianza no autorizada en sitios Web sospechosos.

guardián del sistema	Detecta...
Objetos de ayuda del navegador	El software espía, el software publicitario y los programas potencialmente no deseados que pueden utilizar objetos del ayudante del navegador para rastrear navegaciones en la Web y mostrar anuncios no solicitados.
Barras de Internet Explorer	Los cambios no autorizados en el registro para programas de la barra de Internet Explorar tales como Buscar y Favoritos que pueden afectar a la apariencia y comportamiento de Internet Explorer.
Complementos de Internet Explorer	El software espía, el software publicitario y los programas potencialmente no deseados que pueden instalar complementos de Internet Explorer para rastrear navegaciones en la Web y mostrar anuncios no solicitados.

guardián del sistema	Detecta...
ShellBrowser de Internet Explorer	Los cambios no autorizados en el registro para el shell browser de Internet Explorer que pueden afectar a la apariencia y comportamiento del navegador Web.
WebBrowser de Internet Explorer	Los cambios no autorizados en el registro para el navegador Web de Internet Explorer que pueden afectar a la apariencia y comportamiento del navegador.
Hook de búsqueda de direcciones URL de Internet Explorer	El software espía, el software publicitario y otros programas potencialmente no deseados que pueden realizar cambios no autorizados en el registro de los hooks de búsqueda de direcciones URL de Internet Explorer, lo que permite enviar el navegador a sitios Web sospechosos cuando se hacen búsquedas en Internet.
Direcciones URL de Internet Explorer	El software espía, el software publicitario y otros programas potencialmente no deseados que pueden realizar cambios en el registro de las URL de Internet Explorer, lo que afecta a la configuración del navegador.
Restricciones de Internet Explorer	El software espía, el software publicitario y otros programas potencialmente no deseados que pueden realizar cambios en el registro de las restricciones de Internet Explorer, lo que afecta a la configuración y a las opciones del navegador.
Zonas de seguridad de Internet Explorer	El software espía, el software publicitario y otros programas potencialmente no deseados que pueden realizar cambios en el archivo de zonas de seguridad de Internet Explorer, lo que permite que se ejecuten archivos potencialmente dañinos al iniciar el equipo.
Sitios de confianza de Internet Explorer	El software espía, el software publicitario y otros programas potencialmente no deseados que pueden realizar cambios en el registro de sitios de confianza de Internet Explorer, lo que permite que el equipo confíe en sitios Web sospechosos.
Directiva de Internet Explorer	El software espía, el software publicitario y otros programas potencialmente no deseados que pueden realizar cambios en el registro de directivas de Internet Explorer, lo que afecta a la apariencia y comportamiento del navegador.

Uso de listas de confianza

Si VirusScan detecta un cambio en un archivo o en registro (Guardián del sistema), programa o desbordamiento de búfer, le pedirá que lo añada a una lista de confianza o lo elimine. Si confía en el elemento e indica que en el futuro no desea recibir ninguna notificación sobre esta actividad, el elemento se añade a una lista de confianza y VirusScan no lo detectará nunca más ni nos notificará sobre su actividad. Si se ha añadido un elemento a una lista de confianza pero decide bloquear esta actividad, puede hacerlo. El bloqueo evita que el elemento se ejecute y realice cambios en el ordenador sin notificarle cada vez que lo intenta. También puede quitar un elemento de una lista de confianza. Al quitarlo de la lista, VirusScan podrá detectar de nuevo la actividad del elemento.

Gestión de listas de confianza

Utilice el panel Listas de confianza para confiar en elementos que han sido detectados y en los que se ha confiado anteriormente o para bloquearlos. También puede quitar un elemento de una lista predeterminada para que VirusScan lo detecte de nuevo.

1 Abra el panel Listas de confianza.

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel Inicio de SecurityCenter, haga clic en **Equipo y archivos**.
3. En la zona información Equipo y archivos, haga clic en **Configurar**.
4. En el panel Configuración de Equipo y archivos, asegúrese de que la protección contra virus está activada y haga clic en **Avanzada**.
5. Haga clic en **Listas de confianza** en el panel Protección antivirus.

2 Seleccione uno de los siguientes tipos de listas de confianza:

- **Guardianes del sistema de programas**
- **Guardianes del sistema de Windows**
- **Guardianes del sistema de navegadores**
- **Programas definidos como fiables**
- **Desbordamiento de búfer de confianza**

3 En **Deseo**, elija una de las siguientes opciones:

- Para que el objeto detectado pueda realizar cambios en el registro de Windows o en archivos de sistema importantes de su ordenador sin tener que notificárselo a usted, haga clic en **Confiar**.

- Para evitar que el objeto detectado pueda realizar cambios en el registro de Windows o en archivos de sistema importantes de su ordenador sin tener que notificárselo a usted, haga clic en **Bloquear**.
- Para eliminar el elemento detectado de las listas de confianza, haga clic en **Eliminar**.

4 Haga clic en **Aceptar**.

Nota: para obtener más información sobre los tipos de listas de confianza, consulte Acerca de los tipos de listas de confianza (página 54).

Acerca de los tipos de listas de confianza

Los Guardianes del sistema del panel Listas de confianza representan los cambios no autorizados en el registro y en archivos que VirusScan ha detectado, pero a los que ha decidido asignar desde una alerta o desde el panel de Resultados del análisis. Hay cinco tipos de listas de confianza que pueden gestionarse desde el panel Listas de confianza: Guardianes del sistema de programas, Guardianes del sistema de Windows, Guardianes del sistema de navegadores, Programas fiables y Desbordamientos del búfer de confianza.

Opción	Descripción
Guardianes del sistema de programas	Los Guardianes del sistema de programas del panel Listas de confianza representan los cambios no autorizados en el registro y en archivos que VirusScan ha detectado, pero a los que ha decidido asignar desde una alerta o desde el panel de Resultados del análisis. Los Guardianes del sistema de programas detectan cambios no autorizados en el registro y en archivos asociados con instalaciones de ActiveX, elementos de inicio, hooks de ejecución en shell de Windows y con la actividad de carga retrasada de objeto de servicio de shell. Estos tipos de cambios no autorizados en el registro y en archivos pueden causar daños en el equipo, poner en riesgo la seguridad y dañar archivos importantes del sistema.

Opción	Descripción
Guardianes del sistema de Windows	Los Guardianes del sistema de Windows del panel Listas de confianza representan los cambios no autorizados en el registro y en archivos que VirusScan ha detectado, pero a los que ha decidido asignar desde una alerta o desde el panel de Resultados del análisis. Los Guardianes del sistema de Windows detectan cambios no autorizados en el registro y en archivos asociados con identificadores de menús contextuales, applnit DLLs, el archivo hosts de Windows, Shell Winlogon, proveedores de servicios por niveles (LSP) Winsock, etc. Estos tipos de cambios no autorizados en el registro o en los archivos pueden afectar al modo en que su ordenador envía y recibe la información en Internet, cambiar la apariencia y los hábitos de los programas y permitir la ejecución de programas sospechosos en su equipo.
Guardianes del sistema de navegadores	Los Guardianes del sistema de navegadores del panel Listas de confianza representan los cambios no autorizados en el registro y en archivos que VirusScan ha detectado, pero a los que ha decidido asignar desde una alerta o desde el panel de Resultados del análisis. Los Guardianes del sistema de navegadores detectan los cambios no autorizados en el registro y otros hábitos no autorizados asociados con objetos de ayuda del navegador, complementos de Internet Explorer, complementos de Internet Explorer, URL de Internet Explorer, zonas de seguridad de Internet Explorer, etc. Estos tipos de cambios no autorizados en el registro pueden producir una actividad no autorizada en los navegadores como la redirección a sitios Web sospechosos, cambios en los ajustes y en las opciones del navegador y la confianza en sitios Web sospechosos.
Programas definidos como fiables	Los programas fiables son programas no deseados potencialmente, detectados previamente por VirusScan, pero en los que ha decidido confiar a través de una alerta o a través del panel Resultados del análisis.

Opción	Descripción
Desbordamiento de búfer de confianza	Los desbordamientos del búfer representan una actividad no deseada anteriormente, detectada por VirusScan, pero en los que ha decidido confiar a través de una alerta o a través del panel Resultados del análisis. Los desbordamientos del búfer pueden causar daños en el equipo y dañar archivos. Los desbordamientos del búfer se producen cuando la cantidad de programas o de procesos de información sospechosos almacenada en un búfer supera su capacidad.

CAPÍTULO 11

Exploración del equipo

Al iniciar SecurityCenter por primera vez, la protección frente a virus en tiempo real de VirusScan comienza a proteger su equipo de virus, troyanos y otras amenazas a la seguridad potencialmente peligrosas. A menos que desactive la protección frente a virus en tiempo real, VirusScan supervisa su equipo de manera constante en busca de virus, analizando archivos cada vez que usted o su equipo accede a ellos, utilizando las opciones de análisis en tiempo real definidas por usted. Para asegurarse de que su equipo permanece protegido contra las amenazas de seguridad más recientes, active la protección contra virus en tiempo real y programe análisis manuales periódicos más exhaustivos. Para obtener más información acerca de definir las opciones del análisis en tiempo real y manual, consulte Configurar la protección frente a virus (página 39).

VirusScan ofrece un conjunto más detallado de opciones de análisis para la protección manual frente a virus, permitiéndole ejecutar de manera periódica análisis más amplios. Puede realizar los análisis manuales desde SecurityCenter, seleccionando ubicaciones específicas según un programa ya definido. Sin embargo, también puede realizar análisis manuales directamente en el Explorador de Windows mientras trabaja. El análisis en SecurityCenter tiene la ventaja de poder cambiar las opciones de análisis sin detener el análisis. Sin embargo, realizar un análisis desde el Explorador de Windows aporta un enfoque muy adecuado vinculado con la seguridad informática.

Ya realice un análisis manual desde SecurityCenter o desde el Explorador de Windows, puede visualizar los resultados del análisis cuando éste finalice. Los resultados de un análisis se visualizan para determinar si VirusScan ha detectado, reparado o puesto en cuarentena a virus, troyanos, programas espía, software publicitario, cookies y otros programas potencialmente no deseados. Los resultados de un análisis se pueden mostrar de diferentes formas. Por ejemplo, puede ver un resumen sencillo de los resultados de los análisis o información detallada, como el estado de la infección y el tipo. También puede ver estadísticas generales sobre el análisis y las detecciones.

En este capítulo

Analice su equipo

Puede realizar un análisis manual tanto desde el menú Avanzado como Básico de SecurityCenter. Si realiza un análisis desde el menú Avanzado, puede confirmar las opciones del análisis manual antes de iniciarlo. Si realiza un análisis desde el menú Básico, VirusScan comienza el análisis de manera inmediata, utilizando las opciones de análisis ya existentes. También puede realizar un análisis en Windows Explorer, mediante las opciones de análisis existentes.

- Siga uno de estos procedimientos:

  Análisis en SecurityCenter

Para...	Hacer esto...
Análisis con los ajustes ya existentes	Haga clic en **Analizar** en el menú Básico.
Análisis con los ajustes modificados	Haga clic en **Analizar** en el menú Avanzado, seleccione las ubicaciones en las que se va a realizar el análisis, seleccione las opciones de análisis y, a continuación, haga clic en **Analizar ahora**.

  Realizar un análisis en el Explorador de Windows

  1. Abra el Explorador de Windows.
  2. Haga clic con el botón derecho en un archivo, carpeta o unidad y, a continuación, haga clic en **Analizar**.

Nota: los resultados del análisis aparecen en la alerta de Análisis finalizado. Los resultados incluyen el número de elementos escaneados, detectados, reparados, puestos en cuarentena y eliminados. Haga clic en **Ver detalles del análisis** para saber más sobre los resultados del análisis o sobre cómo trabajar con elementos infectados.

Ver resultados del análisis

Cuando finaliza un análisis manual, debe ver los resultados para determinar qué se encontró y para analizar el estado de protección actual de su equipo. Los resultados de un análisis le indican si VirusScan ha detectado, reparado o puesto en cuarentena a virus, troyanos, programas espía, software publicitario, cookies y otros programas potencialmente no deseados.

- En el menú Básico o Avanzado, haga clic en **Analizar** y siga uno de los siguientes pasos:

Para...	Hacer esto...
Vea los resultados del análisis en la alerta	Vea los resultados del análisis en la alerta de Análisis finalizado.
Vea más información sobre resultados de análisis	Haga clic en **Ver detalles de análisis** en la alerta Análisis finalizado.
Vea un resumen rápido de los resultados de los análisis	Remítase al **icono Análisis finalizado** que se encuentra en el área de notificación de la barra de tareas.
Vea las estadísticas sobre análisis y detección	Haga doble clic en el icono **Análisis finalizado** que se encuentra en el área de notificación de la barra de tareas.
Vea detalles sobre los elementos detectados, el estado y el tipo de infección.	Haga doble clic en el icono **Análisis finalizado** que se encuentra en el área de notificación de la barra de tareas y, a continuación, haga clic en **Ver resultados** en el panel Progreso del análisis: Análisis manual.

CAPÍTULO 12

Trabajar con los resultados de análisis

Si VirusScan detecta una amenaza para la seguridad al ejecutar un análisis manual o en tiempo real, intentará gestionar la amenaza de manera automática según el tipo de amenaza. Por ejemplo, VirusScan intenta limpiar los archivos infectados si detecta un virus, troyano o cookie de rastreo en su equipo. Si no puede limpiar el archivo, VirusScan lo pone en cuarentena.

Cuando se enfrente a determinadas amenazas de seguridad, VirusScan no podrá limpiar o poner en cuarentena satisfactoriamente el archivo infectado. En este caso, VirusScan le pedirá que gestione la amenaza. Puede realizar diferentes acciones según el tipo de amenaza. Por ejemplo, si se detecta un virus en un archivo pero VirusScan no puede limpiar o ponerlo en cuarentena con éxito, también se denegará el acceso a dicho archivo. Si se detectan cookies de rastreo pero VirusScan no puede limpiarlas o ponerlas en cuarentena, puede decidir si eliminarlas o aceptarlas como elemento de confianza. Si se detectan programas potencialmente no deseados, VirusScan no realiza ninguna acción automática; en cambio, le permite decidir si poner el programa en cuarentena o clasificarlo como programa de confianza.

Cuando VirusScan pone elementos en cuarentena, los cifra y aísla en una carpeta para evitar que los archivos, programas o cookies dañen su equipo. Puede restaurar o eliminar los elementos en cuarentena. En la mayoría de los casos puede eliminar una cookie en cuarentena sin que eso le afecte a su equipo, sin embargo, si VirusScan ha puesto en cuarentena un programa que usted reconoce y utiliza, considere la posibilidad de restaurarlo.

En este capítulo

Trabajo con virus y troyanos

Si VirusScan detecta un virus o un troyano en un archivo de su equipo durante un análisis en tiempo real o manual, intentará limpiar el archivo. Si no puede limpiar el archivo, VirusScan intenta ponerlo en cuarentena. Si tampoco es posible realizar esta acción, se deniega el acceso al archivo (sólo en análisis en tiempo real).

1 Abra el panel Resultados del análisis.

¿Cómo?

1. Haga doble clic en el icono **Análisis finalizado** que se encuentra en el área de notificación que se encuentra en la zona más a la derecha de la barra de tareas.
2. En el panel Progreso del análisis: Análisis manual, haga clic en **Ver resultados**.

2 En la lista de resultados del análisis, haga clic en **Virus y troyanos**.

Nota: para trabajar con los archivos que VirusScan ha puesto en cuarentena, consulte Trabajar con archivos en cuarentena (página 63).

Trabaje con programas potencialmente no deseados

Si VirusScan detecta un programa potencialmente no deseado en su equipo durante un análisis en tiempo real o manual, puede eliminarlo o clasificarlo como programa de confianza. Eliminar el programa potencialmente no deseado no lo borra realmente del equipo. En cambio, al eliminarlo el programa se coloca en cuarentena para evitar que dañe su equipo o sus archivos.

1 Abra el panel Resultados del análisis.

¿Cómo?

1. Haga doble clic en el icono **Análisis finalizado** que se encuentra en el área de notificación que se encuentra en la zona más a la derecha de la barra de tareas.
2. En el panel Progreso del análisis: Análisis manual, haga clic en **Ver resultados**.

2 En la lista de resultados del análisis, haga clic en **Programas potencialmente no deseados.**

3 Seleccione un programa potencialmente no deseado.

4 En **Deseo**, haga clic en **Eliminar** o **Confiar**.

5 Confirme su opción seleccionada.

Trabaje con archivos en cuarentena

Cuando VirusScan pone los archivos infectados en cuarentena, los cifra y los coloca en una carpeta para evitar que dañen su equipo. A continuación, puede restaurar o eliminar los archivos en cuarentena.

1 Abra el panel Archivos en cuarentena.

¿Cómo?

1. En el panel izquierdo, haga clic en **Menú Avanzado**.
2. Haga clic en **Restaurar**.
3. Haga clic en **Archivos**.

2 Seleccione un archivo en cuarentena.

3 Siga uno de estos procedimientos:

- Para reparar el archivo infectado y devolverlo a su ubicación original en su equipo, haga clic en **Restaurar**.
- Para eliminar el archivo infectado del equipo, haga clic en **Eliminar**.

4 Haga clic en **Sí** para confirmar su opción seleccionada.

Sugerencia: puede restaurar o eliminar varios archivos al mismo tiempo.

Trabaje con programas y cookies en cuarentena

Cuando VirusScan pone en cuarentena programas potencialmente no deseados o cookies de rastreo, los cifra y después los coloca en una carpeta protegida para evitar que los programas o las cookies dañen el equipo. A continuación, puede restaurar o eliminar los elementos en cuarentena. En la mayoría de los casos puede eliminar un elemento en cuarentena sin que su equipo se vea afectado por ello.

1 Abra el panel Programas en cuarentena y cookies de rastreo.

¿Cómo?

1. En el panel izquierdo, haga clic en **Menú Avanzado**.
2. Haga clic en **Restaurar**.
3. Haga clic en **Programas y cookies**.

2 Seleccione un programa o cookie en cuarentena.

3 Siga uno de estos procedimientos:

- Para reparar el archivo infectado y devolverlo a su ubicación original en su equipo, haga clic en **Restaurar**.
- Para eliminar el archivo infectado del equipo, haga clic en **Eliminar**.

4 Haga clic en **Sí** para confirmar la operación.

Sugerencia: puede restaurar o eliminar varios programas y cookies al mismo tiempo.

CAPÍTULO 13

McAfee Personal Firewall

Personal Firewall ofrece protección avanzada para su equipo y sus datos personales. Personal Firewall establece una barrera entre su equipo e Internet y supervisa en segundo plano si se realizan operaciones de tráfico de Internet que resulten sospechosas.

Nota: SecurityCenter informa de los problemas de protección críticos y no críticos tan pronto como los detecta. Si necesita ayuda para diagnosticar sus problemas de protección, puede ejecutar McAfee Virtual Technician.

En este capítulo

Personal Firewall incluye

Personal Firewall proporciona las siguientes características.

Niveles de protección estándar y personalizada

Protege contra las intrusiones y las actividades sospechosas mediante la configuración de protección predeterminada o personalizable del cortafuegos.

Recomendaciones en tiempo real

Reciba recomendaciones de forma dinámica para ayudarle a determinar si debe concederse acceso a Internet a los programas o si el tráfico de red es fiable.

Gestión de acceso inteligente para los programas

Gestione el acceso a Internet de los programas mediante alertas y registros de eventos, y configure los permisos de acceso de programas específicos.

Protección para juegos

Evite que las alertas de intentos de intrusión y de actividades sospechosas lo distraigan cuando juegue en pantalla completa.

Protección al iniciar el equipo

Tan pronto como Windows® se inicia, el cortafuegos protege su equipo contra los intentos de intrusión, los programas no deseados y el tráfico de red.

Control de puertos de servicio del sistema

Gestione los puertos de servicio del sistema abiertos o cerrados necesarios para algunos programas.

Gestión de conexiones de equipo

Permite o bloquee conexiones remotas entre otros equipos y su propio equipo.

Integración de la información de HackerWatch

Rastree patrones globales de intrusión y piratería informática a través del sitio Web de HackerWatch, que también proporciona información de seguridad actual acerca de los programas de su equipo, así como de eventos de seguridad globales y de estadísticas de puertos de Internet.

Firewall bloqueado

Bloquee instantáneamente todo el tráfico de red entrante y saliente entre el equipo e Internet.

Restaurar Firewall

Restaure al instante la configuración de protección original del cortafuegos.

Detección avanzada de troyanos

Detecte y bloquee aplicaciones potencialmente malintencionadas como, por ejemplo, troyanos, y evite que pasen sus datos personales a Internet.

Registro de eventos

Rastree los eventos de intrusión, entrantes y salientes.

Control del tráfico de Internet

Revise mapas de todo el mundo que muestran el origen de los ataques hostiles y el tráfico. También localiza información detallada de propiedad y datos geográficos correspondientes a las direcciones IP de origen. Además, analice el tráfico entrante y saliente, controle el ancho de banda del programa y la actividad del programa.

Prevención de intrusiones

Proteja su privacidad contra las posibles amenazas de Internet. Gracias a la función heurística, McAfee proporciona un tercer nivel de protección mediante el bloqueo de los elementos que muestren indicios de ataque o intentos de piratería.

Análisis de tráfico sofisticado

Firewall revisa el tráfico entrante y saliente de Internet, así como las conexiones de programas, incluidas aquéllas que están "a la escucha" de conexiones abiertas. Esto permite a los usuarios ver los programas que pueden ser susceptibles de intrusión y actuar en consecuencia.

CAPÍTULO 14

Iniciar el cortafuegos

Desde el mismo momento en que instala el cortafuegos, su equipo queda protegido contra las intrusiones y el tráfico de red no deseado. Por otra parte, ya puede responder a las alertas y gestionar el acceso entrante y saliente a Internet, tanto para programas conocidos como desconocidos. Las recomendaciones inteligentes y el nivel de seguridad fiable (con la opción para permitir programas de acceso saliente a Internet seleccionada) se activan automáticamente.

Si bien puede deshabilitar el cortafuegos desde el panel Configuración de Internet y redes, su equipo ya no estará protegido contra intrusiones y tráfico de red no deseado; tampoco podrá gestionar de manera eficiente las conexiones de Internet entrantes y salientes. Si tiene que deshabilitar la protección del cortafuegos, hágalo de manera temporal y sólo cuando sea realmente necesario. También puede habilitar el cortafuegos desde el panel Configuración de Internet y redes.

El cortafuegos desactiva automáticamente el servidor de seguridad de Windows y se establece como cortafuegos predeterminado.

Nota: Para configurar el cortafuegos, abra el panel Configuración de Internet y redes.

En este capítulo

Iniciar la protección de Firewall

Puede activar el cortafuegos para proteger su equipo contra intrusiones y tráfico de red no deseado, así como gestionar las conexiones a Internet entrantes y salientes.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está desactivada**, haga clic en **Activado**.

Detener la protección de Firewall

Puede desactivar el cortafuegos si no desea proteger su equipo contra intrusiones y tráfico de red no deseado. Cuando el cortafuegos está desactivado, no se pueden gestionar las conexiones entrantes y salientes de Internet.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Desactivado**.

CAPÍTULO 15

Trabajar con alertas

El cortafuegos emplea todo un abanico de alertas para que gestione su seguridad con mayor facilidad. Las alertas se agrupan en tres tipos básicos:

- Alerta roja
- Alerta amarilla
- Alerta verde

Las alertas también pueden contener información de ayuda para que el usuario pueda decidir mejor cómo ordenar las alertas o bien obtener información relativa a los programas que se ejecutan en su equipo.

En este capítulo

Acerca de las alertas

El cortafuegos dispone de tres tipos de alerta básicos. A su vez, algunas alertas incluyen información relativa a los programas que se ejecutan en su equipo o sobre cómo obtener información.

Alerta roja

Una alerta roja que aparece cuando el cortafuegos detecta, y luego bloquea, un troyano en su equipo, y recomienda que analice el equipo en busca de más amenazas. Los troyanos tienen el aspecto de programas válidos, pero pueden trastornar o dañar los equipos, así como proporcionar acceso no autorizado a ellos. Esta alerta se produce en todos los niveles de seguridad, salvo en Abrir.

Alerta amarilla

El tipo de alerta más habitual es la alerta amarilla, que información activa de la actividad de un programa o un evento de red detectado por cortafuegos. Cuando esto se produce, la alerta describe la actividad del programa o el evento de red y, a continuación, proporciona una o varias opciones que necesitan respuesta. Por ejemplo, la alerta **Nueva red detectada** aparece cuando un equipo con cortafuegos instalado se conecta a una red nueva. Puede elegir entre confiar o no confiar en la red. Si la red es fiable, el cortafuegos permite el tráfico desde cualquier otro equipo de la red y la agrega a las Direcciones IP fiables. Si Recomendaciones inteligentes está habilitada, los programas se agregan al panel Permisos de programas.

Alerta verde

En la mayoría de los casos, una alerta verde proporciona información básica acerca de un evento y no requiere ningún tipo de respuesta. De forma predeterminada, las alertas verdes están desactivadas y, por lo general, se producen cuando se establecen los niveles de seguridad Estándar, Fiable, Estricta y Furtivo.

Ayuda al usuario

Muchas alertas del cortafuegos contienen información adicional para facilitarle la gestión de la seguridad de su equipo y consisten en lo siguiente:

- **Obtener más información sobre este programa**: Inicie el sitio Web de seguridad global de McAfee para obtener información acerca de un programa que el cortafuegos ha detectado en su equipo.

- **Notifique a McAfee la existencia de este programa**: Envíe información a McAfee acerca de un archivo desconocido que el cortafuegos ha detectado en su equipo.
- **Recomendaciones de McAfee**: Consejos sobre cómo gestionar las alertas. Por ejemplo, una alerta le puede recomendar que permita acceso a un programa.

CAPÍTULO 16

Gestionar las alertas informativas

El cortafuegos permite visualizar u ocultar alertas de información cuando detecta intentos de intrusión o actividad sospechosa durante determinados eventos; por ejemplo, cuando se juega en pantalla completa.

En este capítulo

Mostrar las alertas mientras se juega

Puede permitir que las alertas de cortafuego informativas se visualicen cuando detecta intentos de intrusión o actividad sospechosa cuando se juega en pantalla completa.

1. En el panel McAfee SecurityCenter, haga clic en **Menú avanzado**.
2. Haga clic en **Configurar**.
3. En el panel Configuración de SecurityCenter, en **Acerca de las alertas** haga clic en **Avanzado**.
4. En el panel Opciones de alerta, seleccione **Mostrar alertas informativas cuando se detecte el modo de juegos**.
5. Haga clic en **Aceptar**.

Ocultar alertas informativas

Puede evitar que las alertas de cortafuego informativas se visualicen cuando detecte intentos de intrusión o una actividad sospechosa.

1. En el panel McAfee SecurityCenter, haga clic en **Menú avanzado**.
2. Haga clic en **Configurar**.
3. En el panel Configuración de SecurityCenter, en **Acerca de las alertas** haga clic en **Avanzado**.
4. En el panel Configuración de SecurityCenter, haga clic en **Alertas informativas**.
5. En el panel Alertas informativas, realice una de las siguientes operaciones:
   - Seleccione **No mostrar alertas informativas** para que se oculten todas las alertas informativas.

- Despeje una alerta para ocultarla.

6 Haga clic en **Aceptar**.

CAPÍTULO 17

Configurar la protección del cortafuegos

El cortafuegos le ofrece varios métodos para gestionar su seguridad y personalizar su respuesta a las alertas y los eventos relacionados con la seguridad.

Después de instalar el cortafuegos por primera vez, el nivel de seguridad de la protección de su equipo se establecerá en Fiable y se permitirá un acceso a Internet únicamente saliente. A pesar de ello, el cortafuegos proporciona otros niveles, desde el más restrictivo al más permisivo.

El cortafuegos también le ofrece la posibilidad de recibir recomendaciones sobre alertas y acceso a Internet para programas.

En este capítulo

Gestionar los niveles de seguridad del cortafuegos

Los niveles de seguridad del cortafuegos controlan el grado de gestión y respuesta a las alertas. Estas alertas aparecen cuando se detecta tráfico de red no deseado y conexiones de Internet entrantes y salientes. De forma predeterminada, el nivel de seguridad del cortafuegos se establece en Fiable, con acceso únicamente saliente.

Cuando se establece el nivel de seguridad Fiable y las recomendaciones inteligentes están activadas, las alertas amarillas dan la opción de permitir o bloquear el acceso a programas desconocidos que necesitan un acceso entrante. Cuando se detectan programas conocidos, aparecen alertas informativas de color verde y se les permite el acceso de forma automática. Permitir el acceso a un programa significa permitirle establecer conexiones salientes y escuchar conexiones entrantes no solicitadas.

Por lo general, cuanto más restrictivo es un nivel de seguridad (Furtiva y Estricta), mayor es el número de opciones y alertas que se muestran y que, por consiguiente, deberá gestionar.

En la tabla siguiente se describen los seis niveles de seguridad del cortafuegos, empezando por el más estricto y acabando por el menos:

Nivel	Descripción
Bloquear tráfico	Bloquea todas las conexiones de red entrantes y salientes, incluido el acceso a los sitios Web, al correo electrónico y a las actualizaciones de seguridad. Este nivel de seguridad da el mismo resultado que si eliminara su conexión de Internet. Puede utilizar esta opción para bloquear puertos que haya definido como abiertos en el panel Servicios del sistema.
Furtivo	Bloquea todas las conexiones de Internet entrantes, salvo los puertos abiertos y oculta la presencia del equipo en Internet. El cortafuegos le alertará cuando un nuevo programa intente una conexión saliente a Internet o si recibe solicitudes de conexión entrantes. Los programas bloqueados y agregados aparecen en el panel Permisos de programas.
Estricta	Alerta cuando un nuevo programa intente una conexión saliente a Internet o si recibe solicitudes de conexión entrantes. Los programas bloqueados y agregados aparecen en el panel Permisos de programas. Si el nivel de seguridad está definido como Estricta, un programa sólo solicita el tipo de acceso que necesita en ese momento, por ejemplo acceso sólo saliente, que usted le puede permitir o bloquear. Más adelante, si el programa solicita tanto una conexión entrante como saliente, puede permitir acceder desde el panel Permisos de programas.

Nivel	Descripción
Estándar	Controla las conexiones entrantes y salientes y le avisa cuando un nuevo programa intente acceder a Internet. Los programas bloqueados y agregados aparecen en el panel Permisos de programas.
Fiable	Permite que los programas tengan acceso entrante y saliente (completo) o sólo saliente. El nivel de seguridad predeterminado es Fiable con la opción para permitir que los programas tengan acceso únicamente saliente seleccionada. Si se permite acceso completo a un programa, el cortafuegos confiará automáticamente en él y lo agregará a la lista de programas permitidos en el panel Permisos de programa. Si se permite acceso únicamente saliente a un programa, el cortafuegos confiará automáticamente en él cuando efectúan una conexión a Internet saliente únicamente. No se confía automáticamente en una conexión entrante.
abierta	Permite acceder a todas las conexiones de Internet entrantes y salientes.

El cortafuegos también le permite restablecer de inmediato su nivel de seguridad en Fiable (y permitir acceso únicamente saliente) desde el panel Restaurar valores predeterminados de protección del cortafuegos.

Definir el nivel de seguridad como Bloqueada

Puede establecer el nivel de seguridad de cortafuegos en Bloquear tráfico para bloquear todas las conexiones de red entrantes y salientes.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Nivel de seguridad, mueva el control deslizante de manera que aparezca **Bloqueada** como el nivel actual.
4. Haga clic en **Aceptar**.

Definir el nivel de seguridad como Furtiva

Puede establecer el nivel de seguridad del cortafuegos en Furtivo para bloquear todas las conexiones de red entrantes, salvo los puertos abiertos, y ocultar la presencia del equipo en Internet.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Nivel de seguridad, mueva el control deslizante de manera que aparezca **Furtiva** como el nivel actual.
4. Haga clic en **Aceptar**.

Nota: en el modo invisible, el cortafuegos le alerta cuando nuevos programas solicitan una conexión de Internet saliente o reciben solicitudes de conexión entrantes.

Definir el nivel de seguridad como Estricta

Puede establecer el nivel de seguridad del cortafuegos en Estricto para recibir alertas cuando hay programas nuevos que intentan conexiones salientes a Internet o reciben solicitudes de conexión entrantes.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Nivel de seguridad, mueva el control deslizante de manera que aparezca **Estricta** como el nivel actual.
4. Haga clic en **Aceptar**.

Nota: en el modo Estricto, un programa sólo solicita el tipo de acceso que necesita en esos momentos; por ejemplo, sólo acceso saliente, que el usuario puede permitir o bloquear. Si el programa solicita más adelante tanto una conexión entrante como saliente, puede permitir acceder desde el panel Permisos de programas.

Definir el nivel de seguridad como Estándar

Puede establecer el nivel de seguridad en Estándar para controlar las conexiones entrantes o salientes y que le alerte cuando nuevos programas intenten acceder a Internet.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Nivel de seguridad, mueva el control deslizante de manera que aparezca **Estándar** como el nivel actual.
4. Haga clic en **Aceptar**.

Definir el nivel de seguridad como Fiable

Puede establecer el nivel de seguridad del cortafuegos en Fiable para permitir un acceso completo o sólo un acceso saliente.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Nivel de seguridad, mueva el control deslizante de manera que aparezca **Fiable** como el nivel actual.
4. Siga uno de estos procedimientos:
   - Para permitir un acceso de red entrante y saliente completo, seleccione **Permitir acceso pleno**.
   - Para permitir sólo el acceso saliente de la red, seleccione **Permitir sólo acceso saliente**.
5. Haga clic en **Aceptar**.

Nota: la opción predeterminada es **Permitir sólo acceso saliente**.

Definir el nivel de seguridad como Abierta

Puede establecer el nivel de seguridad del cortafuegos en Abrir para permitir todas las conexiones de red entrantes y salientes.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Nivel de seguridad, mueva el control deslizante de manera que aparezca **Abierta** como el nivel actual.
4. Haga clic en **Aceptar**.

Configurar Recomendaciones inteligentes para alertas

Puede configurar el cortafuegos para incluir, excluir o mostrar recomendaciones en alertas cuando algún programa intenta acceder a Internet. Al habilitar Recomendaciones inteligentes obtendrá ayuda para decidir la manera cómo ordenar las alertas.

Cuando Recomendaciones inteligentes está activado (y el nivel de seguridad está establecido en Fiable con sólo el acceso saliente activado), el cortafuegos permite o bloquea automáticamente los programas conocidos, y muestra en la alerta una recomendación cuando detecta programas potencialmente peligrosos.

Por el contrario, cuando Recomendaciones inteligentes está desactivado, el cortafuegos ni permite ni bloquea el acceso a Internet, ni recomienda ningún plan de acción en la alerta.

Cuando Recomendaciones inteligentes está establecido en Sólo mostrar, una alerta solicita al usuario que permita o bloquee el acceso, y recomienda un plan de acción en la alerta.

Habilitar Recomendaciones inteligentes

Puede activar Recomendaciones inteligentes para que el cortafuegos permita o bloquee automáticamente programas y le alerte sobre programas no reconocidos y potencialmente peligrosos.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Nivel de seguridad, en **Recomendaciones inteligentes**, seleccione **Habilitar Recomendaciones inteligentes**.
4. Haga clic en **Aceptar**.

