McAfee®

internetsecuritysuite wirelessedition

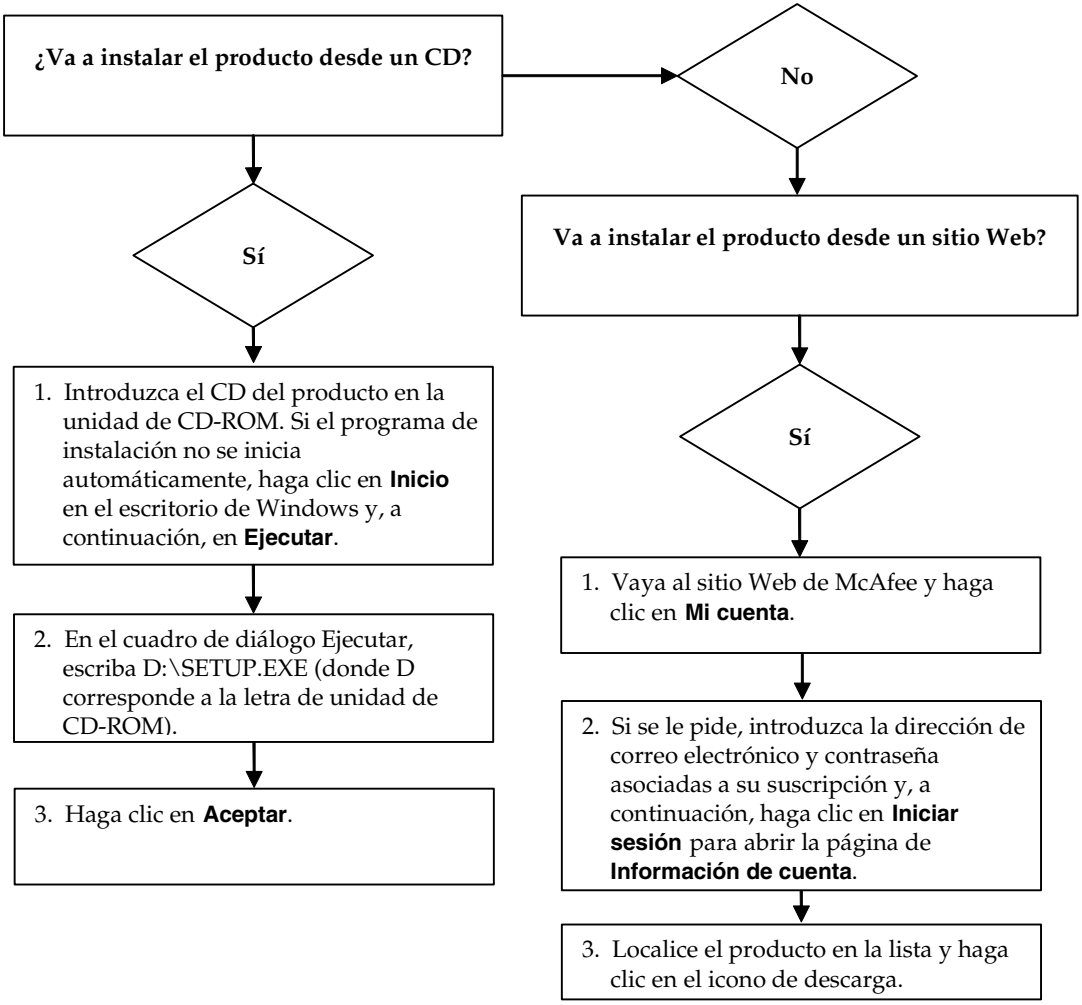
Guía del usuario

Versión 1.1

McAfee®

Tarjeta de inicio rápido

Si va a instalar el producto desde un CD o desde un sitio Web, imprima esta página de referencia.



Más información

Para ver las guías del usuario del CD del producto, asegúrese de que tiene instalado Acrobat Reader; si no es así, instálelo ahora desde el CD del producto de McAfee.

1. Introduzca el CD del producto en la unidad de CD-ROM.
2. Abra el Explorador de Windows. Haga clic en **Inicio** en el escritorio de Windows y, a continuación, en **Buscar**.
3. Localice la carpeta Manuals y haga doble clic en el .PDF de la Guía del usuario que desee abrir.

Ventajas de registrarse

McAfee recomienda que siga los sencillos pasos que se incluyen en el producto para transmitir su registro directamente. Si se registra, podrá disfrutar de soporte técnico especializado y puntual, así como de las ventajas siguientes:

- Soporte electrónico GRATUITO
- Actualizaciones de los archivos de definición de virus (.DAT) durante un año a partir de la instalación tras la adquisición del software VirusScan.

  Vaya a http://es.mcafee.com/ para obtener información sobre el precio de un año adicional de firmas de virus.
- Una garantía de 60 días que le asegura la sustitución del CD de software si está defectuoso o dañado.
- Actualizaciones de filtros de SpamKiller durante un año después de la instalación tras la adquisición del software SpamKiller.

  Vaya a http://es.mcafee.com/ para obtener información sobre el precio de un año adicional de actualizaciones de filtros.
- McAfee Internet Security Suite se actualiza durante un año después de la instalación tras la adquisición del software MIS.

  Vaya a http://es.mcafee.com/ para obtener información sobre el precio de un año adicional de actualizaciones de contenido.

Soporte técnico

Para obtener soporte técnico, visite

http://www.mcafeeayuda.com/.

Nuestro sitio de soporte permite acceder durante las 24 horas del día al sencillo Centro de respuestas para obtener soluciones a las preguntas más comunes.

Los usuarios experimentados también pueden utilizar las opciones avanzadas, que incluyen la búsqueda por palabra clave o el árbol de ayuda. Si no logra encontrar una solución a su problema, puede acceder a nuestros servicios GRATUITOS Chat Now! y Email Express! Estas opciones le permiten ponerse en contacto rápidamente con nuestros ingenieros de soporte técnico cualificados, a través de Internet y sin coste alguno. También puede obtener información de soporte por teléfono en

http://www.mcafeeayuda.com/.

Contenido

Introducción 1

Internet pone a nuestro alcance una ingente cantidad de información y posibilidades de entretenimiento. Sin embargo, tan pronto como se conecta, el equipo queda expuesto a un sinnúmero de amenazas para la privacidad y la seguridad. Proteja la privacidad y la seguridad de su equipo y los datos que contiene con Internet Security Suite-Wireless Network Edition. Gracias a la incorporación de las galardonadas tecnologías de McAfee, McAfee Internet Security Suite-Wireless Network Edition proporciona uno de los paquetes más completos de herramientas de privacidad y seguridad disponibles en la actualidad. McAfee Internet Security Suite-Wireless Network Edition ofrece protección avanzada para su red inalámbrica, sus datos personales y su equipo. Además, destruye virus, se anticipa a los piratas informáticos, asegura su información personal, privatiza su navegación Web, bloquea anuncios y ventanas emergentes, gestiona cookies y contraseñas, bloquea el acceso a archivos, carpetas y unidades, filtra los contenidos censurable y le concede el control de las conexiones entrantes y salientes de su equipo con Internet.

McAfee Internet Security Suite-Wireless Network Edition es una solución de seguridad probada que ofrece una protección eficaz a los usuarios actuales de Internet.

McAfee Internet Security Suite-Wireless Network Edition se compone de los productos siguientes:

- *McAfee Wireless Home Network Security* en la página 19
- *McAfee VirusScan* en la página 45
- *McAfee Personal Firewall Plus* en la página 81
- *McAfee Privacy Service* en la página 115
- *McAfee SpamKiller* en la página 139

Software McAfee Internet Security Suite-Wireless Network Edition

- **McAfee SecurityCenter:** evalúa, informa y advierte sobre la vulnerabilidad de la seguridad de su equipo. Cada índice de seguridad evalúa rápidamente su exposición a las amenazas de seguridad y a las existentes en Internet, y propone recomendaciones para proteger su equipo de manera rápida y segura.
- **McAfee Wireless Home Network Security:** protege la privacidad de su experiencia informática mediante el cifrado de sus datos personales y privados que se envían a través de su red inalámbrica protegida, e impide a los piratas informáticos acceder a su información.
- **McAfee VirusScan:** analiza, detecta, soluciona y elimina virus de Internet. Puede personalizar análisis de virus y determinar la respuesta y la acción que tomar cuando se detecta un virus. También puede configurar VirusScan para que registre acciones relacionadas con virus que ocurran en el equipo.
- **McAfee Personal Firewall Plus:** protege el equipo cuando está conectado a Internet y protege las conexiones entrantes y salientes a Internet que realiza.
- **McAfee Privacy Service:** combina protección de la información personal, bloqueo de anuncios publicitarios en línea y filtrado de contenidos. Protege su información personal a la vez que facilita un mayor control sobre el uso de Internet por parte de su familia. McAfee Privacy Service evita la exposición de información confidencial a amenazas en línea y le protege a usted y a su familia de contenidos inadecuados.
- **McAfee SpamKiller:** el aumento del envío de correo electrónico fraudulento, inapropiado y ofensivo dirigido a adultos, menores y empresas hace de la protección contra el spam un componente fundamental de la estrategia de seguridad de su equipo.

Requisitos del sistema

- Microsoft® Windows 98SE, Me, 2000 o XP
- Equipo personal con procesador Pentium o compatible
  - Windows 98, 2000: 133 MHz o superior
  - Windows Me: 150 MHz o superior
  - Windows XP (Home y Pro): 300 MHz o superior
- RAM
  - Windows 98, Me, 2000: 64 MB
  - Windows XP (Home y Pro): 128 MB

- 100 MB de espacio libre en el disco duro
- Microsoft Internet Explorer 5.5 o posterior

> **NOTA**
> Para actualizar a la última versión de Internet Explorer, visite el sitio Web de Microsoft en http://www.microsoft.com/.

- Sistema operativo diseñado y probado para las variantes del español

Complemento AntiPhishing

- Outlook Express 6.0 o posterior
- Outlook 98, 2000, 2003 o XP
- Internet Explorer 6.0 o posterior

Mensajería instantánea:

- AOL Instant Messenger 2.1 o posterior
- Yahoo Messenger 4.1 o posterior
- Microsoft Windows Messenger 3.6 o posterior
- MSN Messenger 6.0 o posterior

Correo electrónico:

- POP3 (Outlook Express, Outlook, Eudora o Netscape)
- MAPI (Outlook)
- Web (MSN o Hotmail, o una cuenta de correo electrónico con acceso POP3)

Adaptador de red inalámbrico:

- Adaptador de red inalámbrico estándar

Punto de acceso o enrutador inalámbrico:

- Adaptador de red inalámbrico estándar
- Punto de acceso o enrutador inalámbrico estándar, como la mayoría de los modelos Linksys®, NETGEAR®, D-Link® y Belkin®

Instalación de Internet Security Suite-Wireless Network Edition

Puede instalar Internet Security Suite-Wireless Network Edition desde un CD o desde el sitio Web.

Instalación desde un CD

1. Introduzca el CD del producto en la unidad de CD-ROM. Si el programa de instalación no se inicia automáticamente, haga clic en **Inicio** en el escritorio de Windows y en **Ejecutar**.
2. En el cuadro de diálogo **Ejecutar**, escriba D:\SETUP.EXE (donde D corresponde a la letra de unidad de CD-ROM).
3. Haga clic en **Aceptar**.
4. Vaya a *Utilización del asistente de configuración* en la página 23.

Instalación desde el sitio Web

Cuando instala McAfee Internet Security Suite-Wireless Network Edition desde el sitio Web, debe guardar el archivo de instalación. Este archivo se utiliza para instalar McAfee Internet Security Suite-Wireless Network Edition en otros equipos.

1. Vaya al sitio Web de McAfee y haga clic en **Mi cuenta**.
2. Si se le pide, introduzca la dirección de correo electrónico y la contraseña asociadas a su suscripción y, a continuación, haga clic en **Iniciar sesión** para abrir la página de **Información de cuenta**.
3. Localice el producto en la lista y haga clic en **Guardar destino como...** El archivo de instalación se guarda en su equipo.

Instalación desde el archivo

Si ha descargado el paquete de instalación (es decir, no tiene el CD), debe instalar el software en todos los equipos inalámbricos. Una vez que la red está protegida, los equipos inalámbricos no pueden conectarse a ella sin introducir la clave. Siga uno de estos procedimientos.

- Antes de proteger la red, descargue el paquete de instalación en todos y cada uno de los equipos inalámbricos.
- Copie el archivo de instalación en una llave de memoria USB o CD grabable e instale el software en el resto de los equipos inalámbricos.

- Si la red ya está protegida, enchufe un cable en el enrutador para descargar el archivo. También puede hacer clic en **Ver clave actual** para ver la clave actual y conectarse a la red inalámbrica mediante esta clave.

Tras instalar McAfee Internet Security Suite-Wireless Network Edition en todos los equipos, siga las instrucciones que aparecen pantalla. Cuando haga clic en **Finalizar**, aparecerá el Asistente de configuración. Vaya a *Utilización del asistente de configuración* en la página 23.

Utilización de McAfee SecurityCenter

McAfee SecurityCenter es su centro integral de seguridad al que puede acceder desde el icono correspondiente de la bandeja del sistema de Windows o desde el escritorio de Windows. Con ella puede realizar estas útiles tareas:

- Obtener un análisis de seguridad del equipo gratuito.
- Ejecutar, gestionar y configurar todas las suscripciones de McAfee desde el mismo icono.
- Ver alertas de virus actualizadas continuamente y la información más reciente sobre los productos.
- Acceder rápidamente a las preguntas más frecuentes y a información detallada de la cuenta en el sitio Web de McAfee.

> **NOTA**
> Si desea obtener más información sobre las funciones de SecurityCenter, haga clic en **Ayuda** en el cuadro de diálogo **SecurityCenter**.

Mientras SecurityCenter esté en ejecución y cuando estén activadas todas las funciones instaladas de McAfee en el equipo, aparecerá un icono rojo con una **M** en la bandeja del sistema de Windows . Esta área se encuentra normalmente en la esquina inferior derecha del escritorio de Windows e incluye el reloj.

Si alguna de las aplicaciones de McAfee instaladas se encuentra desactivada, el icono de McAfee aparecerá de color negro .

Para abrir McAfee SecurityCenter:

1. Haga clic con el botón derecho del ratón en el icono de McAfee , en la bandeja del sistema de Windows.
2. Haga clic en **Abrir SecurityCenter**.

Para acceder al producto de McAfee:

1 Haga clic con el botón derecho del ratón en el icono de McAfee  , en la bandeja del sistema de Windows.

2 Elija el producto de McAfee adecuado y seleccione la función que desea utilizar.

Eliminación de los programas de Internet Security Suite-Wireless Network Edition

Habrá ocasiones en las que desee eliminar programas de Internet Security Wireless Network.

> **NOTA**
> Para eliminar programas de Internet Security Suite-Wireless Network Edition es necesario que disponga de derechos de administrador.

Para eliminar programas de Internet Security Wireless Network:

1 Guarde todo el trabajo y cierre todas las aplicaciones que se encuentren abiertas.

2 Abra el **Panel de control**.

- En la barra de tareas de Windows, seleccione **Inicio**, elija **Configuración** y después haga clic en **Panel de control** (Windows 98, ME y 2000).
- En la barra de tareas de Windows, seleccione **Inicio** y haga clic en **Panel de control** (Windows XP).

