McAfee®

VirusScan® 2008

Virus and Spyware Protection

Guía del usuario

Contenido

CAPÍTULO 1

McAfee VirusScan

VirusScan con SiteAdvisor ofrece servicios avanzados de detección y protección para optimizar la protección de su equipo contra las últimas amenazas para la seguridad, tales como virus, troyanos, cookies de rastreo, software espía, software publicitario y otros programas potencialmente no deseados. Con VirusScan, la protección se amplía más allá de los archivos y carpetas de su equipo de sobremesa o portátil, centrándose en las amenazas desde diferentes puntos de entrada, tales como el correo electrónico, los mensajes instantáneos e Internet. Con McAfee SiteAdvisor, las valoraciones de seguridad Web le ayudarán a evitar los sitios Web no seguros.

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.

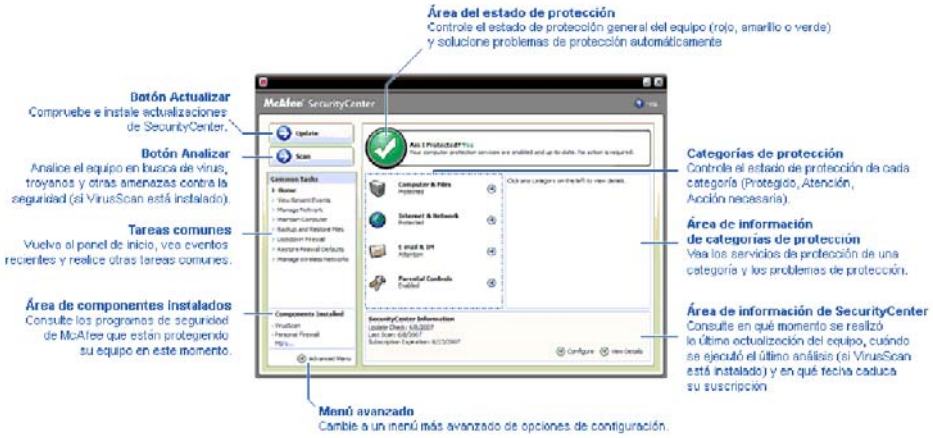
Alertas en tiempo real

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 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 14

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 15

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 16

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 17

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.

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 18

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

E

F

G

H

I

K

L

M

V

W