Deshabilitar Recomendaciones inteligentes

Puede desactivar Recomendaciones inteligentes para que el cortafuegos permita o bloquee programas y le alerte sobre programas no reconocidos y potencialmente peligrosos. No obstante, las alertas no incluirán ninguna recomendación acerca de cómo tratar el acceso de los programas. Si el cortafuegos detecta un programa nuevo que parece sospechoso o que se sabe que puede ser una amenaza, bloqueará automáticamente el acceso a Internet a este programa.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Nivel de seguridad, en **Recomendaciones inteligentes**, seleccione **Deshabilitar Recomendaciones inteligentes**.
4. Haga clic en **Aceptar**.

Mostrar sólo recomendaciones inteligentes

Puede mostrar Recomendaciones inteligentes para que las alertas proporcionen recomendaciones de plan de acción únicamente, a fin de que el usuario pueda decidir si permitirá o bloqueará los programas no reconocidos y potencialmente peligrosos.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Nivel de seguridad, en **Recomendaciones inteligentes**, seleccione **Mostrar sólo**.
4. Haga clic en **Aceptar**.

Optimizar la seguridad del cortafuegos

Existen muchas maneras de poner en peligro la seguridad de su equipo. Por ejemplo, algunos programas pueden intentar conectarse a Internet antes de que se inicie Windows®. Asimismo, otros usuarios informáticos pueden lograr una solicitud de ping en su equipo que les permita saber si está conectado a una red. El cortafuegos le permite defenderse contra estos dos tipos de intrusión porque le da la posibilidad de deshabilitar la protección de inicio y de bloquear las solicitudes de ping. La primera opción bloquea a los programas el acceso a Internet cuando Windows se inicia y la segunda bloquea las solicitudes de ping que permiten a otros usuarios detectar su equipo en una red.

La configuración de instalación estándar incluye una detección automática para los intentos de intrusión más comunes, como los ataques de denegación de servicio o vulnerabilidades. Al utilizar esta configuración se garantiza su protección contra estos ataques y análisis. No obstante, puede deshabilitar la detección automática de uno o varios ataques y análisis en el panel Detección de intrusiones.

Proteger su equipo durante el inicio

Puede proteger su equipo cuando Windows se inicia, para bloquear los programas nuevos que no tenían acceso a Internet durante el arranque y ahora lo necesitan. El cortafuegos muestra las alertas pertinentes para los programas que han solicitado acceso a Internet, que el usuario puede permitir o bloquear. Para utilizar esta opción, su nivel de seguridad no debe estar definido como Abierta o Bloqueada.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Nivel de seguridad, en **Configuración de seguridad**, seleccione **Habilite la protección al iniciar**.
4. Haga clic en **Aceptar**.

Nota: Las conexiones e intrusiones bloqueadas no quedan registradas mientras la protección al iniciar está habilitada.

Configurar solicitudes de ping

Puede permitir o evitar que otros usuarios de equipos detecten su equipo en la red.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Nivel de seguridad, en **Configuración de seguridad**, realice una de las siguientes acciones:
   - Seleccione **Permitir solicitudes de ping ICMP** para permitir que se detecte su equipo en la red mediante solicitudes de ping.
   - Borre **Permitir solicitudes de ping ICMP** para impedir que se detecte su equipo en la red mediante solicitudes de ping.
4. Haga clic en **Aceptar**.

Configurar la detección de intrusiones

Puede detectar los intentos de intrusión para proteger su equipo contra los ataques y los análisis no autorizados. La configuración estándar el cortafuegos incluye la detección automática de los intentos de intrusión más habituales como, por ejemplo, los ataques de denegación de servicio o vulnerabilidades; no obstante, puede desactivar la detección automática de uno o varios ataques o análisis.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos haga clic en **Detección de intrusiones**.
4. En **Detectar intentos de intrusión**, realice una de las siguientes opciones:
   - Seleccione un nombre para detectar el ataque o el análisis de manera automática.
   - Borre un nombre para deshabilitar la detección automática del ataque o el análisis.
5. Haga clic en **Aceptar**.

Configurar los estados de protección del cortafuegos

Puede configurar el cortafuegos para que no tenga en cuenta que problemas específicos de su equipo no se notifican a SecurityCenter.

1. En el panel McAfee SecurityCenter, en **Información de SecurityCenter**, haga clic en **Configurar**.
2. En el panel Configuración de SecurityCenter, en **Estado de protección** haga clic en **Avanzado**.
3. En el panel Problemas omitidos, seleccione una o más de las opciones siguientes:
   - **La protección del cortafuegos está desactivada.**
   - **El cortafuegos está configurado con nivel de seguridad Abierta.**
   - **El servicio de cortafuegos no está en funcionamiento.**
   - **La protección del cortafuegos no está instalada en su equipo.**
   - **Su cortafuegos de Windows está desactivado.**
   - **El cortafuegos saliente no está instalado en este equipo.**
4. Haga clic en **Aceptar**.

Bloquear y restaurar el cortafuegos

Bloquear tráfico bloquea al instante todo el tráfico de red entrante y saliente para ayudarle a aislar y solucionar un problema de su equipo.

Bloquear el cortafuegos de manera instantánea

Puede bloquear el cortafuegos para que bloquee al instante todo el tráfico de red entre el equipo e Internet.

1. En el panel McAfee SecurityCenter, bajo **Tareas comunes**, haga clic en **Firewall bloqueado**.
2. En el panel Bloquear cortafuegos haga clic en **Bloquear**.
3. Haga clic en **Sí** para confirmar.

Sugerencia: también puede bloquear el cortafuegos pulsando con el botón derecho del ratón en el icono de SecurityCenter en el área de notificación ubicada en el extremo derecho de la barra de tareas y, a continuación, haciendo clic en **Vínculos rápidos** y en **Firewall bloqueado**.

Desbloquear el cortafuegos de manera instantánea

Puede desbloquear el cortafuegos para que permita al instante todo el tráfico de red entre el equipo e Internet.

1. En el panel McAfee SecurityCenter, bajo **Tareas comunes**, haga clic en **Firewall bloqueado**.
2. En el panel Bloqueo activado, haga clic en **Desbloquear**.
3. Haga clic en **Sí** para confirmar.

Restaurar la configuración del cortafuegos

Puede restaurar el cortafuegos con su configuración de protección original rápidamente. Esta restauración restablece el nivel de seguridad en Fiable y permite sólo el acceso saliente de red, activa las recomendaciones inteligentes, restaura la lista de programas predeterminados y sus permisos en el panel Permisos de programa, elimina las direcciones IP fiables y no permitidas y restaura los servicios del sistema, la configuración del registro de eventos y la detección de intrusiones.

1. En el panel McAfee SecurityCenter, haga clic en **Restaurar valores predeterminados del cortafuegos**.
2. En el panel Restaurar valores predeterminados de protección del cortafuegos, haga clic en **Restaurar valores predeterminados**.
3. Haga clic en **Sí** para confirmar.

Sugerencia: también puede restaurar la configuración predeterminada del cortafuegos pulsando con el botón derecho del ratón en el icono de SecurityCenter en el área de notificación ubicada en el extremo derecho de la barra de tareas y, a continuación, haciendo clic en **Vínculos rápidos** y en **Restaurar valores predeterminados del cortafuegos**.

CAPÍTULO 18

Gestionar programas y permisos

El cortafuegos le permite gestionar y crear permisos de acceso tanto para programas ya existentes como para programas nuevos que soliciten acceso a Internet entrante y saliente. El cortafuegos le permite controlar el acceso pleno o sólo saliente a estos programas. Aunque también puede bloquearles el acceso.

En este capítulo

Permiso de acceso a Internet para los programas

Algunos programas, como los navegadores de Internet, necesitan acceder a Internet para funcionar correctamente.

El cortafuegos le permite utilizar el panel Permisos de programas para:

- Permite el acceso a los programas
- Permite a los programas sólo acceso saliente
- Bloquear el acceso a los programas

También puede permitir que un programa tenga acceso pleno o sólo saliente desde el registro Eventos salientes y eventos recientes.

Conceder acceso pleno a un programa

Puede permitir que un programa bloqueado de su equipo tenga acceso pleno entrante y saliente a Internet.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos haga clic en **Permisos de programas**.
4. En **Permisos de programas**, seleccione un programa con **Bloqueado** o **Acceso sólo saliente**.
5. En **Acción**, haga clic en **Permitir acceso**.
6. Haga clic en **Aceptar**.

Conceder acceso pleno a un programa nuevo

Puede permitir que un programa nuevo de su equipo tenga acceso pleno entrante y saliente a Internet.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos haga clic en **Permisos de programas**.
4. En **Permisos de programas**, haga clic en **Agregar programa con permiso**.
5. En el cuadro de diálogo **Agregar programa**, navegue hasta el programa que desee agregar y selecciónelo; a continuación, haga clic en **Abrir**.

Nota: Puede modificar los permisos de un programa recién agregado como lo haría con un programa ya existente, es decir, seleccionando el programa y haciendo clic en **Permitir sólo acceso saliente** o bien **Bloquear acceso** en **Acción**.

Permitir acceso pleno desde el registro Eventos recientes

Puede permitir que un programa bloqueado existente que aparece en el registro de eventos recientes tenga acceso pleno entrante y saliente a Internet.

1. En el panel McAfee SecurityCenter, haga clic en **Menú avanzado**.
2. Haga clic en **Informes & registros**.
3. En **Eventos recientes**, seleccione la descripción del evento y luego haga clic en **Permitir acceso**.
4. En el cuadro de diálogo Permisos de programa, haga clic en **Sí** para confirmar.

Temas relacionados

- Ver eventos salientes (página 121)

Permitir acceso pleno desde el registro Eventos salientes

Puede permitir que un programa bloqueado existente que aparece en el registro de eventos salientes tenga acceso pleno entrante y saliente a Internet.

1. En el panel McAfee SecurityCenter, haga clic en **Menú avanzado**.
2. Haga clic en **Informes & registros**.
3. En **Eventos recientes**, haga clic en **Ver registro**.
4. Haga clic en **Internet y redes** y, a continuación, en **Eventos salientes**.
5. Seleccione un programa y en **Deseo**, haga clic en **Permitir acceso**.
6. En el cuadro de diálogo Permisos de programa, haga clic en **Sí** para confirmar.

Permiso para programas de sólo acceso saliente

Algunos programas de su equipo necesitan un acceso a Internet saliente. El cortafuegos le permite configurar permisos para que sea posible el acceso sólo saliente a Internet.

Permitir a un programa sólo acceso saliente

Puede permitir que un programa tenga un acceso a Internet sólo saliente.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos haga clic en **Permisos de programas**.
4. En **Permisos de programas**, seleccione un programa con **Bloqueado** o **Acceso pleno**.
5. En **Acción**, haga clic en **Permitir sólo acceso saliente**.
6. Haga clic en **Aceptar**.

Permitir sólo acceso saliente desde el registro Eventos recientes

Puede permitir que un programa bloqueado existente que aparece en el registro de eventos recientes tenga sólo acceso saliente a Internet.

1. En el panel McAfee SecurityCenter, haga clic en **Menú avanzado**.
2. Haga clic en **Informes & registros**.
3. En **Eventos recientes**, seleccione la descripción del evento y luego haga clic en **Permitir sólo acceso saliente**.
4. En el cuadro de diálogo Permisos de programa, haga clic en **Sí** para confirmar.

Permitir sólo acceso saliente desde el registro Eventos salientes

Puede permitir que un programa bloqueado existente que aparece en el registro de eventos salientes tenga sólo acceso saliente a Internet.

1. En el panel McAfee SecurityCenter, haga clic en **Menú avanzado**.
2. Haga clic en **Informes & registros**.
3. En **Eventos recientes**, haga clic en **Ver registro**.
4. Haga clic en **Internet y redes** y, a continuación, en **Eventos salientes**.
5. Seleccione un programa y en **Deseo**, haga clic en **Permitir sólo acceso saliente**.
6. En el cuadro de diálogo Permisos de programa, haga clic en **Sí** para confirmar.

Bloquear el acceso a Internet a los programas

El cortafuegos le permite bloquear los programas para que no accedan a Internet. Asegúrese de que al bloquear un programa no se va a interrumpir su conexión a Internet o la de otro programa que necesite acceso a Internet para funcionar correctamente.

Bloquear el acceso a los programas

Puede bloquear un programa para que no tenga acceso entrante ni saliente a Internet.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos haga clic en **Permisos de programas**.
4. En **Permisos de programas**, seleccione un programa con **Acceso pleno** o **Sólo acceso saliente**.
5. En **Acción**, haga clic en **Bloquear acceso**.
6. Haga clic en **Aceptar**.

Bloquear el acceso a un nuevo programa

Puede bloquear un programa nuevo para que no tenga acceso entrante ni saliente a Internet.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos haga clic en **Permisos de programas**.
4. En **Permisos de programas**, haga clic en **Agregar programa bloqueado**.
5. En el cuadro de diálogo Agregar programa, navegue hasta el programa que desee agregar y selecciónelo; a continuación, haga clic en **Abrir**.

Nota: Puede modificar los permisos de un programa recién agregado seleccionando el programa y haciendo clic en **Permitir sólo acceso saliente** o bien **Permitir acceso** en **Acción**.

Bloquear el acceso desde el registro Eventos recientes

Puede bloquear un programa que aparezca en el registro Eventos recientes para que no tenga acceso entrante ni saliente a Internet.

1. En el panel McAfee SecurityCenter, haga clic en **Menú avanzado**.
2. Haga clic en **Informes & registros**.
3. En **Eventos recientes**, seleccione la descripción del evento y luego haga clic en **Bloquear acceso**.
4. En el cuadro de diálogo Permisos de programa, haga clic en **Sí** para confirmar.

Eliminar los permisos de acceso de los programas

Antes de eliminar un permiso de un programa, asegúrese de que su ausencia no afectará a la funcionalidad de su equipo o de su conexión a Internet.

Eliminar un permiso de programa

Puede hacer que un programa no tenga acceso entrante ni saliente a Internet.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos haga clic en **Permisos de programas**.
4. En **Permisos de programas**, seleccione un programa.
5. En **Acción**, haga clic en **Eliminar permiso de programa**.
6. Haga clic en **Aceptar**.

Nota: El cortafuegos le impide modificar algunos programas mediante la atenuación y la desactivación de determinadas acciones.

Obtener información sobre los programas

Si no está seguro de qué permiso de programa debe aplicar, puede obtener información acerca del programa en el sitio Web HackerWatch de McAfee.

Obtener información sobre un programa

Puede obtener información del programa en el sitio Web HackerWatch de McAfee para decidir si permitirá o bloqueará el acceso entrante y saliente a Internet.

Nota: asegúrese de que está conectado a Internet para que su navegador pueda lanzar correctamente el sitio Web HackerWatch de McAfee; allí encontrará información actualizada sobre los programas, los requisitos de acceso a Internet y las amenazas de seguridad.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos haga clic en **Permisos de programas**.
4. En **Permisos de programas**, seleccione un programa.
5. En **Acción**, haga clic en **Más información**.

Obtener información sobre el programa desde el registro Eventos salientes

En el registro de eventos salientes, puede obtener información del programa en el sitio Web HackerWatch de McAfee para decidir a qué programas permitirá o bloqueará el acceso entrante y saliente a Internet.

Nota: asegúrese de que está conectado a Internet para que su navegador pueda lanzar correctamente el sitio Web HackerWatch de McAfee; allí encontrará información actualizada sobre los programas, los requisitos de acceso a Internet y las amenazas de seguridad.

1. En el panel McAfee SecurityCenter, haga clic en **Menú avanzado**.
2. Haga clic en **Informes & registros**.
3. En Eventos recientes, seleccione un evento y haga clic en **Ver registro**.
4. Haga clic en **Internet y redes** y, a continuación, en **Eventos salientes**.
5. Seleccione una dirección IP y haga clic en **Más información**.

CAPÍTULO 19

Gestionar los servicios del sistema

Para funcionar correctamente, algunos programas (incluidos los servidores Web o programas servidores de intercambio de archivos), deben aceptar conexiones no solicitadas procedentes de otros equipos a través de puertos de servicio de sistema designados. El cortafuegos suele cerrar estos puertos de servicio de sistema porque constituyen el origen más probable de las inseguridades en su sistema. Sin embargo, para aceptar conexiones procedentes de equipos remotos, los puertos de servicio de sistema deben estar abiertos.

En este capítulo

Configurar puertos de servicio del sistema

Los puertos de servicio del sistema pueden configurarse para permitir o bloquear el acceso en red remoto a un servicio de su equipo.

La lista que mostramos a continuación muestra los servicios del sistema habituales, así como sus puertos asociados:

- Protocolo de transferencia de archivos (FTP): puertos 20-21
- Servidor de correo (IMAP): puerto 143
- Servidor de correo (POP3): puerto 110
- Servidor de correo (SMTP): puerto 25
- Servidor de directorio de Microsoft (MSFT DS): puerto 445
- Microsoft SQL Server (MSFT SQL): puerto 1433
- Network Time Protocol: puerto 123
- Puerto de Remote Desktop/Asistencia remota/Terminal Server (RDP): 3389
- Llamadas a procedimientos remotos (RPC): puerto 135
- Servidor Web seguro (HTTPS): puerto 443
- Plug and Play universal (UPNP): puerto 5000
- Servidor Web (HTTP): puerto 80
- Archivos compartidos en Windows (NETBIOS): puertos 137-139

Los puertos del servicio de sistema también se pueden configurar para que un equipo pueda compartir su conexión a Internet con otros equipos conectados a él a través de la misma red. Esta conexión, conocida como Conexión compartida a Internet (ICS), permite al equipo que comparte la conexión actuar como puerta de enlace a Internet para el otro equipo de la red.

Nota: si el equipo tiene una aplicación que acepta conexiones de servidor a Web o FTP, es posible que el equipo que comparta la conexión necesite abrir el puerto del servicio del sistema asociado y permitir el reenvío de las conexiones entrantes para dichos puertos.

Permitir el acceso a un puerto de servicio del sistema existente

Puede abrir un puerto existente para permitir el acceso remoto a un servicio de red del equipo.

Nota: un puerto de servicio del sistema abierto puede dejar a su equipo totalmente vulnerable ante las amenazas de seguridad de Internet, por lo que es mejor que sólo abra un puerto cuando sea necesario.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos haga clic en **Servicios del sistema**.
4. En **Abrir puerto de servicio del sistema**, seleccione un servicio del sistema para que abra su puerto.
5. Haga clic en **Aceptar**.

Bloquear el acceso a un puerto de servicio del sistema existente

Puede cerrar un puerto existente para bloquear el acceso remoto a un servicio del equipo.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos haga clic en **Servicios del sistema**.
4. En **Abrir puerto de servicio del sistema**, borre un servicio del sistema para que cierre su puerto.
5. Haga clic en **Aceptar**.

Configurar un puerto de servicio del sistema

Puede configurar un puerto de servicio de red nuevo en su equipo, que pueda abrir o cerrar para permitir o bloquear el acceso remoto en su equipo.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos haga clic en **Servicios del sistema**.
4. Haga clic en **Agregar**.
5. En el panel Servicios del sistema, en **Puertos y servicios del sistema**, introduzca lo siguiente:
   - Nombre del programa
   - Puertos TCP/IP entrantes
   - Puertos TCP/IP salientes
   - Puertos UDP entrantes
   - Puertos UDP salientes
6. Si desea enviar la información de actividad de este puerto a otro equipo Windows de la red que comparta la conexión a Internet, seleccione **Reenvíe la actividad de la red en este puerto a los usuarios de la red que utilicen la función de conexión compartida a Internet**.
7. También puede introducir una descripción opcional para la nueva configuración.
8. Haga clic en **Aceptar**.

Nota: si el equipo tiene una aplicación que acepta conexiones de servidor a Web o FTP, es posible que el equipo que comparta la conexión necesite abrir el puerto del servicio del sistema asociado y permitir el reenvío de las conexiones entrantes para dichos puertos. Si utiliza Conexión compartida a Internet (ICS), también deberá agregar una conexión de equipo fiable en la lista Direcciones IP fiables. Para obtener más información, consulte Agregar una conexión de equipo fiable.

Modificar un puerto de servicio del sistema

Puede modificar la información de acceso entrante y saliente a la red de un puerto de servicio del sistema existente.

Nota: si la información del puerto está escrita de manera incorrecta, el servicio del sistema no funciona.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos haga clic en **Servicios del sistema**.
4. Seleccione un servicio del sistema y haga clic en **Editar**.
5. En el panel Servicios del sistema, en **Puertos y servicios del sistema**, introduzca lo siguiente:
   - Nombre del programa
   - Puertos TCP/IP entrantes
   - Puertos TCP/IP salientes
   - Puertos UDP entrantes
   - Puertos UDP salientes
6. Si desea enviar la información de actividad de este puerto a otro equipo Windows de la red que comparta la conexión a Internet, seleccione **Reenvíe la actividad de la red en este puerto a los usuarios de la red que utilicen la función de conexión compartida a Internet**.
7. También puede introducir una descripción opcional para la configuración modificada.
8. Haga clic en **Aceptar**.

Eliminar un puerto de servicio del sistema

Puede eliminar un puerto de servicio del sistema existente de su equipo. Después de su eliminación, los equipos remotos ya no podrán acceder al servicio de red de su equipo.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos haga clic en **Servicios del sistema**.
4. Seleccione un servicio del sistema y haga clic en **Eliminar**.
5. En el indicador, haga clic en **Sí** para confirmar.

CAPÍTULO 20

Gestionar conexiones de equipo

Puede configurar el cortafuegos para gestionar conexiones remotas específicas a su equipo mediante la creación de reglas, basadas en direcciones del protocolo de Internet (IP), que están asociadas a los equipos remotos. Los equipos que están asociados a direcciones IP fiables se pueden conectar a su equipo con confianza, mientras que a las IP que sean desconocidas, sospechosas o no sean fiables, se les puede prohibir que se conecten a su equipo.

Al permitir una conexión, asegúrese de que el equipo en el que confía sea seguro. Si un equipo definido como fiable resulta infectado por un gusano u otro mecanismo, su equipo podría ser infectado. Además, McAfee recomienda que los equipos en los que confía estén protegidos por un cortafuegos y un programa antivirus actualizado. El cortafuegos no registra el tráfico ni genera alertas de los eventos procedentes de las direcciones IP que están en la lista Direcciones IP fiables.

Los equipos asociados a direcciones IP desconocidas, sospechosas o que no son fiables no pueden conectarse a su equipo.

El cortafuegos bloquea todo el tráfico no deseado, por lo que no suele ser necesario prohibir una dirección IP. Se debe definir una dirección IP como no permitida sólo cuando se esté seguro de que una conexión de Internet determinada supone una amenaza específica. Asegúrese de no bloquear direcciones IP importantes, como el servidor DNS o DHCP, u otros servidores pertenecientes al ISP. En función de su configuración de seguridad, el cortafuegos puede alertarle cuando detecte un evento de un equipo no permitido.

En este capítulo

Definir conexiones de equipo como fiables

Puede agregar, editar y eliminar direcciones IP fiables desde el panel IP fiables y prohibidas, en **Direcciones IP fiables**.

La lista **Direcciones IP fiables** del panel Direcciones IP fiables y prohibidas permite que todo el tráfico procedente de un equipo determinado acceda al equipo propio. El cortafuegos no registra el tráfico ni genera alertas de los eventos procedentes de las direcciones IP que están en la lista **Direcciones IP fiables**.

El cortafuegos confía en cualquier dirección IP verificada que esté en la lista y siempre permite pasar a través suyo el tráfico procedente de una dirección IP fiable a cualquier puerto. El cortafuegos no filtra ni analiza la actividad que pueda haber entre el equipo asociado a un dirección IP fiable y su equipo. De forma predeterminada, Direcciones IP fiables muestra en una lista la primera red privada que el cortafuegos encuentra.

Al permitir una conexión, asegúrese de que el equipo en el que confía sea seguro. Si un equipo definido como fiable resulta infectado por un gusano u otro mecanismo, su equipo podría ser infectado. Además, McAfee recomienda que los equipos en los que confía estén protegidos por un cortafuegos y un programa antivirus actualizado.

Agregar una conexión de equipo fiable

Puede agregar una conexión de equipo fiable y su dirección IP asociada.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos, haga clic en **IP fiables y prohibidas**.
4. En el panel IP fiables y prohibidas, seleccione **Direcciones IP fiables** y haga clic en **Agregar**.
5. En **Agregar regla de direcciones IP fiables**, realice una de las acciones siguientes:
   - Seleccione **Dirección IP individual** y luego introduzca la dirección IP.
   - Seleccione un **Intervalo de direcciones IP** y luego introduzca las direcciones IP iniciales y finales en los cuadros de diálogo **Dirección IP inicial** y **Dirección IP final**.

6 Si un servicio del sistema utiliza Conexión compartida a Internet (ICS), podrá agregar el rango de direcciones IP siguiente: de 192.168.0.1 a 192.168.0.255.

7 También tiene la opción de seleccionar **Regla caduca en** e introducir el número de días para aplicar la regla.

8 O también puede escribir una descripción para la regla.

9 Haga clic en **Aceptar**.

10 En el cuadro de diálogo **IP fiables y prohibidas**, haga clic en **Sí** para confirmar.

Nota: para obtener más información acerca de la Conexión compartida a Internet (ICS), consulte Configurar un servicio del sistema nuevo.

Agregar un equipo fiable desde el registro Eventos entrantes

Puede agregar una conexión de equipo fiable y su dirección IP asociada desde el registro Eventos entrantes.

1 En el panel McAfee SecurityCenter, en el panel Tareas comunes, haga clic en **Menú avanzado**.

2 Haga clic en **Informes & registros**.

3 En **Eventos recientes**, haga clic en **Ver registro**.

4 Haga clic en **Internet y redes** y, a continuación, en **Eventos entrantes**.

5 Seleccione una dirección IP de origen y en **Deseo**, haga clic en **Definir como IP fiable**.

6 Haga clic en **Sí** para confirmar.

Editar una conexión de equipo fiable

Puede editar una conexión de equipo fiable y su dirección IP asociada.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos, haga clic en **IP fiables y prohibidas**.
4. En el panel IP fiables y prohibidas, seleccione **Direcciones IP fiables**.
5. Seleccione una dirección IP y haga clic en **Editar**.
6. En **Editar regla de direcciones IP fiables**, realice una de las acciones siguientes:
   - Seleccione **Dirección IP individual** y luego introduzca la dirección IP.
   - Seleccione un **Intervalo de direcciones IP** y luego introduzca las direcciones IP iniciales y finales en los cuadros de diálogo **Dirección IP inicial** y **Dirección IP final**.
7. También tiene la opción de verificar **Regla caduca en** e introducir el número de días para aplicar la regla.
8. O también puede escribir una descripción para la regla.
9. Haga clic en **Aceptar**.

Nota: no puede editar las conexiones predeterminadas del equipo que el cortafuegos ha agregado automáticamente a partir de una red privada fiable.

Eliminar una conexión de equipo fiable

Puede eliminar una conexión de equipo fiable y su dirección IP asociada.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos, haga clic en **IP fiables y prohibidas**.
4. En el panel IP fiables y prohibidas, seleccione **Direcciones IP fiables**.
5. Seleccione una dirección IP y haga clic en **Eliminar**.
6. En el cuadro de diálogo **IP fiables y prohibidas**, haga clic en **Sí** para confirmar.

Prohibir conexiones de equipo

Puede agregar, editar y eliminar direcciones IP no permitidas desde el panel IP fiables y prohibidas, en **Direcciones IP no permitidas**.

Los equipos asociados a direcciones IP desconocidas, sospechosas o que no son fiables no pueden conectarse a su equipo.

El cortafuegos bloquea todo el tráfico no deseado, por lo que no suele ser necesario prohibir una dirección IP. Se debe definir una dirección IP como no permitida sólo cuando se esté seguro de que una conexión de Internet determinada supone una amenaza específica. Asegúrese de no bloquear direcciones IP importantes, como el servidor DNS o DHCP, u otros servidores pertenecientes al ISP. En función de su configuración de seguridad, el cortafuegos puede alertarle cuando detecte un evento de un equipo no permitido.

Agregar una conexión de equipo no permitida

Puede agregar una conexión de equipo prohibida y su dirección IP asociada.

Nota: asegúrese de no bloquear direcciones IP importantes, como el servidor DNS o DHCP, u otros servidores pertenecientes al ISP.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos, haga clic en **IP fiables y prohibidas**.
4. En el panel IP fiables y prohibidas, seleccione **Direcciones IP prohibidas** y haga clic en **Agregar**.
5. En **Agregar regla de direcciones IP prohibidas**, realice una de las acciones siguientes:
   - Seleccione **Dirección IP individual** y luego introduzca la dirección IP.
   - Seleccione un **Intervalo de direcciones IP** y luego introduzca las direcciones IP iniciales y finales en los cuadros de diálogo **Dirección IP inicial** y **Dirección IP final**.

6 También tiene la opción de seleccionar **Regla caduca en** e introducir el número de días para aplicar la regla.

7 O también puede escribir una descripción para la regla.

8 Haga clic en **Aceptar**.

9 En el cuadro de diálogo **IP fiables y prohibidas**, haga clic en **Sí** para confirmar.

Editar una conexión de equipo no permitida

Puede editar una conexión de equipo prohibida y su dirección IP asociada.

1 En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.

2 En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.

3 En el panel Cortafuegos, haga clic en **IP fiables y prohibidas**.

4 En el panel IP fiables y prohibidas, seleccione **Direcciones IP prohibidas** y haga clic en **Editar**.

5 En **Editar dirección IP prohibida**, realice una de las acciones siguientes:

- Seleccione **Dirección IP individual** y luego introduzca la dirección IP.
- Seleccione un **Intervalo de direcciones IP** y luego introduzca las direcciones IP iniciales y finales en los cuadros de diálogo **Dirección IP inicial** y **Dirección IP final**.

6 También tiene la opción de seleccionar **Regla caduca en** e introducir el número de días para aplicar la regla.

7 O también puede escribir una descripción para la regla.

8 Haga clic en **Aceptar**.

Eliminar una conexión de equipo no permitida

Puede eliminar una conexión de equipo prohibida y su dirección IP asociada.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos, haga clic en **IP fiables y prohibidas**.
4. En el panel IP fiables y prohibidas, seleccione **Direcciones IP no permitidas**.
5. Seleccione una dirección IP y haga clic en **Eliminar**.
6. En el cuadro de diálogo **IP fiables y prohibidas**, haga clic en **Sí** para confirmar.

Prohibir un equipo desde el registro Eventos entrantes

Puede prohibir una conexión de equipo y su dirección IP asociada desde el registro Eventos entrantes.

Las direcciones IP que aparecen en el registro Eventos entrantes están bloqueadas. Por consiguiente, aunque prohíba una dirección no ganará protección adicional, a menos que su equipo utilice puertos que estén abiertos de manera intencionada o que su equipo incluya un programa al cual se ha concedido acceso a Internet.

Agregue una dirección IP a su lista de **Direcciones IP no permitidas** sólo si su equipo tiene uno o varios puertos abiertos intencionadamente y tiene razones para creer que debe bloquear el acceso a los puertos abiertos por parte de esa dirección.

Puede utilizar la página Eventos entrantes, que muestra las direcciones IP de todo el tráfico de Internet entrante, para prohibir una dirección IP que crea que es el origen de actividad de Internet no deseada o sospechosa.

1. En el panel McAfee SecurityCenter, bajo **Tareas comunes**, haga clic en **Menú avanzado**.
2. Haga clic en **Informes & registros**.
3. En **Eventos recientes**, haga clic en **Ver registro**.
4. Haga clic en **Internet y redes** y, a continuación, en **Eventos entrantes**.
5. Seleccione una dirección IP de origen y en **Deseo**, haga clic en **Definir como IP no permitida**.
6. En el cuadro de diálogo **Agregar regla de direcciones IP prohibidas**, haga clic en **Sí** para confirmar.

Prohibir un equipo desde el registro Eventos de detección de intrusiones

Puede prohibir una conexión de equipo y su dirección IP asociada desde el registro Eventos de detección de intrusiones.

1. En el panel McAfee SecurityCenter, bajo **Tareas comunes**, haga clic en **Menú avanzado**.
2. Haga clic en **Informes & registros**.
3. En **Eventos recientes**, haga clic en **Ver registro**.
4. Haga clic en **Internet y redes** y luego haga clic en **Eventos de detección de intrusiones**.
5. Seleccione una dirección IP de origen y en **Deseo**, haga clic en **Definir como IP no permitida**.
6. En el cuadro de diálogo **Agregar regla de direcciones IP prohibidas**, haga clic en **Sí** para confirmar.

CAPÍTULO 21

Registro, supervisión y análisis

El cortafuegos proporciona el registro, supervisión y análisis de los eventos y el tráfico de Internet, los cuales resultan muy completos y de fácil lectura. El hecho de comprender mejor el tráfico y los eventos de Internet facilita la gestión de sus conexiones de Internet.

En este capítulo

Registro de eventos

El cortafuegos permite activar o desactivar el registro de eventos y, en el caso de que lo active, qué tipos de evento desea registrar. El registro de eventos le permite ver los eventos entrantes, salientes y de intrusión.

Configurar un registro de eventos

Puede especificar y configurar los tipos de eventos de cortafuegos que se registrarán. De forma predeterminada, el registro de eventos está activado para todos los eventos y actividades.

1. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
2. En el panel Cortafuegos, haga clic en **Configuración de registro de eventos**.
3. Si todavía no la ha seleccionado, seleccione la opción **Activar el Registro de eventos**.
4. En **Activar el Registro de eventos**, seleccione o despeje los tipos de eventos que desee o no desee registrar. Existen los tipos de evento siguientes:
   - Programas bloqueados
   - Pings ICMP
   - Tráfico de direcciones IP no permitidas
   - Eventos en puertos de servicio del sistema
   - Eventos en puertos desconocidos
   - Eventos de detección de intrusiones (IDS)
5. Para evitar el registro en algunos puertos específicos, seleccione **No registrar eventos en los puertos siguientes** e introduzca los números de puerto individuales separados por comas o series de puertos separados por guiones. Por ejemplo, `137-139, 445, 400-5000`.
6. Haga clic en **Aceptar**.

Ver eventos recientes

Si el registro está habilitado, podrá ver los eventos recientes. El panel Eventos recientes muestra la fecha y la descripción del evento. Muestra la actividad de programas a los que se ha bloqueado explícitamente el acceso a Internet.

- En el **Menú avanzado**, en el panel Tareas comunes, haga clic en **Informes & Registros** o **Ver eventos recientes**. Como alternativa, haga clic en **Ver eventos recientes** en el panel Tareas comunes desde el Menú básico.

Ver eventos entrantes

Si el registro está habilitado, podrá ver los eventos entrantes. Los eventos entrantes incluyen la fecha y la hora, la dirección IP de origen, el nombre de host y la información y tipo de evento.

1. Asegúrese de que el Menú avanzado esté activado. En el panel Tareas comunes haga clic en **Informes y Registros**.
2. En **Eventos recientes**, haga clic en **Ver registro**.
3. Haga clic en **Internet y redes** y, a continuación, en **Eventos entrantes**.

Nota: Puede definir una dirección IP como fiable o permitida, o bien rastrearla desde el registro Eventos entrantes.

Ver eventos salientes

Si el registro está habilitado, podrá ver los eventos salientes. Eventos salientes incluye el nombre del programa que intenta obtener acceso saliente, la fecha y la hora del evento, y la ubicación del programa en su equipo.

1. En el panel Tareas comunes haga clic en **Informes y Registros**.
2. En **Eventos recientes**, haga clic en **Ver registro**.
3. Haga clic en **Internet y redes** y, a continuación, en **Eventos salientes**.