3 Haga clic en **Agregar o quitar programas**.

4 Seleccione el asistente para desinstalación de McAfee, a continuación, uno o más programas y finalmente haga clic en **Desinstalar**.

5 Para proceder a la eliminación, haga clic en **Sí**.

Si se le solicita, reinicie el equipo.

McAfee Wireless Home Network Security 2

Bienvenido a McAfee Wireless Home Network Security, un producto que le ofrece protección avanzada para su red inalámbrica, sus datos personales y su equipo.

Este producto está diseñado para equipos que utilizan conexiones inalámbricas. No podrá hacer uso de todas las funciones del producto si lo instala en equipos que se conectan a la red mediante cable.

McAfee Wireless Home Network Security mejora la privacidad de su experiencia informática mediante el cifrado de sus datos personales y privados que se envían a través de su red inalámbrica protegida, e impide a los piratas informáticos acceder a su información.

Utilización de McAfee Wireless Home Network Security

Antes de proteger la red, lea lo siguiente.

- Conexiones con cable: los equipos que están conectados a un enrutador mediante un cable no necesitan protección, ya que las señales que se transmiten a través de cable no puede ser interceptadas.
- Conexiones inalámbricas: los equipos que tienen conexiones inalámbricas deben protegerse porque sus datos sí pueden ser interceptados. Debe utilizarse un equipo inalámbrico para proteger una red, ya que sólo un equipo inalámbrico puede conceder acceso a otro equipo inalámbrico.

Protección de su red

Si se conecta a través de un cable no es necesario que proteja la red.

1. Instale el adaptador inalámbrico en su equipo inalámbrico y asegúrese de que está activado. El adaptador inalámbrico puede ser una tarjeta insertada en el lateral del equipo o en un puerto USB. Muchos de los nuevos equipos vienen con un adaptador inalámbrico incorporado; en este caso, no es necesario que lo instale.
2. Instale el punto de acceso o enrutador inalámbrico (los puntos de acceso se emplean para ampliar el alcance inalámbrico) y compruebe que está encendido y activado. Para ver una definición completa de enrutador y punto de acceso, consulte el *Glosario* en la página 179.

3 Instale McAfee Wireless Home Network Security en todos y cada uno de los equipos de su red. No tiene que instalar el software en equipos que se conecten mediante un cable. Consulte *Instalación de Internet Security Suite-Wireless Network Edition* en la página 16.

4 Proteja la red desde uno de los equipos inalámbricos. Consulte *Protección de redes inalámbricas* en la página 32.

5 Incorpórese a la red desde otros equipos inalámbricos. Consulte *Protección de otros equipos* en la página 31.

McAfee Wireless Home Network Security

Como otros muchos usuarios, dispone de una red inalámbrica en casa porque es una tecnología cómoda y fácil. Las redes inalámbricas permiten acceder a Internet desde cualquier habitación de la casa o incluso desde un patio, sin el coste y los problemas que implica la conexión de cableado. Además, las redes inalámbricas permiten a sus amigos y familiares acceder a la red.

Sin embargo, esta comodidad conlleva una vulnerabilidad de la protección. Las redes inalámbricas emplean ondas de radio para transmitir los datos y estas ondas viajan a través de los muros de su casa. Mediante el uso de antenas especiales, los intrusos pueden acceder a su red inalámbrica o interceptar sus datos desde kilómetros de distancia.

Para proteger su red inalámbrica y su información, necesita limitar el acceso a la red y cifrar los datos. Su punto de acceso o enrutador inalámbrico incluye estándares de seguridad, pero es difícil activar y gestionar de forma adecuada la configuración de seguridad. Más del sesenta por ciento de las redes inalámbricas no utilizan correctamente un nivel alto de seguridad, como el cifrado.

Con Wireless Home Network Security es fácil

McAfee Wireless Home Network Security activa la seguridad en su red inalámbrica y protege todo lo que se envía mediante un sencillo proceso que genera de forma automática una potente clave de cifrado. Los piratas informáticos pueden descifrar sin problemas la mayoría de las claves que se pueden recordar fácilmente. Con Wireless Home Network Security el equipo puede recordar la clave introducida, lo que facilita el uso de claves que son casi imposibles de piratear.

Este software, que se ejecuta en segundo plano de forma inadvertida, crea y distribuye también una nueva clave de cifrado cada pocos minutos, lo que frustra hasta a los piratas más resueltos. Los equipos autorizados, como los de sus amigos y familiares que desean acceder a su red inalámbrica, reciben esta potente clave de cifrado y todas las distribuciones de claves.

Este proceso ofrece una protección sólida y al mismo tiempo no presenta ninguna dificultad para el propietario de una red inalámbrica doméstica. Con sólo hacer clic con el ratón, puede impedir a los piratas robar los datos que envía mediante ondas. Los piratas no pueden insertar troyanos ni ningún otro software maligno en su red. No pueden utilizar la red inalámbrica como plataforma para lanzar ataques de spam o virus. Ni siquiera los usuarios parásitos que pudieran aparecer podrían utilizar su red inalámbrica, por lo que nunca podrán culparle de descargar de forma ilegal películas o música.

Ninguna otra solución ofrece la protección sencilla y robusta que proporciona Wireless Home Network Security. El filtrado de direcciones MAC o la desactivación de difusión de SSID sólo ofrece una protección superficial. Incluso los piratas más novatos pueden burlar estos mecanismos descargando herramientas gratuitas de Internet. Otras utilidades como las redes virtuales VPN no protegen la propia red inalámbrica, por lo que el usuario sigue vulnerable ante miles de ataques.

McAfee Wireless Home Network Security es el primer producto que ofrece protección total para su red inalámbrica doméstica.

Características

Esta versión de Wireless Home Network Security tiene las siguientes características:

- Protección continua: detecta y protege automáticamente las redes inalámbricas vulnerables a las que se conecta.
- Interfaz intuitiva: protege su red sin necesidad de tomar decisiones difíciles ni conocer complicados términos técnicos.
- Cifrado automático robusto: solamente permite el acceso a la red a sus amigos y familiares, y protege los datos que transmite y recibe.
- Solución de software exclusivamente: Wireless Home Network Security funciona con su punto de acceso o enrutador inalámbrico estándar y su software de seguridad. No necesita adquirir hardware adicional.
- Rotación de clave automática: incluso los piratas informáticos más decididos serán incapaces de capturar su información gracias a la rotación continua de clave.
- Incorporación de usuarios a la red: puede conceder fácilmente acceso a la red a sus amigos y familiares.
- Herramienta de conexión intuitiva: la herramienta de conexión inalámbrica es intuitiva e informativa, con detalles sobre la intensidad de la señal y el estado de seguridad.

- Registro de eventos y alertas: los sencillos informes y alertas ofrecen a los usuarios avanzados más información sobre la red inalámbrica.
- Modo de interrupción: suspenda la rotación de clave de manera temporal para que determinadas aplicaciones puedan ejecutarse sin interrupción.
- Compatibilidad con otros equipos: Wireless Home Network Security se actualiza automáticamente con los últimos módulos de punto de acceso o enrutador inalámbrico de las marcas más populares, incluidas: Linksys®, NETGEAR®, D-Link®, Belkin® y otras.

Instalación desde un CD

1. Introduzca el CD del producto en la unidad de CD-ROM. Si el programa de instalación no se inicia automáticamente, haga clic en **Inicio** en el escritorio de Windows y en **Ejecutar**.
2. En el cuadro de diálogo **Ejecutar**, escriba D:\SETUP.EXE (donde D corresponde a la letra de unidad de CD-ROM).
3. Haga clic en **Aceptar**.
4. Vaya a *Utilización del asistente de configuración* en la página 23.

Instalación desde el sitio Web

Cuando instala Wireless Home Network Security desde el sitio Web, debe guardar el archivo de instalación. Este archivo se utiliza para instalar Wireless Home Network Security en otros equipos.

1. Vaya al sitio Web de McAfee y haga clic en **Mi cuenta**.
2. Si se le pide, introduzca la dirección de correo electrónico y la contraseña asociadas a su suscripción y, a continuación, haga clic en **Iniciar sesión** para abrir la página de **Información de cuenta**.
3. Localice el producto en la lista y haga clic en **Guardar destino como...** El archivo de instalación se guarda en su equipo.

Instalación desde el archivo

Si ha descargado el paquete de instalación (es decir, no tiene el CD), debe instalar el software en todos los equipos inalámbricos. Una vez que la red está protegida, los equipos inalámbricos no pueden conectarse a ella sin introducir la clave. Siga uno de estos procedimientos.

- Antes de proteger la red, descargue el paquete de instalación en todos y cada uno de los equipos inalámbricos.
- Copie el archivo de instalación en una llave de memoria USB o CD grabable e instale el software en el resto de los equipos inalámbricos.
- Si la red ya está protegida, enchufe un cable en el enrutador para descargar el archivo. También puede hacer clic en **Ver clave actual** para ver la clave actual y conectarse a la red inalámbrica mediante esta clave.

Tras instalar Wireless Home Network Security en todos los equipos, siga las instrucciones que aparecen pantalla. Cuando haga clic en **Finalizar**, aparecerá el Asistente de configuración. Vaya a *Utilización del asistente de configuración* en la página 23.

Utilización del asistente de configuración

El asistente de configuración permite:

- Proteger la red desde uno de los equipos inalámbricos. Para obtener más información, consulte *Protección de redes inalámbricas* en la página 32.

  Si Wireless Home Network Security no puede determinar el punto de acceso o enrutador correcto, se le pedirá Reintentar o Cancelar. Sitúese más cerca del punto de acceso o enrutador que está protegiendo y, a continuación, haga clic en **Reintentar**.
- Incorporarse a una red protegida (este paso no es necesario si sólo hay un equipo inalámbrico).
- Conectarse a una red. Para obtener más información, consulte *Conexión a una red* en la página 27.

Recibirá una notificación si no se detecta su adaptador inalámbrico o si su punto de acceso o enrutador inalámbrico está apagado

Para ver el estado de su conexión, haga clic con el botón derecho del ratón en el icono de McAfee ( ), elija **Wireless Network Security** y, a continuación, seleccione **Resumen**. Aparecerá la página **Resumen** (figura 2-1).

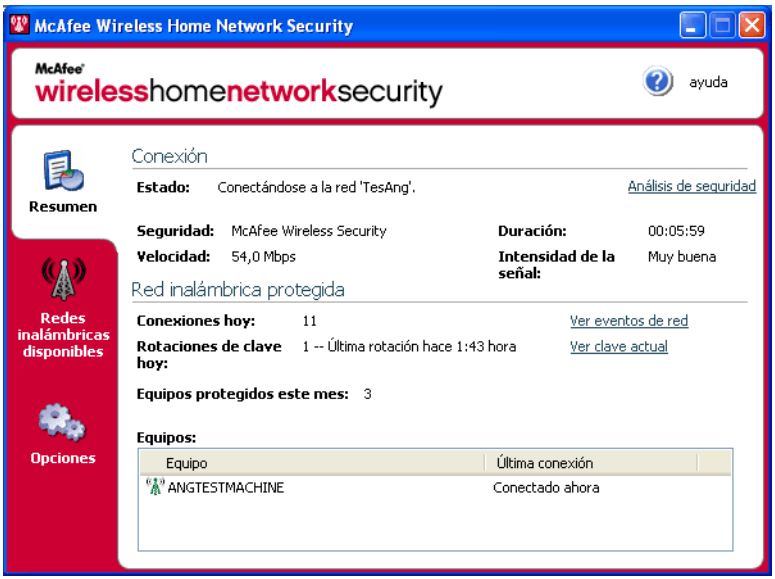


Figura 2-1. Página Resumen

Visualización de su conexión

El panel Conexión muestra el estado de su conexión. Si desea ejecutar un análisis de su conexión inalámbrica, haga clic en **Análisis de seguridad**.

- Estado: si está conectado o desconectado. Si está conectado, aparece el nombre de la red.
- Seguridad: el modo de seguridad de la red.
- Velocidad: velocidad de la conexión desde su tarjeta de interfaz de red (NIC).
- Duración: tiempo que ha estado conectado a la red.
- Intensidad de la señal: intensidad de su conexión inalámbrica.

Visualización de su red inalámbrica protegida

El panel Red inalámbrica protegida proporciona información sobre su red.

- Conexiones hoy: número de veces que los usuarios se han conectado a la red en el día de hoy.
- Rotaciones de clave hoy: número de veces que se ha rotado la clave en el día de hoy, incluido el tiempo transcurrido desde la última vez que se rotó la clave.
- Rotación de clave interrumpida: la rotación de clave está interrumpida en su red. Para reanudar la rotación de clave y asegurarse de que la red está totalmente protegida frente a los piratas informáticos, haga clic en **Reanudar rotación de clave**.
- Equipos protegidos este mes: número de equipos que han sido protegidos este mes.
- Equipos: si está conectado a una red protegida, indica todos los equipos de la red y cuándo se conectó cada equipo por última vez.

   - el equipo está conectado.

   - el equipo se puede volver a conectar sin tener que incorporarse a la red.

   - el equipo no está conectado. Debe volver a incorporarse a la red porque la clave ha sido actualizada.

Haga clic en **Ver eventos de red** para ver los eventos de la red. Consulte *Visualización de eventos* en la página 28.

Haga clic en **Ver clave actual** para ver la clave.

Si conecta a su red dispositivos inalámbricos que Wireless Home Network Security no admite (por ejemplo, un equipo de bolsillo), siga estos pasos:

1. En la pantalla Resumen, haga clic en **Ver clave actual**.
2. Anote la clave.
3. Haga clic en **Interrumpir rotación de clave**. La interrupción de la rotación de clave impide que se desconecten los dispositivos que han sido conectados a la red manualmente.
4. Introduzca la clave en el dispositivo.

Cuando haya terminado de utilizar estos dispositivos, haga clic en **Reanudar rotación de clave.** McAfee recomienda que reanude la rotación de clave para asegurarse de que la red está totalmente protegida frente a piratas informáticos.

Para seleccionar las redes inalámbricas a las que va a conectarse o incorporarse, haga clic con el botón derecho del ratón en el icono de McAfee ( ), elija **Wireless Network Security** y seleccione **Redes inalámbricas**. Aparece la página **Redes inalámbricas disponibles** (figura 2-2).

Figura 2-2. Página Redes inalámbricas

Si está conectado a una red inalámbrica protegida, la información que se envía y recibe estará cifrada. Los piratas informáticos no pueden interceptar los datos que se transmiten por la red protegida ni conectarse a su red.

- la red está protegida.
- la red está protegida con seguridad WEP o WPA-PSK.
- la red no está protegida, pero puede conectarse a ella (no se recomienda).

Gestión de redes inalámbricas

En esta sección se proporciona información sobre la gestión de redes inalámbricas.

Conexión a una red

Para conectarse a una red, seleccione la red adecuada y, a continuación, haga clic en **Conectar**. Si ha configurado manualmente una clave precompartida para su punto de acceso o enrutador, también debe introducir la clave.

Si la red está protegida, antes de conectarse debe incorporarse a ella. Para incorporarse a la red, un usuario que ya esté conectado debe darle permiso.

Una vez que se haya incorporado, para volver a conectarse no es necesario que se incorpore de nuevo. Puede conceder permiso a otros usuarios para que se incorporen a esa red.

Desconexión de una red

Para desconectarse de una red a la que esté conectado, haga clic en **Desconectar**.