Nota: Puede permitir acceso pleno y sólo saliente a un programa desde el registro Eventos salientes. También puede localizar información adicional sobre el programa.

Ver eventos de detección de intrusiones

Si el registro está activado, podrá ver los eventos de intrusiones entrantes. Los eventos de detección de intrusiones muestran la fecha y la hora, la dirección IP de origen, el nombre de host del evento y el tipo de evento.

1. En el panel Tareas comunes haga clic en **Informes y Registros**.
2. En **Eventos recientes**, haga clic en **Ver registro**.
3. Haga clic en **Internet y redes** y luego haga clic en **Eventos de detección de intrusiones**.

Nota: Puede prohibir y rastrear una dirección IP desde el registro Eventos de detección de intrusiones.

Trabajar con estadísticas

El cortafuegos aprovecha el sitio Web HackerWatch de McAfee para proporcionarle estadísticas sobre los eventos de seguridad de Internet y la actividad de puertos en todo el mundo.

Visualizar las estadísticas globales de los eventos de seguridad

HackerWatch rastrea los eventos de seguridad de Internet a nivel mundial, los cuales se pueden visualizar desde SecurityCenter. La información rastreada enumera los incidentes que ha recibido HackerWatch en las últimas 24 horas, 7 días y 30 días.

1. Asegúrese de que el Menú avanzado está habilitado y luego haga clic en **Herramientas**.
2. En el panel Herramientas haga clic en **HackerWatch**.
3. En Seguimiento de eventos, vea las estadísticas de los eventos de seguridad.

Visualizar la actividad global de los puertos de Internet

HackerWatch rastrea los eventos de seguridad de Internet a nivel mundial, los cuales se pueden visualizar desde SecurityCenter. La información que se muestra incluye los puertos de eventos principales que HackerWatch ha registrado durante los últimos siete días. La información que se muestra suele ser de puertos HTTP, TCP y UDP.

1. Asegúrese de que el Menú avanzado está habilitado y luego haga clic en **Herramientas**.
2. En el panel Herramientas haga clic en **HackerWatch**.
3. Visualice los eventos de los puertos principales en **Actividad de puertos reciente**.

Rastrear el tráfico de Internet

El cortafuegos ofrece varias opciones para rastrear el tráfico de Internet. Dichas opciones le permiten rastrear geográficamente un equipo de red, obtener información acerca del dominio y la red, y rastrear equipos desde los registros Eventos entrantes y Eventos de detección de intrusiones.

Rastrear un equipo de red geográficamente

Con Visual Tracer puede localizar geográficamente un equipo que esté conectado o esté intentado conectarse a su equipo, mediante su nombre o dirección IP. También puede acceder a información relativa a la red y al registro mediante Visual Tracer. Al ejecutar Visual Tracer aparece un mapamundi que muestra la ruta más probable que toman los datos entre el equipo de origen y el suyo.

1. Asegúrese de que el Menú avanzado está habilitado y luego haga clic en **Herramientas**.
2. En el panel Herramientas haga clic en **Visual Tracer**.
3. Escriba la dirección IP del equipo y haga clic en **Rastrear**.
4. En **Visual Tracer**, seleccione **Vista de mapa**.

Nota: No se pueden rastrear eventos de direcciones IP de bucle de retorno, privadas o no válidas.

Obtenga información de registro de los equipos

Mediante Visual Trace puede obtener información de registro de un equipo desde SecurityCenter. Dicha información incluye el nombre de dominio, el nombre y la dirección de la persona registrada, y el contacto administrativo.

1. Asegúrese de que el Menú avanzado está habilitado y luego haga clic en **Herramientas**.
2. En el panel Herramientas haga clic en **Visual Tracer**.
3. Escriba la dirección IP del equipo y haga clic en **Rastrear**.
4. En **Visual Tracer**, seleccione **Vista de personas registradas**.

Obtenga información de red de los equipos

Mediante Visual Trace puede obtener información de red de un equipo desde SecurityCenter. La información de red incluye detalles relativos a la red en la que reside el dominio.

1. Asegúrese de que el Menú avanzado está habilitado y luego haga clic en **Herramientas**.
2. En el panel Herramientas haga clic en **Visual Tracer**.
3. Escriba la dirección IP del equipo y haga clic en **Rastrear**.
4. En **Visual Tracer**, seleccione **Vista de red**.

Rastrear un equipo desde el registro Eventos entrantes

Desde el panel Eventos entrantes, se puede rastrear una dirección IP que aparezca en el registro Eventos entrantes.

1. Asegúrese de que el Menú avanzado esté activado. En el panel Tareas comunes haga clic en **Informes y Registros**.
2. En **Eventos recientes**, haga clic en **Ver registro**.
3. Haga clic en **Internet y redes** y, a continuación, en **Eventos entrantes**.
4. En el panel Eventos entrantes, seleccione una dirección IP de origen y luego haga clic en **Rastrear esta dirección**.
5. En el panel Visual Tracer, realice una de las siguientes acciones:
   - **Vista de mapa**: Localiza un equipo geográficamente mediante la dirección IP seleccionada.
   - **Vista de personas registradas**: Localiza información relativa al dominio mediante la dirección IP seleccionada.
   - **Vista de red**: Localiza información relativa a la red mediante la dirección IP seleccionada.
6. Haga clic en **Listo**.

Rastrear un equipo desde el registro Eventos de detección de intrusiones

Desde el panel Eventos de detección de intrusiones, se puede rastrear una dirección IP que aparezca en el registro Eventos de detección de intrusiones.

1. En el panel Tareas comunes haga clic en **Informes y Registros**.
2. En **Eventos recientes**, haga clic en **Ver registro**.
3. Haga clic en **Internet y redes** y luego haga clic en **Eventos de detección de intrusiones**. En el panel Eventos de detección de intrusiones, seleccione una dirección IP de origen y luego haga clic en **Rastrear esta dirección**.
4. En el panel Visual Tracer, realice una de las siguientes acciones:
   - **Vista de mapa**: Localiza un equipo geográficamente mediante la dirección IP seleccionada.
   - **Vista de personas registradas**: Localiza información relativa al dominio mediante la dirección IP seleccionada.
   - **Vista de red**: Localiza información relativa a la red mediante la dirección IP seleccionada.
5. Haga clic en **Listo**.

Rastrear una dirección IP supervisada

Puede rastrear una dirección IP supervisada para obtener una vista geográfica que muestre la ruta más probable que han seguido los datos desde el equipo de origen hasta el suyo. También puede obtener información de red y de registro sobre la dirección IP.

1. Asegúrese de que el Menú avanzado está habilitado y haga clic en **Herramientas**.
2. En el panel Herramientas haga clic en **Control del tráfico**.
3. En **Control del tráfico**, haga clic en **Programas activos**.
4. Seleccione un programa y luego la dirección IP que aparece debajo del nombre del programa.
5. En **Actividad del programa**, haga clic en **Rastrear esta IP**.
6. En **Visual Trace** aparece un mapa que muestra la ruta más probable que toman los datos entre el equipo de origen y el suyo. También puede obtener información de red y de registro sobre la dirección IP.

Nota: Para visualizar las estadísticas más actualizadas, haga clic en **Actualizar** en **Visual Trace**.

Supervisar el tráfico de Internet

El cortafuegos proporciona varios métodos para supervisar su tráfico de Internet, incluido lo siguiente:

- **Gráfico Análisis de tráfico**: Muestra el tráfico de Internet entrante y saliente más reciente.
- **Gráfico Uso del tráfico**: Muestra el porcentaje aproximado de ancho de banda que las aplicaciones más activas han utilizado durante las últimas 24 horas.
- **Programas activos**: Muestra aquellos programas que utilizan actualmente la mayoría de conexiones de Internet en su equipo, así como las direcciones IP a las que acceden dichos programas.

Acerca del gráfico Análisis del tráfico

El gráfico Análisis de tráfico es una representación numérica y gráfica del tráfico entrante y saliente de Internet. Además, el control del tráfico muestra los programas que emplean un mayor número de conexiones de red en el equipo y las direcciones IP a las que acceden los programas.

Desde el panel Análisis de tráfico, se puede visualizar el tráfico de Internet entrante y saliente más reciente, así como las velocidades de transferencia actual, media y máxima. También puede visualizar el volumen de tráfico, incluida la cantidad de tráfico acumulada desde que inició el cortafuegos, y el tráfico total del mes actual o de los meses anteriores.

El panel Análisis de tráfico muestra la actividad de Internet en su equipo a tiempo real, incluidos el volumen y la velocidad del tráfico de Internet entrante y saliente más reciente de su equipo, la velocidad de conexión y el total de bytes transferidos a través de Internet.

La línea continua de color verde representa la velocidad actual de transferencia del tráfico entrante. La línea punteada de color verde representa la velocidad media de transferencia del tráfico entrante. Si la velocidad actual de transferencia y la velocidad media de transferencia coinciden, la línea de puntos no se muestra en el gráfico. La línea continua representa tanto la velocidad de transferencia media como la actual.

La línea continua de color rojo representa la velocidad actual de transferencia del tráfico saliente. La línea punteada de color rojo representa la velocidad media de transferencia del tráfico saliente. Si la velocidad actual de transferencia y la velocidad media de transferencia coinciden, la línea de puntos no se muestra en el gráfico. La línea continua representa tanto la velocidad de transferencia media como la actual.

Analizar el tráfico entrante y saliente

El gráfico Análisis de tráfico es una representación numérica y gráfica del tráfico entrante y saliente de Internet. Además, el control del tráfico muestra los programas que emplean un mayor número de conexiones de red en el equipo y las direcciones IP a las que acceden los programas.

1. Asegúrese de que el Menú avanzado está habilitado y luego haga clic en **Herramientas**.
2. En el panel Herramientas haga clic en **Control del tráfico**.
3. En **Control del tráfico**, haga clic en **Análisis del tráfico**.

Sugerencia: Para ver las estadísticas más actualizadas, haga clic en **Actualizar** en **Análisis del tráfico**.

Supervisar el ancho de banda de un programa

Puede visualizar el gráfico de sectores, que muestra el porcentaje aproximado del ancho de banda utilizado por los programas que han estado más activos en su equipo durante las últimas veinticuatro horas. El gráfico de sectores ofrece una representación visual de las cantidades relativas del ancho de banda utilizado por los programas.

1. Asegúrese de que el Menú avanzado está habilitado y luego haga clic en **Herramientas**.
2. En el panel Herramientas haga clic en **Control del tráfico**.
3. En **Control del tráfico**, haga clic en **Uso del tráfico**.

Sugerencia: Para visualizar las estadísticas más actualizadas, haga clic en **Actualizar** en **Uso del tráfico**.

Supervisar la actividad de un programa

Puede ver la actividad entrante y saliente del programa, que le muestra las conexiones y puertos del equipo.

1. Asegúrese de que el Menú avanzado está habilitado y luego haga clic en **Herramientas**.
2. En el panel Herramientas haga clic en **Control del tráfico**.
3. En **Control del tráfico**, haga clic en **Programas activos**.
4. Puede ver la información siguiente:
   - Gráfico de actividad del programa: Seleccione un programa para que muestre un gráfico de su actividad.
   - Conexión en escucha: Seleccione un elemento en escucha bajo el nombre del programa.
   - Conexión del equipo: Seleccione una dirección IP con el nombre del programa, proceso del sistema o servicio.

Nota: Para visualizar las estadísticas más actualizadas, haga clic en **Actualizar** en **Programas activos**.

CAPÍTULO 22

Obtener más información sobre la seguridad en Internet

El cortafuegos aprovecha el sitio Web de seguridad de McAfee, HackerWatch, para proporcionarle información acerca de los programas y la actividad de Internet en todo el mundo. HackerWatch también pone a su disposición un tutorial HTML sobre el cortafuegos.

En este capítulo

Iniciar el tutorial de HackerWatch

Para obtener información sobre el cortafuegos, puede acceder al tutorial de HackerWatch desde SecurityCenter.

1. Asegúrese de que el Menú avanzado está habilitado y luego haga clic en **Herramientas**.
2. En el panel Herramientas haga clic en **HackerWatch**.
3. En **Recursos de HackerWatch**, haga clic en **Ver tutorial**.

CAPÍTULO 23

McAfee Anti-Spam

Anti-Spam (anteriormente llamado SpamKiller) impide la entrada de correo electrónico no solicitado en su buzón de entrada examinando los mensajes entrantes y marcándolos como correo basura (correo electrónico que solicita que el usuario compre productos) o phishing (correo que solicita que el usuario proporcione información personal en un sitio Web posiblemente fraudulento), y después filtra los mensajes de correo basura en la carpeta de McAfee Anti-Spam.

Para que no se filtren los mensajes de correo electrónico legítimos procedente de amigos que puedan parecer correo basura, agregue sus direcciones a la lista de amigos de Anti-Spam. También puede personalizar el modo de detección de correo basura. Por ejemplo, puede filtrar los mensajes de forma más exhaustiva, especificar los elementos que se deben encontrar en un mensaje y crear sus propios filtros.

Anti-Spam también le protegerá si intenta acceder a un sitio Web posiblemente fraudulento a través del vínculo de un mensaje de correo electrónico. Si hace clic en el vínculo de un sitio Web del que se sospecha que es una página Web falsificada, será redirigido a la página segura de filtrado de phishing. Si hay sitios Web que no desea que se filtren, puede agregarlos a la lista blanca (los sitios Web incluidos aquí no se filtrarán).

Anti-Spam es compatible con distintos programas de correo electrónico como cuentas POP3, POP3 Webmail, Yahoo®, MSN®/Hotmail®, Windows® Live™ Mail y MAPI (Microsoft Exchange Server). Si utiliza un navegador para leer su correo electrónico, debe agregar su cuenta de Webmail a Anti-Spam. El resto de cuentas se configuran automáticamente, por lo que no necesita agregarlas.

Nota: SecurityCenter informa de los problemas de protección críticos y no críticos tan pronto como los detecta. Si necesita ayuda para diagnosticar sus problemas de protección, puede ejecutar McAfee Virtual Technician.

En este capítulo

Funciones de Anti-Spam

Anti-Spam ofrece las funciones siguientes.

Filtrado de correo basura

Los filtros avanzados de Anti-Spam impiden la entrada de correo electrónico no solicitado en su buzón, y se actualizan automáticamente en todas sus cuentas de correo. Además, puede crear filtros personalizados para garantizar que se filtra todo el correo basura e informar directamente a McAfee sobre la presencia de este tipo de correo para que se analice.

Filtrado de phishing

El filtro para phishing identifica sitios Web posiblemente fraudulentos que solicitan información personal.

Procesamiento personalizado de correo basura

Con esta función podrá marcar los mensajes no solicitados como correo basura y moverlos a la carpeta de McAfee Anti-Spam, o marcar los mensajes legítimos como tales y moverlos al buzón de entrada.

Amigos

Importe las direcciones de correo de sus amigos a una lista específica para que sus mensajes no se filtren.

Clasificación de elementos de la lista por importancia

Podrá ordenar los filtros personales, los amigos, las libretas de direcciones y las cuentas de Webmail por importancia, con sólo hacer clic en el nombre de la columna correspondiente.

Soporte adicional

Anti-Spam admite Mozilla® Thunderbird™ 1.5 y 2.0 y ofrece compatibilidad de versiones de 64 bits de Windows Vista™ para Windows Mail. Asimismo, el nuevo modo de juegos detiene los procesos Anti-Spam en segundo plano para que el equipo no pierda velocidad al jugar a videojuegos o reproducir un DVD. Anti-Spam también filtra las cuentas Microsoft® Outlook®, Outlook Express o Windows Mail en cualquier puerto, incluidos los puertos SSL (Secure Socket Layer).

CAPÍTULO 24

Configuración de las cuentas de Webmail

Si utiliza un navegador para leer los mensajes de correo electrónico, deberá configurar Anti-Spam para se conecte a la cuenta y filtre los mensajes. Para agregar la cuenta de Webmail a Anti-Spam, sólo tendrá que agregar la información de cuenta proporcionada por el proveedor de correo electrónico.

Después de agregar la cuenta de Webmail, podrá editar los detalles de dicha cuenta y obtener más información sobre el Webmail filtrado. Si ya no utiliza una cuenta de Webmail o no desea filtrarla, elimínela.

Anti-Spam es compatible con distintos programas de correo electrónico como cuentas POP3, POP3 Webmail, Yahoo®, MSN/Hotmail, Windows Live Mail y MAPI. POP3 es el tipo de cuenta más común y el estándar del correo electrónico de Internet. Si tiene una cuenta POP3, Anti-spam se conecta directamente al servidor de correo electrónico y filtra los mensajes antes de que su programa de correo electrónico los recoja. Las cuentas POP3 Webmail, Yahoo, MSN/Hotmail y Windows Mail se alojan todas en la Web. El proceso de filtrado de las cuentas POP3 Webmail es similar al de las cuentas POP3. MAPI es un sistema diseñado por Microsoft que admite diversos tipos de mensajes, incluyendo correo electrónico por Internet, faxes y mensajes de Exchange Server. En la actualidad, sólo Microsoft Outlook puede funcionar directamente con cuentas MAPI.

Nota: aunque Anti-Spam puede acceder a cuentas MAPI, no filtrará el correo electrónico hasta que el usuario recoja los mensajes con Microsoft Outlook.

En este capítulo

Agregar una cuenta de Webmail

Agregue una cuenta POP3 (por ejemplo, Yahoo), MSN/Hotmail o Windows Mail (sólo son totalmente compatibles las versiones de pago) Webmail si desea filtrar los mensajes en dicha cuenta para impedir la entrada de correo basura.

1 Abra el panel Protección contra spam.

¿Cómo?

1. En el panel Inicio de SecurityCenter, haga clic en **Correo electrónico y MI**.
2. En Correo electrónico y MI, haga clic en **Configurar**.
3. En el panel Configuración de correo electrónico y MI, en la ficha **Protección contra spam**, haga clic en **Avanzadas**.

2 En el panel Protección contra spam, haga clic en **Cuentas de Webmail**.

3 En el panel Cuentas de Webmail, haga clic en **Agregar**.

4 Especifique la información de cuenta (página 138)y, a continuación, haga clic en **Siguiente**.

5 En **Opciones de comprobación**, especifique cuándo debe Anti-Spam comprobar la presencia de spam en la cuenta (página 138).

6 Si está utilizando una conexión de acceso telefónico, especifique cómo debe Anti-Spam conectarse a Internet (página 138).

7 Haga clic en **Finalizar**.

Editar una cuenta de Webmail

Deberá editar la información de la cuenta de Webmail cuando se produzca algún cambio en la misma. Por ejemplo, modifique la cuenta si cambia la contraseña o si desea que Anti-Spam compruebe la presencia de correo basura más frecuentemente.

1 Abra el panel Protección contra spam.

¿Cómo?

1. En el panel Inicio de SecurityCenter, haga clic en **Correo electrónico y MI**.
2. En Correo electrónico y MI, haga clic en **Configurar**.
3. En el panel Configuración de correo electrónico y MI, en la ficha **Protección contra spam**, haga clic en **Avanzadas**.

2 En el panel Protección contra spam, haga clic en **Cuentas de Webmail**.

3 Seleccione la cuenta que va a modificar y haga clic en **Editar**.

4 Especifique la información de cuenta (página 138)y, a continuación, haga clic en **Siguiente**.

5 En **Opciones de comprobación**, especifique cuándo debe Anti-Spam comprobar la presencia de spam en la cuenta (página 138).

6 Si está utilizando una conexión de acceso telefónico, especifique cómo debe Anti-Spam conectarse a Internet (página 138).

7 Haga clic en **Finalizar**.

Eliminar una cuenta de Webmail

Elimine una cuenta de Webmail cuando ya no desee filtrar los mensajes para evitar la entrada de correo basura. Por ejemplo, si la cuenta ya no está activa o está experimentando problemas, puede eliminar la cuenta al tiempo que soluciona dichos problemas.

1 Abra el panel Protección contra spam.

¿Cómo?

1. En el panel Inicio de SecurityCenter, haga clic en **Correo electrónico y MI**.
2. En Correo electrónico y MI, haga clic en **Configurar**.
3. En el panel Configuración de correo electrónico y MI, en la ficha **Protección contra spam**, haga clic en **Avanzadas**.

2 En el panel Protección contra spam, haga clic en **Cuentas de Webmail**.

3 Seleccione la cuenta que desea eliminar y haga clic en **Eliminar**.

Descripción de la información de las cuentas de Webmail

Las tablas siguientes describen la información que deberá especificar al agregar o modificar cuentas de Webmail.

Información de la cuenta

Información	Descripción
Descripción	Describa la cuenta para consultas personales. En este cuadro puede escribir la información que desee.
Dirección de correo electrónico	Especifique la dirección de correo electrónico asociada a esta cuenta.
Tipo de cuenta	Especifique el tipo de cuenta de correo electrónico que va a agregar. (por ejemplo, POP3 Webmail o MSN/Hotmail).
Servidor	Especifique el nombre del servidor de correo que aloja esta cuenta. Si no conoce el nombre del servidor, consulte la información proporcionada por el proveedor de servicios de Internet (ISP).
Nombre de usuario	Especifique el nombre de usuario para esta cuenta. Por ejemplo, si su dirección es *nombre de usuario*@hotmail.com, el nombre de usuario suele ser, en términos generales, *nombre de usuario*.
Contraseña	Especifique la contraseña para esta cuenta.
Confirmar contraseña	Compruebe la contraseña para esta cuenta.

Opciones de comprobación

Opción	Descripción
Comprobar cada	Anti-Spam comprueba esta cuenta en los intervalos especificados (en minutos). El intervalo debe comprender entre 5 y 3.600 minutos.
Comprobar al inicio	Anti-spam comprueba la cuenta cada vez que se reinicia el equipo.

Opciones de conexión

Opción	Descripción
No marcar nunca una conexión	Anti-spam no establece la conexión automáticamente. Debe iniciar una conexión manual.
Marcar cuando no haya una conexión disponible	Si no hay disponible ninguna conexión a Internet, Anti-Spam intenta iniciar sesión mediante la conexión de acceso telefónico especificada.
Marcar siempre la conexión especificada	Anti-Spam intenta iniciar sesión automáticamente con la conexión de acceso telefónico especificada. Si en ese momento se encuentra conectado a través de una conexión de acceso telefónico distinta de la especificada, dicha conexión finalizará.
Marcar esta conexión	Especifique la conexión de acceso telefónico que Anti-Spam deberá utilizar para establecer la conexión a Internet.
Permanecer conectado una vez finalizado el filtrado	El equipo permanece conectado a Internet después de finalizar el filtrado.

CAPÍTULO 25

Configuración de la lista de amigos

Para garantizar que Anti-Spam no filtre mensajes legítimos de sus amigos, puede agregar sus direcciones a la lista de amigos de Anti-Spam.

La manera más sencilla de actualizar esta lista es agregar las libretas de direcciones a Anti-Spam; de esta forma se importarán las direcciones de todos sus amigos. Al agregar una libreta de direcciones, su contenido se importa automáticamente en intervalos programados (diaria, semanal o mensualmente) para evitar que la lista quede anticuada.

También puede actualizar la lista manualmente o agregar un dominio completo si desea agregar a su lista de amigos cada usuario del dominio. Por ejemplo, si agrega el dominio empresa.com, no se filtrará ninguna dirección de correo electrónico de dicha empresa.

En este capítulo

Configuración automática de la lista de amigos

La lista de amigos se actualiza automáticamente al agregar libretas de direcciones a Anti-Spam. Al agregar una libreta de direcciones, Anti-Spam puede importar las direcciones de correo correspondientes y llenar la lista de amigos con ellas.

Cuando agregue una libreta, podrá modificar la frecuencia en que se importará su contenido a la lista de amigos. Asimismo, podrá eliminar una libreta de direcciones si no desea importar sus direcciones.

Agregar una libreta de direcciones

Agregue las libretas de direcciones para que Anti-Spam pueda importar automáticamente todas las direcciones de correo electrónico y actualizar su lista de amigos. De esta forma garantizará que la lista esté siempre actualizada.

1. Abra el panel Protección contra spam.

   ¿Cómo?

   1. En el panel Inicio de SecurityCenter, haga clic en **Correo electrónico y MI**.
   2. En Correo electrónico y MI, haga clic en **Configurar**.
   3. En el panel Configuración de correo electrónico y MI, en la ficha **Protección contra spam**, haga clic en **Avanzadas**.

2. En el panel Protección contra spam, haga clic en **Libretas de direcciones**.
3. En el panel Libretas de direcciones, haga clic en **Agregar**.
4. Seleccione el tipo de libreta de direcciones que desea importar en la lista de **Tipo**.
5. Si se ha agregado contenido a la lista **Origen** , seleccione el origen de la libreta de direcciones. Por ejemplo, si tiene libretas de direcciones de Outlook, deberá seleccionar Outlook en esta lista.
6. En la lista de **Calendario** , haga clic en **Diariamente, Semanalmente** o **Mensualmente** para determinar cuándo Anti-Spam debe comprobar si hay nuevas direcciones en la libreta.
7. Haga clic en **Aceptar**.

Modificar una libreta de direcciones

Después de agregar las libretas de direcciones, puede cambiar la información de importación y el calendario. Por ejemplo, modifique las libretas si desea que Anti-Spam compruebe la existencia de direcciones nuevas con más frecuencia.

1 Abra el panel Protección contra spam.

¿Cómo?

1. En el panel Inicio de SecurityCenter, haga clic en **Correo electrónico y MI**.
2. En Correo electrónico y MI, haga clic en **Configurar**.
3. En el panel Configuración de correo electrónico y MI, en la ficha **Protección contra spam**, haga clic en **Avanzadas**.

2 En el panel Protección contra spam, haga clic en **Libretas de direcciones**.

3 Seleccione la libreta de direcciones que va a modificar y haga clic en **Editar**.

4 Seleccione el tipo de libreta de direcciones que desea importar en la lista de **Tipo**.

5 Si se ha agregado contenido a la lista **Origen** , seleccione el origen de la libreta de direcciones. Por ejemplo, si tiene libretas de direcciones de Outlook, deberá seleccionar Outlook en esta lista.

6 En la lista de **Calendario** , haga clic en **Diariamente, Semanalmente** o **Mensualmente** para determinar cuándo Anti-Spam debe comprobar si hay nuevas direcciones en la libreta.

7 Haga clic en **Aceptar**.

Eliminar una libreta de direcciones

Elimine una libreta si no desea que Anti-Spam importe direcciones automáticamente desde dicha libreta (por ejemplo, en el caso de que esté anticuada y no desee seguir utilizándola).

1 Abra el panel Protección contra spam.

¿Cómo?

1. En el panel Inicio de SecurityCenter, haga clic en **Correo electrónico y MI**.
2. En Correo electrónico y MI, haga clic en **Configurar**.
3. En el panel Configuración de correo electrónico y MI, en la ficha **Protección contra spam**, haga clic en **Avanzadas**.

2 En el panel Protección contra spam, haga clic en **Libretas de direcciones**.

3 Seleccione la libreta de direcciones que va a eliminar y, a continuación, haga clic en **Eliminar**.

Configuración manual de la lista de amigos

Para actualizar la lista de amigos de forma manual deberá editar las entradas una a una. Por ejemplo, si recibe un mensaje de correo de un amigo cuya dirección no está incluida en la libreta de direcciones, puede agregar la dirección directamente de forma manual. La forma más sencilla de hacerlo es a través de la barra de herramientas de Anti-Spam. En caso contrario, deberá especificar la información de la persona concreta.

Agregar un amigo desde la barra de herramientas de Anti-Spam

Si utiliza Outlook, Outlook Express, Windows Mail o programas de correo electrónico de Eudora™ o Thunderbird, puede agregar amigos desde la barra de herramientas de Anti-Spam.

Para agregar un amigo a...	Seleccione un mensaje y haga clic en...
Outlook, Outlook Express, Windows Mail	Haga clic en **Agregar amigo**.
Eudora, Thunderbird	En el menú **Anti-Spam**, haga clic en **Agregar amigo**.

Agregar un amigo manualmente

Si no desea agregar un amigo directamente desde la barra de herramientas, o si ha olvidado hacerlo al recibir un mensaje de correo electrónico, puede agregarlo a la lista sin necesidad de esperar a que anti-Spam lo haga de forma automática.

1 Abra el panel Protección contra spam.

¿Cómo?

1. En el panel Inicio de SecurityCenter, haga clic en **Correo electrónico y MI**.
2. En Correo electrónico y MI, haga clic en **Configurar**.
3. En el panel Configuración de correo electrónico y MI, en la ficha **Protección contra spam**, haga clic en **Avanzadas**.

2 En el panel Protección contra spam, haga clic en **Amigos**.

3 En el panel Amigos, haga clic en **Agregar**.

4 Escriba el nombre de su amigo en el cuadro **Nombre**.

5 Seleccione **Una dirección de correo electrónico** en la lista **Tipo**.

6 Escriba la dirección de correo electrónico de su amigo en el cuadro **Dirección de correo electrónico**.

7 Haga clic en **Aceptar**.

Agregar un dominio

Agregue un dominio completo si desea añadir todos los usuarios de dicho dominio a la lista de amigos. Por ejemplo, si agrega el dominio empresa.com, no se filtrará ninguna dirección de correo electrónico de dicha empresa.

1 Abra el panel Protección contra spam.

¿Cómo?

1. En el panel Inicio de SecurityCenter, haga clic en **Correo electrónico y MI**.
2. En Correo electrónico y MI, haga clic en **Configurar**.
3. En el panel Configuración de correo electrónico y MI, en la ficha **Protección contra spam**, haga clic en **Avanzadas**.

2 En el panel Protección contra spam, haga clic en **Amigos**.

3 En el panel Amigos, haga clic en **Agregar**.

4 Escriba el nombre de la organización o grupo en el cuadro **Nombre**.

5 Seleccione **Dominio completo** en la lista **Tipo**.

6 Escriba el nombre del dominio en el cuadro **Dirección de correo electrónico**.

7 Haga clic en **Aceptar**.

Editar amigo

Si la información de un amigo cambia, puede actualizar la lista para asegurarse de que Anti-Spam no marca sus mensajes como correo basura.

1 Abra el panel Protección contra spam.

¿Cómo?

1. En el panel Inicio de SecurityCenter, haga clic en **Correo electrónico y MI**.
2. En Correo electrónico y MI, haga clic en **Configurar**.
3. En el panel Configuración de correo electrónico y MI, en la ficha **Protección contra spam**, haga clic en **Avanzadas**.

2 En el panel Protección contra spam, haga clic en **Amigos**.

3 Seleccione el amigo cuya información desea modificar y haga clic en **Editar**.

4 Cambie el nombre de su amigo en el cuadro **Nombre**.

5 Cambie la dirección de correo electrónico de su amigo en el cuadro **Dirección de correo electrónico**.

6 Haga clic en **Aceptar**.

Modificar un dominio

Si la información de un dominio cambia, puede actualizar la lista para asegurarse de que Anti-Spam no marca los mensajes de dicho dominio como correo basura.

1 Abra el panel Protección contra spam.

¿Cómo?

1. En el panel Inicio de SecurityCenter, haga clic en **Correo electrónico y MI**.
2. En Correo electrónico y MI, haga clic en **Configurar**.
3. En el panel Configuración de correo electrónico y MI, en la ficha **Protección contra spam**, haga clic en **Avanzadas**.

2 En el panel Protección contra spam, haga clic en **Amigos**.

3 En el panel Amigos, haga clic en **Agregar**.

4 Cambie el nombre de la organización o grupo en el cuadro **Nombre**.

5 Seleccione **Dominio completo** en la lista **Tipo**.

6 Cambie el nombre del dominio en el cuadro **Dirección de correo electrónico**.

7 Haga clic en **Aceptar**.

Eliminar un amigo

Si una persona o un dominio incluido en la lista de amigos le envía un correo basura, elimínelo de la lista de Anti-Spam para que puedan filtrarse sus mensajes de correo la próxima vez.

1. Abra el panel Protección contra spam.

   ¿Cómo?

   1. En el panel Inicio de SecurityCenter, haga clic en **Correo electrónico y MI**.
   2. En Correo electrónico y MI, haga clic en **Configurar**.
   3. En el panel Configuración de correo electrónico y MI, en la ficha **Protección contra spam**, haga clic en **Avanzadas**.

2. En el panel Protección contra spam, haga clic en **Amigos**.
3. Seleccione el amigo que desea eliminar y, a continuación, haga clic en **Eliminar.**

CAPÍTULO 26

Configuración de la detección de correo basura

Anti-Spam le permite personalizar la forma de detectar correo basura. Puede filtrar mensajes de forma más exhaustiva, especificar los elementos que se deben buscar en un mensaje o localizar un conjunto determinado de caracteres al analizar este tipo de correo no deseado. Asimismo, puede crear filtros personales para precisar con más exactitud qué mensajes debe identificar Anti-Spam como correo basura. Por ejemplo, si no se filtran mensajes no deseados que contengan la palabra "hipoteca", puede agregar un filtro que incluya dicho término.

Si experimenta problemas con su correo electrónico, puede desactivar la protección contra el correo basura para intentar solucionar el problema.

En este capítulo

Desactivar la protección contra spam

Puede desactivar la protección contra el correo basura para evitar que Anti-Spam siga filtrando el correo electrónico.

1. En el menú avanzado, haga clic en **Configurar**.
2. En el panel Configurar, haga clic en **Correo electrónico y MI**.
3. En **Protección contra spam**, haga clic en **Desactivado**.

Sugerencia: Recuerde hacer clic en **Activado** en **Protección contra spam** para seguir protegido contra el correo basura.

Configuración de las opciones de filtrado

Ajuste las opciones de filtrado de Anti-spam para filtrar mensajes de forma más exhaustiva, especificar los elementos que se deben buscar en un mensaje o localizar un conjunto determinado de caracteres al analizar el correo no deseado.

Nivel de filtrado

El nivel de filtrado determina la exhaustividad con la que se filtrará el correo electrónico. Por ejemplo, si no se filtra el correo basura y el nivel de filtrado está establecido en Medio, puede cambiarlo a Alto. Sin embargo, si el nivel está establecido en Alto, sólo se aceptarán los mensajes de los remitentes incluidos en la lista de amigos, los demás se filtrarán.

Filtros especiales

Un filtro especifica qué es lo que Anti-spam debe buscar en un mensaje de correo electrónico. Los filtros especiales detectan mensajes que contienen texto oculto, imágenes incrustadas, errores intencionados de formato HTML y otras técnicas que suelen utilizar los responsables del correo basura. Dado que los mensajes que contienen estas características suelen ser correo basura, los filtros especiales están activados de forma predeterminada. Por ejemplo, si desea recibir mensajes de correo que contengan imágenes incrustadas, deberá desactivar primero el filtro de imágenes.

Juegos de caracteres

Anti-spam puede buscar juegos de caracteres específicos al analizar el correo basura. Los juegos de caracteres se utilizan para representar un idioma, incluido el alfabeto, los dígitos y demás símbolos de dicho idioma. Si recibe correo basura en griego, por ejemplo, puede filtrar todos los mensajes que contengan el juego de caracteres del griego

y no filtrar los juegos de caracteres de los idiomas en los que suele recibir correos electrónicos legítimos. Por ejemplo, si sólo desea filtrar mensajes en italiano, deberá seleccionar Europa occidental, ya que Italia pertenece a este grupo. Sin embargo, si recibe mensajes legítimos en inglés, al haber seleccionado esta opción también se filtrarán los mensajes en este idioma y en cualquier otro que contenga el juego de caracteres correspondiente al grupo Europa occidental. En este caso, no podrá filtrar mensajes sólo en italiano.

Nota: el filtrado de mensajes que contienen caracteres de un juego específico es una opción para usuarios avanzados.