Utilización de las opciones avanzadas

Si desea utilizar las opciones de conexión avanzadas, haga clic en **Avanzadas**. Aparecerá el cuadro de diálogo **Configuración avanzada**. Desde este cuadro de diálogo, puede realizar lo siguiente:

- Cambiar el orden de las redes a las que se conecta automáticamente. La red situada al principio de la lista es la última a la que se conectó y es la primera a la que intenta conectarse Wireless Home Network Security. Para mover una red, selecciónela y haga clic en **Subir** o **Bajar**. Por ejemplo, si se ha trasladado a otro lugar, y la red a la que se conectó la última vez se encuentra lejos y la señal es débil, puede situar la red que tenga la mejor señal al principio de la lista.
- Suprimir redes preferidas de esta lista. Por ejemplo, si se ha conectado a la red de su vecino por error, ésta estará ahora incluida en esta lista. Para suprimirla, selecciónela y haga clic en **Quitar**.
- Modificar las propiedades de la red. Si tiene problemas para conectarse a una red que no está protegida, puede modificar sus propiedades. Tenga en cuenta que esta opción sólo se aplica a las redes no protegidas. Para modificar propiedades, seleccione una red y haga clic en **Propiedades**.
- Agregar redes que no difunden el SSID; por ejemplo, si intenta conectarse a la red inalámbrica de un amigo, pero ésta no aparece en la lista, haga clic en **Agregar** e introduzca la información adecuada. Wireless Home Network Security no puede proteger la redes que añade.

Para configurar las opciones, haga clic con el botón derecho del ratón en el icono de McAfee ( ), elija **Wireless Network Security** y seleccione **Opciones**. Aparece la página de opciones (figura 2-3).

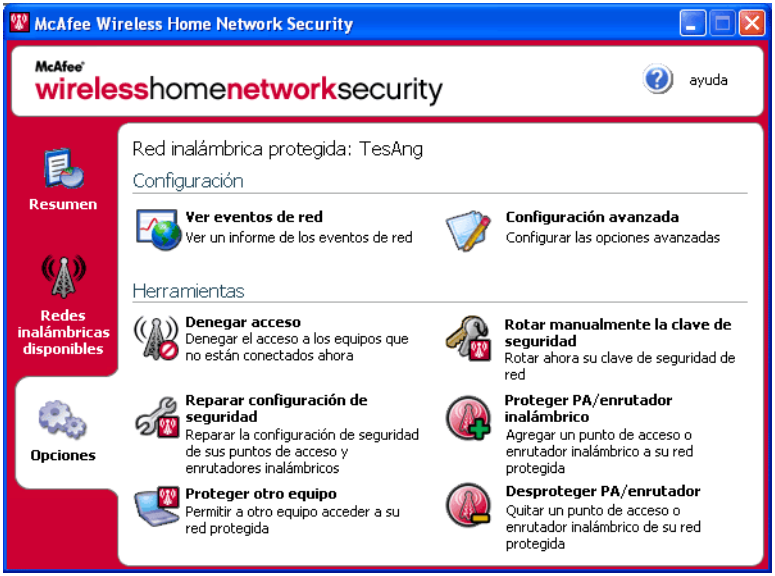


Figura 2-3. Página de opciones

Visualización de eventos

Las acciones que realiza Wireless Home Network Security se almacenan en registros de eventos. Para ver estos registros, haga clic en **Ver eventos de red**. La información se muestra en orden cronológico de forma predeterminada.

En el cuadro **Eventos de la red**, se pueden seleccionar los tipos de eventos que se van a mostrar (todos los eventos siguen registrados) y se pueden ver los eventos de las redes a las que pertenece (si pertenece a más de una red).

Cuando se produce un evento, aparece un mensaje de alerta con una breve descripción.

Configuración de opciones avanzadas

Esta sección está destinada a usuarios avanzados. Haga clic en **Configuración avanzada** para configurar la seguridad, las alertas y otros parámetros.

Después de modificar un parámetro, haga clic en **Aceptar** para que surtan efecto los cambios. Tenga en cuenta que tras hacer clic en **Aceptar**, todos los equipos que estén conectados perderán la conectividad durante unos minutos.

Definición de la configuración de seguridad

Utilice la ficha **Configuración de seguridad** para modificar los parámetros de seguridad.

- Nombre de red inalámbrica protegida: nombre de la red protegida actual. Cuando cambia el nombre de una red, éste aparece en la lista **Redes inalámbricas disponibles** y debe volver a conectarse a la red.
- Modo de seguridad: modo de seguridad actual. Para cambiar el modo de seguridad predeterminado (WEP), seleccione WPA-PSK TKIP para obtener un cifrado más robusto. Asegúrese de que los puntos de acceso, enrutadores y adaptadores inalámbricos que se conectan a su red admiten este modo; de lo contrario no podrán conectarse. Para obtener más información acerca de la actualización del adaptador, consulte *Actualización del adaptador inalámbrico* en la página 41.
- Activar rotación de clave automática: para suspender la rotación de clave, desactive esta opción. Para cambiar la frecuencia de rotación, mueva la barra deslizante. Para obtener más información acerca de la rotación de clave, consulte *Visualización de su red inalámbrica protegida* en la página 25.
- Cambiar nombre de usuario o contraseña: por razones de seguridad, puede cambiar el nombre de usuario o la contraseña predeterminados del punto de acceso o enrutador inalámbrico. Para ello, selecciónelos y haga clic en **Cambiar nombre de usuario o contraseña**. Estos valores son los que ha utilizado para conectarse y configurar su punto de acceso o enrutador.

Configuración de los parámetros de alerta

Utilice la ficha **Configuración de alertas** para cambiar la configuración de las alertas.

Seleccione el tipo de eventos para los que desea recibir alertas y haga clic en **Aceptar**. Si no desea recibir una alerta cuando se produzcan determinados eventos, desactive la casilla correspondiente.

Configuración de otros parámetros

Utilice la ficha **Otras opciones** para modificar otros parámetros.

- Mostrar claves como texto: para redes no protegidas mediante Wireless Home Network Security. Las claves para las redes no protegidas que aparecen en la lista **Redes inalámbricas disponibles** se pueden mostrar como texto en lugar de utilizar asteriscos. Por razones de seguridad, si muestra las claves como texto, éstas no se almacenan.
- Descartar claves guardadas: para redes no protegidas mediante Wireless Home Network Security. Se eliminan todas las claves que se hayan guardado. Tenga en cuenta que si se eliminan estas claves, debe volver a introducir una clave cuando se conecte a redes WEP y WPA-PSK.

- Abandonar red: para redes protegidas con Wireless Home Network Security. Puede renunciar a sus derechos de acceso a una red inalámbrica protegida. Por ejemplo, si desea salir de una red y no cree que vaya a volver a conectarse, selecciónela en la lista y haga clic en **Abandonar red**.
- Mostrar mensaje de notificación cuando esté conectado a una red inalámbrica: cuando se establece una conexión, aparece un mensaje de notificación.

Denegación de acceso a la red

Para impedir que los equipos que se han incorporado a la red, pero que no están conectados a ella, tengan acceso a la red:

1. Haga clic en **Denegar acceso**. Aparece el cuadro de diálogo **Denegar acceso**.
2. Haga clic en **Denegar**.

Se restablece la rotación de clave de la red y los equipos que están conectados reciben la nueva clave y siguen conectados. Los equipos que no están conectados no reciben la clave actualizada y deben volver a incorporarse a la red antes de conectarse.

Cuando deniega el acceso a un equipo, ese equipo debe volver a incorporarse a la red para conectarse de nuevo a la red protegida. Para ello, el equipo debe tener Wireless Home Network Security instalado (consulte *Instalación de Internet Security Suite-Wireless Network Edition* en la página 16), volver a conectarse a la red protegida e incorporarse a ella (consulte *Conexión a una red* en la página 27).

Reparación de la configuración de seguridad

Sólo se debe reparar la configuración de seguridad cuando se tienen problemas con la red inalámbrica. Para obtener más información, consulte *No es posible realizar la conexión* en la página 41.

Para corregir la configuración del punto de acceso o enrutador de la red actual, siga estos pasos:

1. Haga clic en **Reparar configuración de seguridad.** Aparece el cuadro de diálogo **Reparar**.
2. Haga clic en **Reparar**.
3. Haga clic en **Cerrar** cuando haya terminado.

Si no se puede establecer una conexión con los puntos de acceso o enrutadores de la red, aparece un mensaje de error. Conecte su red con un cable e intente repararla. Si la contraseña del punto de acceso o enrutador ha cambiado, aparecerá un mensaje para que especifique la contraseña nueva.

Protección de otros equipos

Para obtener más información sobre la protección de otros equipos y sobre cómo concederles acceso a la red protegida, haga clic en **Proteger otro equipo**.

Para proteger otro equipo:

1. Instale McAfee Wireless Home Network Security en el equipo que desea proteger.
2. En el equipo que desea proteger, haga clic con el botón derecho del ratón en el icono de McAfee ( ), elija **Wireless Network Security** y seleccione **Redes inalámbricas disponibles**. Aparece la página **Redes inalámbricas**.
3. Seleccione una red protegida a la que desea incorporarse y haga clic en **Conectar**. Tenga en cuenta que un usuario que ya esté conectado a la red debe concederle permiso para incorporarse.

   Una vez que se haya incorporado, para volver a conectarse no es necesario que se incorpore de nuevo. Puede conceder permiso a otros usuarios para que se incorporen a esa red.
4. Haga clic en **Aceptar** en el cuadro de dialogo de confirmación.

Si conecta a su red dispositivos inalámbricos que Wireless Home Network Security no admite (por ejemplo, un equipo de bolsillo), siga estos pasos:

1. En la pantalla Resumen, haga clic en **Ver clave actual**.
2. Anote la clave.
3. Haga clic en **Interrumpir rotación de clave**. La interrupción de la rotación de clave impide que se desconecten los dispositivos que han sido conectados a la red manualmente.
4. Introduzca la clave en el dispositivo.

Cuando haya terminado de utilizar estos dispositivos, haga clic en **Reanudar rotación de clave.** McAfee recomienda que reanude la rotación de clave para asegurarse de que la red está totalmente protegida frente a piratas informáticos.

Rotación de claves

Para rotar la clave de seguridad de la red, haga clic en **Rotar manualmente la clave de seguridad**.

Protección de redes inalámbricas

Para proteger un punto de acceso o enrutador, siga estos pasos:

1. Haga clic en **Proteger PA/enrutador inalámbrico**. Aparece el cuadro de diálogo **Proteger red inalámbrica**. Si el punto de acceso o enrutador no aparece en la lista, haga clic en **Actualizar**.
2. Seleccione el punto de acceso o enrutador que desea proteger y haga clic en **Proteger**.

Desprotección de redes inalámbricas

Debe estar conectado al punto de acceso o enrutador inalámbrico que desea desproteger.

Para desproteger un punto de acceso o enrutador, siga estos pasos:

1. Haga clic en **Desproteger PA/enrutador inalámbrico**. Aparece el cuadro de diálogo **Desproteger PA/enrutador inalámbrico**. Si el punto de acceso o enrutador no aparece en la lista, haga clic en **Actualizar**.
2. Seleccione el punto de acceso o enrutador que desea desproteger y haga clic en **Desproteger**.

Mientras está conectado a Internet, Wireless Home Network Security comprueba cada cuatro horas la existencia de actualizaciones de software y, a continuación, las descarga e instala automáticamente sin interrumpir su trabajo. La descarga de estas actualizaciones causa un impacto mínimo en el rendimiento del sistema.

Cuando se actualiza un producto, aparece una alerta. Cuando aparezca la alerta, tiene la opción de actualizar Wireless Home Network Security.

Comprobación automática de actualizaciones

McAfee SecurityCenter está configurado para buscar automáticamente actualizaciones de todos los servicios de McAfee de los que disponga cada cuatro horas mientras haya conexión a Internet para, a continuación, avisarle mediante alertas y sonidos. De forma predeterminada, SecurityCenter descarga e instala automáticamente cualquier actualización disponible.

NOTA
En algunos casos, se le pedirá que reinicie el equipo para completar la actualización. Guarde su trabajo y cierre todas las aplicaciones antes de reiniciar el equipo.

Comprobación manual de actualizaciones

Además de buscar automáticamente actualizaciones cuando esté conectado a Internet, también puede buscar actualizaciones manualmente cuando lo desee.

Para comprobar manualmente si hay actualizaciones de Wireless Home Network Security:

1. Asegúrese de que el equipo está conectado a Internet.
2. Haga clic con el botón derecho del ratón en el icono de McAfee y seleccione **Actualizaciones**. Aparece el cuadro de diálogo **Actualizaciones de SecurityCenter**.
3. Haga clic en **Comprobar ahora**.

   Si existe una actualización, aparecerá el cuadro de diálogo **McAfee SecurityCenter**. Haga clic en **Actualizar** para continuar.

   Si no hay actualizaciones disponibles, aparecerá un cuadro de diálogo que le indicará que Wireless Home Network Security está actualizado. Haga clic en **Aceptar** para cerrar el cuadro de diálogo.
4. Regístrese en el sitio Web si se lo solicita un mensaje. El asistente de actualización instalará la actualización automáticamente.
5. Haga clic en **Finalizar** cuando la actualización haya terminado de instalarse.

   NOTA
   En algunos casos, se le pedirá que reinicie el equipo para completar la actualización. Guarde su trabajo y cierre todas las aplicaciones antes de reiniciar el equipo.

Las alertas aparecen cuando se producen eventos y le informan sobre cambios en la red.

Acceso denegado

Un usuario ha actualizado la clave de red. Para obtener más información, consulte *Denegación de acceso a la red* en la página 30.

Equipo conectado

Un usuario se ha conectado a la red. Para obtener más información, consulte *Conexión a una red* en la página 27.

Equipo desconectado

Un usuario se ha desconectado de la red. Para obtener más información, consulte *Desconexión de una red* en la página 27.

Equipo protegido

Un usuario que tiene acceso a la red protegida ha concedido acceso a otro usuario. Por ejemplo: 'Lance' ha concedido acceso a 'Mercks' y ambos pueden utilizar ahora la red inalámbrica 'CoppiWAP'.

Rotación de clave no realizada

La rotación de clave no se ha realizado por los siguientes motivos:

- Los datos de inicio de sesión para su punto de acceso o enrutador inalámbrico han cambiado. Si conoce los datos de inicio de sesión consulte *Reparación de la configuración de seguridad* en la página 30.
- La versión de firmware de su punto de acceso o enrutador ha cambiado a una versión que no se admite. Para obtener más información, consulte *No es posible realizar la conexión* en la página 41.
- Su punto de acceso o enrutador no está disponible. Asegúrese de que el punto de acceso o enrutador está encendido y conectado a la red.
- Se ha producido un error de administrador duplicado. Para obtener más información, consulte *Error de administrador duplicado* en la página 38.

Si tiene problemas para conectarse a la red, consulte *Reparación de la configuración de seguridad* en la página 30.

Rotación de clave reanudada

Un usuario ha reanudado la rotación de clave. La rotación de clave impide a los piratas informáticos acceder a la red.

Rotación de clave interrumpida

Un usuario ha interrumpido la rotación de clave. McAfee recomienda que reanude la rotación de clave para asegurarse de que la red está totalmente protegida frente a piratas informáticos.

Configuración de seguridad de red modificada

Un usuario ha modificado el modo de seguridad de la red. Para obtener más información, consulte *Definición de la configuración de seguridad* en la página 29.

Cambio de nombre de red

Un usuario ha cambiado el nombre de la red y debe conectarse de nuevo. Para obtener más información, consulte *Conexión a una red* en la página 27.

Red reparada

Un usuario ha intentado reparar la red por problemas de conexión.

Configuración de red modificada

Un usuario va a cambiar la configuración de seguridad de la red. La conexión se interrumpirá brevemente durante esta operación. El cambio que se va a realizar puede tratarse de uno o varios de los siguientes valores:

- Nombre de la red
- Modo de seguridad
- Frecuencia de rotación de clave
- Estado de rotación de clave automática

Contraseña modificada

Un usuario ha modificado el nombre de usuario o la contraseña de un punto de acceso o enrutador de la red. Para obtener más información, consulte *Definición de la configuración de seguridad* en la página 29.

Clave de seguridad rotada

Se ha rotado la clave de seguridad de la red . McAfee Wireless Home Network Security rota de forma automática la clave de cifrado de la red, lo que hace más difícil que los piratas informáticos puedan interceptar sus datos o conectarse a la red.

Frecuencia de rotación de clave de seguridad modificada

Se ha modificado la frecuencia de rotación de la clave de seguridad de la red. McAfee Wireless Home Network Security rota de forma automática la clave de cifrado de la red, lo que hace más difícil que los piratas informáticos puedan interceptar sus datos o conectarse a la red.

PA/enrutador inalámbrico protegido

Se ha protegido en la red un punto de acceso o enrutador inalámbrico. Para obtener más información, consulte *Protección de redes inalámbricas* en la página 32.

PA/enrutador inalámbrico no protegido

Se ha suprimido de la red un punto de acceso o enrutador inalámbrico. Para obtener más información, consulte *Desprotección de redes inalámbricas* en la página 32.

Solución de problemas

En este capítulo se describen procedimientos de solución de problemas para McAfee Wireless Home Network Security y equipos de terceros.

Instalación

En esta sección se explica cómo resolver problemas generales.

Equipos en los que se instala este software

Instale McAfee Wireless Home Network Security en todos y cada uno de los equipos inalámbricos de la red (a diferencia de otras aplicaciones de McAfee, puede instalar este software en varios equipos).

Puede (aunque no es obligatorio) realizar la instalación en equipos que no tienen adaptadores inalámbricos; sin embargo, el software no estará activo en esos equipos, ya que no necesitan protección inalámbrica. Para proteger la red, debe proteger el punto de acceso o enrutador (consulte *Protección de redes inalámbricas* en la página 32) desde uno de los equipos inalámbricos.

No se ha detectado el adaptador inalámbrico

Si su adaptador inalámbrico no se detecta una vez instalado y activado, reinicie el equipo. Si aún así no se detecta, siga estos pasos:

1. Abra el cuadro de diálogo **Propiedades de Conexiones de red inalámbricas**.
2. Desactive la casilla **Filtro MWL** y, a continuación, vuelva a seleccionarla.
3. Haga clic en **Aceptar**.

Si esto no funciona, es posible que no se admita su adaptador inalámbrico. Actualice el adaptador o compre uno nuevo. Para ver la lista de adaptadores admitidos, vaya a http://www.mcafee.com/es/router. Para actualizar el adaptador, consulte *Actualización del adaptador inalámbrico* en la página 41.

Varios adaptadores inalámbricos

Si un error indica que tiene instalados varios adaptadores inalámbricos, debe desactivar o desenchufar uno de ellos. Wireless Home Network Security sólo funciona con un adaptador inalámbrico.

No se puede descargar en los equipos inalámbricos porque la red ya está protegida

Si tiene un CD, utilícelo para instalar McAfee Wireless Home Network Security en todos los equipos inalámbricos.

Si ha instalado el software en un equipo inalámbrico y ha protegido la red antes de instalar el software en el resto de equipo inalámbricos, puede hacer lo siguiente:

- Desproteja la red (consulte *Desprotección de redes inalámbricas* en la página 32). A continuación, descargue el software e instálelo en todos los equipos inalámbricos. Proteja de nuevo la red (consulte *Protección de redes inalámbricas* en la página 32).
- Vea la clave de red (consulte *Visualización de su red inalámbrica protegida* en la página 25). A continuación, introduzca la clave en su equipo inalámbrico para conectarse a la red. Descargue e instale el software e incorpórese a la red desde el equipo inalámbrico (consulte *Protección de otros equipos* en la página 31).
- Descargue el ejecutable en el equipo que ya está conectado a la red y guárdelo en una llave de almacenamiento USB o cópielo en un CD de manera que pueda instalarlo en otros equipos.

Protección o configuración de la red

En esta sección se explica cómo resolver problemas al proteger o configurar su red.

Punto de acceso o enrutador no admitido

Si un error le indica que es posible que su punto de acceso o enrutador no se admita, quiere decir que McAfee Wireless Home Network Security no ha podido configurar su dispositivo porque no lo ha reconocido o no lo ha encontrado.

Solicite una actualización para asegurarse de que dispone de la última versión de Wireless Home Network Security (McAfee agrega constantemente nuevos puntos de acceso o enrutadores compatibles). Si su punto de acceso o enrutador aparece en la lista de http://www.mcafee.com/es/router y el error no desaparece, entonces quiere decir que tiene problemas de comunicación entre el equipo y el punto de acceso o enrutador. Consulte *No es posible realizar la conexión* en la página 41 antes de proteger de nuevo su red.

Actualización del firmware del punto de acceso o enrutador

Si un error le indica que la revisión de firmware de su punto de acceso o enrutador no se admite, su dispositivo es compatible, pero no la revisión de firmware del mismo. Solicite una actualización para asegurarse de que dispone de la última versión de Wireless Home Network Security (McAfee agrega constantemente nuevas revisiones de firmware).

Si dispone de la última versión de Wireless Home Network Security, consulte el sitio Web o solicite asistencia del fabricante de su punto de acceso o enrutador e instale una revisión de firmware que aparezca en la lista de http://www.mcafee.com/es/router.

Error de administrador duplicado

Después de configurar el punto de acceso o enrutador, debe cerrar la sesión de la interfaz de administración. En algunos casos, si no lo hace, el punto de acceso o enrutador se comporta como si otro equipo continuara configurándolo y aparece un mensaje de error.

Si no puede cerrar la sesión, desenchufe el punto de acceso o enrutador y enchúfelo de nuevo.

La red aparece como no segura

Si su red se muestra como no segura, significa que no está protegida. Debe protegerla (consulte *Protección de redes inalámbricas* en la página 32). Tenga en cuenta que McAfee Wireless Home Network Security sólo funciona con puntos de acceso y enrutadores compatibles (visite http://www.mcafee.com/es/router).

No se puede reparar

Si la reparación no funciona, intente lo siguiente. Tenga en cuenta que cada procedimiento es independiente.

- Conecte su red con un cable e intente repararla.
- Desenchufe el punto de acceso o enrutador, enchúfelo de nuevo y, a continuación, intente la conexión.
- Restablezca los valores predeterminados de fábrica del punto de acceso o enrutador inalámbrico y repare la red.
- Mediante las opciones avanzadas, salga de la red desde todos los equipos y restablezca los valores predeterminados del punto de acceso o enrutador inalámbrico. A continuación, proteja la red.

Conexión de equipos a la red

En esta sección se explica cómo resolver problemas al conectar equipos a su red.

Esperando autorización

Si está intentando incorporarse a una red protegida y su equipo permanece en espera de autorización, compruebe lo siguiente:

- Hay un equipo inalámbrico que tiene acceso a la red y está encendido y conectado a la misma.
- Hay alguien físicamente presente para concederle acceso a ese equipo cuando aparece.
- Los equipos están situados dentro de su alcance inalámbrico.

Si no aparece la opción **Conceder** en el equipo que ya tiene acceso la red, inténtelo desde otro equipo.

Si no hay otros equipos disponibles, desproteja la red desde el equipo que ya tiene acceso y protéjala desde el equipo que no tiene acceso. A continuación, incorpórese a la red desde el equipo que protegía la red originalmente.

Concesión de acceso a un equipo desconocido

Cuando reciba una solicitud acceso de un equipo desconocido, compruebe que se trata de alguien de confianza. Alguien podría estar intentando acceder a la red de manera ilegítima.

Conexión a una red o a Internet

En esta sección se explica cómo resolver problemas al conectarse a una red o a Internet.

Conexión a Internet defectuosa

Si no se puede conectar, intente acceder a la red utilizando un cable y, a continuación, conéctese a Internet. Si a pesar de todo no puede conectarse, compruebe lo siguiente:

- El módem está encendido.
- La configuración de PPPoE (consulte el *Glosario* en la página 179) es correcta.
- Su línea DSL o de cable está activa.

Los problemas de conectividad, como la velocidad y la intensidad de la señal, también pueden estar provocados por interferencias inalámbricas. Cambie el canal de su teléfono inalámbrico, elimine posibles fuentes de interferencias o cambie a otro lugar el punto de acceso, el enrutador inalámbrico o su equipo.

La conexión se interrumpe por momentos

Cuando la conexión se interrumpe brevemente (por ejemplo, durante el transcurso de un juego en línea), la rotación de clave podría estar provocando ligeros retrasos en la red. Suspenda momentáneamente la rotación de clave. McAfee recomienda que reanude la rotación de clave tan pronto como sea posible para asegurarse de que la red está totalmente protegida frente a los piratas informáticos.

Dispositivos (no su equipo) que pierden la conexión

Si hay dispositivos que pierden la conexión cuando utiliza McAfee Wireless Home Network Security, interrumpa la rotación de clave.

Se le ha pedido introducir la clave WEP o WPA

Si ha tenido que introducir una clave WEP o WPA para conectarse a la red, lo más probable es que no instalara el software en su equipo. Para que funcione correctamente, Wireless Home Network Security debe estar instalado en todos los equipos inalámbricos de la red. Consulte *Protección o configuración de la red* en la página 38.

No es posible realizar la conexión

Si no puede conectarse, intente lo siguiente. Tenga en cuenta que cada procedimiento es independiente.

- Si no se va a conectar a una red protegida, compruebe que dispone de la clave correcta e inténtelo de nuevo.
- Desenchufe el adaptador inalámbrico y vuelva a enchufarlo, o bien desactívelo y actívelo de nuevo.
- Apague el punto de acceso o enrutador, vuelva a encenderlo y, a continuación, intente la conexión.
- Compruebe que el punto de acceso o enrutador inalámbrico está conectado y repare la configuración de seguridad (consulte *Reparación de la configuración de seguridad* en la página 30).

  Si no funciona la reparación, consulte *No se puede reparar* en la página 39.
- Reinicie el equipo.
- Actualice el adaptador inalámbrico o compre uno nuevo. Para actualizar el adaptador, consulte *Actualización del adaptador inalámbrico* en la página 41. Por ejemplo, su red podría estar utilizando seguridad WPA-PSK TKIP y tal vez su adaptador inalámbrico no admita el modo de seguridad de la red (las redes muestran WEP, aunque estén definidas como WPA).
- Si no puede conectarse tras ampliar el punto de acceso o enrutador inalámbrico, es posible que haya ampliado a una versión no admitida. Compruebe que el punto de acceso o enrutador es compatible. Si no lo es, retroceda la ampliación a una versión compatible o espere hasta que haya disponible una actualización de Wireless Home Network Security.

Actualización del adaptador inalámbrico

Para proteger su adaptador, siga estos pasos:

1. En el escritorio, haga clic en **Inicio**, seleccione **Configuración** y, a continuación, **Panel de control**.
2. Haga doble clic en el icono **Sistema**. Aparece el cuadro de diálogo **Propiedades del sistema**.
3. Seleccione la ficha **Hardware** y, a continuación, haga clic en **Administrador de dispositivos**.
4. En la lista **Administrador de dispositivos**, haga doble clic en su adaptador.

5 Seleccione la ficha **Controlador** y anote el controlador que tiene.

6 Vaya al sitio Web del fabricante del adaptador y compruebe si hay disponible una actualización. Los controladores se encuentran generalmente en la sección de asistencia técnica o de descargas.

7 Si hay un controlador disponible, siga las instrucciones del sitio Web para descargarlo.

8 Vaya a la ficha **Controlador** y haga clic en **Actualizar controlador**. Aparece una ventana de asistente.

9 Siga las instrucciones que aparecen en pantalla.

Nivel de señal débil

Si la conexión se interrumpe o es lenta, es posible que el nivel de la señal sea insuficiente. Para mejorar la señal, intente lo siguiente:

- Asegúrese de que sus dispositivos inalámbricos no están bloqueados por objetos metálicos como calderas, tuberías o electrodomésticos grandes. Las señales inalámbricas no transmiten bien a través de este tipo de objetos.
- Si la señal atraviesa paredes, asegúrese de que no tiene que cruzar un ángulo llano. Cuanto más tiempo pase la señal en el interior del muro, más débil será cuando llegue.
- Si su punto de acceso o enrutador inalámbrico tiene más de una antena, intente orientar las dos antenas de forma que se crucen perpendicularmente (por ejemplo, una en posición vertical y la otra en horizontal, en un ángulo de 90 grados).
- Algunos fabricantes tienen antenas de alta ganancia. La antenas dirigidas proporcionan un mayor alcance, aunque las omnidireccionales ofrecen la máxima versatilidad. Consulte las instrucciones de instalación del fabricante para instalar su antena.

Si estos pasos no solucionan el problema, agregue a su red un punto de acceso que se encuentre más cerca del equipo al que intenta conectarse. Si configura su segundo punto de acceso con el mismo nombre de red (SSID) y un canal diferente, el adaptador encontrará automáticamente la señal más potente y se conectará a través del punto de acceso adecuado.

Windows no puede configurar su conexión inalámbrica

Si le aparece un mensaje que indica que Windows no puede configurar su conexión inalámbrica, ignórelo. Utilice Wireless Home Network Security para conectarse y configurar las redes inalámbricas. En el cuadro de diálogo de Windows **Propiedades de Conexiones de red inalámbricas**, en la ficha **Redes inalámbricas**, asegúrese de que está desactivada la casilla **Usar Windows para establecer mi configuración de red inalámbrica**.

Windows no muestra ninguna conexión

Si está conectado, pero el icono de red de Windows muestra una X (sin conexión), ignórelo. Su conexión es buena.

Otros problemas

En esta sección se explica cómo resolver otro tipo de problemas.

El nombre de la red es distinto al utilizar otros programas

Si el nombre de la red se ve distinto desde otros programas (por ejemplo, _SafeAaf como parte del nombre), no se alarme, es normal. Wireless Home Network Security marca las redes con un código cuando está protegidas.

Problemas al configurar los puntos de acceso o enrutadores inalámbricos

Si aparece un error al configurar el punto de acceso o enrutador o al agregar varios enrutadores a la red, compruebe que todos los enrutadores y puntos de acceso tienen una dirección IP distinta.

Si el nombre de su punto de acceso o enrutador inalámbrico aparece en el cuadro de diálogo **Punto de acceso o enrutador inalámbrico**, pero al configurarlo se muestra un error, compruebe que el punto de acceso o enrutador es compatible. Para ver una lista con los puntos de acceso o enrutadores admitidos, vaya a http://www.mcafee.com/es/router.