Cambiar el nivel de filtrado

Puede establecer el grado de exhaustividad con el que desea filtrar los mensajes. Por ejemplo, si se están filtrando los mensajes de correo electrónico legítimos, puede reducir el nivel.

1 Abra el panel Protección contra spam.

¿Cómo?

1. En el panel Inicio de SecurityCenter, haga clic en **Correo electrónico y MI**.
2. En Correo electrónico y MI, haga clic en **Configurar**.
3. En el panel Configuración de correo electrónico y MI, en la ficha **Protección contra spam**, haga clic en **Avanzadas**.

2 En el panel Protección contra spam, haga clic en **Opciones de filtrado**.

3 En **Opciones de filtrado**, mueva la barra deslizante al nivel apropiado y haga clic en **Aceptar**.

Nivel	Descripción
Bajo	se aceptan la mayoría de los mensajes.
Medio-bajo	sólo se filtran los mensajes que son claramente correos basura.
Medio	el correo electrónico se filtrará al nivel recomendado.
Medio-alto	se filtran todos los mensajes que parecen ser spam.
Alto	sólo se aceptan los mensajes cuyos remitentes están en la lista de amigos.

Desactivar un filtro especial

Los filtros especiales están activados de forma predeterminada, ya que filtran el tipo de mensajes que los responsables del correo basura suelen enviar. Por ejemplo, aquellos mensajes de correo que contengan imágenes incrustadas suelen ser correo basura; sin embargo, si suele recibir mensajes legítimos con este tipo de imágenes, deberá desactivar el filtro de imágenes.

1 Abra el panel Protección contra spam.

¿Cómo?

1. En el panel Inicio de SecurityCenter, haga clic en **Correo electrónico y MI**.
2. En Correo electrónico y MI, haga clic en **Configurar**.
3. En el panel Configuración de correo electrónico y MI, en la ficha **Protección contra spam**, haga clic en **Avanzadas**.

2 En el panel Protección contra spam, haga clic en **Opciones de filtrado**.

3 En **Filtros especiales**, marque o desactive las casillas de verificación adecuadas y haga clic en **Aceptar**.

Filtro	Descripción
Filtrar mensajes que contengan texto oculto	Busca texto oculto, ya que se trata de una característica que suelen utilizar los remitentes de correo basura para evitar la detección.
Filtrar los mensajes que contengan determinados porcentajes de imágenes en relación al texto	Busca imágenes incrustadas, ya que los mensajes con este tipo de imágenes suelen ser correo basura.
Filtrar los mensajes que contengan errores de formato HTML intencionados	Busca mensajes que contengan un formato no válido, ya que esto se utiliza para que los filtros no puedan filtrar el correo basura.
No filtrar los mensajes con un tamaño superior a:	No busca mensajes con un tamaño mayor al tamaño especificado, ya que los mensajes de gran tamaño pueden no ser correo basura. El tamaño de mensaje se puede aumentar o reducir (el intervalo válido es 0-250 KB).

Aplicar filtros de juego de caracteres

Nota: El filtrado de mensajes que contienen caracteres de un juego específico es una opción para usuarios avanzados.

A través de esta opción podrá filtrar juegos de caracteres de idiomas específicos. Sin embargo, tenga cuidado de no filtrar juegos de caracteres para idiomas en los que recibe mensajes legítimos.

1 Abra el panel Protección contra spam.

¿Cómo?

1. En el panel Inicio de SecurityCenter, haga clic en **Correo electrónico y MI**.
2. En Correo electrónico y MI, haga clic en **Configurar**.
3. En el panel Configuración de correo electrónico y MI, en la ficha **Protección contra spam**, haga clic en **Avanzadas**.

2 En el panel Protección contra spam, haga clic en **Juegos de caracteres**.

3 Active las casillas situadas junto a los juegos de caracteres que desea filtrar.

4 Haga clic en **Aceptar**.

Utilización de filtros personales

Un filtro especifica qué es lo que Anti-spam debe buscar en un mensaje de correo electrónico. Cuando se localiza correo basura, el mensaje se marca como tal y puede permanecer en el buzón de entrada o moverse a la carpeta McAfee Anti-Spam. Para obtener más información acerca de la gestión del correo basura, consulte Modificar la forma en que se debe procesar y marcar un mensaje (página 158).

De forma predeterminada, Anti-Spam utiliza numerosos filtros; sin embargo, se pueden crear filtros nuevos o editar los filtros existentes para precisar con más exactitud los mensajes que deben identificarse como spam. Por ejemplo, si agrega un filtro que contenga la palabra "hipoteca", Anti-Spam filtrará los mensajes que incluyan dicho término. Tenga cuidado de no crear filtros con palabras comunes que puedan aparecer en mensajes legítimos, ya que en ese caso también se filtrará este correo. Después de crear un filtro, puede modificarlo si cree que no aún no detecta determinado tipo de correo basura. Por ejemplo, si ha creado un filtro para buscar la palabra "viagra" en el campo Asunto, pero aún recibe mensajes que contienen dicha palabra en el cuerpo del mensaje, cambie el filtro para que busque el término en el cuerpo del mensaje en lugar de en el asunto.

Las expresiones regulares (RegEx) son caracteres y secuencias especiales que pueden utilizarse también en filtros personales; sin embargo, McAfee sólo recomienda utilizarlas en el caso de usuarios avanzados. Si no está familiarizado con las expresiones regulares o desea más información sobre cómo utilizarlas, puede buscar este tipo de expresiones en la Web (por ejemplo, vaya a http://en.wikipedia.org/wiki/Regular_expression).

Agregar un filtro personal

Puede agregar filtros para precisar con más exactitud qué mensajes debe identificar Anti-Spam como correo basura.

1 Abra el panel Protección contra spam.

¿Cómo?

1. En el panel Inicio de SecurityCenter, haga clic en **Correo electrónico y MI**.
2. En Correo electrónico y MI, haga clic en **Configurar**.
3. En el panel Configuración de correo electrónico y MI, en la ficha **Protección contra spam**, haga clic en **Avanzadas**.

2 En el panel Protección contra spam, haga clic en **Filtros personales**.

3 Haga clic en **Agregar**.

4 Especificar qué es lo que el filtro personal debe buscar (página 156) en un mensaje de correo electrónico.

5 Haga clic en **Aceptar**.

Modificar un filtro personal

Modifique los filtros existentes para precisar con más exactitud qué mensajes deben identificarse como spam.

1 Abra el panel Protección contra spam.

¿Cómo?

1. En el panel Inicio de SecurityCenter, haga clic en **Correo electrónico y MI**.
2. En Correo electrónico y MI, haga clic en **Configurar**.
3. En el panel Configuración de correo electrónico y MI, en la ficha **Protección contra spam**, haga clic en **Avanzadas**.

2 En el panel Protección contra spam, haga clic en **Filtros personales**.

3 Seleccione el filtro que desea editar y haga clic en **Editar**.

4 Especificar qué es lo que el filtro personal debe buscar (página 156) en un mensaje de correo electrónico.

5 Haga clic en **Aceptar**.

Eliminar un filtro personal

Puede quitar de forma permanente los filtros que ya no desea utilizar.

1 Abra el panel Protección contra spam.

¿Cómo?

1. En el panel Inicio de SecurityCenter, haga clic en **Correo electrónico y MI**.
2. En Correo electrónico y MI, haga clic en **Configurar**.
3. En el panel Configuración de correo electrónico y MI, en la ficha **Protección contra spam**, haga clic en **Avanzadas**.

2 En el panel Protección contra spam, haga clic en **Filtros personales**.

3 Seleccione el filtro que desea eliminar y, a continuación, haga clic en **Eliminar**.

4 Haga clic en **Aceptar**.

Especificar un filtro personal

La tabla siguiente describe qué es lo que el filtro personal busca un mensaje de correo electrónico.

Información	Descripción
Elemento	Haga clic en una entrada para determinar si el filtro debe buscar las palabras o frases en el asunto, el cuerpo, el encabezado o el remitente del mensaje.
Condición	Haga clic en una entrada para determinar si el filtro debe buscar un mensaje que contenga o no contenga las palabras o frases especificadas.
Palabras o expresiones	Escriba qué se debe buscar en los mensajes. Por ejemplo, si especifica "hipoteca", se filtrarán todos los mensajes que contengan esa palabra.
Este filtro utiliza expresiones regulares (RegEx)	Especifique los patrones de caracteres que se utilizarán en las condiciones de filtrado. Para comprobar un patrón de caracteres, haga clic en **Probar**.

CAPÍTULO 27

Filtrado de correo electrónico

Anti-Spam examina el correo electrónico entrante y lo clasifica como correo basura (mensajes de correo electrónico que solicitan que el usuario compre productos) o phishing (mensajes que solicitan que el usuario proporcione información personal en un sitio Web posiblemente fraudulento). De forma predeterminada, Anti-Spam marcará después cada mensaje no deseado como correo basura o phishing (la etiqueta [SPAM] o [PHISH] aparecerá en el apartado Asunto del mensaje) y lo moverá a la carpeta McAfee Anti-Spam.

Para personalizar el filtrado que debe realizar Anti-Spam de los mensajes de correo electrónico, puede marcar cada mensaje como spam o no spam desde la barra de herramientas de Anti-Spam, cambiar la ubicación a la que deben moverse los mensajes no deseados o cambiar la etiqueta que aparece en el asunto.

Para cambiar la forma en que el correo basura debe procesarse y marcarse, puede personalizar la ubicación a la que mover los mensajes de spam y phishing y también el nombre de la etiqueta que aparece en el asunto.

Asimismo, también puede desactivar las barras de herramientas de Anti-Spam si debe solucionar algún problema relacionado con el programa de correo electrónico.

En este capítulo

Marcar un mensaje desde la barra de herramientas de Anti-Spam

Cuando se marca un mensaje como spam, se agrega la etiqueta [SPAM] u otra etiqueta personalizada al mensaje y se deja en el buzón de entrada, en la carpeta de McAfee Anti-Spam (Outlook, Outlook Express, Windows Mail, Thunderbird) o en la carpeta Junk (Eudora®). Cuando un mensaje se marca como no spam, se quita la etiqueta del mensaje y se mueve al buzón de entrada.

Para marcar un mensaje en...	Seleccione un mensaje y haga clic en...
Outlook, Outlook Express, Windows Mail	Haga clic en **Marcar como spam** o **Marcar como no es spam**.
Eudora, Thunderbird	En el menú de **Anti-Spam**, haga clic en **Marcar como Spam** o **Marcar como no es spam**.

Modificar la forma en que se debe procesar y marcar un mensaje

Puede cambiar el modo en que el spam se marca y procesa. Por ejemplo, puede decidir si se deja el mensaje en el buzón de entrada o en la carpeta de McAfee Anti-Spam, y cambiar la etiqueta [SPAM] o [PHISH] que aparece en el campo Asunto del mensaje.

1 Abra el panel Protección contra spam.

¿Cómo?

1. En el panel Inicio de SecurityCenter, haga clic en **Correo electrónico y MI**.
2. En Correo electrónico y MI, haga clic en **Configurar**.
3. En el panel Configuración de correo electrónico y MI, en la ficha **Protección contra spam**, haga clic en **Avanzadas**.

2 En el panel Protección contra spam, haga clic en **Procesamiento**.

3 Seleccione o desactive las casillas de verificación correspondientes y haga clic en **Aceptar**.

Opción	Descripción
Marcar el correo basura y moverlo a la carpeta de McAfee Anti-Spam	Éste es el parámetro predeterminado. Los mensajes spam se trasladan a la carpeta de McAfee Anti-Spam.

Opción	Descripción
Marcar como correo basura y dejarlo en el Buzón de entrada	Los mensajes spam permanecen en el buzón de entrada.
Agregar esta etiqueta personalizable al asunto de los mensajes de correo basura	La etiqueta que especifique se añadirá a la línea de asunto del correo electrónico de los mensajes spam.
Agregar esta etiqueta personalizable al asunto de los mensajes de phishing	La etiqueta que especifique se añadirá a la línea de asunto del correo electrónico de los mensajes de phishing.

Desactivar la barra de herramientas de Anti-Spam

Si utiliza Outlook, Outlook Express, Windows Mail o programas de correo electrónico de Eudora o Thunderbird, puede desactivar la barra de herramientas de Anti-Spam.

1 Abra el panel Protección contra spam.

¿Cómo?

1. En el panel Inicio de SecurityCenter, haga clic en **Correo electrónico y MI**.
2. En Correo electrónico y MI, haga clic en **Configurar**.
3. En el panel Configuración de correo electrónico y MI, en la ficha **Protección contra spam**, haga clic en **Avanzadas**.

2 En el panel Protección contra spam, haga clic en **Barras de herramientas de correo electrónico**.

3 Desactive la casilla situada junto a la barra de herramientas que va a deshabilitar.

4 Haga clic en **Aceptar**.

Sugerencia: Puede volver a habilitar las barras de herramientas de Anti-Spam en cualquier momento volviendo a seleccionar las casillas correspondientes.

CAPÍTULO 28

Trabajar con correo electrónico filtrado

En algunas ocasiones puede que el correo basura no se detecte. Si esto ocurre, puede enviar una notificación a McAfee sobre los mensajes spam para que los analice y actualice los filtros.

Si utiliza una cuenta de Webmail, puede copiar, eliminar y obtener más información sobre los mensajes de correo electrónico filtrados. Esto resulta muy útil si no está seguro de que se haya filtrado un mensaje legítimo o si desea saber cuándo se filtró un mensaje concreto.

En este capítulo

Informar del spam a McAfee.

Puede enviar una notificación a McAfee sobre los mensajes spam para que los analice y actualice los filtros.

1 Abra el panel Protección contra spam.

¿Cómo?

1. En el panel Inicio de SecurityCenter, haga clic en **Correo electrónico y MI**.
2. En Correo electrónico y MI, haga clic en **Configurar**.
3. En el panel Configuración de correo electrónico y MI, en la ficha **Protección contra spam**, haga clic en **Avanzadas**.

2 En el panel Protección contra spam, haga clic en **Notificar a McAfee**.

3 Seleccione las casillas de verificación correspondientes y haga clic en **Aceptar**.

Opción	Descripción
Permitir informar cuando se hace clic en Marcar como spam	cada vez que marque un mensaje como spam, este mensaje se enviará a McAfee.
Permitir informar cuando se hace clic en Marcar como no es spam	cada vez que marque un mensaje como no spam, este mensaje se enviará a McAfee.

Opción	Descripción
Enviar mensaje entero (no sólo los encabezados)	envía a McAfee todo el mensaje y no sólo los encabezados.

Copiar o eliminar un mensaje de Webmail filtrado

Puede copiar o eliminar los mensajes que se hayan filtrado en una cuenta de correo en Web.

1. Bajo **Tareas comunes,** haga clic en **Ver eventos recientes**.
2. En el panel Eventos recientes, haga clic en **Ver registro**.
3. En el panel de la izquierda, expanda la lista **Correo electrónico y MI** y, a continuación, haga clic en **Eventos de filtrado de correo en Web**.
4. Seleccione un mensaje.
5. En **Deseo**, elija una de las siguientes opciones:
   - Haga clic en **Copiar** para copiar el mensaje en el portapapeles.
   - Haga clic en **Eliminar** para eliminar el mensaje.

Ver un evento para el correo de Webmail

Puede consultar la fecha y la hora a la que los mensajes fueron filtrados y la cuenta en que se recibieron.

1. Bajo **Tareas comunes,** haga clic en **Ver eventos recientes**.
2. En el panel Eventos recientes, haga clic en **Ver registro**.
3. En el panel de la izquierda, expanda la lista **Correo electrónico y MI** y, a continuación, haga clic en **Eventos de filtrado de correo en Web**.
4. Seleccione el registro que desea consultar.

CAPÍTULO 29

Cómo configurar la protección contra phishing

Anti-Spam clasifica los mensajes no deseados como correo basura (mensajes de correo electrónico que solicitan que el usuario compre productos) o phishing (mensajes que solicitan que el usuario proporcione información personal en un sitio Web posiblemente fraudulento). La protección contra phishing le protege de acceder a sitios Web fraudulentos. Si hace clic en un vínculo incluido en un mensaje que le lleva a un sitio Web fraudulento conocido o que puede ser fraudulento, Anti-Spam le redirigirá a la página segura de filtrado de phishing.

Si hay sitios Web que no desea filtrar, puede agregarlos a la lista blanca de phishing. Asimismo, puede editar o eliminar sitios Web de esta lista. No necesita agregar sitios como Google®, Yahoo o McAfee, ya que estos sitios no se consideran fraudulentos.

Nota: si tiene instalado SiteAdvisor en su equipo, no recibirá protección contra phishing de Anti-Spam, ya que SiteAdvisor ya tiene una protección de este tipo similar a la de Anti-Spam.

En este capítulo

Agregar un sitio Web a la lista blanca

Si hay sitios Web que no desea filtrar, puede agregarlos a la lista blanca.

1. Abra el panel Protección contra phishing.

   ¿Cómo?

   1. En el panel Inicio de SecurityCenter, haga clic en **Internet y redes.**
   2. En el área de información de Internet y redes, haga clic en **Configurar**.

2. En el panel Protección contra phishing, haga clic en **Avanzadas**.
3. En **Lista blanca,** haga clic en **Agregar.**
4. Escriba la dirección del sitio Web y haga clic en **Aceptar**.

Modificar sitios de la lista blanca

Si cambia la dirección de un sitio Web que ha agregado a la lista blanca, puede actualizarlo.

1 Abra el panel Protección contra phishing.

¿Cómo?

1. En el panel Inicio de SecurityCenter, haga clic en **Internet y redes.**
2. En el área de información de Internet y redes, haga clic en **Configurar**.

2 En el panel Protección contra phishing, haga clic en **Avanzadas**.

3 En **Lista blanca,** seleccione el sitio Web que desea actualizar y haga clic en **Editar.**

4 Escriba la dirección del sitio Web y haga clic en **Aceptar**.

Eliminar un sitio Web de la lista blanca

Si ha agregado un sitio Web a la lista blanca pero ahora desea filtrarlo, deberá eliminarlo de dicha lista.

1 Abra el panel Protección contra phishing.

¿Cómo?

1. En el panel Inicio de SecurityCenter, haga clic en **Internet y redes.**
2. En el área de información de Internet y redes, haga clic en **Configurar**.

2 En el panel Protección contra phishing, haga clic en **Avanzadas**.

3 En **Lista blanca,** seleccione el sitio Web que desea eliminar y haga clic en **Eliminar.**

Desactivar la protección contra phishing

Si tiene instalado un software contra phishing que no es de McAfee y se producen problemas, puede deshabilitar la protección contra phishing de Anti-Spam.

1. En el panel Inicio de SecurityCenter, haga clic en **Internet y redes.**
2. En el área de información de Internet y redes, haga clic en **Configurar**.
3. En **Protección contra phishing**, haga clic en **Desactivado**.

Sugerencia: Cuando haya acabado, no olvide hacer clic en **Activado** en **Protección contra phishing** para seguir protegido contra sitios Web fraudulentos.

CAPÍTULO 30

McAfee Privacy Service

Privacy Service ofrece protección avanzada para usted, su familia, sus archivos personales y su equipo. Le ayuda a protegerse con el robo de identidad en línea, bloquear la transmisión de información potencial y filtrar posible contenido en línea ofensivo (incluidas imágenes). Además, ofrece controles paternos avanzados que permiten a los adultos supervisar, controlar y registrar algunos hábitos de navegación Web no autorizados, así como un área de almacenamiento seguro para contraseñas.

Antes de empezar a utilizar Privacy Service, familiarícese primero con algunas de sus funciones más conocidas. En la ayuda de Privacy Service hallará toda la información acerca de cómo configurar y utilizar dichas funciones.

Nota: SecurityCenter informa de los problemas de protección críticos y no críticos tan pronto como los detecta. Si necesita ayuda para diagnosticar sus problemas de protección, puede ejecutar McAfee Virtual Technician.

En este capítulo

Características de Privacy Service

Privacy Service ofrece las siguientes funciones:

- Control parental
- Protección de información personal
- Caja fuerte de contraseñas

Control parental

Control parental permite filtrar imágenes potencialmente inapropiadas, configurar grupos de clasificación de contenido (grupos de edad utilizados para restringir los sitios Web y el contenido que un usuario puede ver), y establecer límites de tiempo de navegación Web (el período y duración del tiempo de acceso de un usuario a la Web) para los usuarios de SecurityCenter. Control parental también permite restringir el acceso universal a determinados sitios Web y conceder o bloquear el acceso basándose en palabras claves asociadas.

Protección de información personal

La protección de información personal le permite bloquear la transmisión de información sensible o confidencial (por ejemplo, números de tarjetas de crédito, números de cuentas bancarias, direcciones, etc.) por Internet.

Caja fuerte de contraseñas

La Caja fuerte de contraseñas es un área de almacenamiento seguro para sus contraseñas personales. Le permite almacenar sus contraseñas con la seguridad de que ningún otro usuario (ni siquiera un administrador) pueda acceder a ellas.

CAPÍTULO 31

Configuración de Control parental

Si sus hijos utilizan su equipo, puede configurar el Control parental para ellos. Control parental se utiliza para ayudar a regular qué ven y qué hacen los niños mientras navegan por Internet. Para configurar Control parental, puede activar o desactivar el filtrado de imágenes, elegir un grupo de clasificación de contenido y establecer un límites temporal de navegación por Internet. El filtrado de imágenes bloquea y evita que las imágenes inapropiadas se visualicen cuando un niño explora la Web; el grupo de clasificación de contenido determina el tipo de contenido y los sitios Web a los que puede acceder un niño, basándose en el grupo de edad al que éste pertenece y los límites temporales de navegación por Internet definen los días y horas en los que un niño puede tener acceso a Internet. Control parental también permite filtrar (bloquear o permitir) determinados sitios Web para todos los niños.

Nota: es necesario ser Administrador para configurar los controles paternos.

En este capítulo

Configuración de usuarios

Para configurar Control parental, es preciso asignar permisos a los usuarios de SecurityCenter. De forma predeterminada, los usuarios de SecurityCenter corresponden a los usuarios de Windows que se han configurado en el equipo. No obstante, si ha efectuado una actualización desde una versión anterior de SecurityCenter que utilizaba usuarios de McAfee, se conservarán los usuarios de McAfee, así como sus permisos.

Nota: para configurar usuarios, es preciso iniciar sesión en SecurityCenter como administrador.

Trabajo con usuarios de Windows

Para configurar Control parental, es preciso asignar permisos a los usuarios que determinen qué puede ver y hacer cada usuario en Internet. De forma predeterminada, los usuarios de SecurityCenter corresponden a los usuarios de Windows que se han configurado en el equipo. Se puede editar un usuario y la información de cuenta de un usuario o eliminar un usuario en Computer Management en Windows. Se puede configurar Control parental para los usuarios de SecurityCenter.

Si ha efectuado la actualización desde una versión anterior de SecurityCenter que utilizaba usuarios de McAfee, consulte Trabajo con usuarios de McAfee (página 172).

Trabajo con usuarios de McAfee

Si ha efectuado una actualización desde una versión anterior de SecurityCenter que utilizaba usuarios de McAfee, se conservarán automáticamente los usuarios de McAfee, así como sus permisos. Puede seguir configurando y gestionando usuarios de McAfee; no obstante, para facilitar las tareas de mantenimiento, McAfee recomienda que pase a usuarios de Windows. Una vez que esté en usuarios de Windows, no podrá volver nunca a usuarios de McAfee.

Si sigue utilizando usuarios de McAfee, podrá agregar, editor o quitar usuarios y cambiar o recuperar la contraseña de administrador de McAfee.

Cambiar a usuarios de Windows

A fin de facilitar las tareas de mantenimiento, McAfee recomienda que cambie a usuarios de Windows. Una vez que esté en usuarios de Windows, no podrá volver nunca a usuarios de McAfee.

1 Abra el panel Configuración de usuarios.

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel Inicio de SecurityCenter, haga clic en **Controles paternos**.
3. En la sección de información de Controles paternos, haga clic en **Configurar**.
4. En el panel Configuración de Controles paternos, haga clic en **Avanzada**.

2 En dicho panel, haga clic en **Cambiar**.

3 Confirme la operación.

Agregue un usuario de McAfee

Después de crear un usuario de McAfee, puede configurar Control parental para el usuario. Para obtener más información, consulte la ayuda de Privacy Service.

1 Inicie sesión en SecurityCenter como usuario Administrador.

2 Abra el panel Configuración de usuarios.

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel Inicio de SecurityCenter, haga clic en **Controles paternos**.
3. En la sección de información de Controles paternos, haga clic en **Configurar**.
4. En el panel Configuración de Controles paternos, haga clic en **Avanzada**.

3 En dicho panel, haga clic en **Agregar**.

4 Siga las instrucciones que aparezcan en pantalla para configurar un nombre de usuario, una contraseña, un tipo de cuenta y el control parental.

5 Haga clic en **Crear**.

Edición de la información de cuenta de un usuario de McAfee

Puede cambiar la contraseña, tipo de cuenta o la capacidad de inicio de sesión automático de un usuario de McAfee.

1 Inicie sesión en SecurityCenter como usuario Administrador.

2 Abra el panel Configuración de usuarios.

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel Inicio de SecurityCenter, haga clic en **Controles paternos**.
3. En la sección de información de Controles paternos, haga clic en **Configurar**.
4. En el panel Configuración de Controles paternos, haga clic en **Avanzada**.

3 En el panel Configuración de usuarios, haga clic en un nombre de usuario y, a continuación, en **Editar**.

4 Siga las instrucciones que aparezcan en pantalla para editar la contraseña, el tipo de cuenta o el control parental del usuario.

5 Haga clic en **Aceptar**.

Eliminación de un usuario de McAfee

Puede eliminar un usuario de McAfee en cualquier momento.

Para eliminar a un usuario de McAfee:

1 Inicie sesión en SecurityCenter como usuario Administrador.

2 Abra el panel Configuración de usuarios.

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel Inicio de SecurityCenter, haga clic en **Controles paternos**.
3. En la sección de información de Controles paternos, haga clic en **Configurar**.
4. En el panel Configuración de Controles paternos, haga clic en **Avanzada**.

3 En el panel Configuración de usuarios, en **Cuentas de usuario de McAfee**, seleccione un nombre de usuario y haga clic en **Quitar**.

Cambio de la contraseña del administrador de McAfee

Si tiene problemas para recordar la contraseña de administrador de McAfee o sospecha que no es segura, puede cambiarla.

1 Inicie sesión en SecurityCenter como usuario Administrador.

2 Abra el panel Configuración de usuarios.

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel Inicio de SecurityCenter, haga clic en **Controles paternos**.
3. En la sección de información de Controles paternos, haga clic en **Configurar**.
4. En el panel Configuración de Controles paternos, haga clic en **Avanzada**.

3 En el panel Configuración de usuarios, en **Cuentas de usuario de McAfee**, seleccione **Administrador** y, a continuación, haga clic en **Editar**.

4 En el cuadro de diálogo Modificar cuentas de usuario, escriba una nueva contraseña en el cuadro **Nueva contraseña** y, a continuación, vuelva a escribirla en el cuadro **Vuelva a introducir la contraseña**.

5 Haga clic en **Aceptar**.

Recuperación de la contraseña del administrador de McAfee

Si olvida la contraseña del Administrador, no podrá recuperarla.

1. Haga clic con el botón derecho del ratón en el icono de SecurityCenter y, a continuación, haga clic en **Cambiar usuario**.
2. En la lista **Nombre de usuario**, seleccione **Administrador** y, a continuación, haga clic en **¿Olvidó su contraseña?**
3. Escriba la respuesta a la pregunta secreta del cuadro **Respuesta**.
4. Haga clic en **Enviar**.

Filtrado de imágenes Web potencialmente inapropiadas

Según la edad del usuario o el nivel de madurez, puede filtrar (bloquear o permitir) imágenes potencialmente inapropiadas cuando el usuario navega por Internet. Por ejemplo, puede bloquear la aparición de imágenes potencialmente inapropiadas cuando sus hijos están navegando por Internet y permitir que aparezcan para los adolescentes más mayores y los adultos. De forma predeterminada, el filtrado de imágenes está desactivado para todos los miembros adultos, lo que significa que las imágenes potencialmente inapropiadas se ven cuando dichos usuarios navegan por Internet. Para obtener más información acerca de cómo configurar el grupo de edad de un usuario, consulte Establecimiento del grupo de clasificación de contenido (página 177).

Filtrado de imágenes Web potencialmente inapropiadas

De forma predeterminada, los usuarios nuevos se agregan al grupo de adultos y el filtrado de imágenes está desactivado. Si desea bloquear la aparición de imágenes potencialmente inapropiadas cuando un usuario particular navegue por Internet, puede activar el filtrado de imágenes. Cada imagen de la Web que sea potencialmente inapropiada se sustituye automáticamente por una imagen de McAfee estática.

1. Abra el panel Configuración de usuarios.

   ¿Cómo?

   1. En el panel Inicio de SecurityCenter, haga clic en **Controles paternos**.
   2. En la sección de información de Controles paternos, haga clic en **Configurar**.
   3. En el panel Configuración de Controles paternos, haga clic en **Avanzada**.
   4. En el panel Control parental, haga clic en **Configuración de usuarios**.

2. En el panel Configuración de usuarios, haga clic en un nombre de usuario y, a continuación, en **Editar**.
3. En la ventana Modificar cuentas de usuario, en **Filtrado de imágenes**, haga clic en **Activado**.
4. Haga clic en **Aceptar**.

Establecimiento del grupo de clasificación de contenido

Un usuario puede pertenecer a uno de los siguientes grupos de clasificación de contenido:

- Niño de corta edad
- Niño
- Adolescente
- Joven
- Adulto

Privacy Service evalúa (bloquea o permite) el contenido Web, según el grupo al que el usuario pertenezca. De esta forma, podrá bloquear o permitir determinados sitios Web para determinados usuarios de su hogar. Por ejemplo, puede bloquear un sitio Web a usuarios que pertenezcan al grupo de niños de corta edad, pero permitirlo a usuarios del grupo de adolescentes. Si desea evaluar de forma más estricta el contenido para un usuario, puede permitir que dicho usuario vea únicamente los sitios Web que están permitidos en la lista **Sitios Web filtrados**. Para obtener más información, consulte Filtrado de sitios Web (página 180).

De forma predeterminada, los usuarios nuevos se agregan al grupo de adultos, lo que les permite tener acceso a todo el contenido de la Web.

Configurar un grupo de clasificación de contenido para un usuario

De forma predeterminada, los usuarios nuevos se agregan al grupo de adultos, lo que les permite tener acceso a todo el contenido de la Web. A continuación, puede ajustar el grupo de clasificación del contenido según la edad y nivel de madurez del individuo.

1 Abra el panel Configuración de usuarios.

¿Cómo?

1. En el panel Inicio de SecurityCenter, haga clic en **Controles paternos**.
2. En la sección de información de Controles paternos, haga clic en **Configurar**.
3. En el panel Configuración de Controles paternos, haga clic en **Avanzada**.
4. En el panel Control parental, haga clic en **Configuración de usuarios**.

2 En el panel Configuración de usuarios, haga clic en un nombre de usuario y, a continuación, en **Editar**.

3 En la ventana Modificar cuentas de usuario, en **Clasificación del contenido**, haga clic en el grupo de edad que desee asignar al usuario.

Para evitar que el usuario navegue por sitios Web que están bloqueados en la lista **Sitios Web filtrados**, seleccione la casilla **Este usuario sólo puede acceder a sitios de la lista de Sitios Web permitidos**.

4 Haga clic en **Aceptar**.

Configuración de los límites de tiempo de navegación por Internet

Si el uso excesivo o irresponsable de Internet es un tema que le preocupa, puede establecer límites de tiempo apropiados para la navegación por Internet de sus hijos. Si restringe a sus hijos el horario de navegación por Internet, puede confiar en que SecurityCenter aplicará dichas restricciones, incluso cuando usted se encuentre fuera de casa.

De forma predeterminada, se permite a un niño navegar por Internet a todas horas, ya sea de día o de noche, los siete días de la semana; no obstante, puede limitar la navegación por Internet a horas o días específicos o prohibir por completo la navegación por Internet. Si un niño intenta utilizar Internet durante un período prohibido, McAfee le notificará que no puede hacerlo. Si prohíbe totalmente la navegación por Internet, el niño podrá iniciar sesión en el equipo y utilizar, entre otros, programas de Internet como el correo electrónico, la mensajería instantánea, ftp, juegos, etc... si bien no podrá navegar por Internet.

Configuración de los límites de tiempo de navegación por Internet

Puede utilizar el cuadrante de límite de tiempo de navegación por la Web para restringir el tiempo de navegación por la Web de un niño a días y horas específicos.

1 Abra el panel Configuración de usuarios.

¿Cómo?

1. En el panel Inicio de SecurityCenter, haga clic en **Controles paternos**.
2. En la sección de información de Controles paternos, haga clic en **Configurar**.
3. En el panel Configuración de Controles paternos, haga clic en **Avanzada**.
4. En el panel Control parental, haga clic en **Configuración de usuarios**.

2 En el panel Configuración de usuarios, haga clic en un nombre de usuario y, a continuación, en **Editar**.

3 En la ventana Modificar cuentas de usuario, en **Límites de tiempo de Internet**, arrastre el ratón para especificar los días y horas en los que este usuario no podrá navegar por la Web.

4 Haga clic en **Aceptar**.

Filtrado de sitios Web

Puede filtrar (bloquear o permitir) sitios Web a todos los usuarios, salvo a aquellos que pertenezcan al grupo de adultos. Un sitio Web se bloquea para evitar que los niños accedan a él cuando navegan por Internet. Si un niño intenta acceder a un sitio Web bloqueado, aparece un mensaje que le indica que no se puede acceder al sitio porque está bloqueado por McAfee.

Un sitio Web se permite cuando McAfee lo ha bloqueado de forma predeterminada, pero usted desea que los niños puedan tener acceso a él. Para obtener más información acerca de los sitios Web que McAfee bloquea por defecto, consulte Filtrado de sitios Web mediante palabras clave (página 183). También se puede actualizar o eliminar un sitio Web filtrado en cualquier momento.

Nota: los usuarios (incluidos los administradores) que pertenezcan al grupo de adultos pueden tener acceso a todos los sitios Web, incluso a aquellos que se han bloqueado. Para probar los sitios Web bloqueados, debe iniciar sesión como usuario menor de edad.

Bloquear un sitio Web.

Un sitio Web se bloquea para evitar que los niños accedan a él cuando navegan por Internet. Si un niño intenta acceder a un sitio Web bloqueado, aparece un mensaje que le indica que no se puede acceder al sitio porque está bloqueado por McAfee.

1 Abrir el panel Control parental

¿Cómo?

1. En el panel Inicio de SecurityCenter, haga clic en **Controles paternos**.
2. En la sección de información de Controles paternos, haga clic en **Configurar**.
3. En el panel Configuración de Controles paternos, cerciórese de que Controles paternos está activado y luego haga clic en **Avanzado**.

2 En el panel Control parental, haga clic en **Sitios Web filtrados**.

3 En el panel Sitios Web filtrados, escriba la dirección de un sitio Web en el cuadro **http://** y luego haga clic en **Bloquear**.

4 Haga clic en **Aceptar**.

Sugerencia: puede bloquear un sitio Web que anteriormente estaba permitido, haciendo clic en la dirección del sitio Web en la lista **Sitios Web filtrados** y, a continuación, haciendo clic en **Bloquear**.

Permitir un sitio Web

Un sitio Web se permite para asegurarse de que otros usuarios no lo bloqueen. Si permite un sitio Web que McAfee ha bloqueado de forma predeterminado, anulará el valor predeterminado.

1 Abrir el panel Control parental

¿Cómo?

1. En el panel Inicio de SecurityCenter, haga clic en **Controles paternos**.
2. En la sección de información de Controles paternos, haga clic en **Configurar**.
3. En el panel Configuración de Controles paternos, cerciórese de que Controles paternos está activado y luego haga clic en **Avanzado**.

2 En el panel Control parental, haga clic en **Sitios Web filtrados**.

3 En el panel Sitios Web filtrados, escriba la dirección de un sitio Web en el cuadro **http://** y luego haga clic en **Permitir**.

4 Haga clic en **Aceptar**.

Sugerencia: puede permitir un sitio Web que anteriormente estaba bloqueado, haciendo clic en la dirección del sitio Web en la lista **Sitios Web filtrados** y, a continuación, haciendo clic en **Permitir**.

Actualización de un sitio Web filtrado

Si la dirección de un sitio Web cambia o bien se equivoca al introducirla para bloquearla o permitirla, tiene la posibilidad de actualizarla.

1 Abrir el panel Control parental

¿Cómo?

1. En el panel Inicio de SecurityCenter, haga clic en **Controles paternos**.
2. En la sección de información de Controles paternos, haga clic en **Configurar**.
3. En el panel Configuración de Controles paternos, cerciórese de que Controles paternos está activado y luego haga clic en **Avanzado**.

2 En el panel Control parental, haga clic en **Sitios Web filtrados**.

3 En el panel Sitios Web filtrados, haga clic en una entrada de la lista **Sitios Web filtrados**, modifique la dirección del sitio Web en el cuadro **http://** y luego haga clic en **Actualizar**.

4 Haga clic en **Aceptar**.

Eliminación de un sitio Web filtrado

Puede eliminar un sitio Web filtrado si ya no desea bloquearlo o permitirlo.

1 Abrir el panel Control parental

¿Cómo?

1. En el panel Inicio de SecurityCenter, haga clic en **Controles paternos**.
2. En la sección de información de Controles paternos, haga clic en **Configurar**.
3. En el panel Configuración de Controles paternos, cerciórese de que Controles paternos está activado y luego haga clic en **Avanzado**.

2 En el panel Control parental, haga clic en **Sitios Web filtrados**.

3 En el panel Sitios Web filtrados, haga clic en una entrada de la lista **Sitios Web filtrados** y luego haga otro clic en **Eliminar**.

4 Haga clic en **Aceptar**.

Filtrado de sitios Web mediante palabras clave

El filtrado mediante palabras clave permite bloquear a los usuarios que no son adultos las visitas a sitios Web que contienen palabras potencialmente inapropiadas. Cuando el filtrado mediante palabras clave está activado, se utiliza una lista predeterminada de palabras clave y sus reglas correspondientes para evaluar el contenido para los usuarios, de acuerdo con su grupo de clasificación de contenido. Los usuarios deben pertenecer a un determinado grupo para acceder a sitios Web que contengan palabras clave específicas. Por ejemplo, sólo los miembros del grupo Adulto pueden visitar los sitios Web que contienen la palabra *porno*, y sólo los miembros del grupo de niños (y mayores) pueden visitar los sitios Web que contengan la palabra *drogas*.

También puede agregar sus propias palabras clave a la lista predeterminada y asociarlas con ciertos grupos de clasificación de contenido. Las reglas de palabras clave que agregue sobrescribirán cualquier regla que ya esté asociada con una palabra clave coincidente de la lista predeterminada.

Desactivación del filtrado mediante palabras clave

De forma predeterminada, el filtrado mediante palabras clave está activado, lo que significa que se utiliza una lista de palabras clave predeterminadas y sus reglas correspondientes para evaluar el contenido para los usuarios, de acuerdo con su grupo de clasificación de contenido. Si bien McAfee no recomienda hacerlo, puede desactivar el filtrado de palabras clave en cualquier momento.

1 Abrir el panel Control parental

¿Cómo?

1. En el panel Inicio de SecurityCenter, haga clic en **Controles paternos**.
2. En la sección de información de Controles paternos, haga clic en **Configurar**.
3. En el panel Configuración de Controles paternos, cerciórese de que Controles paternos está activado y luego haga clic en **Avanzado**.

2 En el panel Control parental, haga clic en **Palabras clave.**

3 En el panel Palabras clave, haga clic en **Desactivado**.

4 Haga clic en **Aceptar**.

Bloquear sitios Web basándose en palabras clave

Si desea bloquear sitios Web debido a su contenido inapropiado, pero no sabe cuáles son sus direcciones de sitio específicas, puede bloquear dichos sitios basándose en palabras clave. Sólo tiene que escribir una palabra clave y luego indicar qué grupos de clasificación de contenido pueden visualizar los sitios Web que contienen esa palabra clave.

1 Abrir el panel Control parental

¿Cómo?

1. En el panel Inicio de SecurityCenter, haga clic en **Controles paternos**.
2. En la sección de información de Controles paternos, haga clic en **Configurar**.
3. En el panel Configuración de Controles paternos, cerciórese de que Controles paternos está activado y luego haga clic en **Avanzado**.

2 En el panel Control parental, haga clic en **Palabras clave** y compruebe que el filtrado de palabras clave esté activado.

3 En **Lista de palabras clave**, escriba una palabra clave en el cuadro **Buscar**.

4 Mueva el control deslizante **Edad mínima** para especificar un grupo de edad mínima.
Los usuarios de este grupo de edad y los mayores pueden visualizar sitios Web que contengan esta palabra clave.

5 Haga clic en **Aceptar**.

CAPÍTULO 32

Protección de la información en la Web

Cuando navegue por Internet, puede proteger los archivos y la información privada bloqueando la información. Por ejemplo, puede impedir que su información personal (como su nombre y dirección o los números de su tarjeta de crédito y su cuenta corriente) sea transmitida a través de Internet con sólo agregarla al área de información bloqueada.

Nota: Privacy Service no bloquea la transmisión de información personal efectuada a través de sitios Web seguros (es decir, sitios Web que utilicen el protocolo https://), como los sitios de bancos.

En este capítulo

Protección de la información personal

Evite que su información personal (como su nombre y dirección o los números de su tarjeta de crédito y su cuenta corriente) se transmita a través de Internet bloqueándola. Si McAfee detecta que información personal contenida en algún elemento (por ejemplo, un campo de formulario o un archivo) está a punto de enviarse por Internet, se producirá lo siguiente:

- Si usted es el Administrador, deberá confirmar si desea enviar la información.
- Si no es usted el Administrador, la parte bloqueada se sustituirá por asteriscos (*). Por ejemplo, si un sitio Web dañino intenta enviar su número de tarjeta de crédito a otro equipo, el número en si estará sustituido por asteriscos.

Protección de la información personal

Puede bloquear los siguientes tipos de información personal: nombre, dirección, código postal, información de la seguridad social, número de teléfono, números de la tarjeta de crédito, cuentas bancarias, cuentas de intermediación y tarjetas telefónicas. Si desea bloquear información personal de otro tipo, puede establecer el tipo en **otro**.

1 Abra el panel Información protegida.

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel Inicio de SecurityCenter, haga clic en **Internet y redes**.
3. En la sección de información de Internet y redes, haga clic en **Configurar**.
4. En el panel Configuración de Internet y redes, asegúrese de que la Protección de información personal está activada y luego haga clic en **Avanzada**.

2 En el panel Información protegida, haga clic en **Agregar**.

3 Seleccione de la lista el tipo de información que desee bloquear.

4 Escriba su información personal y haga clic en **Aceptar**.

CAPÍTULO 33

Protección de contraseñas

La Caja fuerte de contraseñas es un área de almacenamiento seguro para sus contraseñas personales. Le permite almacenar sus contraseñas con la seguridad de que ningún otro usuario (ni siquiera un administrador) pueda acceder a ellas.

En este capítulo

Configuración de la Caja fuerte de contraseñas

Antes de empezar a utilizar la Caja fuerte de contraseñas, deberá configurar una contraseña para ésta. Sólo los usuarios que sepan esta contraseña podrán tener acceso a la Caja fuerte de contraseñas. Si olvida la contraseña de acceso a la Caja fuerte de contraseñas, podrá restablecerla; sin embargo, todas las contraseñas almacenadas en la Caja fuerte, se eliminarán.

Tras configurar una contraseña para la Caja fuerte de contraseñas, podrá agregar contraseñas a la caja, editarlas o eliminarlas. También puede cambiar la contraseña de la Caja fuerte de contraseñas en cualquier momento.

Agregación de una contraseña

Si le cuesta recordar sus contraseñas, puede agregarlas a la Caja fuerte de contraseñas. La Caja fuerte de contraseñas es una ubicación segura, ya que sólo pueden acceder a ella los usuarios que conocen la contraseña.

1. Abra el panel Caja fuerte de contraseñas.

   ¿Cómo?

   1. En **Tareas comunes**, haga clic en **Inicio**.
   2. En el panel Inicio de SecurityCenter, haga clic en **Internet y redes**.
   3. En la sección de información de Internet y redes, haga clic en **Configurar**.
   4. En el panel Configuración de Internet y redes, haga clic en **Avanzada** en **Caja fuerte de contraseñas**.

2. Escriba su contraseña de la Caja fuerte de contraseñas en el cuadro **Contraseña** y vuelva a escribirla en el cuadro **Vuelva a introducir la contraseña**.
3. Haga clic en **Abrir**.
4. En el panel Gestionar Caja fuerte de contraseñas, haga clic en **Agregar**.
5. Escriba una descripción de la contraseña (por ejemplo, para qué sirve) en el cuadro **Descripción** y luego escriba la contraseña en el cuadro **Contraseña**.
6. Haga clic en **Aceptar**.

Modificación de una contraseña

Para asegurarse de que las entradas en su Caja fuerte de contraseñas son siempre precisas y fiables, deberá actualizarlas siempre que cambie las contraseñas.

1. Abra el panel Caja fuerte de contraseñas.

   ¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel Inicio de SecurityCenter, haga clic en **Internet y redes**.
3. En la sección de información de Internet y redes, haga clic en **Configurar**.
4. En el panel Configuración de Internet y redes, haga clic en **Avanzada** en **Caja fuerte de contraseñas**.

2 Escriba su contraseña de la Caja fuerte de contraseñas en el cuadro **Contraseña**.

3 Haga clic en **Abrir**.

4 En el panel Gestionar Caja fuerte de contraseñas, haga clic en una contraseña y otro clic en **Editar**.

5 Modifique la descripción de la contraseña (por ejemplo, para qué sirve) en el cuadro **Descripción** o modifique la contraseña en el cuadro **Contraseña**.

6 Haga clic en **Aceptar**.

Eliminación de una contraseña

Puede eliminar una contraseña de la Caja fuerte de contraseñas en cualquier momento. Es imposible recuperar una contraseña que se ha eliminado de la caja fuerte.

1 Abra el panel Caja fuerte de contraseñas.

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel Inicio de SecurityCenter, haga clic en **Internet y redes**.
3. En la sección de información de Internet y redes, haga clic en **Configurar**.
4. En el panel Configuración de Internet y redes, haga clic en **Avanzada** en **Caja fuerte de contraseñas**.

2 Escriba su contraseña de la Caja fuerte de contraseñas en el cuadro **Contraseña**.

3 Haga clic en **Abrir**.

4 En el panel Gestionar Caja fuerte de contraseñas, haga clic en una contraseña y otro clic en **Eliminar**.

5 En el cuadro de diálogo de confirmación de eliminación, haga clic en **Sí**.

Cambie la contraseña de la caja fuerte de contraseñas

Puede cambiar la contraseña de la Caja fuerte de contraseñas en cualquier momento.

1 Abra el panel Caja fuerte de contraseñas.

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel Inicio de SecurityCenter, haga clic en **Internet y redes**.
3. En la sección de información de Internet y redes, haga clic en **Configurar**.
4. En el panel Configuración de Internet y redes, haga clic en **Avanzada** en **Caja fuerte de contraseñas**.

2 En el panel Caja fuerte de contraseñas, escriba la contraseña actual en el cuadro **Contraseña** y, a continuación, haga clic en **Abrir**.

3 En el panel Gestionar Caja fuerte de contraseñas, haga clic en **Cambiar contraseña**.

4 Escriba una nueva contraseña de en el cuadro **Elija una contraseña** y vuelva a escribirla en el cuadro **Vuelva a introducir la contraseña**.

5 Haga clic en **Aceptar**.

6 En el cuadro de diálogo Se ha modificado la contraseña de la Caja fuerte de contraseñas, haga clic en **Aceptar**.

Restablecimiento de la contraseña de la Caja fuerte de contraseñas

Si olvida la contraseña de acceso a la Caja fuerte de contraseñas, podrá restablecerla; sin embargo, todas las contraseñas introducidas anteriormente, se eliminarán.

1 Abra el panel Caja fuerte de contraseñas.

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel Inicio de SecurityCenter, haga clic en **Internet y redes**.
3. En la sección de información de Internet y redes, haga clic en **Configurar**.
4. En el panel Configuración de Internet y redes, haga clic en **Avanzada** en **Caja fuerte de contraseñas**.

2 En **Restablecer Caja fuerte de contraseñas**, escriba una contraseña nueva en el cuadro **Contraseña** y escríbala de nuevo en el cuadro **Vuelva a introducir la contraseña**.

3 Haga clic en **Restablecer**.

4 En el cuadro de diálogo Confirmación de restablecimiento de contraseña, haga clic en **Sí**.

CAPÍTULO 34

McAfee Data Backup

Utilice Data Backup para evitar la pérdida accidental de sus datos archivando sus archivos en CD, DVD, unidad USB, disco duro externo o unidad de red. El almacenamiento local le permite archivar (realizar una copia de seguridad) de sus datos personales en CD, DVD, unidad USB, disco duro externo o unidad de red. De este modo se crea una copia local de sus registros, documentos y demás material de interés personal en caso de pérdida accidental.

Antes de empezar a utilizar Data Backup, puede familiarizarse con algunas de las funciones más conocidas. Encontrará información más detallada sobre la configuración y uso de estas funciones en la ayuda de Data Backup. Después de consultar las funciones del programa, debe asegurarse de que cuenta con los soportes de archivo necesarios para realizar almacenamientos locales.

En este capítulo

Funciones

Data Backup ofrece las funciones siguientes para guardar y restaurar sus fotos, música y otros archivos importantes.

Archivo planificado local

Proteja sus datos archivando archivos y carpetas en CD, DVD, unidad USB, disco duro externo o unidad de red. Después de iniciar la primera operación de archivo, se realizarán operaciones de archivo incrementales automáticamente.

Restaurar con un clic

Si los archivos o carpetas se eliminan por error o se corrompen en su equipo, puede recuperar las versiones más recientes archivadas desde el soporte de archivo utilizado.

Compresión y encriptación

De forma predeterminada, se comprimen los archivos archivados, de modo que se ahorra espacio en los soportes de archivo. Como medida de seguridad adicional, se encriptan los archivos de forma predeterminada.

CAPÍTULO 35

Cómo archivar archivos

Puede utilizar McAfee Data Backup para archivar una copia de los archivos de su equipo en CD, DVD, unidad USB, disco duro externo o unidad de red. Al archivar sus ficheros de esta manera, le resultará fácil recuperar la información en caso de pérdida o daño accidental de los datos.

Antes de empezar a archivar los archivos, debe seleccionar su ubicación predeterminada (CD, DVD, unidad USB, disco duro externo o unidad de red). McAfee ha preconfigurado algunos ajustes más; por ejemplo, las carpetas y los tipos de archivo que desea archivar, pero usted puede modificar estos ajustes.

Después de configurar las opciones del archivo local, puede modificar los ajustes predeterminados referentes a cada cuánto tiempo Data Backup ejecuta archivos rápidos o completos. Puede realizar archivos manuales en cualquier momento.

En este capítulo

Configuración de las opciones de archivo

Antes de empezar a archivar sus datos, debe configurar algunas opciones del archivo local. Por ejemplo, debe establecer las ubicaciones y los tipos de archivos observados. Las ubicaciones de observación son las carpetas de su equipo en las que Data Backup controla y busca nuevos archivos o cambios en éstos. Los tipos de archivos observados son los tipos de archivo (por ejemplo, .doc, .xls, etc.) que Data Backup archiva en las ubicaciones de observación. Por defecto, Data Backup observa todos los tipos de archivo almacenados en sus ubicaciones de observación.

Puede configurar dos tipos de ubicaciones de observación: ubicaciones de observación en profundidad y ubicaciones de observación superficial. Si se establece una ubicación de observación en profundidad, Data Backup archiva una copia de los tipos de archivos observados en dicha carpeta y sus subcarpetas. Si se establece una ubicación de observación superficial, Data Backup crea una copia de los tipos de archivos observados únicamente en dicha carpeta (no en sus subcarpetas). También puede identificar las ubicaciones que desea excluir del archivo local. Por defecto, el Escritorio de Windows y Mis documentos se configuran como ubicaciones de observación en profundidad.

Después de configurar los tipos de archivos y las ubicaciones de observación, debe seleccionar la ubicación del archivo (es decir, el CD, DVD, unidad USB, disco duro externo o unidad de red donde se almacenarán los datos archivados). Puede cambiar la ubicación del archivo en cualquier momento.

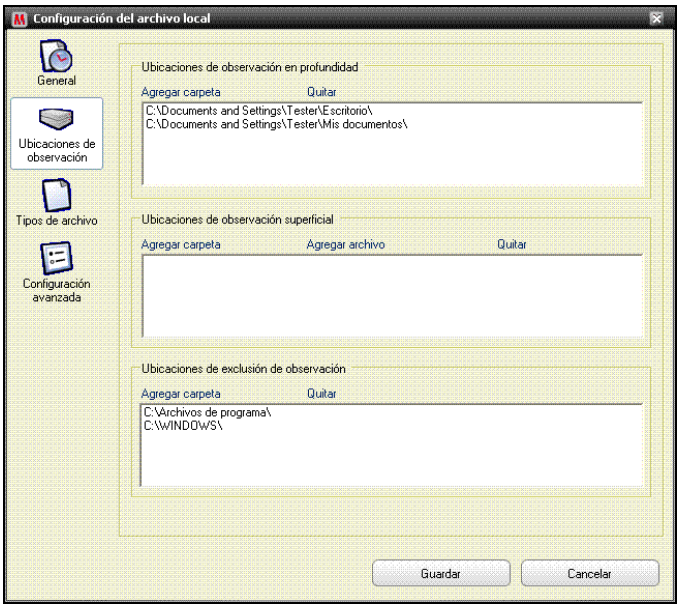
Por motivos de seguridad o problemas de tamaño, el cifrado y la compresión están habilitados por defecto para sus ficheros archivados. El contenido de los archivos cifrados se transforma de texto en código, de forma que la información queda oculta y resulta ilegible para aquellas personas que no saben cómo descifrarla. Los archivos comprimidos se comprimen en un formato que minimiza el espacio necesario para su almacenamiento y transmisión. Si bien McAfee no recomienda hacerlo, puede desactivar el cifrado o la compresión en cualquier momento.

Cómo incluir una ubicación en el archivo

Puede configurar dos tipos de ubicaciones de observación para archivar: en profundidad y superficial. Si se establece una ubicación de observación en profundidad, Data Backup controla los cambios del contenido de dicha carpeta y sus subcarpetas. Si se establece una ubicación de observación superficial, Data Backup controla únicamente el contenido de dicha carpeta (no de sus subcarpetas).

Para incluir una ubicación en el archivo:

1. Haga clic en **Archivo local**.
2. En el panel izquierdo, haga clic en **Configuración**.
3. En el cuadro de diálogo Configuración del archivo local, haga clic en **Ubicaciones de observación**.



4. Siga uno de estos procedimientos:
   - Para archivar el contenido de una carpeta, incluido el contenido de sus subcarpetas, haga clic en **Agregar carpeta** bajo **Ubicaciones de observación en profundidad**.
   - Para archivar el contenido de una carpeta, pero no del contenido de sus subcarpetas, haga clic en **Agregar carpeta** bajo **Ubicaciones de observación superficial**.

5 En el cuadro de diálogo Buscar carpeta, acceda a la carpeta que desee observar y haga clic en **Aceptar**.

6 Haga clic en **Guardar**.

Sugerencia: Si desea que Data Backup observe una carpeta que aún no ha creado, puede hacer clic en **Crear nueva carpeta** en el cuadro de diálogo Buscar carpeta para agregar una carpeta y configurarla como ubicación de observación al mismo tiempo.

Configuración de los tipos de fichero del archivo

Puede especificar los tipos de ficheros archivados en las ubicaciones de observación en profundidad o superficial. Puede seleccionarlos de una lista de tipos de ficheros existente o agregar un nuevo tipo de fichero a la lista.

Para configurar los tipos de fichero del archivo:

1 Haga clic en **Archivo local**.

2 En el panel izquierdo, haga clic en **Configuración**.

3 En el cuadro de diálogo Configuración del archivo local, haga clic en **Tipos de archivo**.

4 Amplíe las listas de tipos de archivo y active las casillas situadas junto a los tipos de archivo que desea archivar.

5 Haga clic en **Guardar**.

Sugerencia: Para agregar un nuevo tipo de archivo a la lista **Tipos de archivo seleccionados**, escriba la extensión del archivo en el cuadro de diálogo **Agregar tipo de archivo personalizado a "Otros"** y haga clic en **Agregar**. El nuevo tipo de archivo se convierte automáticamente en un tipo de archivo de observación.

Cómo excluir una ubicación del archivo

Puede excluir una ubicación del archivo si desea evitar que dicha ubicación (carpeta) y su contenido se archiven.

Para excluir una ubicación del archivo:

1. Haga clic en **Archivo local**.
2. En el panel izquierdo, haga clic en **Configuración**.
3. En el cuadro de diálogo Configuración del archivo local, haga clic en **Ubicaciones de observación**.
4. Haga clic en **Agregar carpeta** bajo **Ubicaciones de exclusión de observación**.
5. En el cuadro de diálogo Buscar carpeta, acceda a la carpeta que desee excluir, selecciónela y haga clic en **Aceptar**.
6. Haga clic en **Guardar**.

Sugerencia: Si desea que Data Backup excluya una carpeta que aún no ha creado, puede hacer clic en **Crear nueva carpeta** en el cuadro de diálogo Buscar carpeta para agregar una carpeta y excluirla al mismo tiempo.

Cómo cambiar la ubicación del archivo

Al cambiar la ubicación del archivo, los ficheros previamente archivados en una ubicación diferente aparecen como *Nunca archivado*.

Para cambiar la ubicación del archivo:

1. Haga clic en **Archivo local**.
2. En el panel izquierdo, haga clic en **Configuración**.
3. Haga clic en **Cambiar ubicación de archivo**.
4. En el cuadro de diálogo Ubicación del archivo, realice una de las acciones siguientes:
   - Haga clic en **Seleccionar grabador de CD/DVD**, pulse la unidad de CD o DVD de se equipo en la lista **Grabador** y haga clic en **Guardar**.
   - Haga clic en **Seleccionar ubicación del disco**, vaya al disco USB, al disco local o al disco duro externo, selecciónelo y haga clic en **Aceptar**.
   - Haga clic en **Seleccionar ubicación de red**, vaya a la carpeta de red, selecciónela y haga clic en **Aceptar**.

5 Verifique la nueva ubicación del archivo en **Ubicación de archivo seleccionada** y haga clic en **Aceptar**.

6 En el cuadro de diálogo de confirmación, haga clic en **Aceptar**.

7 Haga clic en **Guardar**.

Desactivación del cifrado y la compresión de archivos

El cifrado de los ficheros archivados protege la confidencialidad de sus datos ocultando el contenido de los archivos para que sean ilegibles. La compresión de los ficheros archivados ayuda a minimizar el tamaño de los archivos. Por defecto, tanto el cifrado como la compresión están habilitados; sin embargo, puede desactivar estas opciones en cualquier momento.

Para desactivar el cifrado y la compresión de archivos:

1 Haga clic en **Archivo local**.

2 En el panel izquierdo, haga clic en **Configuración**.

3 En el cuadro de diálogo Configuración del archivo local, haga clic en **Configuración avanzada**.

4 Desactive la casilla **Activar cifrado para aumentar seguridad**.

5 Desactive la casilla **Activar compresión para reducir almacenamiento**.

6 Haga clic en **Guardar**.

Nota: McAfee le aconseja que no desactive el cifrado ni la compresión al archivar sus archivos.

Uso de archivos completos y rápidos

Puede utilizar dos tipos de archivo: completo o rápido. Al utilizar un archivo completo, se archiva un conjunto de datos completo basado en las ubicaciones y los tipos de archivos observados que haya configurado. Al utilizar un archivo rápido, archiva únicamente aquellos archivos observados que se han modificado desde la última operación de archivado rápido.

Por defecto, Data Backup está programado para realizar un archivado completo de los tipos de archivos observados en sus ubicaciones de observación los lunes a las 9:00 y un archivado rápido cada 48 horas después del último archivado completo o rápido. Esta programación garantiza que en todo momento se mantenga un archivo de sus archivos actualizado. Pese a ello, si no desea archivar cada 48 horas, puede ajustar la programación a sus necesidades.

Si desea archivar el contenido de sus ubicaciones de observación cuando lo solicite, puede hacerlo en todo momento. Por ejemplo, si desea modificar un archivo y archivarlo, pero Data Backup no está programado para realizar un archivado completo o rápido hasta dentro de 60 minutos, puede archivar los archivos de manera manual. Al archivar archivos manualmente, se restablece el intervalo configurado para los archivados automáticos.

También puede interrumpir un archivado automático o manual si se produce en un momento inadecuado. Por ejemplo, si está realizando una tarea que consume muchos recursos y se inicia un archivado automático, usted puede detenerlo. Al detener un archivado automático se restablece el intervalo configurado para los archivados automáticos.

Programación de los archivados automáticos

Puede configurar la frecuencia de los archivos rápidos y completos para asegurarse de que sus datos están permanentemente protegidos.

Para programar archivos automáticos:

1. Haga clic en **Archivo local**.
2. En el panel izquierdo, haga clic en **Configuración**.
3. En el cuadro de diálogo Configuración del archivo local, haga clic en **General**.
4. Para realizar un archivo completo todos los días, semanas o meses, haga clic en lo siguiente bajo **Archivo completo cada**:
   - **Día**
   - **Semana**
   - **Mes**

5 Active la casilla situada junto al día en el que desea realizar el archivo completo.

6 Haga clic en un valor de la lista **A las** para especificar la hora en la que desea realizar el archivo completo.

7 Para realizar un archivo rápido diariamente, haga clic en lo siguiente bajo **Archivo rápido**:

- **Horas**
- **Días**

8 Escriba un número que represente la frecuencia en el cuadro **Archivo rápido cada**.

9 Haga clic en **Guardar**.

Interrupción de un archivo automático

Data Backup archiva automáticamente los archivos de sus ubicaciones de observación en función de la programación que usted defina. Sin embargo, si se está archivando automáticamente y desea interrumpir la operación, puede hacerlo en todo momento.

Para interrumpir un archivo automático:

1 En el panel izquierdo, haga clic en **Detener el archivado**.

2 En el cuadro de diálogo de confirmación, haga clic en **Sí**.

Nota: El enlace **Detener el archivado** únicamente aparece cuando hay un archivado en progreso.

Ejecutar archivados manualmente

Pese a que los archivados automáticos se realizan en función de una programación predefinida, puede realizar archivados completos o rápidos de manera manual en cualquier momento. Un archivado rápido archiva únicamente aquellos archivos que se han modificado desde la última operación de archivado rápido o completo. Un archivo completo archiva los tipos de archivos observados de todas las ubicaciones de observación.

Para ejecutar un archivo rápido o completo manualmente:

1 Haga clic en **Archivo local**.

2 Para ejecutar un archivo rápido, haga clic en **Archivo rápido** en el panel de la izquierda.

3 Para ejecutar un archivo completo, haga clic en **Archivo completo** en el panel de la izquierda.

4 En el cuadro de diálogo Listo para iniciar el proceso de archivo, verifique su espacio de almacenamiento y su configuración y haga clic en **Continuar**.

CAPÍTULO 36

Cómo trabajar con archivos archivados

Después de archivar algunos archivos, puede utilizar Data Backup para trabajar con ellos. Los archivos archivados se presentan en la vista tradicional del navegador, lo que le permite localizarlos fácilmente. A medida que su archivo aumenta, es posible que desee ordenar los archivos o buscarlos. También puede abrir los archivos directamente en la vista del navegador para examinar el contenido sin tener que recuperar los archivos.

Puede recuperar los archivos de un archivo si la copia local del mismo no está actualizada, se daña o falta. Data Backup también le ofrece la información necesaria para gestionar sus archivos locales y su espacio de almacenamiento.

En este capítulo

Uso del navegador del archivo local

El navegador del archivo local le permite visualizar y manipular los archivos que ha archivado localmente. Puede ver el nombre, tipo, ubicación, tamaño, estado (archivado, no archivado o archivo en progreso) y la fecha en la que cada archivo se archivó por última vez. También puede ordenar los archivos por cualquiera de estos criterios.

Si tiene un archivo grande, puede encontrar un archivo rápidamente al buscarlo. Puede buscar por el nombre completo del archivo, por parte de él o por su ruta y puede restringir su búsqueda especificando el tamaño de archivo aproximado y la fecha en la que se archivó por última vez.

Cuando ubique un archivo, puede abrirlo directamente en el navegador del archivo local. Data Backup abre el archivo en su programa nativo, permitiéndole realizar cambios sin salir del navegador del archivo local. El archivo se guarda en la ubicación de observación original del equipo y se archiva automáticamente en función de la programación de archivado definida.

Cómo ordenar archivos archivados

Puede ordenar los archivos y las carpetas archivadas por los siguientes criterios: nombre, tipo de archivo, tamaño, estado (es decir, archivado, no archivado o archivo en progreso), la fecha en la que se archivaron los archivos por última vez o la ubicación de los archivos en su equipo (ruta).

Para ordenar archivos archivados:

1. Haga clic en **Archivo local**.
2. En el panel de la derecha, haga clic en el nombre de una columna.

Cómo buscar un archivo archivado

Si tiene un amplio repositorio de archivos archivados, puede encontrar un archivo rápidamente al buscarlo. Puede buscar por el nombre completo del archivo, por parte de él o por su ruta y puede restringir su búsqueda especificando el tamaño de archivo aproximado y la fecha en la que se archivó por última vez.

Para buscar un archivo archivado:

1. Escriba el nombre completo o parte de él en el cuadro de diálogo **Buscar** situado en la parte superior de la pantalla y pulse INTRO.
2. Escriba la ruta completa o parte de ella en el cuadro de diálogo **Todo o parte de la ruta**.
3. Especifique el tamaño aproximado del archivo que está buscando realizando uno de los siguientes pasos:
   - Haga clic en **<100 KB**, **<1 MB** o **>1 MB**.

- Haga clic en **Tamaño en KB** y especifique los valores de tamaño apropiados en los cuadros de diálogo.

4 Especifique la fecha aproximada en la que se realizó la última copia en línea del archivo realizando uno de los siguientes pasos:

- Haga clic en **Esta semana**, **Este mes** o **Este año**.
- Haga clic en **Especificar fechas**, haga clic en **Archivados** en la lista y haga clic en los valores de fecha adecuados en las listas de fecha.

5 Haga clic en **Buscar**.

Nota: Si desconoce el tamaño o la fecha del último archivo aproximados, haga clic en **Desconocidos**.

Cómo abrir un archivo archivado

Puede examinar el contenido de un archivo archivado abriéndolo directamente en el navegador del archivo local.

Para abrir un archivo archivado:

1 Haga clic en **Archivo local**.

2 En el panel de la derecha, haga clic en un nombre de archivo y clic en **Abrir**.

Sugerencia: También puede abrir un archivo archivado haciendo doble clic en el nombre del archivo.

Recuperación de archivos archivados

Si un archivo observado se daña, falta o se elimina por error, puede recuperar una copia reciente del mismo desde un archivo local. Por este motivo, es importante asegurarse de que archiva sus archivos de forma regular. También puede recuperar versiones de archivos anteriores desde un archivo local. Por ejemplo, si archiva un archivo de manera regular, pero desea restablecer una versión anterior de un archivo, puede hacerlo localizando el archivo en la ubicación del archivado. Si la ubicación del archivo es un disco local o de red, puede buscar el archivo. Si la ubicación del archivo es un disco duro externo o USB, debe conectar el disco al equipo y a continuación buscar el archivo. Si la ubicación del archivo es un CD o DVD, debe introducirlo en el equipo y a continuación buscar el archivo.

También puede recuperar archivos que haya archivado en equipo desde otro equipo diferente. Por ejemplo, si archiva un conjunto de archivos en un disco duro externo en el equipo A, puede recuperarlos en el equipo B. Para ello, debe instalar McAfee Data Backup en el equipo B y conectar el disco duro externo. A continuación, en Data Backup, busque los archivos que se añaden a la lista **Archivos que faltan** para su recuperación.

Si desea obtener más información sobre el archivado de archivos, consulte Cómo archivar archivos. Si elimina un archivo observado de su equipo de manera intencionada, también puede eliminar la entrada de la lista **Archivos que faltan**.

Recuperación de archivos que faltan desde un archivo local

El archivo local de Data Backup le permite recuperar datos que faltan desde una ubicación de observación de su equipo local. Por ejemplo, si un archivo se saca de una carpeta de observación o si se elimina, y ya se ha archivado, puede recuperarlo desde el archivo local.

Para recuperar un archivo que falta desde un archivo local:

1. Haga clic en **Archivo local**.
2. En **Archivos que faltan** en la parte inferior de la pantalla, seleccione la casilla situada junto al nombre del archivo que desea recuperar.
3. Haga clic en **Restaurar**.

Sugerencia: Puede recuperar todos los archivos de la lista **Archivos que faltan** haciendo clic en **Restaurar todo**.

Recuperación de una versión anterior de un archivo desde el archivo local

Si desea recuperar una versión anterior de un archivo archivado, puede localizarlo y agregarlo a la lista **Archivos que faltan**. A continuación, puede recuperar el archivo, del mismo modo que cualquier otro archivo en la lista **Archivos que faltan**.

Para recuperar una versión anterior de un archivo desde el archivo local:

1. Haga clic en **Archivo local**.
2. En **Archivos que faltan** en la parte inferior de la pantalla, haga clic en **Examinar** y vaya a la ubicación en la que se almacena el archivo.

   Los nombres de las carpetas archivadas tienen el siguiente formato: `cre ddmmaa_hh-mm-ss_***`, donde `ddmmaa` es la fecha en la que se archivaron los archivos, `hh-mm-ss` es la hora en la que se archivaron los archivos y `***` es `Completo` o `Inc`, en función de si se ha realizado un archivo completo o rápido.
3. Seleccione la ubicación y haga clic en **Aceptar**.

   Los archivos contenidos en la ubicación seleccionada aparecen en la lista **Archivos que faltan**, listos para ser recuperados. Para obtener más información, consulte Recuperación de archivos que faltan desde un archivo local.

Eliminación de archivos de la lista de archivos que faltan

Cuando un archivo archivado se saca de una carpeta observada o se elimina, aparece automáticamente en la lista **Archivos que faltan**. Esto le advierte del hecho de que existe una incoherencia entre los archivos archivados y los archivos dentro de las carpetas observadas. Si el archivo se ha sacado de la carpeta observada o si se ha eliminado intencionadamente, puede eliminarlo de la lista **Archivos que faltan**.