Si el punto de acceso o enrutador está configurado, pero no parece estar en la red adecuada (por ejemplo, no se pueden ver otros equipos conectados a la LAN), compruebe que ha configurado el punto de acceso o enrutador apropiado y no el de su vecino. Desenchufe el punto de acceso o enrutador y asegúrese de que la conexión se interrumpe. Si ha configurado el punto de acceso o enrutador equivocado, desprotéjalo y, a continuación, proteja el punto de acceso o enrutador correcto.

Si no puede configurar ni agregar el punto de acceso o enrutador a pesar de ser compatible, puede que haya realizado algunos cambios que impidan que pueda configurarse adecuadamente.

- Siga las instrucciones del fabricante para configurar su punto de acceso o enrutador inalámbrico para que utilice DHCP, o con la dirección IP correcta. En algunos casos, el fabricante proporciona una herramienta de configuración.
- Restablezca los valores predeterminados de fábrica del punto de acceso o enrutador, e intente reparar la red de nuevo. Es posible que haya modificado el puerto de administración del punto de acceso o enrutador, o que haya desactivado la administración inalámbrica. Asegúrese de que utiliza la configuración predeterminada y de que está activada la configuración inalámbrica. Otra posibilidad es que esté desactivada la administración http. En ese caso, compruebe que está activada.
- Si el punto de acceso o enrutador no aparece en la lista de puntos de acceso o enrutadores disponibles para proteger y conectar, active la difusión de SSID y compruebe que el punto de acceso o enrutador está activado.
- Si se desconecta o si no puede establecer una conexión, puede que el filtrado de direcciones MAC esté activado. Desactive el filtrado de direcciones MAC.
- Si no puede realizar operaciones de red (por ejemplo, compartir archivos o imprimir en impresoras compartidas) entre dos equipos con conexión inalámbrica a la red, compruebe que no ha activado el aislamiento de puntos de acceso. El aislamiento de puntos de acceso impide a los equipos inalámbricos conectarse entre ellos en la red.

Sustitución de equipos

Si se ha cambiado el equipo que protege la red y no hay ningún otro equipo que disponga de acceso (por lo tanto, no se puede acceder a la red), restablezca los valores predeterminados de fábrica del punto de acceso o enrutador inalámbrico.

El software no funciona tras ampliar los sistemas operativos

Si Wireless Home Network Security no funciona tras realizar una ampliación de sistemas operativos, desinstálelo y vuelva a instalarlo.

McAfee VirusScan 3

Bienvenido a McAfee VirusScan.

McAfee VirusScan es un servicio de suscripción antivirus que ofrece una protección completa, fiable y actualizada contra virus. Mediante la galardonada tecnología de análisis de McAfee, VirusScan protege contra virus, gusanos, archivos troyanos, secuencias de comandos sospechosas, ataques híbridos y otras amenazas.

Gracias a él, disfrutará de las funciones siguientes:

ActiveShield: analiza los archivos cuando el usuario o el equipo acceden a ellos.

Análisis: detecta la existencia de virus y otras amenazas en las unidades de disco duro, unidades de disquete y en cada una de las carpetas y archivos.

En cuarentena: permite cifrar y aislar temporalmente archivos sospechosos en la carpeta de cuarentena hasta que se tome alguna medida.

Detección de actividades hostiles: supervisa el equipo para detectar actividades características de los virus provocada por gusanos o por secuencias de comandos sospechosas.

Funciones nuevas

Esta versión de VirusScan incluye las siguientes funciones nuevas:

- **Detección y eliminación de software espía (spyware) y de publicidad no deseada (adware)**
  VirusScan identifica y elimina spyware, adware y otros programas que ponen en peligro su privacidad y reducen el rendimiento del equipo.
- **Actualizaciones automáticas diarias**
  Las actualizaciones automáticas de VirusScan protegen frente a las amenazas informáticas más recientes, incluso las aún no identificadas.
- **Análisis rápido en segundo plano**
  Los análisis rápidos y discretos identifican y destruyen virus, troyanos, gusanos, software espía, de publicidad y de marcación, y otros tipos de amenazas sin interrumpir el trabajo.

- **Alertas de seguridad en tiempo real**
  Las alertas de seguridad indican la aparición de brotes de virus y amenazas contra la seguridad y ofrecen opciones de respuesta para eliminar la amenaza, neutralizarla u obtener más información sobre ella.

- **Detección y limpieza en varios puntos de entrada**
  VirusScan supervisa y limpia en los puntos de entrada principales del equipo: correo electrónico, archivos adjuntos de mensajes instantáneos y descargas de Internet.

- **Supervisión en el correo electrónico de actividades características de los gusanos**
  WormStopper™ supervisa comportamientos susceptibles de ser correo masivo y detiene la propagación de virus y gusanos a otros equipos a través del correo electrónico.

- **Supervisión en las secuencias de comandos de actividades características de los gusanos**
  ScriptStopper™ supervisa ejecuciones de secuencias de comandos sospechosas y detiene la propagación de virus y gusanos a otros equipos a través del correo electrónico.

- **Soporte técnico gratuito a través de mensajería instantánea y correo electrónico**
  El soporte técnico en tiempo real a través mensajería instantánea y correo electrónico proporciona ayuda de forma rápida y sencilla.

Comprobación de VirusScan

Antes de utilizar VirusScan por primera vez, es recomendable comprobar su instalación. Siga las instrucciones que se indican a continuación para verificar por separado las funciones Analizar y ActiveShield.

Comprobación de ActiveShield

NOTA
Para comprobar el funcionamiento de ActiveShield desde la ficha VirusScan de SecurityCenter, haga clic en **Comprobar VirusScan** para ver en línea una lista de preguntas más frecuentes de soporte que contiene estos pasos.

Para comprobar ActiveShield:

1. Utilice su navegador Web para ir a la dirección http://www.eicar.com/.
2. Haga clic en el vínculo **The AntiVirus testfile eicar.com** (Archivo de prueba antivirus de eicar.com).
3. Desplácese hasta la parte inferior de la página. En **Download** (Descargar) verá cuatro vínculos.
4. Haga clic en **eicar.com**.

Si ActiveShield funciona correctamente, detectará el archivo eicar.com inmediatamente después de hacer clic en el vínculo. Puede intentar suprimir o poner en cuarentena archivos detectados para comprobar el tratamiento que da ActiveShield a las posibles amenazas. Para obtener más información, consulte *Descripción de las alertas de seguridad* en la página 60.

Comprobación de la función Analizar

Antes de poder comprobar la función Analizar, debe desactivar ActiveShield para evitar que detecte los archivos de prueba antes que Analizar y, a continuación, descargar los archivos de prueba.

Para descargar los archivos de prueba:

1. Desactive ActiveShield. Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y, a continuación, haga clic en **Desactivar**.
2. Descargue los archivos de prueba de EICAR del sitio Web de EICAR:
   a. Vaya a la dirección http://www.eicar.com/.
   b. Haga clic en el vínculo **The AntiVirus testfile eicar.com** (Archivo de prueba antivirus de eicar.com).

c Desplácese hasta la parte inferior de la página. En **Download** (Descargar) verá los vínculos siguientes:

eicar.com incluye una línea de texto que VirusScan detectará como virus.

eicar.com.txt (opcional) es el mismo archivo, pero con un nombre diferente, para aquellos usuarios que experimenten algún problema al descargar el primer vínculo. Sencillamente cambie su nombre a "eicar.com" después de descargarlo.

eicar_com.zip es una copia del virus de prueba incluido en un archivo comprimido con la extensión .ZIP (archivo comprimido mediante WinZip™).

eicarcom2.zip es una copia del virus de prueba incluido en un archivo comprimido con la extensión .ZIP, que se encuentra a su vez en un archivo comprimido con la extensión .ZIP.

d Haga clic en cada uno de los vínculos para descargar el archivo correspondiente. Se mostrará el cuadro de diálogo **Descarga de archivo** para efectuar la descarga de cada uno de ellos.

e Haga clic en **Guardar**, a continuación, en el botón **Crear carpeta nueva** y cambie el nombre de la carpeta por **Carpeta de análisis de VSO**.

f Haga doble clic en **Carpeta de análisis de VSO** y después en **Guardar** en cada cuadro de diálogo **Guardar como**.

3 Cuando haya terminado de descargar los archivos, cierre Internet Explorer.

4 Active ActiveShield: Haga clic con el botón derecho del ratón en el icono de McAfee, elija **VirusScan** y, a continuación, haga clic en **Activar**.

Para comprobar el funcionamiento de Analizar:

1 Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y haga clic en **Analizar**.

2 Utilizando el árbol de directorios del panel izquierdo del cuadro de diálogo, vaya a la carpeta **Carpeta de análisis de VSO** en la que guardó los archivos:

a Haga clic en el signo **+** situado junto al icono de la unidad C.

b Haga clic en la carpeta **Carpeta de análisis de VSO** para resaltarla (no lo haga en el signo **+** situado junto a ella).

De esta forma se indica a Analizar que sólo compruebe dicha carpeta. Si desea obtener una demostración más convincente de la capacidad de detección de Analizar, coloque los archivos en distintas ubicaciones del disco duro de forma aleatoria.

3 En el área **Opciones de análisis** del cuadro de diálogo **Analizar**, asegúrese de que todas las opciones se encuentren seleccionadas.

4 Haga clic en el botón **Analizar** situado en la parte inferior derecha del cuadro de diálogo.

VirusScan analizará la **Carpeta de análisis de VSO**. Los archivos de comprobación EICAR guardados en dicha carpeta aparecerán en la **Lista de archivos detectados**. Si es así, la función Analizar funciona correctamente.

Puede intentar eliminar o poner en cuarentena los archivos detectados para comprobar el tratamiento que da Analizar a las posibles amenazas. (Para obtener más información, consulte *Descripción de las detecciones de amenazas* en la página 71.)

Utilización de ActiveShield

Cuando ActiveShield se inicia (se carga en la memoria del equipo) y se activa, el equipo queda protegido en todo momento. ActiveShield analiza los archivos cuando el usuario o el equipo acceden a ellos. Cuando ActiveShield detecta un archivo, intenta limpiar el virus automáticamente. Si no lo consigue, el usuario puede poner en cuarentena el archivo o eliminarlo.

Activación o desactivación de ActiveShield

De manera predeterminada, ActiveShield se inicia (se carga en la memoria del equipo) y se activa (indicado mediante el rojo  de la bandeja del sistema de Windows) al reiniciar el equipo tras el proceso de instalación.

Si se detiene ActiveShield (no se carga) o se desactiva (indicado mediante el icono negro ), puede ejecutarlo manualmente y configurarlo para que se inicie automáticamente junto con Windows.

Activación de ActiveShield

Para activar ActiveShield únicamente durante la sesión actual de Windows:

Haga clic con el botón derecho del ratón en el icono de McAfee, elija **VirusScan** y, a continuación, haga clic en **Activar**. El icono de McAfee se mostrará de color rojo  .

Si ActiveShield sigue configurado para iniciarse junto con Windows, se mostrará un mensaje que indica que ya está protegido frente al ataque de posibles amenazas. De lo contrario, aparecerá un cuadro de diálogo que le permitirá configurar ActiveShield para que se inicie al abrir Windows (figura 3-1 en la página 50).

Desactivación de ActiveShield

Para desactivar ActiveShield únicamente durante la sesión actual de Windows:

1. Haga clic con el botón derecho del ratón en el icono de McAfee, elija **VirusScan** y, a continuación, haga clic en **Desactivar**.
2. Haga clic en **Sí** para confirmar.

   El icono de McAfee se mostrará de color negro .

Si ActiveShield sigue configurado para iniciarse junto con Windows, el equipo estará nuevamente protegido frente al ataque de posibles amenazas cuando lo reinicie.

Configuración de las opciones de ActiveShield

Puede modificar las opciones de inicio y análisis de ActiveShield en la ficha **ActiveShield** del cuadro de diálogo **VirusScan - Opciones** (figura 3-1), a la que puede acceder a través del icono de McAfee situado en la bandeja del sistema de Windows.

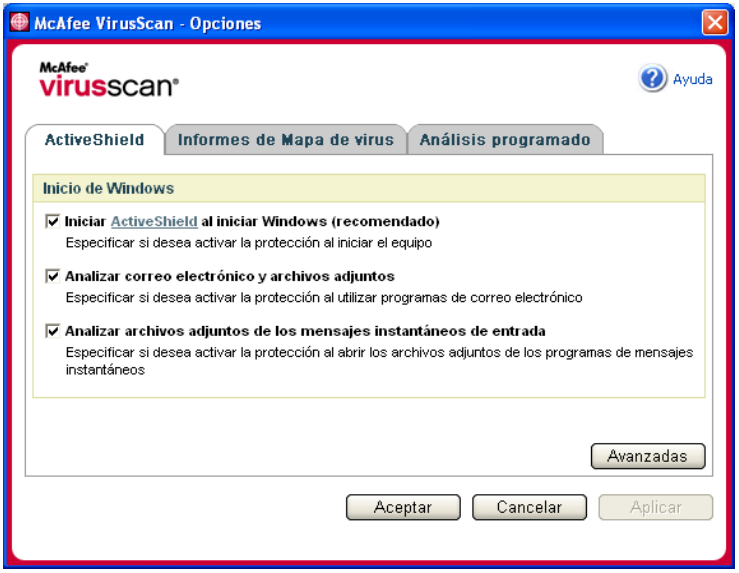


Figura 3-1. Opciones de ActiveShield

Inicio de ActiveShield

De manera predeterminada, ActiveShield se inicia (se carga en la memoria del equipo) y se activa (indicado mediante el icono rojo ) al reiniciar el equipo tras el proceso de instalación.

Si ActiveShield se detiene (indicado mediante el icono negro ), puede configurarlo para que se inicie automáticamente junto con Windows (opción recomendada).

> **NOTA**
> Durante las actualizaciones de VirusScan, el **Asistente para la actualización** podría cerrar ActiveShield temporalmente para instalar archivos nuevos. Cuando el **Asistente para la actualización** le pida que haga clic en **Finalizar**, ActiveShield se iniciará de nuevo.

Para iniciar ActiveShield automáticamente al arrancar Windows:

1. Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y, a continuación, haga clic en **Opciones**.

   Se abrirá el cuadro de diálogo **VirusScan - Opciones** (figura 3-1 en la página 50).

2. Marque la casilla de verificación **Iniciar ActiveShield al iniciar Windows (recomendado)** y haga clic en **Aplicar** para guardar los cambios.

3. Haga clic en **Aceptar** para confirmar y, a continuación, de nuevo en **Aceptar**.

Detención de ActiveShield

> **ADVERTENCIA**
> Si detiene ActiveShield, su equipo dejará de estar protegido frente a posibles amenazas. Si necesita detener ActiveShield para realizar otra tarea que no sea la actualización de VirusScan, asegúrese de no estar conectado a Internet.

Para hacer que ActiveShield no se inicie al arrancar Windows:

1. Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y, a continuación, haga clic en **Opciones**.

   Se abrirá el cuadro de diálogo **VirusScan - Opciones** (figura 3-1 en la página 50).

2. Anule la selección de la casilla de verificación **Iniciar ActiveShield al iniciar Windows (recomendado)** y haga clic en **Aplicar** para guardar los cambios.

3. Haga clic en **Aceptar** para confirmar y, a continuación, de nuevo en **Aceptar**.

Análisis del correo electrónico y los archivos adjuntos

De forma predeterminada, el análisis y la limpieza automática del correo electrónico se activa con la opción **Analizar correo electrónico y archivos adjuntos** (figura 3-1 en la página 50).

Cuando esta opción está activada, ActiveShield analiza y trata de limpiar automáticamente todos los mensajes de correo electrónico entrantes (POP3) y salientes (SMTP), así como los archivos adjuntos detectados de los clientes de correo electrónico más conocidos, incluidos los siguientes:

- Microsoft Outlook Express 4.0 o posterior
- Microsoft Outlook 97 o posterior
- Netscape Messenger 4.0 o posterior
- Netscape Mail 6.0 o posterior
- Eudora Light 3.0 o posterior
- Eudora Pro 4.0 o posterior
- Eudora 5.0 o posterior
- Pegasus 4.0 o posterior

NOTA

El análisis del correo electrónico no es posible en los clientes siguientes: correo electrónico basado en Web, IMAP, AOL, POP3 SSL y Lotus Notes. Sin embargo, ActiveShield analiza los archivos adjuntos del correo electrónico cuando se abren.

Si desactiva la opción **Analizar correo electrónico y archivos adjuntos**, las casillas de verificación incluidas en Opciones de análisis y WormStopper (figura 3-2 en la página 53) se desactivan automáticamente. Si desactiva el análisis de correo electrónico saliente, las opciones de WormStopper se desactivan automáticamente.

Si cambia las opciones de análisis de correo electrónico, debe reiniciar el programa de correo electrónico para completar los cambios.

Correo electrónico entrante

Si un mensaje de correo electrónico o un archivo adjunto entrante han sido detectados, ActiveShield realiza los pasos siguientes:

- Intenta limpiar el correo electrónico detectado.
- Intenta poner en cuarentena o eliminar el correo electrónico que no puede limpiar.
- Incluye un archivo de alerta en el correo electrónico entrante que contiene información sobre las acciones efectuadas para eliminar la posible amenaza.

Correo electrónico saliente

Si un mensaje de correo electrónico o un archivo adjunto saliente han sido detectados, ActiveShield realiza los pasos siguientes:

- Intenta limpiar el correo electrónico detectado.
- Intenta poner en cuarentena o eliminar el correo electrónico que no puede limpiar.

> **NOTA**
> Para obtener detalles sobre los errores de análisis de correo electrónico saliente, consulte la ayuda en línea.

Desactivación del análisis del correo electrónico

De forma predeterminada, ActiveShield analiza tanto el correo electrónico entrante como el saliente. Sin embargo, para lograr un mejor control, puede definir ActiveShield para que sólo analice el correo entrante o el saliente.

Para desactivar el análisis del correo entrante o saliente:

1. Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y haga clic en **Opciones**.
2. Haga clic en **Avanzadas** y, a continuación, en la ficha **Correo electrónico** (figura 3-2).
3. Anule la selección de **Mensajes de correo electrónico entrantes** o **Mensajes de correo electrónico salientes** y haga clic en **Aceptar**.

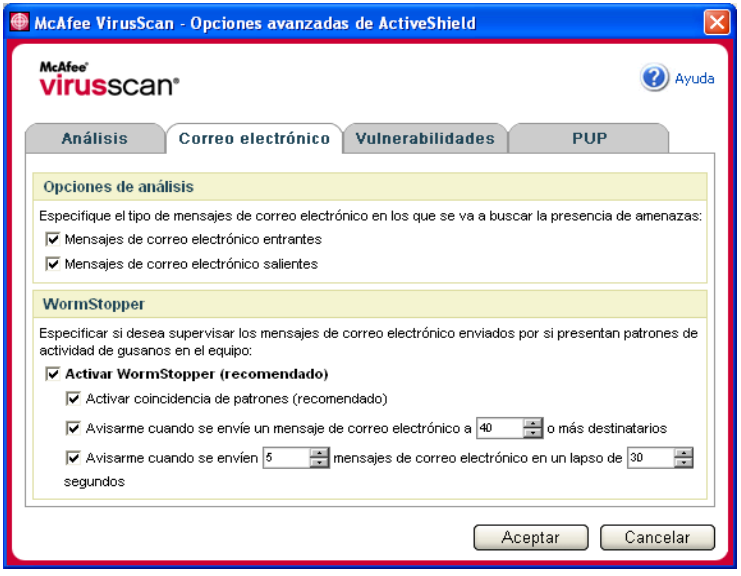


Figura 3-2. Opciones avanzadas de ActiveShield: ficha Correo electrónico

Análisis de gusanos

VirusScan supervisa el equipo para analizar la actividad sospechosa que pueda indicar la presencia de una amenaza. Mientras VirusScan limpia los virus y otras amenazas, WormStopper™ evita la proliferación de virus y gusanos.

Un "gusano" informático es un virus capaz de replicarse, que reside en la memoria activa y puede enviar copias de sí mismo a través de correo electrónico. Sin WormStopper, únicamente detectaría la presencia de gusanos cuando su replicación descontrolada consumiera tantos recursos del sistema que redujeran su rendimiento o detuvieran tareas.

El mecanismo de protección de WormStopper detecta, notifica y bloquea la actividad sospechosa. La actividad sospechosa puede incluir las acciones siguientes en el equipo:

- Intento de reenviar correo electrónico a un buen número de contactos de la libreta de direcciones.
- Intentos de reenviar varios mensajes de correo electrónico en rápida sucesión.

Si configura ActiveShield para que utilice la opción predeterminada **Activar WormStopper (recomendado)** en el cuadro de diálogo **Opciones avanzadas**, WormStopper supervisará la actividad del correo electrónico para detectar patrones sospechosos y le avisará cuando se supere un número concreto de mensajes o destinatarios dentro del intervalo especificado.

Para configurar ActiveShield de modo que analice en los mensajes de correo electrónico actividades características de los gusanos:

1. Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y, a continuación, haga clic en **Opciones**.
2. Haga clic en **Avanzadas** y, a continuación, en la ficha **Correo electrónico**.
3. Haga clic en **Activar WormStopper (recomendado)** (figura 3-3).

   De forma predeterminada están activadas las siguientes opciones detalladas:

   - Activar coincidencia de patrones (recomendado).
   - Avisarme cuando se envíe un mensaje de correo electrónico a 40 o más destinatarios
   - Avisarme cuando se envíen 5 mensajes de correo electrónico en un lapso de 30 segundos

     NOTA
     Si modifica el número de destinatarios o de segundos en la supervisión de mensajes de correo enviados, se podrían realizar detecciones no válidas. McAfee recomienda que haga clic en **No** para conservar el valor predeterminado. En caso contrario, haga clic en **Sí** para cambiar la configuración predeterminada al valor que prefiera.

Esta opción se puede activar automáticamente después de la primera vez que se detecta un posible gusano (consulte *Gestión de gusanos potenciales* en la página 62 para obtener información detallada):

- Bloqueo automático de mensajes de correo electrónico saliente sospechosos

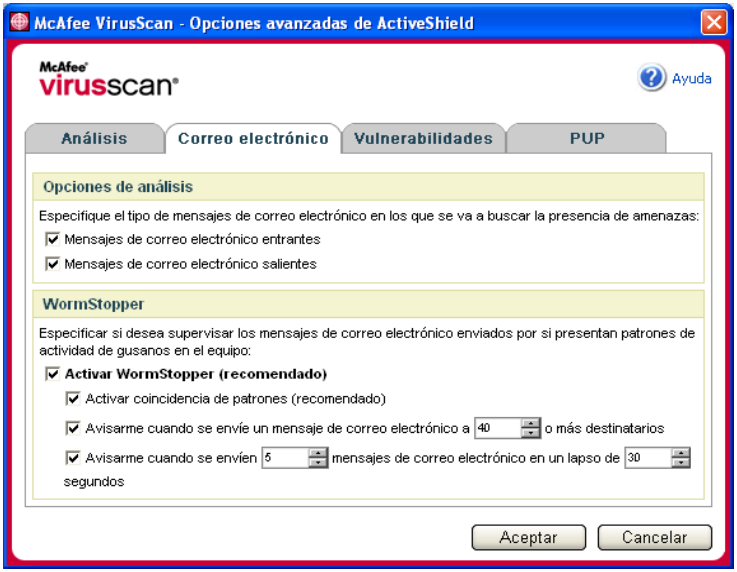


Figura 3-3. Opciones avanzadas de ActiveShield: ficha Correo electrónico

Análisis de archivos adjuntos de mensajes instantáneos entrantes

De forma predeterminada, el análisis de los archivos adjuntos de los mensajes instantáneos se activa con la opción **Analizar archivos adjuntos de los mensajes instantáneos de entrada** (figura 3-1 en la página 50).

Cuando esta opción está activada, VirusScan analiza y trata de limpiar automáticamente los archivos adjuntos de los mensajes instantáneos entrantes de los programas de mensajería instantánea más conocidos, incluidos los siguientes:

- MSN Messenger 6.0 o posterior
- Yahoo Messenger 4.1 o posterior
- AOL Instant Messenger 2.1 o posterior

NOTA
Como medida de protección, no es posible desactivar la limpieza automática de los archivos adjuntos de los mensajes instantáneos.

Si el archivo adjunto de un mensaje instantáneo entrante ha sido detectado, VirusScan realiza el procedimiento siguiente:

- Intenta limpiar el mensaje detectado.
- Si el mensaje no puede limpiarse, pregunta al usuario si lo pone en cuarentena o lo elimina.

Análisis de todos los archivos

Si se ha configurado ActiveShield para utilizar la opción predeterminada **Todos los archivos (recomendado),** se analizarán se analizarán todos los tipos de archivos que utilice su equipo al intentar usarlos. Utilice esta función para obtener el máximo provecho posible del análisis.

Para configurar ActiveShield de modo que analice todos los tipos de archivo:

1. Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y, a continuación, haga clic en **Opciones**.
2. Haga clic en **Avanzadas** y, a continuación, en la ficha **Análisis** (figura 3-4 en la página 57).

3 Haga clic en **Todos los archivos (recomendado)** y, a continuación, en **Aceptar**.

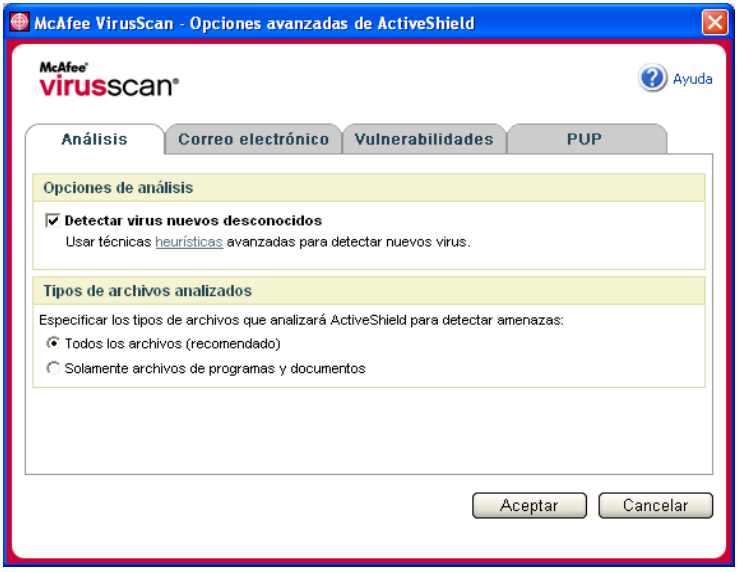


Figura 3-4. Opciones avanzadas de ActiveShield: ficha Análisis

Análisis exclusivo de archivos de programas y documentos

Si configura ActiveShield para que utilice la opción **Solamente archivos de programas y documentos**, no se analizará ningún otro tipo de archivo utilizado por el equipo. El archivo de definición de virus más actualizado (archivo DAT) determina qué tipo de archivos analizará ActiveShield. Para definir ActiveShield de modo que analice únicamente documentos y archivos de programa:

1 Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y, a continuación, haga clic en **Opciones**.

2 Haga clic en **Avanzadas** y, a continuación, en la ficha **Análisis** (figura 3-4).

3 Haga clic en **Solamente archivos de programas y documentos** y, a continuación, en **Aceptar**.

Detección de virus nuevos desconocidos

Si configura ActiveShield para que utilice la opción predeterminada **Detectar virus nuevos desconocidos**, se emplearán técnicas heurísticas que comparan los archivos con las definiciones de virus conocidos y también buscan signos que revelen la presencia de virus no identificados en los archivos.

Para configurar ActiveShield de modo que detecte los virus nuevos desconocidos:

1. Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y, a continuación, haga clic en **Opciones**.
2. Haga clic en **Avanzadas** y, a continuación, en la ficha **Análisis** (figura 3-4).
3. Haga clic en **Detectar virus nuevos desconocidos** y, a continuación, en **Aceptar**.

Análisis de secuencias de comandos

VirusScan supervisa el equipo para analizar la actividad sospechosa que pueda indicar la presencia de una amenaza. Mientras VirusScan limpia los virus y otras amenazas, ScriptStopper™ evita que los archivos troyanos ejecuten secuencias de comandos que puedan aumentar la propagación de virus.

Un "caballo de Troya" o "troyano" es un programa sospechoso que se hace pasar por una aplicación benigna. Los troyanos no son virus porque no se replican, pero pueden ser igual de destructivos.

El mecanismo de protección de ScriptStopper detecta, notifica y bloquea la actividad sospechosa. La actividad sospechosa puede incluir la acción siguiente en el equipo:

- Ejecución de una secuencia de comandos que provoque la creación, copia o eliminación de archivos, o bien la apertura del registro de Windows.

Si configura ActiveShield para que utilice la opción predeterminada **Activar ScriptStopper (recomendado)** en el cuadro de diálogo **Opciones avanzadas**, ScriptStopper supervisará la actividad de la secuencia de comandos para detectar patrones sospechosos y le avisará cuando se supere un número concreto de mensajes o destinatarios dentro del intervalo especificado.

Para configurar ActiveShield de modo que analice secuencias de comandos en ejecución para detectar actividades características de los gusanos:

1. Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y, a continuación, haga clic en **Opciones**.
2. Haga clic en **Avanzadas** y, a continuación, en la ficha **Vulnerabilidades** (figura 3-5).

3 Haga clic en **Activar ScriptStopper (recomendado)** y, a continuación, en **Aceptar**.

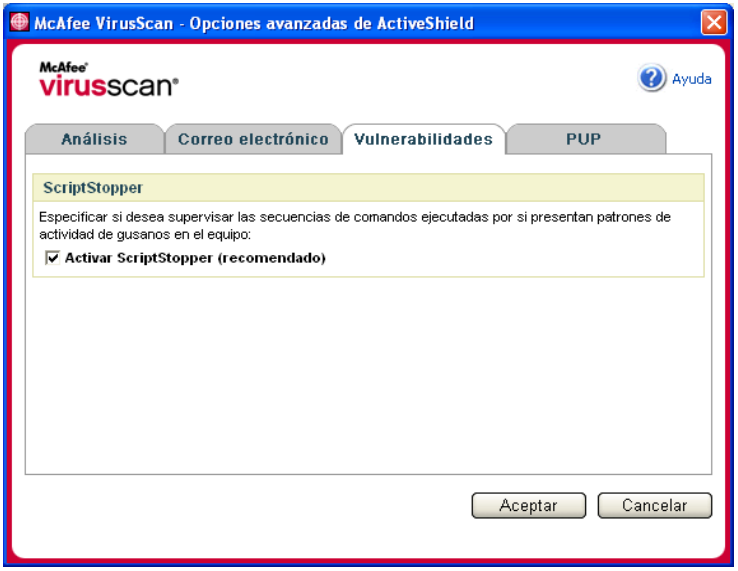


Figura 3-5. Opciones avanzadas de ActiveShield: ficha Vulnerabilidades

Análisis de programas potencialmente no deseados (PUP)

NOTA
Si McAfee AntiSpyware está instalado en el equipo, gestiona toda la actividad de programas potencialmente no deseados. Abra McAfee AntiSpyware para configurar las opciones personales.