Para eliminar un archivo de la lista Archivos que faltan:

1. Haga clic en **Archivo local**.
2. En **Archivos que faltan** en la parte inferior de la pantalla, seleccione la casilla situada junto al nombre del archivo que desea eliminar.
3. Pulse en **Eliminar**.

Sugerencia: Puede eliminar todos los archivos de la lista **Archivos que faltan** haciendo clic en **Suprimir todo**.

Gestión de archivos

Puede ver un resumen de la información sobre sus archivos completos y rápidos en cualquier momento. Por ejemplo, puede ver la información sobre la cantidad de datos observados actualmente, la cantidad de datos archivados y la cantidad de datos actualmente observada pero que aún no han sido archivados. También puede ver información sobre la programación de archivo, como la fecha del último y el siguiente archivo.

Cómo ver un resumen de su actividad de archivado

Puede ver la información sobre su actividad de archivado en cualquier momento. Por ejemplo, puede ver el porcentaje de archivos archivados, el tamaño de los datos observados, el tamaño de los datos archivados y el tamaño de los datos observados pero que aún no han sido archivados. También puede ver las fechas del último y el siguiente archivo.

Para ver un resumen de su actividad de copias de seguridad:

1. Haga clic en **Archivo local**.
2. En la parte superior de la pantalla, haga clic en **Resumen de la cuenta**.

CAPÍTULO 37

McAfee QuickClean

QuickClean mejora el rendimiento de su equipo mediante la eliminación de archivos que pueden crear desorden en el equipo. Vacía la Papelera de reciclaje y elimina los archivos temporales, accesos directos, fragmentos de archivos perdidos, archivos de registro, archivos en la caché, cookies, archivos del historial de navegación, correos electrónicos enviados y eliminados, archivos usados recientemente, archivos de Active-X y archivos de puntos de restauración del sistema. QuickClean también protege su privacidad mediante el uso del componente McAfee Shredder para eliminar de manera segura y permanente elementos que puedan contener información personal y delicada, como su nombre y dirección. Si desea información sobre la purga de archivos, consulte McAfee Shredder.

El Desfragmentador de disco organiza los archivos y las carpetas de su equipo para asegurar que no se esparzan (es decir, que no se fragmenten) cuando se guardan en el disco duro de su equipo. Mediante la desfragmentación de su disco duro de manera periódica, se garantiza que estos archivos y carpetas fragmentados se consoliden para poder recuperarlos rápidamente más adelante.

Si no desea mantener su equipo manualmente, puede programar QuickClean y el Desfragmentador de disco para que se ejecuten de manera automática, como tareas independientes con cualquier frecuencia que desee.

Nota: SecurityCenter informa de los problemas de protección críticos y no críticos tan pronto como los detecta. Si necesita ayuda para diagnosticar sus problemas de protección, puede ejecutar McAfee Virtual Technician.

En este capítulo

Características de QuickClean

QuickClean ofrece varios limpiadores que eliminan de manera segura y eficaz archivos innecesarios. Mediante la eliminación de estos archivos, aumenta el espacio de su disco duro y mejora su rendimiento.

Limpiando el equipo

QuickClean elimina los archivos que pueden colapsar su equipo. Vacía la Papelera de reciclaje y elimina los archivos temporales, accesos directos, fragmentos de archivos perdidos, archivos de registro, archivos en la caché, cookies, archivos del historial de navegación, correos electrónicos enviados y eliminados, archivos usados recientemente, archivos de Active-X y archivos de puntos de restauración del sistema. QuickClean elimina estos elementos sin que eso afecte a otra información esencial.

Puede utilizar cualquiera de los limpiadores de QuickClean para eliminar archivos innecesarios de su equipo. La siguiente tabla describe los limpiadores de QuickClean:

Nombre	Función
Limpiador de Papelera de reciclaje	Elimina los archivos de la Papelera de reciclaje.
Limpiador de archivos temporales	Elimina los archivos almacenados en las carpetas temporales.
Limpiador de accesos directos	Elimina los accesos directos deshabilitados y aquellos que no tienen un programa asociado.
Limpiador de fragmentos de archivos perdidos	Elimina del equipo los fragmentos de archivos perdidos.
Limpiador del Registro	Elimina la información de los programas que ya no están en el equipo del Registro de Windows®. El registro es una base de datos en la que Windows almacena su información de configuración. El registro contiene perfiles para cada usuario del equipo e información acerca del hardware, los programas instalados y los ajustes de propiedades del sistema. Windows consulta continuamente esta información durante su funcionamiento.

Nombre	Función
Limpiador de caché	Elimina los archivos de la caché que se almacenan mientras navega por páginas Web. Estos archivos se almacenan, por lo general, como archivos temporales en una carpeta de la caché. Una carpeta de la caché es un área de almacenamiento temporal de su equipo. Para aumentar la eficacia y velocidad de navegación de páginas Web, su explorador puede recuperar una página Web desde la caché la siguiente vez que desee verla, en lugar de tener que hacerlo desde un servidor remoto.
Limpiador de cookies	Elimina las cookies. Estos archivos se almacenan, por lo general, como archivos temporales. Una cookie es un pequeño archivo que contiene información y que, por lo general, incluye un nombre de usuario y la fecha y hora actual, que se almacena en el equipo de una persona que navega por Internet. Las cookies son utilizadas principalmente por los sitios Web para identificar a los usuarios que se han registrado previamente o que han visitado el sitio; sin embargo, también pueden ser una fuente de información para los piratas informáticos.
Limpiador del historial del navegador	Elimina el historial del navegador Web.
Limpiador de correo de Outlook Express y Outlook (para elementos eliminados y enviados)	Elimina los correos electrónicos enviados y eliminados de Outlook® y Outlook Express.
Limpiador utilizado recientemente	Elimina archivos usados recientemente que se hayan creado con cualquiera de estos programas: ▪ Adobe Acrobat® ▪ Corel® WordPerfect® Office (Corel Office) ▪ Jasc® ▪ Lotus® ▪ Microsoft® Office® ▪ RealPlayer™ ▪ Windows History ▪ Windows Media Player ▪ WinRAR® ▪ WinZip®

Nombre	Función
Limpiador de ActiveX	Elimina los controles ActiveX. ActiveX es un componente de software que utilizan los programas o páginas Web para añadir funciones que se integran y aparecen como parte normal de esos programas o páginas Web. La mayor parte de los controles ActiveX son inofensivos; sin embargo, algunos pueden capturar información de su equipo.
Limpiador de punto de restauración del sistema	Elimina puntos antiguos de restauración del sistema de su equipo (excepto los más recientes). Windows crea los puntos de restauración del sistema para marcar cualquier cambio realizado en el equipo con el fin de que usted pueda volver a un estado anterior si tuviese lugar cualquier problema.

Limpieza del equipo

Puede utilizar cualquiera de los limpiadores de QuickClean para eliminar archivos innecesarios de su equipo. Al finalizar, bajo **Resumen de QuickClean**, puede ver la cantidad de espacio en disco recuperada tras la limpieza, el número de archivos eliminados y la fecha y hora en la que se ejecutó la última operación de QuickClean de su equipo.

1. En el panel McAfee SecurityCenter, bajo **Tareas comunes**, haga clic en **Mantener equipo**.
2. En **McAfee QuickClean**, haga clic en **Inicio**.
3. Siga uno de estos procedimientos:
   - Haga clic en **Siguiente** para aceptar los limpiadores predeterminados de la lista.
   - Active o desactive los limpiadores correspondientes y haga clic en **Siguiente.** Si selecciona el Limpiador utilizado recientemente, puede hacer clic en **Propiedades** para seleccionar o borrar los archivos que se han creado recientemente con los programas de la lista y, a continuación, haga clic en **Aceptar**.
   - Haga clic en **Restaurar valores predeterminados** para restaurar los limpiadores predeterminados y, a continuación, haga clic en **Siguiente.**

4 Una vez realizado el informe, haga clic en **Siguiente**.

5 Haga clic en **Siguiente** para confirmar la eliminación de los archivos.

6 Siga uno de estos procedimientos:

- Haga clic en **Siguiente** para aceptar la opción predeterminada **No, deseo borrar los archivos con el método de eliminación estándar de Windows**.
- Haga clic en **Sí, deseo usar Shredder para borrar de modo seguro los archivos** y especifique el número de veces que se ejecutará el proceso, hasta un máximo de 10 y, a continuación, haga clic en **Siguiente**. La purga de archivos puede ser un proceso largo si la cantidad de información que se ha de borrar es grande.

7 Si se bloquearon archivos o elementos durante la limpieza, puede que se le solicite que reinicie el equipo. Haga clic en **Aceptar** para cerrar la solicitud.

8 Haga clic en **Finalizar**.

Nota: Los archivos eliminados con Shredder no se pueden recuperar. Si desea información sobre la purga de archivos, consulte McAfee Shredder.

Desfragmentación del equipo

El Desfragmentador de disco organiza los archivos y las carpetas de su equipo para que no se esparzan (es decir, que no se fragmenten) cuando se guardan en el disco duro de su equipo. Mediante la desfragmentación de su disco duro de manera periódica, se garantiza que estos archivos y carpetas fragmentados se consoliden para poder recuperarlos rápidamente más adelante.

Desfragmentación del equipo

Puede desfragmentar su equipo para mejorar el acceso y recuperación a sus archivos y carpetas.

1. En el panel McAfee SecurityCenter, bajo **Tareas comunes**, haga clic en **Mantener equipo**.
2. En **Desfragmentador de disco**, haga clic en **Analizar**.
3. Siga las instrucciones que aparecen en pantalla.

Nota: Si desea obtener más información acerca del Desfragmentador de disco, consulte la ayuda de Windows.

Planificación de una tarea

El Planificador de tareas automatiza la frecuencia a la que QuickClean o el Desfragmentador de disco se ejecutan en su equipo. Por ejemplo, puede programar una tarea de QuickClean para vaciar su Papelera de reciclaje cada domingo a las 9:00 P.M. o una tarea del Desfragmentador de disco para desfragmentar el disco duro de su equipo el último día de cada mes. Puede crear, modificar o eliminar una tarea en cualquier momento. Debe haber iniciado sesión en su equipo para que se ejecute una tarea programada. Si, por cualquier motivo, no se ejecutase una tarea, se volverá a programar cinco minutos después de que se inicie sesión de nuevo.

Programación de una tarea de QuickClean

Puede programar una tarea de QuickClean para limpiar de manera automática su equipo usando uno o más limpiadores. Cuando acabe, bajo **Resumen de QuickClean**, puede ver la fecha y hora a la que su tarea está programada para ejecutarse de nuevo.

1. Abra el panel del Planificador de tareas.

   ¿Cómo?

   1. En el panel McAfee SecurityCenter, bajo **Tareas comunes**, haga clic en **Mantener equipo**.
   2. En **Planificador de tareas**, haga clic en **Inicio**.

2. En la lista **Seleccione la operación que desee programar**, haga clic en **McAfee QuickClean**.
3. Escriba un nombre para la tarea en el cuadro **Nombre de la tarea** y, a continuación, haga clic en **Crear.**
4. Siga uno de estos procedimientos:
   - Haga clic en **Siguiente** para aceptar los limpiadores de la lista.
   - Active o desactive los limpiadores correspondientes y haga clic en **Siguiente**. Si selecciona el Limpiador utilizado recientemente, puede hacer clic en **Propiedades** para seleccionar o borrar los archivos que se han creado recientemente con los programas de la lista y, a continuación, haga clic en **Aceptar**.
   - Haga clic en **Restaurar valores predeterminados** para restaurar los limpiadores predeterminados y, a continuación, haga clic en **Siguiente**.
5. Siga uno de estos procedimientos:
   - Haga clic en **Calendario** para aceptar la opción predeterminada **No, deseo borrar los archivos con el método de eliminación estándar de Windows**.

- Haga clic en **Sí, deseo usar Shredder para borrar de modo seguro los archivos** y especifique el número de veces que se ejecutará el proceso, hasta un máximo de 10 y, a continuación, haga clic en **Calendario**.

6 Seleccione la frecuencia a la que desea que se ejecute la tarea en el cuadro de diálogo **Calendario** y, a continuación, haga clic en **Aceptar**.

7 Si realizó cambios en las propiedades del Limpiador utilizado recientemente, puede que se le solicite que reinicie el equipo. Haga clic en **Aceptar** para cerrar la solicitud.

8 Haga clic en **Finalizar**.

Nota: Los archivos eliminados con Shredder no se pueden recuperar. Si desea información sobre la purga de archivos, consulte McAfee Shredder.

Modificación de una tarea de QuickClean

Puede modificar una tarea planificada de QuickClean para cambiar los limpiadores que utiliza o la frecuencia a la que se ejecutará de manera automática en su equipo. Cuando acabe, bajo **Resumen de QuickClean**, puede ver la fecha y hora a la que su tarea está programada para ejecutarse de nuevo.

1 Abra el panel del Planificador de tareas.

¿Cómo?

1. En el panel McAfee SecurityCenter, bajo **Tareas comunes**, haga clic en **Mantener equipo**.
2. En **Planificador de tareas**, haga clic en **Inicio**.

2 En la lista **Seleccione la operación que desee programar**, haga clic en **McAfee QuickClean**.

3 Seleccione la tarea en la lista **Seleccione una tarea existente** y, a continuación, haga clic en **Modificar**.

4 Siga uno de estos procedimientos:

- Haga clic en **Siguiente** para aceptar los limpiadores para la tarea.
- Active o desactive los limpiadores correspondientes y haga clic en **Siguiente**. Si selecciona el Limpiador utilizado recientemente, puede hacer clic en **Propiedades** para seleccionar o borrar los archivos que se han creado recientemente con los programas de la lista y, a continuación, haga clic en **Aceptar**.
- Haga clic en **Restaurar valores predeterminados** para restaurar los limpiadores predeterminados y, a continuación, haga clic en **Siguiente.**

5 Siga uno de estos procedimientos:

- Haga clic en **Calendario** para aceptar la opción predeterminada **No, deseo borrar los archivos con el método de eliminación estándar de Windows**.
- Haga clic en **Sí, deseo usar Shredder para borrar de modo seguro los archivos**, especifique el número de veces que se ejecutará el proceso, hasta un máximo de 10 y, a continuación, haga clic en **Calendario**.

6 Seleccione la frecuencia a la que desea que se ejecute la tarea en el cuadro de diálogo **Calendario** y, a continuación, haga clic en **Aceptar**.

7 Si realizó cambios en las propiedades del Limpiador utilizado recientemente, puede que se le solicite que reinicie el equipo. Haga clic en **Aceptar** para cerrar la solicitud.

8 Haga clic en **Finalizar**.

Nota: Los archivos eliminados con Shredder no se pueden recuperar. Si desea información sobre la purga de archivos, consulte McAfee Shredder.

Eliminación de una tarea de QuickClean

Puede eliminar una tarea planificada de QuickClean si ya no desea que se ejecute automáticamente.

1 Abra el panel del Planificador de tareas.

¿Cómo?

1. En el panel McAfee SecurityCenter, bajo **Tareas comunes**, haga clic en **Mantener equipo**.
2. En **Planificador de tareas**, haga clic en **Inicio**.

2 En la lista **Seleccione la operación que desee programar**, haga clic en **McAfee QuickClean**.

3 Seleccione la tarea de la lista **Seleccione una tarea existente**.

4 Haga clic en **Eliminar** y, a continuación, haga clic en **Sí** para confirmar la eliminación.

5 Haga clic en **Finalizar**.

Planificación de una tarea del Desfragmentador de disco

Puede planificar una tarea del Desfragmentador de disco para planificar la frecuencia a la que se desfragmenta automáticamente el disco duro de su equipo. Cuando acabe, bajo **Desfragmentador de disco**, puede ver la fecha y hora a la que su tarea está programada para ejecutarse de nuevo.

1 Abra el panel del Planificador de tareas.

¿Cómo?

1. En el panel McAfee SecurityCenter, bajo **Tareas comunes**, haga clic en **Mantener equipo**.
2. En **Planificador de tareas**, haga clic en **Inicio**.

2 En la lista **Seleccione la operación que desee programar**, haga clic en **Desfragmentador de disco**.

3 Escriba un nombre para la tarea en el cuadro **Nombre de la tarea** y, a continuación, haga clic en **Crear**.

4 Siga uno de estos procedimientos:

- Haga clic en **Calendario** para aceptar la opción predeterminada **Realizar la desfragmentación aunque haya poco espacio libre**.
- Desactive la opción **Realizar la desfragmentación aunque haya poco espacio libre** y, a continuación, haga clic en **Calendario**.

5 Seleccione la frecuencia a la que desea que se ejecute la tarea en el cuadro de diálogo **Calendario** y, a continuación, haga clic en **Aceptar**.

6 Haga clic en **Finalizar**.

Modificación de una tarea del Desfragmentador de disco

Puede modificar una tarea planificada del Desfragmentador de disco para cambiar la frecuencia a la que se ejecuta automáticamente en su equipo. Cuando acabe, bajo **Desfragmentador de disco**, puede ver la fecha y hora a la que su tarea está programada para ejecutarse de nuevo.

1 Abra el panel del Planificador de tareas.

¿Cómo?

1. En el panel McAfee SecurityCenter, bajo **Tareas comunes**, haga clic en **Mantener equipo**.
2. En **Planificador de tareas**, haga clic en **Inicio**.

2 En la lista **Seleccione la operación que desee programar**, haga clic en **Desfragmentador de disco**.

3 Seleccione la tarea en la lista **Seleccione una tarea existente** y, a continuación, haga clic en **Modificar**.

4 Siga uno de estos procedimientos:

- Haga clic en **Calendario** para aceptar la opción predeterminada **Realizar la desfragmentación aunque haya poco espacio libre**.
- Desactive la opción **Realizar la desfragmentación aunque haya poco espacio libre** y, a continuación, haga clic en **Calendario**.

5 Seleccione la frecuencia a la que desea que se ejecute la tarea en el cuadro de diálogo **Calendario** y, a continuación, haga clic en **Aceptar**.

6 Haga clic en **Finalizar**.

Eliminación de una tarea del Desfragmentador de disco

Puede eliminar una tarea planificada del Desfragmentador de disco si ya no desea que se ejecute automáticamente.

1 Abra el panel del Planificador de tareas.

¿Cómo?

1. En el panel McAfee SecurityCenter, bajo **Tareas comunes**, haga clic en **Mantener equipo**.
2. En **Planificador de tareas**, haga clic en **Inicio**.

2 En la lista **Seleccione la operación que desee programar**, haga clic en **Desfragmentador de disco**.

3 Seleccione la tarea de la lista **Seleccione una tarea existente**.

4 Haga clic en **Eliminar** y, a continuación, haga clic en **Sí** para confirmar la eliminación.

5 Haga clic en **Finalizar**.

CAPÍTULO 38

McAfee Shredder

McAfee Shredder elimina (o purga) permanentemente elementos de la unidad de disco duro de su equipo. Incluso si elimina archivos y carpetas manualmente, vacía la Papelera de reciclaje o elimina su carpeta de Archivos temporales de Internet, puede recuperar esta información utilizando herramientas forenses informáticas. Del mismo modo, un archivo eliminado se puede recuperar debido a que algunos programas crean copias ocultas y temporales de los archivos abiertos. Shredder protege su privacidad al eliminar de forma eficaz y definitiva estos archivos no deseados. Recuerde que los archivos purgados no se pueden restaurar.

Nota: SecurityCenter informa de los problemas de protección críticos y no críticos tan pronto como los detecta. Si necesita ayuda para diagnosticar sus problemas de protección, puede ejecutar McAfee Virtual Technician.

En este capítulo

Características de Shredder

Shredder elimina elementos del disco duro para que la información asociada a ellos no se pueda recuperar. Protege su privacidad eliminando de manera segura y permanente archivos y carpetas, elementos de la Papelera de reciclaje y de la carpeta de Archivos temporales de Internet y el contenido entero de los discos del equipo, como CD regrabables, discos duros externos y unidades de disquete.

Purga de archivos, carpetas y discos

Shredder garantiza que la información contenida en los archivos y carpetas eliminados de su Papelera de reciclaje y de la carpeta de Archivos temporales de Internet no se pueda recuperar, ni siquiera con herramientas especiales. Con Shredder, puede especificar cuántas veces (hasta un máximo de 10) desea que se purgue un elemento. Cuanto mayor sea al número de veces que se realiza esta operación, más eficaz será la eliminación del archivo.

Purgar archivos y carpetas

Puede purgar archivos y carpetas del disco duro de su equipo, incluidos los elementos de la Papelera de reciclaje y de la carpeta de Archivos temporales de Internet.

1. Abrir **Shredder**.

   ¿Cómo?

   1. En el panel McAfee SecurityCenter, bajo **Tareas comunes**, haga clic en **Menú avanzado**.
   2. En el panel izquierdo, haga clic en **Herramientas**.
   3. Haga clic en **Shredder**.

2. En el panel Purgar archivos y carpetas, bajo **Deseo**, haga clic en **Borrar archivos y carpetas**.
3. En **Nivel de purga**, haga clic en uno de los siguientes niveles de purga:
   - **Rápido**: Purga una vez los elementos seleccionados.
   - **Exhaustivo**: Purga siete veces los elementos seleccionados.
   - **Personalizado**: Purga los elementos seleccionados un máximo de diez veces.
4. Haga clic en **Siguiente**.
5. Siga uno de estos procedimientos:
   - En la lista **Seleccione los archivos que desee purgar**, haga clic en **Contenido de la Papelera de reciclaje** o **Archivos temporales de Internet**.
   - Haga clic en **Examinar**, acceda a los archivos que desee purgar, selecciónelos y, a continuación, haga clic en **Abrir**.

6 Haga clic en **Siguiente**.

7 Haga clic en **Iniciar**.

8 Cuando Shredder acabe, haga clic en **Listo**.

Nota: No trabaje con estos archivos hasta que Shredder complete esta tarea.

Purgar un disco completo

Puede purgar el contenido entero de un disco de una sola vez. Sólo se pueden purgar las unidades extraíbles, como los discos duros externos, los CD grabables y los disquetes.

1 Abrir **Shredder**.

¿Cómo?

1. En el panel McAfee SecurityCenter, bajo **Tareas comunes**, haga clic en **Menú avanzado**.
2. En el panel izquierdo, haga clic en **Herramientas**.
3. Haga clic en **Shredder**.

2 En el panel Purgar archivos y carpetas, bajo **Deseo**, haga clic en **Borrar un disco entero**.

3 En **Nivel de purga**, haga clic en uno de los siguientes niveles de purga:

- **Rápido**: Purga la unidad seleccionada una vez.
- **Exhaustivo**: Purga siete veces la unidad seleccionada.
- **Personalizado**: Purga la unidad seleccionada un máximo de diez veces.

4 Haga clic en **Siguiente**.

5 En la lista **Seleccione el disco**, haga clic en la unidad que desee purgar.

6 Haga clic en **Siguiente** y, a continuación, en **Sí** para confirmar.

7 Haga clic en **Iniciar**.

8 Cuando Shredder acabe, haga clic en **Listo**.

Nota: No trabaje con estos archivos hasta que Shredder complete esta tarea.

CAPÍTULO 39

McAfee Network Manager

Network Manager ofrece una representación gráfica de los equipos y componentes que forman una red doméstica. Con Network Manager podrá supervisar de forma remota el estado de protección de cada uno de los equipos gestionados en la red, así como reparar también de forma remota todas las vulnerabilidades de seguridad que se hayan registrado en cualquiera de esos equipos.

Antes de comenzar a usar Network Manager, puede familiarizarse con algunas de las funciones más conocidas. En la ayuda de Network Manager hallará toda la información acerca de cómo configurar y utilizar dichas funciones.

Nota: SecurityCenter informa de los problemas de protección críticos y no críticos tan pronto como los detecta. Si necesita ayuda para diagnosticar sus problemas de protección, puede ejecutar McAfee Virtual Technician.

En este capítulo

Funciones de Network Manager

Network Manager ofrece las siguientes funciones:

Mapa de la red gráfica

El mapa de la red de Network Manager ofrece una visión general gráfica del estado de la protección de los equipos y componentes que forman su red doméstica. Cuando realice cambios en su red (por ejemplo, cuando agregue un equipo), el mapa de la red reconoce estos cambios. Puede actualizar el mapa de la red, cambiar el nombre de la red, y mostrar u ocultar componentes del mapa de la red para personalizar su vista. También puede ver los detalles asociados con cualquiera de los componentes mostrados en el mapa de la red.

Gestión remota

Utilice el mapa de la red de Network Manager para gestionar el estado de protección de los equipos que forman su red doméstica. Puede invitar a un equipo a conectarse a la red gestionada, controlar el estado de protección del equipo gestionado y solucionar vulnerabilidades de seguridad conocidas desde un equipo remoto de la red.

Descripción de los iconos de Network Manager

La siguiente tabla describe los iconos que más se utilizan en el mapa de la red de Network Manager.

Icono	Descripción
	Representa un equipo gestionado, en línea
	Representa un equipo gestionado, sin conexión
	Representa un equipo no gestionado que tiene instalado SecurityCenter
	Representa un equipo no gestionado y sin conexión
	Representa un equipo en línea que no tiene instalado el SecurityCenter, o un dispositivo de red desconocido
	Representa un equipo sin conexión que no tiene instalado SecurityCenter o un dispositivo de red desconocido sin conexión
	Indica que el elemento correspondiente está protegido y conectado
	Indica que el elemento correspondiente requiere su atención
	Indica que el elemento correspondiente requiere su atención inmediata
	Representa un enrutador doméstico inalámbrico
	Representa un enrutador doméstico estándar
	Representa Internet cuando está conectado
	Representa Internet cuando está desconectado

CAPÍTULO 40

Configuración de una red gestionada

Para configurar una red gestionada, debe trabajar con los elementos del mapa de la red y agregar miembros (equipos) a la misma. Es preciso que un equipo se convierta primero en miembro de confianza de la red antes de poder gestionarlo de forma remota o antes de concederle el permiso para que gestione otros equipos de la red de forma remota. Los miembros (equipos) ya existentes en la red que poseen permisos de administración son los que conceden el título de miembro de la red a los equipos nuevos.

Puede consultar la información relacionada con cualquiera de los componentes que aparecen en el mapa de la red incluso después de modificar la red (cuando, por ejemplo, agrega un equipo).

En este capítulo

Trabajar con el mapa de la red

Cada vez que conecte un equipo a la red, Network Manager analizará la red para determinar si existen miembros gestionados o no, los atributos del enrutador y el estado de Internet. Si no encuentra a ningún miembro, Network Manager supone que el equipo conectado actualmente es el primer equipo de la red y lo trata como a un miembro gestionado con permisos de administración. De forma predeterminada, el nombre de la red incluye el grupo de trabajo o el nombre de dominio del primer equipo que se conecta a la red con SecurityCenter instalado; de todos modos, puede cambiar el nombre de la red en cualquier momento.

Siempre que realice cambios en la red (por ejemplo, cuando agregue un equipo), puede personalizar el mapa de la red. Por ejemplo, puede actualizar el mapa de la red, cambiar el nombre de la red y mostrar u ocultar componentes del mapa de la red para personalizar su vista. También puede ver los detalles asociados con cualquiera de los componentes mostrados en el mapa de la red.

Acceder al mapa de la red

El mapa de la red le ofrece una representación gráfica de los equipos y componentes que forman su red doméstica.

- En el menú básico o avanzado, haga clic en **Gestionar red**.

Nota: la primera vez que accede al mapa de red, se le pide que confíe en otros equipos de esta red.

Actualizar el mapa de la red

El mapa de la red se puede actualizar en cualquier momento; por ejemplo, después de que se haya incorporado otro equipo a la red gestionada.

1. En el menú básico o avanzado, haga clic en **Gestionar red**.
2. Haga clic en **Actualizar el mapa de la red** en **Deseo**.

Nota: el enlace **Actualizar el mapa de la red** sólo está disponible cuando no hay ningún elemento seleccionado en el mapa de la red. Para desactivar un elemento, haga clic en el elemento seleccionado o en cualquier espacio en blanco del mapa de la red.

Cambiar el nombre de la red

De forma predeterminada, el nombre de la red incluye el grupo de trabajo o el nombre de dominio del primer equipo que se conecta a la red con SecurityCenter instalado. Si prefiere utilizar otro nombre, puede cambiarlo.

1. En el menú básico o avanzado, haga clic en **Gestionar red**.
2. Haga clic en **Cambiar nombre de red** en **Deseo**.
3. Escriba el nombre de la red en el cuadro **Nombre de red**.
4. Haga clic en **Aceptar**.

Nota: el enlace **Cambiar el nombre de la red** sólo está disponible cuando no hay ningún elemento seleccionado en el mapa de la red. Para desactivar un elemento, haga clic en el elemento seleccionado o en cualquier espacio en blanco del mapa de la red.

Mostrar u ocultar un elemento en el mapa de la red

De forma predeterminada, el mapa de la red muestra todos los equipos y componentes de su red doméstica. Si tiene elementos ocultos, puede volver a mostrarlos en cualquier momento. Sólo se pueden ocultar los elementos no gestionados, los equipos gestionados no se pueden ocultar.

Para...	En el menú Básico o Avanzado, haga clic en **Gestionar red** y luego haga lo siguiente:
Ocultar un elemento en el mapa de la red	Haga clic en un elemento del mapa de la red y otro clic en **Ocultar este elemento** en **Deseo**. En el cuadro de diálogo de confirmación, haga clic en **Sí**.
Mostrar elementos ocultos en el mapa de la red	En **Deseo**, haga clic en **Mostrar elementos ocultos**.

Ver detalles de un elemento

Para visualizar información detallada acerca de un componente de la red, seleccione el componente en cuestión en el mapa de la red. Dicha información incluye el nombre del componente, su estado de protección y demás información necesaria para gestionar el componente.

1. Haga clic en el icono del elemento en el mapa de la red.
2. En **Detalles**, visualice la información sobre el elemento.

Incorporación a la red gestionada

Es preciso que un equipo se convierta primero en miembro de confianza de la red antes de poder gestionarlo de forma remota o antes de concederle el permiso para que gestione otros equipos de la red de forma remota. Los miembros (equipos) ya existentes en la red que poseen permisos de administración son los que conceden el título de miembro de la red a los equipos nuevos. Para asegurar que sólo los equipos de confianza se incorporan a la red, tanto los usuarios de los equipos que conceden el permiso como los de los equipos que se incorporan tienen que autenticarse.

Cuando un equipo se incorpora a la red, se le pide que exponga su estado de protección McAfee a los demás equipos de la red. Si el equipo accede a exponer su estado de protección, se convierte en miembro gestionado de la red. Si el equipo se niega a exponer su estado de protección, se convierte en miembro no gestionado de la red. Los miembros no gestionados de la red suelen ser equipos invitados que desean acceder a otras funciones de la red (por ejemplo, enviar archivos o compartir impresoras).

Nota: tras incorporarse a la red, y en el caso de que tenga instalados otros programas de redes McAfee (por ejemplo, EasyNetwork), esos programas también reconocerán al equipo como equipo gestionado. El nivel de permisos que se asigna a un equipo en Network Manager es aplicable al resto de programas de redes McAfee. Para más información acerca del significado de los distintos permisos (invitado, pleno o administrador) en otros programas de red McAfee, consulte la documentación correspondiente a cada programa.

Incorporarse a una red gestionada

Cuando reciba una invitación para incorporarse a una red gestionada, podrá aceptarla o rechazarla. También puede determinar si desea que éste y otros equipos de la red se supervisen entre ellos las configuraciones de seguridad (por ejemplo, si los servicios de protección antivirus de un equipo están actualizados o no).

1. Asegúrese de que está seleccionada la casilla de verificación **Permitir que todos los equipos de esta red supervisen la configuración de seguridad** en el cuadro de diálogo Red gestionada.
2. Haga clic en **Incorporar**.
   Al aceptar la invitación, se muestran dos tarjetas.
3. Confirme que se trata de las mismas tarjetas que se mostraron en el equipo que le invitó a incorporarse a la red gestionada.
4. Haga clic en **Aceptar**.

Nota: si el equipo que le invitó a incorporarse a la red gestionada no muestra las mismas tarjetas que aparecen en el cuadro de diálogo de confirmación, significa que ha habido un ataque a la seguridad en la red gestionada. En ese caso, la incorporación a la red puede poner en peligro a su equipo; por consiguiente, haga clic en **Cancelar** en el cuadro de diálogo Red gestionada.

Invitar a un equipo a que se incorpore a la red gestionada

Si un equipo se agrega a la red gestionada, o bien existe un equipo no gestionado en la red, puede invitar a ese equipo a incorporarse a la red gestionada. Sólo los equipos con permisos administrativos en la red pueden invitar a otros equipos a que se incorporen a ella. Al enviar la invitación se especifica también el nivel de permisos que se desea asignar al equipo que se incorpora.

1. Haga clic en el icono del equipo no gestionado en el mapa de la red.
2. Haga clic en **Supervisar este equipo** en **Deseo**.
3. En el cuadro de diálogo Invitar a un equipo a incorporarse a la red gestionada, realice una de las siguientes opciones:
   - Haga clic en **Permitir acceso de invitado a programas de redes gestionadas** para permitir que el equipo acceda a la red (puede utilizar esta opción para usuarios temporales de su equipo doméstico).
   - Haga clic en **Permitir acceso completo a programas de redes gestionadas** para permitir que el equipo acceda a la red.

- Haga clic en **Permitir acceso administrativo a programas de redes gestionadas** para permitir que el equipo acceda a la red con permisos de administrador. Asimismo, permite que el equipo conceda acceso, a su vez, a otros equipos que desean incorporarse a la red gestionada.

4 Haga clic en **Aceptar**.
El equipo recibe una invitación para incorporarse a la red gestionada. Cuando el equipo acepta la invitación, se muestran dos tarjetas.

5 Confirme que se trata de las mismas tarjetas que se muestran en el equipo que ha invitado a incorporarse a la red gestionada.

6 Haga clic en **Conceder acceso**.

Nota: si el equipo que ha invitado a incorporarse a la red gestionada no muestra las mismas tarjetas que aparecen en el cuadro de diálogo de confirmación, significa que se ha producido un ataque a la seguridad en la red gestionada. Si permite que el equipo se incorpore a la red, puede poner en peligro a otros equipos; por consiguiente, haga clic en **Denegar acceso** en el cuadro de diálogo de confirmación de seguridad.

Dejar de confiar en los equipos de la red

Si ha confiado en otros equipos de la red por error, puede dejar de hacerlo.

- Haga clic en **Dejar de confiar en los equipos de esta red**, en **Deseo**.

Nota: el enlace **Dejar de confiar en los equipos de esta red** no está disponible si tiene permisos administrativos y existen otros equipos gestionados en la red.

CAPÍTULO 41

Gestión remota de la red

Después de configurar su red gestionada, puede gestionar de forma remota los equipos y componentes que forman la red. Puede supervisar el estado y los niveles de permiso de los equipos y componentes, así como solucionar problemas de seguridad de forma remota.

En este capítulo

Supervisión de estados y permisos

Una red gestionada dispone de miembros gestionados y no gestionados. Los miembros gestionados permiten que otros equipos de la red supervisen su estado de protección de McAfee; los miembros no gestionados no lo permiten. Los miembros no gestionados suelen ser equipos invitados que desean acceder a otras funciones de la red (por ejemplo, enviar archivos o compartir impresoras). Un equipo gestionado de la red puede invitar en cualquier momento a un equipo no gestionado a que se convierta en equipo gestionado. Asimismo, un equipo gestionado puede convertirse en no gestionado en cualquier momento.