Si configura ActiveShield para que utilice la opción predeterminada **Analizar programas potencialmente no deseados (recomendado)** del cuadro de diálogo **Opciones avanzadas de ActiveShield**, la protección frente a programas potencialmente no deseados (PUP) detecta, bloquea y elimina rápidamente spyware, adware y otro software dañino que obtiene y transmite datos privados sin su autorización.

Para configurar ActiveShield de modo que analice PUP:

1 Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y, a continuación, haga clic en **Opciones**.

2 Haga clic en **Avanzadas** y, a continuación, en la ficha **PUP** (figura 3-6).

3 Haga clic en **Analizar programas potencialmente no deseados (recomendado)** y, a continuación, en **Aceptar**.

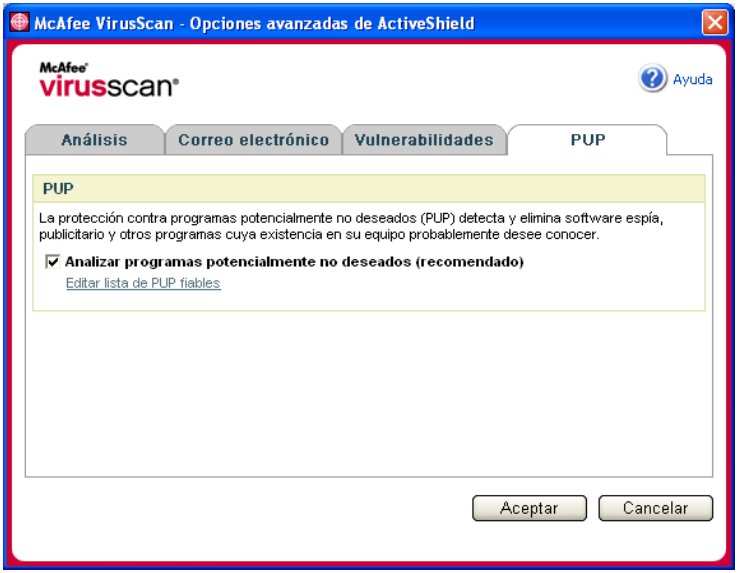


Figura 3-6. Opciones avanzadas de ActiveShield: ficha PUP

Descripción de las alertas de seguridad

Si ActiveShield descubre un virus, aparecerá una alerta similar a esta: figura 3-7. ActiveShield intenta limpiar automáticamente la mayor parte de los virus, archivos troyanos y gusanos y muestra una alerta. En el caso de programas potencialmente no deseados (PUP), ActiveShield detecta el archivo, lo bloquea automáticamente y le muestra una alerta.

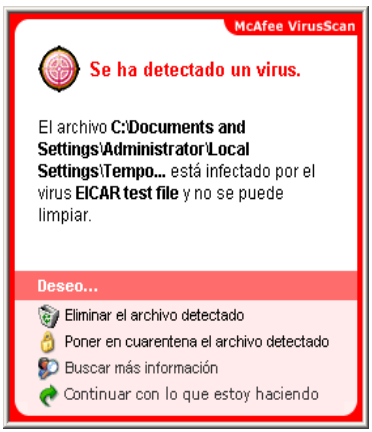


Figura 3-7. Alerta de virus

A continuación, puede elegir cómo desea gestionar los archivos detectados, el correo electrónico detectado, las secuencias de comandos sospechosas y los posibles gusanos o PUP; si lo desea, también puede enviar los archivos detectados a los laboratorios de McAfee AVERT para su investigación.

Para conseguir una protección adicional, siempre que ActiveShield detecta un archivo sospechoso le pedirá inmediatamente que inicie un análisis de todo el equipo. A menos que elija ocultar la petición de análisis, ésta se lo recordará periódicamente hasta que realice el análisis.

Gestión de archivos detectados

1 Si ActiveShield es capaz de limpiar el archivo, puede obtener más información al respecto o hacer caso omiso de la alerta:

- Haga clic en **Buscar más información** para ver el nombre del archivo, la ubicación y el nombre del virus asociado al archivo detectado.
- Haga clic en **Continuar con lo que estoy haciendo** para hacer caso omiso de a alerta y cerrarla.

2 Si ActiveShield no puede limpiar el archivo, haga clic en **Poner en cuarentena el archivo detectado** para cifrar y aislar temporalmente los archivos sospechosos en el directorio de cuarentena hasta que se pueda tomar una medida oportuna.

Aparecerá un mensaje de confirmación y se le pedirá que examine su equipo en busca de amenazas. Haga clic en **Analizar** para completar el proceso de cuarentena.

3 Si ActiveShield no puede poner el archivo en cuarentena, haga clic en **Eliminar el archivo detectado** para intentar eliminar el archivo.

Gestión del correo electrónico detectado

De forma predeterminada, el análisis de correo electrónico intenta limpiar automáticamente los mensajes detectados. Un archivo de alerta, que se incluye en el mensaje entrante, le notifica si el correo electrónico se ha limpiado, se ha puesto en cuarentena o se ha eliminado.

Administración de secuencias de comandos sospechosas

Si ActiveShield detecta una secuencia de comandos sospechosa, puede obtener más información y, a continuación, detener la secuencia de comandos si no tenía intención de iniciarla:

- Haga clic en **Buscar más información** para ver el nombre, la ubicación y la descripción de la actividad asociada a la secuencia de comandos sospechosa.
- Haga clic en **Detener esta secuencia de comandos** para evitar la ejecución de la secuencia de comandos sospechosa.

Si está seguro de que la secuencia de comandos es fiable, puede permitir que se ejecute:

- Haga clic en **Permitir este guión esta vez** para dejar que todas las secuencias de comandos contenidas en un archivo concreto se ejecuten una vez.
- Haga clic en **Continuar con lo que estoy haciendo** para hacer caso omiso de la alerta y dejar que se ejecute la secuencia de comandos.

Gestión de gusanos potenciales

Si ActiveShield detecta un gusano potencial, puede obtener más información y detener la actividad de correo electrónico si no tenía intención de iniciarla:

- Haga clic en **Buscar más información** para ver la lista de destinatarios, el asunto, el cuerpo del mensaje y la descripción de la actividad sospechosa asociados al mensaje de correo electrónico detectado.
- Haga clic en **Detener este mensaje de correo electrónico** para evitar que el mensaje sospechoso se envíe y eliminarlo de la cola de mensajes.

Si está seguro de que la actividad de correo electrónico es fiable, haga clic en **Continuar con lo que estoy haciendo** para hacer caso omiso de la alerta y permitir el envío del mensaje.

Gestión de PUP

Si ActiveShield detecta y bloquea un programa potencialmente no deseado (PUP), puede obtener más información y eliminar el programa si no tenía intención de instalarlo:

- Haga clic en **Buscar más información** para ver el nombre, la ubicación y la acción recomendada asociados al archivo PUP.
- Haga clic en **Eliminar este PUP** para eliminar el programa si no pretendía instalarlo.

  Aparece un mensaje de confirmación.

  - Si (a) no reconoce el PUP o (b) no lo instaló como parte de un paquete de programas ni aceptó un acuerdo de licencia relacionado con tales programas, haga clic en **Aceptar** para eliminar el programa utilizando el método de eliminación de McAfee.

  - En caso contrario, haga clic en **Cancelar** para salir del proceso de eliminación automático. Si cambia de opinión más adelante, puede eliminar el programa manualmente utilizando el desinstalador de ese producto.
- Haga clic en **Continuar con lo que estoy haciendo** para hacer caso omiso de la alerta y bloquear el programa esta vez.

Si (a) reconoce el PUP o (b) puede haberlo instalado como parte de un paquete de programas o haber aceptado un acuerdo de licencia relacionado con tales programas, puede permitir que se ejecute:

- Haga clic en **Definir como PUP fiable** para agregar este programa a la lista blanca y permitir siempre su ejecución en el futuro.

  Para obtener más información, consulte "*Gestión de PUP fiables*".

Gestión de PUP fiables

McAfee VirusScan no detectará ningún programa que agregue a la lista de PUP fiables.

Un PUP que se detecta y agrega a la lista de PUP fiables, puede eliminarse posteriormente de esta lista.

Si la lista de PUP fiables está llena, será necesario eliminar algunos elementos antes de poder definir como fiable otro archivo PUP.

Para eliminar un programa de la lista de PUP fiables:

1. Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y, a continuación, haga clic en **Opciones**.
2. Haga clic en **Avanzadas** y, a continuación, en la ficha **PUP**.
3. Haga clic en **Editar lista de PUP fiables**, seleccione la casilla de verificación que aparece delante del nombre de archivo y haga clic en **Eliminar**. Cuando haya terminado de eliminar elementos, haga clic en **Aceptar**.

Análisis manual del equipo

La función Analizar permite buscar selectivamente virus y otras amenazas en discos duros, disquetes, y archivos y carpetas individuales. Cuando Analizar localiza un archivo sospechoso, intenta limpiarlo automáticamente, a menos que se trate de un programa potencialmente no deseado. Si Analizar no puede limpiar el archivo, puede elegir ponerlo en cuarentena o eliminarlo.

Análisis manual para detectar virus y otras amenazas

Para analizar su equipo:

1 Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y haga clic en **Analizar**.

Se abrirá el cuadro de diálogo **Analizar** (figura 3-8).

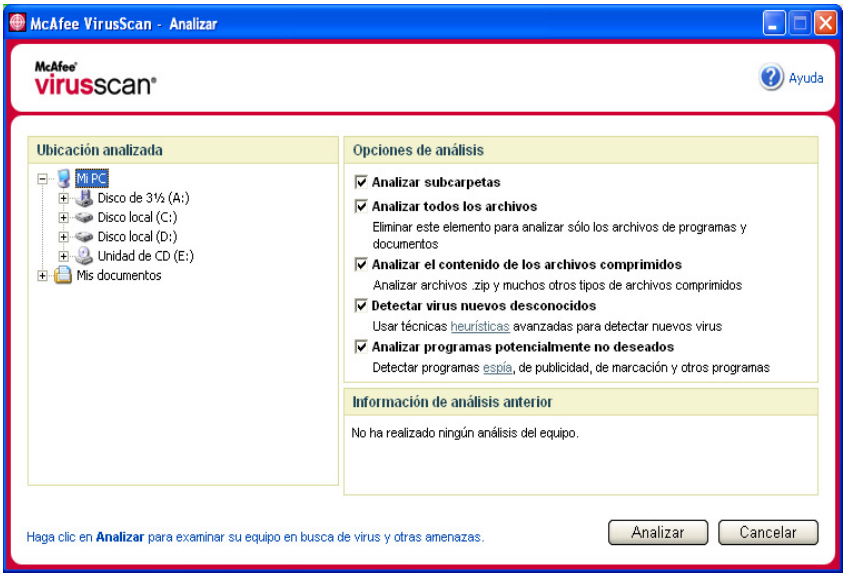


Figura 3-8. Cuadro de diálogo Analizar

2 Haga clic en la unidad, la carpeta o el archivo que desea analizar.

3 Seleccione las **Opciones de análisis** deseadas. De manera predeterminada, todas las **Opciones de análisis** están preseleccionadas para aplicar el análisis más completo (figura 3-8):

- **Analizar subcarpetas**: utilice esta opción para analizar los archivos incluidos en subcarpetas. Anule la selección de esta casilla de verificación para analizar únicamente los archivos visibles al abrir una carpeta o unidad.

  Ejemplo: Los archivos de la figura 3-9 son los únicos que se analizarán si se anula la selección de la casilla de verificación **Analizar subcarpetas**. Las carpetas y sus contenidos no se analizarán. Para analizar dichas carpetas y sus contenidos, debe dejar marcada la casilla de verificación.

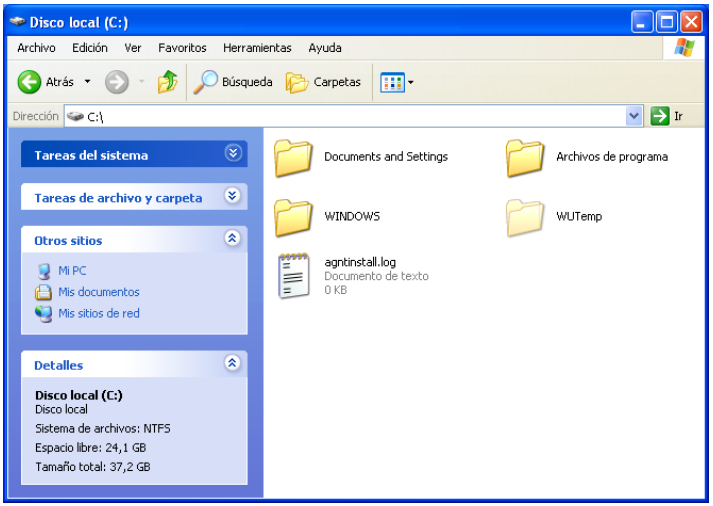


Figura 3-9. Contenido del disco local

- **Analizar todos los archivos**: utilice esta opción para realizar un análisis completo de todos los tipos de archivos. Anule la selección de esta casilla de verificación para reducir el tiempo de análisis y examinar únicamente los archivos de programas y documentos.

- **Analizar el contenido de los archivos comprimidos**: utilice esta opción para encontrar archivos ocultos dentro de archivos .ZIP y otros archivos comprimidos. Anule la selección de esta casilla de verificación para no analizar ningún archivo (comprimido o no) incluido dentro del archivo comprimido.

  En ocasiones, los creadores de virus colocan virus en un archivo .ZIP y, a su vez, insertan este archivo .ZIP dentro de otro archivo .ZIP con el objeto de intentar eludir la acción de los analizadores antivirus. La función Analizar los puede detectar si esta opción está seleccionada.

- **Detectar virus nuevos desconocidos** : utilice esta opción para encontrar los virus más recientes, para los que puede suceder que no se haya desarrollado aún el "antídoto". Esta opción utiliza técnicas heurísticas que comparan archivos con las definiciones de virus conocidos y a la vez buscan signos que denotan la presencia de virus no identificados en los archivos.

  Este método de análisis también busca atributos de archivos que normalmente puedan descartar la existencia de virus. De esta manera se minimizan las posibilidades de que la función Analizar genere una falsa alarma. Sin embargo, si un análisis heurístico detecta un virus, el archivo se debería tratar con la misma precaución como si se supiera con certeza que contiene un virus.

  Esta opción proporciona el análisis más completo, pero suele resultar más lenta que un análisis normal.

- **Analizar programas potencialmente no deseados:** utilice esta opción para detectar spyware, adware y otros programas que obtienen y transmiten datos privados sin su autorización.

  NOTA
  Deje todas las opciones seleccionadas para realizar el análisis más completo. Se analizarán todos los archivos de la unidad o carpeta seleccionada, por lo que la operación tardará bastante tiempo en completarse. Cuanto mayor sea el tamaño del disco duro y más archivos contenga, más tiempo llevará la operación de análisis.