Los equipos gestionados tienen permisos administrativos, completos o de invitado. Los permisos administrativos permiten al equipo gestionado gestionar el estado de protección de todos los demás equipos gestionados de la red y conceder el título de miembro de la red a otros equipos. Los permisos pleno y de invitado sólo permiten al equipo acceder a la red. El nivel de permisos de un equipo se puede modificar en cualquier momento.

Dado que una red gestionada también puede tener dispositivos como, por ejemplo, enrutadores, puede utilizar Network Manager para gestionarlos. Asimismo, es posible configurar y modificar las propiedades de visualización de un dispositivo en el mapa de la red.

Supervisar el estado de protección de un equipo

Si no se está supervisando el estado de protección de un equipo en la red (en el caso, por ejemplo, de que el equipo no sea un miembro o sea un miembro no gestionado), puede solicitar su supervisión.

1. Haga clic en el icono del equipo no gestionado en el mapa de la red.
2. Haga clic en **Controlar este equipo** en **Deseo**.

Interrumpir la supervisión del estado de protección de un equipo

Puede dejar de supervisar el estado de protección de un equipo gestionado de la red; sin embargo, este equipo dejará de estar gestionado, por lo que no podrá supervisar su estado de protección de forma remota.

1. Haga clic en el icono de un equipo gestionado en el mapa de la red.
2. Haga clic en **Interrumpir el control en este equipo** en **Deseo**.
3. En el cuadro de diálogo de confirmación, haga clic en **Sí**.

Modificar los permisos de un equipo gestionado

Se pueden modificar los permisos de un equipo gestionado en cualquier momento. Esto permite modificar los equipos que pueden supervisar el estado de protección de otros equipos de la red.

1. Haga clic en el icono de un equipo gestionado en el mapa de la red.
2. Haga clic en **Modificar los permisos para este equipo** en **Deseo**.
3. En el cuadro de diálogo de modificación de permisos, active o desactive la casilla para determinar si este y otros equipos de la red gestionada pueden supervisarse mutuamente el estado de protección.
4. Haga clic en **Aceptar**.

Gestionar un dispositivo

Puede gestionar un dispositivo accediendo a su página Web de administración desde Network Manager.

1. Haga clic en el icono de un dispositivo en el mapa de la red.
2. Haga clic en **Gestionar este dispositivo**, en **Deseo**.
   Se abrirá un navegador Web que mostrará la página Web de administración del dispositivo.
3. En su navegador Web, introduzca sus datos de inicio de sesión y configure la seguridad del dispositivo.

Nota: si el dispositivo es un enrutador inalámbrico o un punto de acceso protegido por Wireless Network Security, deberá utilizar Wireless Network Security para configurar la seguridad del dispositivo.

Modificar las propiedades de visualización de un dispositivo

Al modificar las propiedades de visualización de un dispositivo, puede cambiar el nombre de visualización del mismo en el mapa de la red y especificar si se trata de un enrutador inalámbrico.

1. Haga clic en el icono de un dispositivo en el mapa de la red.
2. Haga clic en **Modificar propiedades de dispositivos** en **Deseo**.
3. Para especificar el nombre de visualización de un dispositivo, escriba el nombre en el cuadro **Nombre**.
4. Para especificar el tipo de dispositivo, haga clic en **Enrutador estándar** si no es un enrutador inalámbrico o **Enrutador inalámbrico** si lo es.
5. Haga clic en **Aceptar**.

Solución de vulnerabilidades de seguridad

Los equipos gestionados con permisos administrativos pueden supervisar el estado de protección McAfee de otros equipos gestionados de la red, así como solucionar de forma remota cualquier tipo de vulnerabilidad de seguridad que se registre. Por ejemplo, si el estado de protección McAfee de un equipo gestionado indica que VirusScan está desactivado, otro equipo gestionado que posea permisos administrativos puede activar VirusScan de forma remota.

Al solucionar vulnerabilidades de seguridad de forma remota, Network Manager repara los problemas más habituales. No obstante, algunas vulnerabilidades de seguridad pueden precisar la intervención manual en el equipo local. En tal caso, Network Manager soluciona aquellos problemas que se pueden resolver de forma remota y luego le solicita que solucione los temas restantes iniciando la sesión en SecurityCenter desde el equipo vulnerable y siguiendo las recomendaciones propuestas. En algunos casos, la solución sugerida consiste en instalar la versión más reciente de SecurityCenter en el equipo o equipos remotos de la red.

Solucionar vulnerabilidades de seguridad

Puede utilizar Network Manager para solucionar la mayoría de las vulnerabilidades de seguridad en equipos gestionados remotos. Por ejemplo, si VirusScan está desactivado en un equipo remoto, podrá activarlo.

1. Haga clic en el icono del elemento en el mapa de la red.
2. Visualice el estado de protección de un elemento en **Detalles**.
3. Haga clic en **Solucionar vulnerabilidades de seguridad** en **Deseo**.
4. Una vez solucionados los problemas de seguridad, haga clic en **Aceptar**.

Nota: si bien Network Manager soluciona automáticamente la mayoría de las vulnerabilidades de seguridad, algunas reparaciones pueden requerir que inicie SecurityCenter en el equipo vulnerable y siga las instrucciones que aparecen en pantalla.

Instalar el software de seguridad McAfee en equipos remotos

Si uno o más equipos de su red no tienen instalada la versión más reciente de SecurityCenter, su estado de protección no se podrá supervisar de forma remota. Si desea supervisar estos equipos de forma remota, deberá ir a cada uno de ellos e instalar la versión más reciente de SecurityCenter.

1. Abra SecurityCenter en el equipo en el que desea instalar el software de seguridad.
2. En **Tareas comunes**, haga clic en **Mi cuenta**.
3. Inicie sesión utilizando la dirección de correo electrónico y la contraseña que empleó para registrar el software de seguridad la primera vez que lo instaló.
4. Seleccione el producto correspondiente, haga clic en el icono **Descargar/Instalar** y siga las instrucciones que aparecerán en pantalla.

CAPÍTULO 42

McAfee EasyNetwork

EasyNetwork permite compartir archivos de forma segura, simplificar la transferencia de archivos y compartir impresoras entre los equipos de su red doméstica. No obstante, todos los equipos de su red doméstica deben tener instalado EasyNetwork para poder acceder a sus funciones.

Antes de usar EasyNetwork, puede familiarizarse con algunas de sus funciones. Encontrará información mas detallada sobre la configuración y uso de estas funciones en la ayuda de EasyNetwork.

Nota: SecurityCenter informa de los problemas de protección críticos y no críticos tan pronto como los detecta. Si necesita ayuda para diagnosticar sus problemas de protección, puede ejecutar McAfee Virtual Technician.

En este capítulo

Funciones de EasyNetwork

EasyNetwork ofrece las funciones siguientes.

Uso compartido de archivos

EasyNetwork hace que compartir archivos con otros equipos de la red sea muy fácil. Cuando comparte archivos, proporciona acceso de sólo lectura a otros equipos a estos archivos. Sólo los equipos con acceso completo o de administrador a su red gestionada (miembros) pueden compartir archivos o acceder a archivos compartidos por otros miembros.

Transferencia de archivos

Puede enviar archivos a otros equipos con acceso completo o de administrador a su red gestionada (miembros). Cuando reciba un archivo, aparecerá en su buzón de entrada de EasyNetwork. El buzón de entrada es una ubicación de almacenamiento temporal para todos aquellos archivos que le envíen otros equipos de la red.

Uso compartido de la impresora automatizado

Después de conectarse a una red gestionada, puede compartir con otros miembros cualquier impresora local que esté conectada con su equipo, utilizando el nombre actual de la impresora como nombre de impresora compartida. También detecta impresoras compartidas por otros equipos de la red y le permite configurar y utilizar estas impresoras.

CAPÍTULO 43

Configuración de EasyNetwork

Antes de poder utilizar EasyNetwork, deberá iniciarlo e incorporarse a una red gestionada. Tras incorporarse a una red gestionada, podrá compartir, buscar y enviar archivos a otros equipos de la red. También puede compartir impresoras. Puede decidir salir de la red en cualquier momento.

En este capítulo

Abrir EasyNetwork

De forma predeterminada, se le pedirá que inicie EasyNetwork después de la instalación; sin embargo, también puede iniciar EasyNetwork más tarde.

- En el menú **Inicio**, seleccione **Programas**, **McAfee** y, a continuación, haga clic en **McAfee EasyNetwork**.

Sugerencia: si ha creado iconos de escritorio e inicio rápido durante la instalación, también puede iniciar EasyNetwork haciendo doble clic en el icono de McAfee EasyNetwork del escritorio o en el área de notificación, situada en el extremo derecho de la barra de tareas.

Incorporarse a una red gestionada

Si ningún equipo de la red a la que está conectado dispone de SecurityCenter, se convertirá en miembro de la red y se le pedirá que identifique si la red es de confianza. Cuando el primer equipo se une a la red, el nombre de su equipo está incluido en el nombre de la red; sin embargo, puede cambiar el nombre de la red en cualquier momento.

Cuando un equipo se conecta a la red, envía una solicitud de incorporación a los equipos que están en la red. Cualquier equipo con permisos administrativos en la red puede conceder la solicitud. El equipo que la admita puede determinar también el nivel de permiso para el equipo que se une a la red; por ejemplo, como invitado (solamente transferencia de archivos) o completo/administrador (transferir y compartir archivos). En EasyNetwork, los equipos con acceso de administrador pueden conceder el acceso a otros equipos y administrar permisos (promover o degradar equipos); los equipos con un acceso completo realizan estas tareas administrativas.

Nota: tras incorporarse a la red, y en el caso de que tenga instalados otros programas de redes McAfee (por ejemplo, Network Manager), esos programas también reconocerán al equipo como equipo gestionado. El nivel de permisos que se asigna a un equipo en EasyNetwork se aplica a todos los programas de conexión a redes de McAfee. Para más información acerca del significado de los distintos permisos (invitado, pleno o administrador) en otros programas de red McAfee, consulte la documentación correspondiente a cada programa.

Incorporación a la red

Cuando un equipo se conecta a una red de confianza por primera vez tras instalar EasyNetwork, aparece un mensaje preguntándole si desea incorporarse a la red gestionada. Si el equipo está de acuerdo con la incorporación, se envía una solicitud a todos los demás equipos de la red que tengan derechos de administrador. Esta solicitud debe admitirse antes de que el equipo pueda compartir impresoras o archivos, o enviar y copiar archivos en la red. El primer equipo de la red obtiene permisos de administrador automáticamente.

1. En la ventana Archivos compartidos, haga clic en **Incorporarse a esta red**.
   Cuando un equipo de administrador de la red admite su solicitud, aparece un mensaje preguntándole si desea permitir que este equipo y otros equipos de la red gestionen la configuración de seguridad de los demás.
2. Para permitir que este y otros equipos de la red gestionen la configuración de seguridad de los demás, haga clic en **Aceptar**; de lo contrario, haga clic en **Cancelar**.
3. Compruebe que el equipo que concede el permiso muestre las tarjetas que aparecen en el cuadro de diálogo de confirmación de la seguridad y, a continuación, haga clic en **Aceptar**.

Nota: si el equipo que le invitó a incorporarse a la red gestionada no muestra las mismas tarjetas que aparecen en el cuadro de diálogo de confirmación, significa que ha habido un ataque a la seguridad en la red gestionada. En ese caso, la incorporación a la red puede poner en peligro a su equipo; por consiguiente, haga clic en **Cancelar**en el cuadro de diálogo de confirmación.

Concesión de acceso a la red

Cuando un equipo solicita incorporarse a una red gestionada, se envía un mensaje a todos los demás equipos de la red que tengan derechos de administrador. El primer equipo que responde se convierte en el equipo que realiza la concesión. Como tal, usted es responsable de decidir qué tipo de acceso desea conceder al equipo: invitado, completo o administrador.

1. En la alerta, haga clic en el nivel de acceso adecuado.
2. En el cuadro de diálogo Invitar a un equipo a incorporarse a la red gestionada, realice una de las siguientes opciones:
   - Haga clic en **Permitir acceso de invitado a programas de redes gestionadas** para permitir que el equipo acceda a la red (puede utilizar esta opción para usuarios temporales de su equipo doméstico).
   - Haga clic en **Permitir acceso completo a programas de redes gestionadas** para permitir que el equipo acceda a la red.

- Haga clic en **Permitir acceso administrativo a programas de redes gestionadas** para permitir que el equipo acceda a la red con permisos de administrador. Asimismo, permite que el equipo conceda acceso, a su vez, a otros equipos que desean incorporarse a la red gestionada.

3 Haga clic en **Aceptar**.

4 Compruebe que el equipo muestre las tarjetas que aparecen en el cuadro de diálogo de confirmación de la seguridad y, a continuación, haga clic en **Conceder acceso**.

Nota: si el equipo no muestra las mismas tarjetas que aparecen en el cuadro de diálogo de confirmación de la seguridad, se ha producido una brecha de seguridad en la red gestionada. La concesión de acceso a este equipo puede poner su equipo en peligro; por lo tanto, haga clic en **Rechazar acceso** en el cuadro de diálogo de confirmación de la seguridad.

Cambiar el nombre de la red

De forma predeterminada, el nombre de la red incluye el nombre del primer equipo que se incorporó a ella; sin embargo, puede cambiar el nombre de la red en cualquier momento. Cuando cambie el nombre de la red, cambie la descripción de la red mostrada en EasyNetwork.

1. En el menú **Opciones** , haga clic en **Configurar**.
2. En el cuadro de diálogo Configurar, escriba el nombre de la red en el cuadro **Nombre de red**.
3. Haga clic en **Aceptar**.

Abandonar una red gestionada

Si se incorpora a una red gestionada y después decide que no quiere seguir siendo miembro de ella, puede abandonarla. Tras abandonar la red gestionada podrá reincorporase a ella siempre que lo desea; sin embargo, deberá obtener el permiso nuevamente. Para obtener más información acerca de la incorporación, consulte Incorporación a una red gestionada (página 246).

Abandonar una red gestionada

Puede abandonar una red gestionada a la que se haya incorporado previamente.

1. En el menú **Herramientas**, haga clic en **Abandonar red**.
2. En el cuadro de diálogo Abandonar red, seleccione el nombre de la red que desea abandonar.
3. Haga clic en **Abandonar red**.

CAPÍTULO 44

Compartir y enviar archivos

EasyNetwork hace que compartir y enviar archivos con los otros equipos de la red sea muy fácil. Cuando comparte archivos, proporciona acceso de sólo lectura a estos archivos a otros equipos. Sólo los equipos que sean miembros de la red gestionada (con acceso completo o de administrador) pueden compartir archivos o acceder a archivos compartidos por otros equipos miembros.

Nota: si está compartiendo un número de archivos elevado, los recursos de su equipo pueden verse afectados.

En este capítulo

Cómo compartir archivos

Sólo los equipos que sean miembros de la red gestionada (con acceso completo o de administrador) pueden compartir archivos o acceder a archivos compartidos por otros equipos miembros. Si comparte una carpeta, se comparten todos los archivos incluidos en esa carpeta y sus subcarpetas; sin embargo, los archivos que se agreguen posteriormente a la carpeta no se compartirán automáticamente. Si se elimina un archivo o carpeta, se elimina de la ventana Archivos compartidos. Puede dejar de compartir un archivo en cualquier momento.

Para acceder a un archivo compartido, ábralo directamente desde EasyNetwork o cópielo en su equipo para abrirlo desde ahí. Si la lista de archivos compartidos es demasiado larga para ver dónde está el archivo, puede buscarlo.

Nota: no se puede acceder a los archivos compartidos con EasyNetwork desde otros equipos con el Explorador de Windows porque los archivos EasyNetwork deben compartirse a través de conexiones seguras.

Compartir un archivo

Cuando se comparte un archivo, todos los miembros pueden acceder a él con acceso completo o derechos de administrador a la red gestionada.

1. En el Explorador de Windows, localice el archivo que desea compartir.
2. Arrastre el archivo desde su ubicación en el Explorador de Windows hasta la ventana Archivos compartidos de EasyNetwork.

Sugerencia: también puede compartir un archivo haciendo clic en **Compartir archivos** del menú **Herramientas** . En el cuadro de diálogo Compartir, acceda a la carpeta donde esté almacenado el archivo que desee compartir, seleccione el archivo y, a continuación, haga clic en **Compartir**.

Detener el uso compartido de un archivo

Si comparte un archivo en la red gestionada, puede detener el uso compartido en cualquier momento. Cuando deja de compartir un archivo, otros miembros de la red gestionada ya no pueden acceder a él.

1. En el menú **Herramientas**, haga clic en **Detener el uso compartido de archivos**.
2. En el cuadro de diálogo Detener el uso compartido de archivos, seleccione el archivo que ya no desea compartir.
3. Haga clic en **Aceptar**.

Copiar un archivo compartido

Copie un archivo compartido si desea tenerlo después de que deje de compartirse. Puede copiar un archivo compartido desde cualquier equipo de la red gestionada.

- Arrastre un archivo desde la ventana Archivos compartidos en EasyNetwork hasta una ubicación del Explorador de Windows o al escritorio de Windows.

Sugerencia: también puede copiar un archivo compartido seleccionando el archivo en EasyNetwork y haciendo clic en **Copiar a** del menú **Herramientas**. En el cuadro de diálogo Copiar a carpeta, acceda a la carpeta en la que quiera copiar el archivo, selecciónela y haga clic en **Guardar**.

Buscar un archivo compartido

Puede buscar un archivo que no lo haya compartido usted ni ningún otro miembro de la red. Mientras escribe sus criterios de búsqueda, EasyNetwork muestra los resultados correspondientes en la ventana Archivos compartidos.

1. En la ventana Archivos compartidos, haga clic en **Buscar**.
2. Haga clic en la opción adecuada (página 253) de la lista **Contiene**.
3. Escriba parte o todo el nombre del archivo en la lista **Nombre de archivo o ruta**.
4. Haga clic en el tipo de archivo (página 253) adecuado de la lista **Tipo**.
5. En las listas **De** y **A**, haga clic en las fechas que representan el intervalo de fechas en las que se haya creado el archivo.

Criterios de búsqueda

Las siguientes tablas describen los criterios de búsqueda que puede especificar al buscar archivos compartidos.

Nombre del archivo o ruta

Contiene	Descripción
Contiene todas las palabras	Busca un nombre de archivo o una ruta que contenga todas las palabras que especifique en la lista **Nombre de archivo o ruta**, en cualquier orden.
Contiene alguna de las palabras	Busca un nombre de archivo o una ruta que contenga alguna de las palabras que especifique en la lista **Nombre de archivo o ruta**.

Contiene	Descripción
Contiene la cadena de texto exacta	Busca un nombre de archivo o una ruta que contenga la frase exacta que especifique en la lista **Nombre de archivo o ruta**.

Tipo de archivo

Tipo	Descripción
Cualquiera	Busca todos los tipos de archivos compartidos.
Documento	Busca todos los archivos compartidos.
Imagen	Busca todos los archivos de imagen compartidos.
Vídeo	Busca todos los archivos de vídeo compartidos.
Audio	Busca todos los archivos de audio compartidos.
Comprimido	Busca todos los archivos comprimidos (por ejemplo, archivos .zip).

Envío de archivos a otros equipos

Puede enviar archivos a otros equipos que sean miembros de la red gestionada. Antes de enviar un archivo, EasyNetwork comprueba que el equipo que recibe el archivo tiene suficiente espacio disponible en el disco.

Cuando reciba un archivo, aparecerá en su buzón de entrada de EasyNetwork. El buzón de entrada es una ubicación de almacenamiento temporal para todos aquellos archivos que le envíen otros equipos de la red. Si tiene abierto EasyNetwork al recibir un archivo, este archivo aparece al instante en su buzón de entrada; de lo contrario, aparece un mensaje en el área de notificación, situada en el extremo derecho de la barra de herramientas de Windows. Si no quiere recibir mensajes de notificación (por ejemplo, porque interrumpen las tareas que está realizando), puede desactivar esta opción. Si ya existe un archivo con el mismo nombre en el buzón de entrada, el nuevo archivo cambia de nombre por un sufijo numérico. Los archivos se mantienen en el buzón de entrada hasta que los acepte (deberá copiarlos en su equipo).

Enviar un archivo a otro equipo

Puede enviar un archivo a otro equipo de la red gestionada sin compartirlo. Antes de que el usuario del equipo receptor pueda ver el archivo, deberá guardarlo en una ubicación local. Para obtener más información, consulte Aceptar un archivo de otro equipo (página 256).

1. En el Explorador de Windows, localice el archivo que desea enviar.
2. Arrastre el archivo desde su ubicación en el Explorador de Windows hasta el icono de un equipo activo de EasyNetwork.

Sugerencia: para enviar múltiples archivos a un equipo presione CTRL al seleccionar los archivos. También puede enviar archivos haciendo clic en **Enviar** del menú **Herramientas**, seleccionando los archivos y después haciendo clic en **Enviar**.

Aceptar un archivo de otro equipo

Si otro equipo de la red gestionada le envía un archivo, deberá aceptarlo guardándolo en su equipo. Si EasyNetwork no se está ejecutando cuando se envía un archivo a su equipo, recibirá un mensaje de notificación en el área de notificación, situada en el extremo derecho de la barra de tareas. Haga clic en el mensaje de notificación para abrir EasyNetwork y acceder al archivo.

- Haga clic en **Recibido** y arrastre el archivo desde el buzón de entrada de EasyNetwork a una carpeta del Explorador de Windows.

Sugerencia: también puede recibir un archivo desde otro equipo seleccionando el archivo en su buzón de entrada de EasyNetwork y, a continuación, haciendo clic en **Aceptar** del menú **Herramientas** . En el cuadro de diálogo Aceptar en la carpeta, acceda a la carpeta en la que quiera guardar los archivos que esté recibiendo, selecciónela y, a continuación, haga clic en **Guardar**.

Recibir una notificación cuando se envíe el archivo

Puede recibir un mensaje de notificación cuando otro equipo de la red gestionada le envíe un archivo. Si EasyNetwork no se está ejecutando, el mensaje de notificación aparece en el área de notificación, situada en el extremo derecho de la barra de herramientas.

1. En el menú **Opciones** , haga clic en **Configurar**.
2. En el cuadro de diálogo Configurar, marque la casilla de verificación **Notificarme cuando otro equipo me envíe archivos**.
3. Haga clic en **Aceptar**.

CAPÍTULO 45

Compartir impresoras

Después de conectarse a una red gestionada, EasyNetwork comparte las impresoras locales que estén conectadas con su equipo y utiliza el nombre de la impresora como nombre de impresora compartida. EasyNetwork también detecta impresoras compartidas por otros equipos de la red y le permite configurarlas y utilizarlas.

Si ha configurado un controlador de impresora para imprimir a través de un servidor de impresión en red (por ejemplo, un servidor de impresión USB inalámbrico), EasyNetwork considera que la impresora es una impresora local y la comparte en la red. También puede dejar de compartir una impresora en cualquier momento.

En este capítulo

Trabajar con impresoras compartidas

EasyNetwork detecta las impresoras compartidas por los equipos de la red. Si EasyNetwork detecta una impresora remota que no esté conectada a su equipo, el vínculo **Impresoras de red disponibles** de la ventana Archivos compartidos aparece al abrir EasyNetwork por primera vez. Entonces puede instalar impresoras disponibles o desinstalar impresoras que ya estén conectadas a su equipo. Asimismo, puede actualizar la lista de impresoras para asegurarse de estar visualizando la información actualizada.

Si aún no se ha incorporado a una red gestionada pero está conectada a ella, puede acceder a las impresoras compartidas desde el panel de control de impresoras de Windows.

Detener el uso compartido de una impresora

Cuando deja de compartir una impresora, los miembros ya no pueden usarla.

1. En el menú **Herramientas**, haga clic en **Impresoras**.
2. En el cuadro de diálogo Gestionar impresoras de red, haga clic en el nombre de la impresora que ya no desea compartir.
3. Haga clic en **No compartir**.

Instalar una impresora de red disponible

Si es miembro de una red gestionada, puede acceder a las impresoras que estén compartidas; sin embargo, debe instalar el controlador de la impresora utilizado por dicha impresora. Si el propietario de la impresora deja de compartirla, no podrá utilizarla.

1. En el menú **Herramientas**, haga clic en **Impresoras**.
2. En el cuadro de diálogo Impresoras de red disponibles, haga clic en un nombre de impresora.
3. Haga clic en **Instalar**.

Referencia

El glosario de términos lista y define la terminología de seguridad más comúnmente utilizada en los productos de McAfee.

Glosario

8

802.11

Conjunto de estándares IEEE para transmitir datos a travçes de una red inalámbrica. 802.11 se conoce comúnmente como Wi-Fi.

802.11a

Extensión de 802.11 que transmite datos a una velocidad de hasta 54 Mbps en la banda de 5 GHz. Aunque la velocidad de transmisión es mayor que en el caso de 802.11b, la distancia de cobertura es mucho menor.

802.11b

Extensión de 802.11 que transmite datos a una velocidad de hasta 11 Mbps en la banda de 2.4 GHz. Aunque la velocidad de transmisión es menor que en el caso de 802.11a, la distancia de cobertura es mucho mayor.

802.1x

Estándar IEEE para la autenticación de redes con cable e inalámbricas. 802.1x se utiliza normalmente con redes inalámbricas 802.11.

A

acceso directo

Archivo que contiene únicamente la ubicación de otro archivo en el equipo.

adaptador inalámbrico

Dispositivo que agrega la capacidad inalámbrica a un equipo o PDA. Se conecta mediante un puerto USB, una ranura de PC Card (CardBus), una ranura de tarjeta de memoria o internamente en el bus PCI.

Análisis bajo demanda

Análisis que se inicia bajo demanda (es decir, cuando ejecuta la operación). A diferencia del análisis en tiempo real, los análisis bajo demanda no se inician automáticamente.

Análisis en tiempo real

Analizar archivos y carpetas en busca de virus y otra actividad cuando usted o el equipo acceden a ellos.

ancho de banda

Cantidad de datos que pueden transmitirse en un período de tiempo fijo.

archivado completo

Archivado de un conjunto de datos completo basado en los tipos y ubicaciones de los archivos observados que haya configurado. Véase también archivado rápido.

archivado rápido

Sirve para archivar únicamente aquellos archivos que se han modificado desde la última operación de archivado rápido o completo. Véase también archivado completo.

archivar

Crear una copia de archivos importantes en un CD, un DVD, una unidad USB, un disco duro externo o una unidad de red.

archivo temporal

Un archivo, creado en la memoria o en un disco mediante el sistema operativo o algún otro programa, que se utiliza durante una sesión para desecharlo posteriormente.

ataque de diccionario

Tipo de ataque de fuerza bruta que utiliza palabras habituales para intentar descubrir una contraseña.

ataque de fuerza bruta

Método de descodificación de datos cifrados como, por ejemplo, contraseñas, que se lleva a cabo mediante un esfuerzo exhaustivo (fuerza bruta), en vez de a estrategia intelectual. Se considera que la fuerza bruta es un método de ataque infalible, aunque lleva mucho tiempo. Los ataques de fuerza bruta también se denominan de descifrado de fuerza bruta.

ataque de intermediario

Método para interceptar y, posiblemente, modificar mensajes entre dos partes sin que ninguna de ellas sepa que su vínculo de comunicación ha sido interceptado.

autenticación

Proceso de identificación de un individuo, que habitualmente consiste en un único nombre de usuario y una contraseña.

B

biblioteca

Área de almacenamiento en línea para archivos cuya copia de seguridad ha efectuado y que ha publicado. La biblioteca Data Backup es un sitio Web de Internet al que puede acceder cualquier persona con acceso a Internet.

browser

Programa utilizado para ver páginas Web en Internet. Entre los navegadores Web más habituales figuran Microsoft Internet Explorer y Mozilla Firefox.

C

caché

Área de almacenamiento temporal del equipo. Por ejemplo, para aumentar la eficacia y velocidad de navegación de páginas Web, su explorador puede recuperar una página Web desde la caché la siguiente vez que desee verla, en lugar de tener que hacerlo desde un servidor remoto.

Caja fuerte de contraseñas

Área de almacenamiento segura de las contraseñas personales. Le permite almacenar sus contraseñas con la seguridad de que ningún otro usuario (incluso un administrador) pueda acceder a ellas.

cifrado

Proceso mediante el que los datos se transforman de texto en código, de forma que la información queda oculta y resulta ilegible para aquellas personas que no saben cómo descifrarla. Los datos cifrados también se denominan texto cifrado.

clave

Serie de letras y números utilizados por dos dispositivos con objeto de autenticar sus comunicaciones. Ambos dispositivos deben disponer de la clave. Véase también WEP, WPA, WPA2, WPA-PSK y WPA2- PSK.

cliente

Aplicación que se ejecuta en un equipo personal o estación de trabajo y que depende de un servidor para realizar algunas operaciones. Por ejemplo, un cliente de correo electrónico es una aplicación que permite enviar y recibir mensajes de correo electrónico.

cliente de correo electrónico

Programa que se ejecuta en el equipo para enviar y recibir correo electrónico (por ejemplo, Microsoft Outlook).

código de autenticación de mensajes (MAC)

Código de seguridad utilizado para cifrar mensajes que se transmiten entre equipos. El mensaje se acepta si el equipo reconoce el código descifrado como válido.

compartir

Permitir a los destinatarios de mensajes de correo electrónico acceder a los archivos copiados seleccionados durante un período de tiempo limitado. Cuando se comparte un archivo, el usuario manda una copia del archivo a los destinatarios de correo electrónico especificados. Los destinatarios reciben un mensaje de correo electrónico procedente de Data Backup en el que se indica que se han compartido archivos con ellos. Este mensaje contiene también un vínculo a los archivos compartidos.

complemento

Un pequeño programa de software que trabaja con un programa más grande para proporcionar una funcionalidad añadida. Por ejemplo, los complementos permiten que un navegador Web acceda a archivos que están incorporados en documentos HTML y que tienen formatos que normalmente no podría reconocer (por ejemplo, archivos de animación, vídeo y audio) y le permite ejecutarlos.

compresión

Proceso mediante el cual los archivos se comprimen en un formato que minimiza el espacio necesario para su almacenamiento y transmisión.

contraseña

Código (por lo general formado por letras y números) utilizado para acceder al equipo, a un programa o a un sitio Web.

Control ActiveX

Componente de software que utilizan los programas o páginas web para añadir funciones que aparecen como parte normal de esos programas o páginas Web. La mayor parte de los controles ActiveX son inofensivos; sin embargo, algunos pueden capturar información de su equipo.

Control parental

Configuración que ayuda a regular qué ven y qué hacen los niños mientras navegan por Internet. Para configurar Control parental, puede activar o desactivar el filtrado de imágenes, elegir un grupo de clasificación de contenido y establecer un límites temporal de navegación por Internet.

cookie

Pequeño archivo que contiene información y que, por lo general, incluye un nombre de usuario y la fecha y hora actual, que se almacena en el equipo de una persona que navega por Internet. Las cookies son utilizadas principalmente por los sitios Web para identificar a los usuarios que se han registrado previamente o que han visitado el sitio; sin embargo, también pueden ser una fuente de información para los piratas informáticos.

correo electrónico

(correo electrónico) Mensajes enviados y recibidos electrónicamente, en una red informática. Véase también Webmail.

cortafuegos

Sistema (hardware, software o ambos) diseñado para impedir el acceso no autorizado de entrada o salida de una red privada. Se utilizan con frecuencia para impedir que usuarios de Internet no autorizados accedan a redes privadas conectadas a Internet y, en particular, a una intranet. Todos los mensajes que entran o salen de la intranet pasan por el cortafuegos, que examina cada uno de ellos y bloquea aquellos que no cumplen los criterios de seguridad especificados.

crear copia de seguridad

Crear una copia de los archivos importantes en un servidor en línea seguro.

cuarentena

Para aislar. Por ejemplo, en VirusScan, se detectan y poner en cuarentena los archivos sospechosos, a fin de que no produzcan daños ni en el equipo, ni en los archivos.

cuenta de correo electrónico estándar

Véase POP3.

D

DAT

(Archivos de firma de datos) Archivos que contienen las definiciones utilizadas al detectar virus, troyanos, software espía, software publicitario y otros programas potencialmente no deseados en el equipo o la unidad USB.

denegación de servicio

Tipo de ataque que ralentiza o detiene el tráfico de una red. Un ataque de denegación de servicio (ataque DoS) se produce cuando se desborda una red con tantas solicitudes adicionales que el tráfico habitual se ralentiza o se detiene por completo. Por lo general, no se produce robo de información ni otras vulnerabilidades de seguridad.

desbordamiento del búfer

Condición que se produce cuando procesos o programas sospechosos intentan almacenar en un búfer (área de almacenamiento temporal) del equipo más datos de los que realmente puede contener. Los desbordamientos de búfer dañan o sobrescriben los datos de los búferes adyacentes.

Dirección IP

Identificador de un equipo o dispositivo de una red TCP/IP. Las redes que utilizan el protocolo TCP/IP dirigen los mensajes en función de la dirección IP del destino. El formato de una dirección IP es una dirección numérica de 32 bits escrita como cuatro números separados por puntos. Cada número puede estar comprendido entre 0 y 255 (por ejemplo, 192.168.1.100).

Dirección MAC

(Media Access Control address) Número de serie único asignado a un dispositivo físico que accede a la red.

disco duro externo

Disco duro que se encuentra fuera del equipo.

DNS

(Sistema de nombres de dominio) Un sistema que convierte los nombres de servidor o nombres de dominio en direcciones IP. En la Web, se utiliza DNS para convertir las direcciones Web fácilmente legibles (por ejemplo, www.myhostname.com) en direcciones IP (por ejemplo, 111.2.3.44) de modo que se pueda recuperar el sitio Web. Sin DNS, el usuario tendría que escribir él mismo la dirección IP en el navegador Web.

dominio

Subred local o descriptor de sitios de Internet.

En una red de área local (LAN), un dominio es una subred formada por equipos servidor y cliente controlados mediante una base de datos de seguridad. Dentro de este contexto, los dominios pueden mejorar el rendimiento. En Internet, un dominio es una parte de todas las direcciones Web (por ejemplo, en www.abc.com, abc es el dominio).

E

enrutador o router

Dispositivo de red que reenvía paquetes de datos de una red a otra. Los enrutadores están basados en las tablas de enrutamiento internas, leen todos los paquetes entrantes y deciden cómo reenviarlos basándose en cualquier combinación de la dirección de origen y destino, así como en las condiciones de tráfico actuales (como la carga, los costes de línea y las líneas defectuosas). En ocasiones, se denomina a los enrutadores Puntos de acceso (AP).

ESS

(Extended Service Set) Conjunto de dos o más redes que forman una única subred.

evento

Acción iniciada por el usuario, un dispositivo o el mismo equipo y que inicia una respuesta. McAfee registra los eventos en su registro de eventos.

F

falsificación de IP

Como su propio nombre indica, se trata de la falsificación de la dirección IP de un paquete IP. Se utiliza en muchos tipos de ataques, incluidos los secuestros de sesiones. También se utiliza con frecuencia en la falsificación de encabezados de mensajes SPAM, para complicar su seguimiento.

filtrado de imágenes

Opción de Control parental que evita, bloqueándolas, que aparezcan imágenes Web potencialmente inapropiadas.

fragmentos de archivos

Restos de un archivo dispersos por un disco. La fragmentación de archivos se produce a medida que se agregan o eliminan archivos y puede ralentizar el rendimiento del equipo.

G

grupo de clasificación de contenido

En Control parental, grupo de edad al que pertenece el usuario. El contenido se bloquea o bien está disponible según el grupo de clasificación de contenido al que pertenezca el usuario. Los grupos de clasificación de contenido incluyen: Niños de corta edad, niños, adolescentes, jóvenes y adultos.

guardián del sistema

Alertas de McAfee que detectan cambios no autorizados en el equipo y lo notifican al usuario cuando esto ocurre.

gusano

Un virus capaz de replicarse que reside en la memoria activa y puede enviar copias de sí mismo a través de correo electrónico. Los gusanos replican y consumen los recursos del sistema, reducen su rendimiento o interrumpen tareas.

H

hotspot o zona de cobertura inalámbrica

Zona geográfica cubierta por un punto de acceso (AP) Wi-Fi (802.11). Los usuarios que entran en un hotspot con un portátil inalámbrico se pueden conectar a Internet, siempre y cuando el hotspot emita señales (es decir, que anuncie su presencia) y no sea preciso efectuar una autenticación. A menudo, los hotspots se encuentran con frecuencia en zonas con gran afluencia de público como aeropuertos.

I

Internet

Internet se compone de un número ingente de redes interconectadas que utilizan los protocolos TCP/IP para localizar y transferir datos. Internet evolucionó a partir de un proyecto de conexión de equipos de universidades y facultades (a finales de los años 60 y principios de los 70) financiado por el Departamento de Defensa de EE.UU., que se denominó ARPANET. Hoy en día Internet es una red mundial integrada por unas 100.000 redes independientes.

intranet

Red informática privada, a menudo en el interior de una organización, a la que sólo pueden acceder los usuarios autorizados.

itinerancia

Capacidad para moverse de una zona de cobertura de un punto de acceso (AP) a otra sin que se produzca una interrupción del servicio ni una pérdida de conectividad.

K

kit de raíz

Recopilación de herramientas (programa) que garantizan a un usuario, acceso de nivel de administrador a un equipo o una red de equipos. Los kits de raíz pueden estar formados por software espía y otros programas potencialmente no deseados que pueden poner en riesgo la seguridad o la privacidad de los datos de su equipo o de su información personal.

L

LAN

(Red de área local) Red de equipos que se distribuye por una zona relativamente pequeña (por ejemplo, un único edificio). Los equipos de una LAN pueden comunicarse entre si y compartir recursos como impresoras y archivos.

Launchpad

Componente de interfaz U3 que actúa como punto de inicio para abrir y gestionar programas USB U3.

lista blanca

Lista de sitios Web a los que se permite el acceso a los usuarios, dado que dichos sitios no se consideran fraudulentos.

lista de confianza

Contiene elementos en los que tiene confianza y que no se detectan. Si por error indica que tiene confianza en un elemento (como un programa potencialmente no deseado o un cambio del registro) o bien desea que se vuelva a detectar el elemento, deberá suprimirlo de la lista.

lista negra

En antiphishing, una lista de sitios Web considerados fraudulentos.

M

mapa de la red

Representación gráfica de los equipos y componentes que forman una red doméstica.

MAPI

(Interfaz de programación de aplicaciones de mensajería) Especificación de interfaz de Microsoft que permite que diferentes aplicaciones de mensajería y grupos de trabajo (incluido el correo electrónico, el correo de voz y el fax) funcionen a través de un único cliente, como el cliente de Exchange.

marcador

Software que ayuda a establecer una conexión de Internet. Cuando se utilizan con fines malintencionados, los marcadores pueden redirigir las conexiones de Internet a un Proveedor de servicios de Internet (ISP) que no sea el proveedor predeterminado, todo ello sin informar al usuario de los costes adicionales.

MSN

(Microsoft Network) Grupo de servicios basados en la Web ofrecidos por Microsoft Corporation, formados por un motor de búsqueda, correo electrónico, mensajería instantánea y un portal.

N

NIC

(Tarjeta de interfaz de red) Tarjeta que se inserta en un portátil u otro dispositivo y que conecta el dispositivo a la red LAN.

nodo

Un solo equipo conectado a una red.

P

palabra clave

Palabra que se puede asignar a un archivo de copia de seguridad para establecer una relación o conexión entre este archivo y otros archivos que tengan las misma palabra clave asignada. Al asignar palabras clave, resulta más fácil buscar los archivos que están publicados en Internet.

Papelera de reciclaje

Papelera simulada para almacenar los archivos y carpetas eliminados en Windows.

phishing

Estafa por Internet diseñada para obtener información valiosa (como números de tarjeta de crédito y de la seguridad social, ID de usuario y contraseñas) de personas no conscientes de ellos, con el fin de utilizarla con fines fraudulentos.

POP3

(Post Office Protocol 3 - Protocolo de oficina postal 3) Interfaz entre un programa cliente de correo electrónico y el servidor de correo electrónico. La mayoría de los usuarios domésticos tienen una cuenta de correo electrónico POP3, también conocida como cuenta de correo electrónico estándar.

PPPoE

(Protocolo punto a punto en Ethernet) Método para utilizar el protocolo de acceso telefónico PPP (protocolo punto a punto) con Ethernet como transporte.

Programa potencialmente no deseado (PUP)

Programa que recopila y transmite información personal sin su permiso (por ejemplo, software espía y software publicitario).

protocolo

Formato (hardware o software) para transmitir datos entre dos dispositivos. El equipo o dispositivo debe ser compatible con el protocolo correcto si se desea comunicarse con otros equipos.

proxy

Un equipo (o el software que lo ejecuta) que actúa como barrera entre una red e Internet presentando únicamente una sola dirección de red a los sitios externos. Al representar a todos los equipos internos, el proxy protege las identidades de la red y, al mismo tiempo, proporciona acceso a Internet. Véase también servidor proxy.

publicar

Hacer pública la copia de seguridad de un archivo en Internet. Se puede acceder a los archivos publicados buscando en la biblioteca de Data Backup.

puerta de enlace integrada

Dispositivo que combina las funciones de un punto de acceso, un enrutador y un cortafuegos. Algunos dispositivos también pueden incluir funciones de mejora de la seguridad y enlace inalámbrico.

puerto

Lugar por donde la información entra en el equipo o sale de éste. Por ejemplo, un módem analógico convencional se conecta a un puerto serie.

Punto de acceso

Un dispositivo de red (conocido comúnmente como enrutador inalámbrico) que se conecta a un hub Ethernet o conmutador para ampliar el rango físico del servicio para un usuario inalámbrico. Cuando los usuarios inalámbricos se encuentran en itinerancia con sus dispositivos móviles, la transmisión pasa de un Punto de acceso (AP) al otro para mantener la conectividad.

punto de acceso no autorizado

Tal como su nombre indica, se trata de un punto de acceso no autorizado. Los puntos de acceso no autorizados se instalan en una red de empresa fiable, a fin de garantizar acceso a la red a partes no autorizadas. También se pueden crear para que un atacante pueda llevar a cabo un ataque de intermediario.

punto de restauración del sistema

Una instantánea (imagen) del contenido de la memoria del equipo o de una base de datos. Windows crea periódicamente puntos de restauración y en el momento de eventos significativos del sistema (como cuando se instala un programa o un controlador). También se puede crear y nombrar puntos de restauración propios en cualquier momento.

R

RADIUS

(Remote Access Dial-In User Service) Protocolo que proporciona autenticación de usuarios; por lo general en el contexto del acceso remoto. Originalmente definido para el uso con servidores de acceso telefónico remoto, este protocolo RADIUS se utiliza en la actualidad en varios entornos de autenticación, entre ellos, en la autenticación 802.1x de un secreto compartido de usuario WLAN.

red

Conjunto de puntos de acceso y sus usuarios asociados, equivalente a un ESS.

red doméstica

Dos o varios equipos que están conectados en un hogar de modo que puedan compartir archivos y acceder a Internet. Véase también LAN.

red gestionada

Una red doméstica con dos tipos de miembros: miembros gestionados y miembros no gestionados. Los miembros gestionados permiten que otros equipos de la red supervisen su estado de protección; los miembros no gestionados no lo permiten.

registro

Base de datos en la que Windows almacena su información de configuración. El registro contiene perfiles para cada usuario del equipo e información acerca del hardware, los programas instalados y los ajustes de propiedades del sistema. Windows consulta continuamente esta información durante su funcionamiento.

repositorio de la copia de seguridad en línea

Ubicación del servidor en línea en la que se almacenan archivos observados después de hacer la copia de seguridad.

restaurar

Recuperar una copia de un fichero desde un repositorio de copias de seguridad en línea o un archivo.

S

secreto compartido

Cadena o clave (por lo general una contraseña) que se ha compartido entre las dos partes de la comunicación antes de iniciar ésta. Un secreto compartido se utiliza para proteger las partes importantes de los mensajes RADIUS.

secuencia de comandos

Lista de comandos que se pueden ejecutar automáticamente (es decir, sin interacción con el usuario). A diferencia de los programas, las secuencias de comandos se almacenan normalmente en forma de texto normal y se compilan cada vez que se ejecutan. Las macros y los archivos por lotes también se denominan secuencias de comandos o scripts.

servidor

Equipo o programa que acepta conexiones de otros equipos o programas y devuelve las respuestas apropiadas. Por ejemplo, el programa de correo electrónico se conecta a un servidor de correo electrónico cada vez que se envían o reciben mensajes.

servidor DNS

(Servidor del sistema de nombres de dominio) Equipo que muestra la dirección IP asociada a un nombre de servidor o dominio. Véase también DNS.

servidor proxy

Un cortafuegos que gestiona el tráfico de Internet desde y hacia una red de área local (LAN). Un servidor proxy puede mejorar el rendimiento suministrando datos que se solicitan con frecuencia, como una página Web muy visitada, y puede filtrar y desechar solicitudes que el titular no considere convenientes, como el acceso no autorizado a archivos de propiedad.

sincronizar

Resolver inconsistencias entre los archivos copiados y los archivos almacenados en el equipo local. Los archivos se sincronizan cuando la versión del archivo que se encuentra en el repositorio de la copia de seguridad en línea es más reciente que la versión de otros equipos.

SMTP

(Protocolo simple de transferencia de correo.) Protocolo TCP/IP para el envío de mensajes de un equipo a otro en una red. Este protocolo se utiliza en Internet para enrutar los correos electrónicos.

SSID

(Service Set Identifier) Un token (clave secreta) que identifica a una red Wi-Fi (802.11). El administrador de red configura el SSID que los usuarios que desean unirse a la red deben suministrar.

SSL

(Secure Sockets Layer) Protocolo desarrollado por Netscape para transmitir documentos privados a través de Internet. SSL utiliza una clave pública para cifrar datos que se transfieren a través de la conexión SSL. Las direcciones URL que requieren una conexión SSL empiezan por https: en lugar de por http.

T

tarjeta adaptadora inalámbrica PCI

(Interconexión de componentes periféricos) Tarjeta adaptadora inalámbrica que se conecta a una ranura de expansión PCI dentro del equipo.

tarjeta adaptadora inalámbrica USB

Tarjeta adaptadora inalámbrica que se conecta en una ranura USB del equipo.

texto cifrado

Texto codificado. El texto cifrado es ilegible hasta que se convierte en texto normal (es decir, se descifra).

texto normal

Texto sin cifrar. Véase también cifrado.

tipos de archivos observados

Tipos de archivos (por ejemplo, .doc, .xls, etc.) que Data Backup copia o archiva en las ubicaciones de observación.

TKIP

(Temporal Key Integrity Protocol) Protocolo que se ocupa de los puntos débiles de la seguridad WEP, en concreto de la reutilización de las claves de cifrado. TKIP cambia las claves temporales cada 10.000 paquetes, proporcionando un método de distribución dinámico que mejora de manera significativa la seguridad en la red. El proceso de seguridad TKIP comienza con una clave temporal de 128 bits compartida entre clientes y puntos de acceso. TKIP combina la clave temporal con la dirección MAC del cliente y agrega entonces un vector de inicialización de 16 octetos relativamente grande para generar la clave que cifra los datos. Este procedimiento garantiza que cada estación utilice secuencias de claves distintas para cifrar los datos. TKIP utiliza RC4 para realizar el cifrado.

Troyano

Programa que aparece como legítimo pero que puede dañar archivos importantes, alterar el rendimiento y permitir accesos no autorizados al equipo.

U

U3

(Usuario: simplificado, más inteligente, móvil) Plataforma para ejecutar programas de Windows 2000 o XP directamente desde una unidad USB. La iniciativa U3 fue fundada en 2004 por M-Systems y SanDisk y permite a los usuarios ejecutar programas U3 en un equipo Windows sin instalar ni almacenar datos u opciones en el equipo.

ubicación de observación en profundidad

Carpeta del equipo en la que se supervisan los cambios que se realizan mediante Data Backup. Si se establece una ubicación de observación en profundidad, Data Backup crea una copia de los tipos de archivo observados en dicha carpeta y sus subcarpetas.

ubicaciones de observación

Carpetas del equipo supervisadas por Data Backup.

ubicaciones de observación superficial

Carpeta del equipo en la que se supervisan los cambios que se realizan mediante Data Backup. Si establece una ubicación de observación superficial, Data Backup hace una copia de los tipos de archivos observados en dicha carpeta, pero no incluye sus subcarpetas.

unidad de red

Disco o unidad magnética que se conecta a un servidor de una red que comparten varios usuarios. Las unidades de red se denominan a veces unidades remotas.

Unidad inteligente

Consulte unidad USB.

Unidad USB

Pequeña unidad de memoria que se conecta al puerto USB del equipo. Una unidad USB actúa como un pequeño disco duro que facilita la transferencia de archivos de un equipo a otro.

URL

(Localizador de recursos universales) El formato estándar de las direcciones de Internet.

USB

(Universal Serial Bus) Interfaz informática serie estandarizada que le permite conectar dispositivos periféricos como teclados, joysticks e impresoras al equipo.

V

ventanas emergentes

Pequeñas ventanas que aparecen en la parte superior de otras ventanas en la pantalla del equipo. Las ventanas emergentes se utilizan con frecuencia en los navegadores Web para mostrar anuncios.

Virus

Programas que se reproducen automáticamente para alterar otros archivos o datos. A menudo parecen proceder de un remitente de confianza, o parecen ser de contenido inofensivo.

VPN

(Red privada virtual) Red privada configurada en una red pública a fin de aprovechar los recursos de gestión de la red pública. Las empresas utilizan las VPN para crear redes de área ancha (WAN) que se extienden por grandes zonas geográficas y poder proporcionar conexiones de sitio a sitio con sucursales o permitir a los usuarios móviles marcar a las LAN de su empresa.

W

wardriver

Persona que buscar redes Wi-Fi (802.11) conduciendo por las ciudades con un equipo Wi-Fi y algún hardware o software especial.

Web bugs

Pequeños archivos de gráficos que pueden incorporarse a las páginas HTML y permitir que un origen no autorizado introduzca cookies en el equipo. Estos cookies pueden transmitir información a la fuente no autorizada. Los Web bugs también se denominan microespías, señales o balizas Web, pixel tags o GIF invisibles.

Webmail

Mensajes que se envían y reciben electrónicamente por Internet. Véase también correo electrónico.

WEP

(Wired Equivalent Privacy) Protocolo de cifrado y autenticación definido como parte del estándar Wi-Fi (802.11). Las versiones iniciales se basan en algoritmos de cifrado RC4 y presentan fallos importantes. WEP tiene como objetivo proporcionar seguridad mediante el cifrado de los datos a través de ondas de radio para protegerlos cuando se transmiten de un punto a otro. Sin embargo, se ha demostrado que el protocolo WEP no es tan seguro como se pensaba al principio.

Wi-Fi

(Wireless Fidelity) Término utilizado por la Wi-Fi Alliance al referirse a cualquier tipo de red 802.11.

Wi-Fi Alliance

Organización formada por los principales proveedores de hardware y software inalámbrico. Wi-Fi Alliance lucha para que todos los productos basados en 802.11 puedan certificarse como interoperables y para promocionar el uso del término Wi-Fi como nombre de marca global en todos los mercados de las LAN inalámbricas basadas en 802.11. La organización actúa como consorcio, laboratorio de pruebas y centro de intercambio de información para proveedores que deseen promocionar el crecimiento de la industria.

Wi-Fi Certified

Probado y aprobado por la Wi-Fi Alliance. Se considera que los productos Wi-Fi Certified son interoperables aunque puedan provenir de diferentes fabricantes. Un usuario que disponga de un producto Wi-Fi Certified puede utilizar cualquier marca de punto de acceso con otra marca de hardware cliente que también esté certificada.

WLAN

(Red de área local inalámbrica) Red de área local (LAN) que utiliza una conexión inalámbrica. Una WLAN utiliza ondas de radio de alta frecuencia en vez de cables para permitir a los equipos comunicarse entre si.

WPA

(Wi-Fi Protected Access) Especificación estándar que aumenta de manera significativa el nivel de protección de los datos y el control de acceso de los sistemas LAN inalámbricos actuales y futuros. Diseñada para ejecutarse en hardware existente como ampliación de software, WPA procede del estándar IEEE 802.11i y es compatible con él. Cuando se instala adecuadamente, ofrece a los usuarios de una LAN inalámbrica amplias garantías de que sus datos permanecen protegidos y de que sólo los usuarios autorizados pueden acceder a la red.

WPA-PSK

Modo WPA especial para usuarios domésticos que no necesitan seguridad de tipo empresarial y que no tienen acceso a servidores de autenticación. En este modo, el usuario introduce la contraseña inicial para activar el modo Wi-Fi Protected Access con clave precompartida y debe cambiar regularmente la contraseña larga en cada equipo inalámbrico y punto de acceso. Véase también WPA2-PSK y TKIP.

WPA2

Actualización del estándar de seguridad WPA en el estándar IEEE 802.11i.

WPA2-PSK

Modo WPA especial similar a WPA-PSK basado en el estándar WPA2. Una característica común de WPA2-PSK es que los dispositivos normalmente admiten varios modos de cifrado (p. ej. AES, TKIP) simultáneamente, mientras que otros dispositivos sólo admiten por lo general un único modo de cifrado a la vez (es decir, todos los clientes tendrían que utilizar el mismo modo de cifrado).

Acerca de McAfee

McAfee, Inc., con sede central en Santa Clara, California, y líder mundial en prevención de intrusiones y gestión de riesgos de seguridad, proporciona servicios y soluciones proactivas y probadas que protegen sistemas y redes en todo el mundo. Su experiencia y su compromiso inigualable con la innovación permiten a McAfee dotar a usuarios particulares, empresas, sector público y proveedores de servicios de la capacidad de bloquear ataques, evitar problemas y controlar y mejorar de manera continua su seguridad.

Copyright

Licencia

AVISO A TODOS LOS USUARIOS: LEA DETENIDAMENTE EL CONTRATO LEGAL CORRESPONDIENTE A LA LICENCIA ADQUIRIDA, QUE ESTIPULA LOS TÉRMINOS GENERALES Y CONDICIONES DE USO DEL SOFTWARE CON LICENCIA. SI NO SABE QUÉ TIPO DE LICENCIA HA ADQUIRIDO, CONSULTE LOS DOCUMENTOS DE VENTA Y OTROS DOCUMENTOS RELACIONADOS CON LA CONCESIÓN DE LA LICENCIA O CON LA ORDEN DE COMPRA QUE ACOMPAÑAN AL PAQUETE DE SOFTWARE O QUE HAYA RECIBIDO POR SEPARADO COMO PARTE DE LA COMPRA (POR EJEMPLO, UN MANUAL, UN ARCHIVO DEL CD DEL PRODUCTO O UN ARCHIVO DEL SITIO WEB DESDE EL QUE DESCARGÓ EL PAQUETE DE SOFTWARE). SI NO ESTÁ DE ACUERDO CON TODOS LOS TÉRMINOS DESCRITOS EN EL ACUERDO, NO INSTALE EL SOFTWARE. SEGÚN CORRESPONDA, PUEDE DEVOLVER EL PRODUCTO A MCAFEE, INC. O AL ESTABLECIMIENTO DE COMPRA PARA QUE SE LE REEMBOLSE EL IMPORTE COMPLETO.

CAPÍTULO 46

Servicio al cliente y soporte técnico

SecurityCenter informa de los problemas de protección críticos y no críticos tan pronto como los detecta. Los problemas de protección críticos requieren una acción inmediata y ponen en peligro su estado de protección (el color cambia a rojo). Los problemas de protección no críticos no requieren acciones inmediatas y pueden poner en peligro o no su estado de protección (dependiendo del tipo de problema). Para conseguir un estado de protección de color verde, debe solucionar todos los problemas críticos y solucionar u omitir todos los problemas que no sean críticos. Si necesita ayuda para diagnosticar sus problemas de protección, puede ejecutar McAfee Virtual Technician. Si desea obtener más información sobre McAfee Virtual Technician, consulte la ayuda de McAfee Virtual Technician.

Si adquirió su software de seguridad a través de un distribuidor o proveedor distinto de McAfee, abra un navegador Web y visite www.mcafeeayuda.com. Una vez allí, en enlaces de proveedores, seleccione su proveedor para acceder a McAfee Virtual Technician.

Nota: para instalar y ejecutar McAfee Virtual Technician, debe iniciar sesión en su equipo como Administrador de Windows. En caso contrario, Virtual Technician no podrá resolver sus problemas. Si desea obtener información sobre cómo iniciar sesión como Administrador de Windows, consulte la Ayuda de Windows. En Windows Vista™, se le solicita al ejecutar Virtual Technician. Cuando esto ocurra, haga clic en **Aceptar**. Virtual Technician no funciona con Mozilla® Firefox.

En este capítulo

Utilización de McAfee Virtual Technician

Al igual que un representante personal de soporte técnico, Virtual Technician recopila información sobre sus programas de SecurityCenter para poder resolver los problemas de protección de su equipo. Al ejecutar Virtual Technician, realiza una comprobación para asegurarse de que sus programas de SecurityCenter funcionan correctamente. Si detecta algún problema, Virtual Technician se ofrece a solucionarlo por usted o le facilita información más detallada sobre dicho problema. Al finalizar, Virtual Technician muestra los resultados de su análisis y, en caso necesario, le permite buscar soporte técnico adicional de McAfee.

Para mantener la seguridad y la integridad de su equipo y archivos, Virtual Technician no recopila información personal e identificable.

Nota: para obtener más información sobre Virtual Technician, haga clic en el icono **Ayuda** de Virtual Technician.

Iniciar Virtual Technician

Virtual Technician recopila información sobre sus programas de SecurityCenter para poder resolver sus problemas de protección. Para proteger su privacidad, esta información no incluye información personal e identificable.

1. En **Tareas comunes**, haga clic en **McAfee Virtual Technician**.
2. Siga las instrucciones que aparecen en pantalla para descargar y ejecutar Virtual Technician.

Soporte técnico y Descargas

Consulte las siguientes tablas para conocer los sitios de Soporte técnico y Descargas de McAfee en su país, incluidas las Guías de usuario.

Soporte técnico y Descargas

País	Soporte de McAfee	Descargas de McAfee
Australia	www.mcafeehelp.com	au.mcafee.com/root/downloads.asp
Brasil	www.mcafeeajuda.com	br.mcafee.com/root/downloads.asp
Canadá (inglés)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp

Canadá (francés)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
China (chn)	www.mcafeehelp.com	cn.mcafee.com/root/downloads.asp
China (tw)	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
República Checa	www.mcafeenapoveda.com	cz.mcafee.com/root/downloads.asp
Dinamarca	www.mcafeehjaelp.com	dk.mcafee.com/root/downloads.asp
Finlandia	www.mcafeehelp.com	fi.mcafee.com/root/downloads.asp
Francia	www.mcafeeaide.com	fr.mcafee.com/root/downloads.asp
Alemania	www.mcafeehilfe.com	de.mcafee.com/root/downloads.asp
Gran Bretaña	www.mcafeehelp.com	uk.mcafee.com/root/downloads.asp
Italia	www.mcafeeaiuto.com	it.mcafee.com/root/downloads.asp
Japón	www.mcafeehelp.jp	jp.mcafee.com/root/downloads.asp
Corea	www.mcafeehelp.com	kr.mcafee.com/root/downloads.asp
México	www.mcafeehelp.com	mx.mcafee.com/root/downloads.asp
Noruega	www.mcafeehjelp.com	no.mcafee.com/root/downloads.asp
Polonia	www.mcafeepomoc.com	pl.mcafee.com/root/downloads.asp
Portugal	www.mcafeeajuda.com	pt.mcafee.com/root/downloads.asp
España	www.mcafeeayuda.com	es.mcafee.com/root/downloads.asp
Suecia	www.mcafeehjalp.com	se.mcafee.com/root/downloads.asp
Turquía	www.mcafeehelp.com	tr.mcafee.com/root/downloads.asp
Estados Unidos	www.mcafeehelp.com	us.mcafee.com/root/downloads.asp

Guías de usuario de McAfee Total Protection

País	Guías de usuario de McAfee
Australia	download.mcafee.com/products/manuals/en-au/MTP_userguide_2008.pdf
Brasil	download.mcafee.com/products/manuals/pt-br/MTP_userguide_2008.pdf
Canadá (inglés)	download.mcafee.com/products/manuals/en-ca/MTP_userguide_2008.pdf
Canadá (francés)	download.mcafee.com/products/manuals/fr-ca/MTP_userguide_2008.pdf
China (chn)	download.mcafee.com/products/manuals/zh-cn/MTP_userguide_2008.pdf
China (tw)	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
República Checa	download.mcafee.com/products/manuals/cz/MTP_userguide_2008.pdf
Dinamarca	download.mcafee.com/products/manuals/dk/MTP_userguide_2008.pdf
Finlandia	download.mcafee.com/products/manuals/fi/MTP_userguide_2008.pdf
Francia	download.mcafee.com/products/manuals/fr/MTP_userguide_2008.pdf
Alemania	download.mcafee.com/products/manuals/de/MTP_userguide_2008.pdf
Gran Bretaña	download.mcafee.com/products/manuals/en-uk/MTP_userguide_2008.pdf
Holanda	download.mcafee.com/products/manuals/nl/MTP_userguide_2008.pdf
Italia	download.mcafee.com/products/manuals/it/MTP_userguide_2008.pdf
Japón	download.mcafee.com/products/manuals/ja/MTP_userguide_2008.pdf
Corea	download.mcafee.com/products/manuals/ko/MTP_userguide_2008.pdf
México	download.mcafee.com/products/manuals/es-mx/MTP_userguide_2008.pdf
Noruega	download.mcafee.com/products/manuals/no/MTP_userguide_2008.pdf
Polonia	download.mcafee.com/products/manuals/pl/MTP_userguide_2008.pdf

Portugal	download.mcafee.com/products/manuals/pt/MTP_userguide_2008.pdf
España	download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf
Suecia	download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf
Turquía	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf
Estados Unidos	download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf

Guías de usuario de McAfee Internet Security

País	Guías de usuario de McAfee
Australia	download.mcafee.com/products/manuals/en-au/MIS_userguide_2008.pdf
Brasil	download.mcafee.com/products/manuals/pt-br/MIS_userguide_2008.pdf
Canadá (inglés)	download.mcafee.com/products/manuals/en-ca/MIS_userguide_2008.pdf
Canadá (francés)	download.mcafee.com/products/manuals/fr-ca/MIS_userguide_2008.pdf
China (chn)	download.mcafee.com/products/manuals/zh-cn/MIS_userguide_2008.pdf
China (tw)	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
República Checa	download.mcafee.com/products/manuals/cz/MIS_userguide_2008.pdf
Dinamarca	download.mcafee.com/products/manuals/dk/MIS_userguide_2008.pdf
Finlandia	download.mcafee.com/products/manuals/fi/MIS_userguide_2008.pdf
Francia	download.mcafee.com/products/manuals/fr/MIS_userguide_2008.pdf
Alemania	download.mcafee.com/products/manuals/de/MIS_userguide_2008.pdf
Gran Bretaña	download.mcafee.com/products/manuals/en-uk/MIS_userguide_2008.pdf
Holanda	download.mcafee.com/products/manuals/nl/MIS_userguide_2008.pdf
Italia	download.mcafee.com/products/manuals/it/MIS_userguide_2008.pdf

Japón	download.mcafee.com/products/manuals/ja/MIS_userguide_2008.pdf
Corea	download.mcafee.com/products/manuals/ko/MIS_userguide_2008.pdf
México	download.mcafee.com/products/manuals/es-mx/MIS_userguide_2008.pdf
Noruega	download.mcafee.com/products/manuals/no/MIS_userguide_2008.pdf
Polonia	download.mcafee.com/products/manuals/pl/MIS_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/MIS_userguide_2008.pdf
España	download.mcafee.com/products/manuals/es/MIS_userguide_2008.pdf
Suecia	download.mcafee.com/products/manuals/sv/MIS_userguide_2008.pdf
Turquía	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf
Estados Unidos	download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf

Guías de usuario de McAfee VirusScan Plus

País	Guías de usuario de McAfee
Australia	download.mcafee.com/products/manuals/en-au/VSP_userguide_2008.pdf
Brasil	download.mcafee.com/products/manuals/pt-br/VSP_userguide_2008.pdf
Canadá (inglés)	download.mcafee.com/products/manuals/en-ca/VSP_userguide_2008.pdf
Canadá (francés)	download.mcafee.com/products/manuals/fr-ca/VSP_userguide_2008.pdf
China (chn)	download.mcafee.com/products/manuals/zh-cn/VSP_userguide_2008.pdf
China (tw)	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf
República Checa	download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf
Dinamarca	download.mcafee.com/products/manuals/dk/VSP_userguide_2008.pdf
Finlandia	download.mcafee.com/products/manuals/fi/VSP_userguide_2008.pdf

Francia	download.mcafee.com/products/manuals/fr/VSP_userguide_2008.pdf
Alemania	download.mcafee.com/products/manuals/de/VSP_userguide_2008.pdf
Gran Bretaña	download.mcafee.com/products/manuals/en-uk/VSP_userguide_2008.pdf
Holanda	download.mcafee.com/products/manuals/nl/VSP_userguide_2008.pdf
Italia	download.mcafee.com/products/manuals/it/VSP_userguide_2008.pdf
Japón	download.mcafee.com/products/manuals/ja/VSP_userguide_2008.pdf
Corea	download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf
México	download.mcafee.com/products/manuals/es-mx/VSP_userguide_2008.pdf
Noruega	download.mcafee.com/products/manuals/no/VSP_userguide_2008.pdf
Polonia	download.mcafee.com/products/manuals/pl/VSP_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/VSP_userguide_2008.pdf
España	download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf
Suecia	download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf
Turquía	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf
Estados Unidos	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf

Guías de usuario de McAfee VirusScan

País	Guías de usuario de McAfee
Australia	download.mcafee.com/products/manuals/en-au/VS_userguide_2008.pdf
Brasil	download.mcafee.com/products/manuals/pt-br/VS_userguide_2008.pdf
Canadá (inglés)	download.mcafee.com/products/manuals/en-ca/VS_userguide_2008.pdf
Canadá (francés)	download.mcafee.com/products/manuals/fr-ca/VS_userguide_2008.pdf

China (chn)	download.mcafee.com/products/manuals/zh-cn/VS_userguide_2008.pdf
China (tw)	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
República Checa	download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf
Dinamarca	download.mcafee.com/products/manuals/dk/VS_userguide_2008.pdf
Finlandia	download.mcafee.com/products/manuals/fi/VS_userguide_2008.pdf
Francia	download.mcafee.com/products/manuals/fr/VS_userguide_2008.pdf
Alemania	download.mcafee.com/products/manuals/de/VS_userguide_2008.pdf
Gran Bretaña	download.mcafee.com/products/manuals/en-uk/VS_userguide_2008.pdf
Holanda	download.mcafee.com/products/manuals/nl/VS_userguide_2008.pdf
Italia	download.mcafee.com/products/manuals/it/VS_userguide_2008.pdf
Japón	download.mcafee.com/products/manuals/ja/VS_userguide_2008.pdf
Corea	download.mcafee.com/products/manuals/ko/VS_userguide_2008.pdf
México	download.mcafee.com/products/manuals/es-mx/VS_userguide_2008.pdf
Noruega	download.mcafee.com/products/manuals/no/VS_userguide_2008.pdf
Polonia	download.mcafee.com/products/manuals/pl/VS_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/VS_userguide_2008.pdf
España	download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf
Suecia	download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf
Turquía	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf
Estados Unidos	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf

Consulte la siguiente tabla para conocer los sitios del Centro de amenazas e Información sobre virus de McAfee en su país.

País	Centros de seguridad	Información de virus
Australia	www.mcafee.com/us/threat_center	au.mcafee.com/virusInfo
Brasil	www.mcafee.com/us/threat_center	br.mcafee.com/virusInfo
Canadá (inglés)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Canadá (francés)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
China (chn)	www.mcafee.com/us/threat_center	cn.mcafee.com/virusInfo
China (tw)	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
República Checa	www.mcafee.com/us/threat_center	cz.mcafee.com/virusInfo
Dinamarca	www.mcafee.com/us/threat_center	dk.mcafee.com/virusInfo
Finlandia	www.mcafee.com/us/threat_center	fi.mcafee.com/virusInfo
Francia	www.mcafee.com/us/threat_center	fr.mcafee.com/virusInfo
Alemania	www.mcafee.com/us/threat_center	de.mcafee.com/virusInfo
Gran Bretaña	www.mcafee.com/us/threat_center	uk.mcafee.com/virusInfo
Holanda	www.mcafee.com/us/threat_center	nl.mcafee.com/virusInfo
Italia	www.mcafee.com/us/threat_center	it.mcafee.com/virusInfo
Japón	www.mcafee.com/us/threat_center	jp.mcafee.com/virusInfo
Corea	www.mcafee.com/us/threat_center	kr.mcafee.com/virusInfo
México	www.mcafee.com/us/threat_center	mx.mcafee.com/virusInfo
Noruega	www.mcafee.com/us/threat_center	no.mcafee.com/virusInfo

Polonia	www.mcafee.com/us/threat_center	pl.mcafee.com/virusInfo
Portugal	www.mcafee.com/us/threat_center	pt.mcafee.com/virusInfo
España	www.mcafee.com/us/threat_center	es.mcafee.com/virusInfo
Suecia	www.mcafee.com/us/threat_center	se.mcafee.com/virusInfo
Turquía	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo
Estados Unidos	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo

Consulte la siguiente tabla para conocer los sitios de HackerWatch en su país.

País	HackerWatch
Australia	www.hackerwatch.org
Brasil	www.hackerwatch.org/?lang=pt-br
Canadá (inglés)	www.hackerwatch.org
Canadá (francés)	www.hackerwatch.org/?lang=fr-ca
China (chn)	www.hackerwatch.org/?lang=zh-cn
China (tw)	www.hackerwatch.org/?lang=zh-tw
República Checa	www.hackerwatch.org/?lang=cs
Dinamarca	www.hackerwatch.org/?lang=da
Finlandia	www.hackerwatch.org/?lang=fi
Francia	www.hackerwatch.org/?lang=fr
Alemania	www.hackerwatch.org/?lang=de
Gran Bretaña	www.hackerwatch.org
Holanda	www.hackerwatch.org/?lang=nl
Italia	www.hackerwatch.org/?lang=it
Japón	www.hackerwatch.org/?lang=jp
Corea	www.hackerwatch.org/?lang=ko
México	www.hackerwatch.org/?lang=es-mx
Noruega	www.hackerwatch.org/?lang=no
Polonia	www.hackerwatch.org/?lang=pl

Portugal	www.hackerwatch.org/?lang=pt-pt
España	www.hackerwatch.org/?lang=es
Suecia	www.hackerwatch.org/?lang=sv
Turquía	www.hackerwatch.org/?lang=tr
Estados Unidos	www.hackerwatch.org

Índice

D

E

F

N

O

P

R

S

T

U

V

W