4 Haga clic en **Analizar** para comenzar a analizar los archivos.

Cuando haya concluido el análisis, un resumen del mismo mostrará la cantidad de archivos analizados, de archivos detectados, de programas potencialmente no deseados y de archivos detectados que se limpiaron automáticamente.

5 Haga clic en **Aceptar** para cerrar el resumen y ver la lista de los archivos detectados en el cuadro de diálogo **Analizar** (figura 3-10).

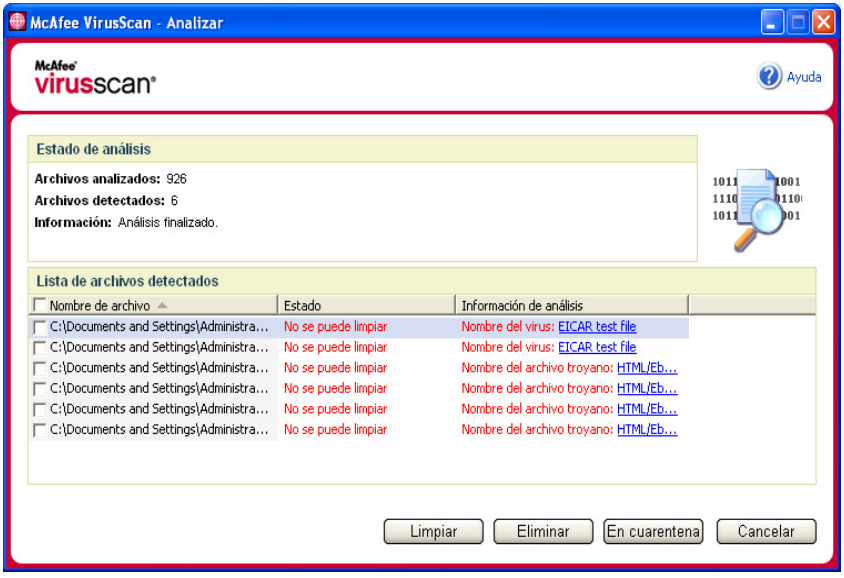


Figura 3-10. Resultados del análisis

NOTA
La función Analizar contabiliza cada archivo comprimido (.ZIP, .CAB, etc.) como un solo archivo al hacer el recuento de **Archivos analizados**. Además, el número de archivos analizados puede variar si se han eliminado los archivos temporales de Internet desde el último análisis.

6 Si la función Analizar detecta virus ni ninguna otra amenaza, haga clic en **Atrás** para seleccionar otra unidad o carpeta para analizar, o bien en **Cerrar** para cerrar el cuadro de diálogo. En cualquier otro caso, consulte *Descripción de las detecciones de amenazas* en la página 71.

Análisis mediante el Explorador de Windows

VirusScan proporciona un menú de métodos abreviados para analizar los archivos, las carpetas o las unidades seleccionados en busca de virus y de otras amenazas desde el Explorador de Windows.

Para analizar archivos en el Explorador de Windows:

1. Abra el Explorador de Windows.
2. Haga clic con el botón derecho del ratón en la unidad, la carpeta o el archivo que desea analizar y, a continuación, en **Analizar**.

   Se abrirá el cuadro de diálogo **Analizar** y se iniciará el análisis de los archivos. De manera predeterminada, todas las **Opciones de análisis** están preseleccionadas para aplicar el análisis más completo (figura 3-8 en la página 64).

Análisis mediante Microsoft Outlook

VirusScan proporciona un icono de la barra de herramientas para analizar la presencia de virus y de otras amenazas en los almacenes de mensajes seleccionados y sus subcarpetas, las carpetas de correo o los mensajes de correo electrónico que contengan archivos adjuntos desde el propio Microsoft Outlook 97 o una versión posterior.

Para analizar el correo electrónico en Microsoft Outlook:

1. Abra Microsoft Outlook.
2. Haga clic en el almacén de mensajes, la carpeta o el mensaje de correo electrónico que contenga un archivo adjunto que desee analizar y haga clic en el icono de análisis de correo electrónico de la barra de herramientas  .

   Se abrirá el analizador de correo electrónico y empezará a analizar los archivos. De manera predeterminada, todas las **Opciones de análisis** están preseleccionadas para aplicar el análisis más completo (figura 3-8 en la página 64).

Análisis automático en busca de virus y otras amenazas

Aunque VirusScan analiza los archivos cuando el usuario o el equipo tienen acceso a ellos, puede programar la función de análisis automático en la ventana Programador de tareas de Windows para analizar el equipo exhaustivamente en busca de virus y otras amenazas a intervalos especificados.

Para programar un análisis:

1 Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y, a continuación, haga clic en **Opciones**.

Se abrirá el cuadro de diálogo **VirusScan - Opciones**.

2 Haga clic en la ficha **Análisis programado** (figura 3-11 en la página 69).

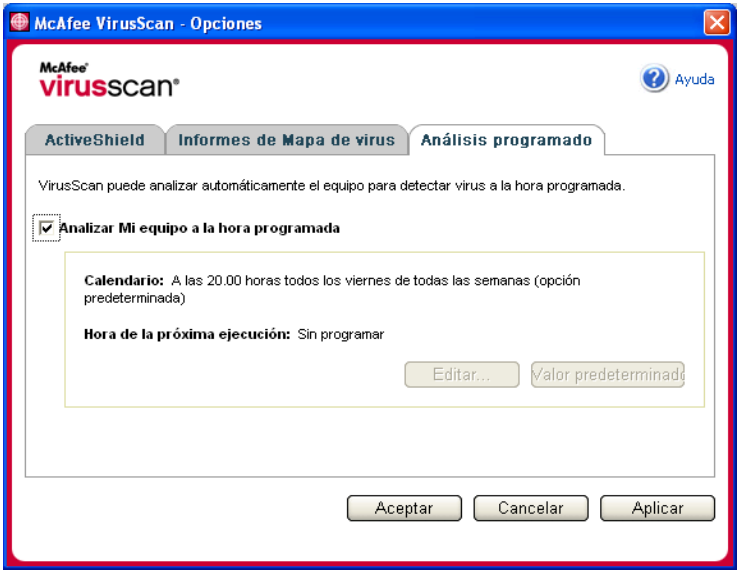


Figura 3-11. Opciones - Análisis programado

3 Marque la casilla de verificación **Analizar Mi equipo a la hora programada** para activar el análisis automático.

4 Especifique una programación para el análisis automático:

- Para aceptar la programación predeterminada (los viernes a las 20:00 horas), haga clic en **Aceptar**.
- Para modificar la programación:

  a. Haga clic en **Editar**.

  b. Seleccione la frecuencia con la que desea analizar el equipo en la lista **Programar tarea** y seleccione las opciones adicionales en el área dinámica situada debajo:

  Diariamente: especifique el número de días entre análisis.

  Semanalmente (opción predeterminada): especifique el número de semanas entre análisis, así como los nombres de los días de la semana.

  Mensualmente: especifique qué día del mes desea realizar el análisis. Haga clic en **Seleccionar meses** para especificar en qué meses desea realizar el análisis y haga clic en **Aceptar**.

  Sólo una vez: especifique en qué fecha desea realizar el análisis.

  NOTA
  No se admiten estas opciones del Programador de tareas de Windows:
  Al iniciar el sistema, **Cuando esté inactivo** y **Mostrar todas las programaciones**. El último programa admitido permanecerá activado hasta que seleccione otra opción válida.

  c. Seleccione la hora del día en la que analizar el equipo en el cuadro **Hora de inicio**.

  d. Para seleccionar opciones avanzadas, haga clic en **Opciones avanzadas**.

  Se abrirá el cuadro de diálogo **Opciones de programación avanzadas**.

  i. Especifique una fecha de inicio, una fecha de finalización, la duración y una hora de finalización. También puede especificar si se detiene la tarea a una determinada hora en caso de que el análisis esté todavía en ejecución.

  ii. Haga clic en **Aceptar** para guardar los cambios y cerrar el cuadro de diálogo. En caso contrario, haga clic en **Cancelar**.

5 Haga clic en **Aceptar** para guardar los cambios y cerrar el cuadro de diálogo. En caso contrario, haga clic en **Cancelar**.

6 Si desea restablecer la programación predeterminada, haga clic en **Valor predeterminado**. De lo contrario, haga clic en **Aceptar**.

Descripción de las detecciones de amenazas

La función Analizar intenta limpiar automáticamente la mayor parte de los virus, troyanos y gusanos de los archivos. A continuación, puede elegir la forma de gestionar los archivos detectados, incluso si desea enviarlos a los laboratorios de McAfee AVERT para su investigación. Si la función Analizar detecta un programa potencialmente no deseado, puede intentar limpiarlo manualmente, ponerlo en cuarentena o eliminarlo (envío a AVERT no disponible).

Para gestionar un virus o un programa potencialmente no deseado:

1 Si aparece un archivo en la **Lista de archivos Detectados**, haga clic en la casilla de verificación situada delante del archivo para seleccionarlo.

> **NOTA**
> Si la lista contiene más de un archivo, puede marcar la casilla de verificación situada delante de la lista **Nombre de archivo** para aplicar la misma acción a todos los archivos. También puede hacer clic en el nombre del archivo en la lista **Información de análisis** para ver los detalles de la biblioteca de información de virus.

2 Si el archivo es un programa potencialmente no deseado, puede hacer clic en **Limpiar** para intentar limpiarlo.

3 Si la función Analizar no consigue limpiar el archivo, haga clic en **En cuarentena** para cifrar y aislar temporalmente los archivos sospechosos en el directorio de cuarentena hasta que se pueda tomar una acción oportuna. (Para obtener más información, consulte *Gestión de archivos en cuarentena* en la página 72.)

4 Si la función Analizar no puede limpiar el archivo o ponerlo en cuarentena, puede realizar una de las acciones siguientes:

- Haga clic en **Eliminar** para eliminar el archivo.
- Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin aplicar ninguna otra medida.

Si la función Analizar no puede limpiar ni eliminar el archivo detectado, consulte la biblioteca de información de virus en http://es.mcafee.com/virusInfo/ para obtener instrucciones sobre la eliminación manual de archivos.

Si el archivo detectado no permite utilizar la conexión a Internet o impide usar el equipo, pruebe a utilizar un disco de emergencia para iniciarlo. En muchos casos, el disco de emergencia permite iniciar un equipo inutilizado por un archivo detectado. Para obtener más información, consulte *Creación de un disco de emergencia* en la página 74.

Si desea obtener ayuda adicional, póngase en contacto con el equipo de soporte técnico de McAfee en http://www.mcafeeayuda.com/.

Gestión de archivos en cuarentena

La función En cuarentena cifra y aísla temporalmente los archivos sospechosos en el directorio de cuarentena hasta que se pueda adoptar una medida conveniente. Una vez limpio, puede restablecer en su ubicación original el archivo que estaba en cuarentena.

Para gestionar un archivo que se ha puesto en cuarentena:

1 Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y después haga clic en **Administración de archivos en cuarentena**.

Aparecerá una lista de archivos en cuarentena (figura 3-12).

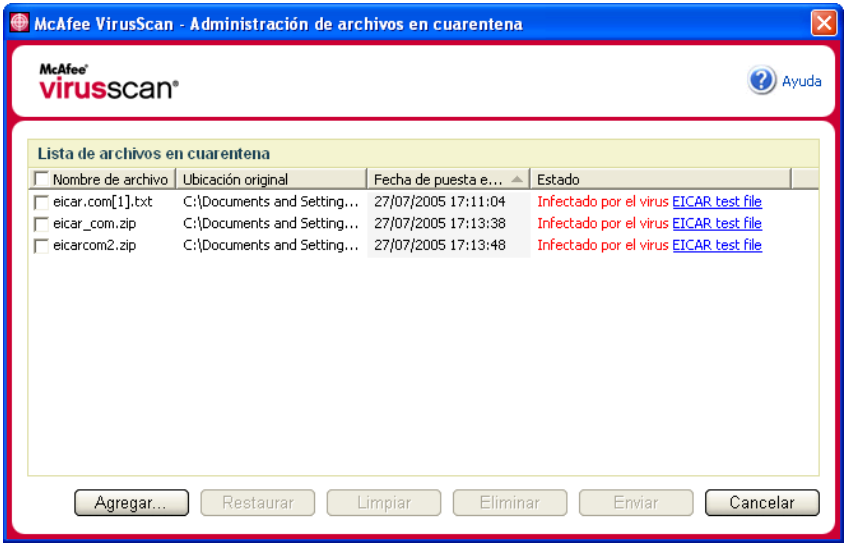


Figura 3-12. Cuadro de diálogo Administración de archivos en cuarentena

2 Marque la casilla de verificación situada junto a los archivos que desea limpiar.

NOTA
Si la lista contiene más de un archivo, puede marcar la casilla de verificación situada delante de la lista **Nombre de archivo** para aplicar la misma acción a todos los archivos. También puede hacer clic en el nombre del virus en la lista **Estado** para ver los detalles de la biblioteca de información de virus.

O bien, puede hacer clic en **Agregar**, seleccionar el archivo sospechoso para agregarlo a la lista de cuarentena, hacer clic en **Abrir** y, a continuación, seleccionarlo en la lista de cuarentena.

3 Haga clic en **Limpiar**.

4 Si el archivo está limpio, haga clic en **Restaurar** para devolverlo a su ubicación original.

5 Si VirusScan no puede limpiar el virus, haga clic en **Eliminar** para eliminar el archivo.

6 Si VirusScan no puede limpiar ni eliminar el archivo, y si no se trata de un programa potencialmente no deseado, puede enviarlo para su investigación a AVERT™ (siglas en inglés de McAfee AntiVirus Emergency Response Team o Equipo de respuesta de emergencia antivirus de McAfee):

   a Actualice los archivos de definición de virus si tienen más de dos semanas de antigüedad.

   b Compruebe su suscripción.

   c Seleccione el archivo y haga clic en **Enviar** para enviar el archivo a AVERT.

   VirusScan enviará el archivo infectado como archivo adjunto con un mensaje de correo electrónico que contendrá la dirección de correo electrónico del usuario, el país, la versión de software, el sistema operativo, el nombre original del archivo y su ubicación. El volumen máximo del envío es de un archivo de 1,5 MB por día.

7 Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin aplicar ninguna otra medida.

Creación de un disco de emergencia

Disco de emergencia es una utilidad que crea un disquete de arranque que se puede utilizar para iniciar el equipo y detectar los virus que contenga, en caso de que un virus no permita su inicio con normalidad.

> **NOTA**
> Para descargar la imagen del disco de emergencia es necesario estar conectado a Internet. Disco de emergencia sólo está disponible para equipos con particiones de disco duro FAT (FAT 16 y FAT 32). No es necesario para particiones NTFS.

Para crear un disco de emergencia:

1. Inserte un disquete no infectado en la unidad A de un equipo no infectado. Puede utilizar la función Analizar para asegurarse de que el equipo y el disquete están limpios de virus. (Para obtener más información, consulte *Análisis manual para detectar virus y otras amenazas* en la página 64.)

2. Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y haga clic en **Crear disco de emergencia**.

   Se abrirá el cuadro de diálogo **Crear disco de emergencia** (figura 3-13).

Figura 3-13. Cuadro de diálogo Crear disco de emergencia

3. Haga clic en **Crear** para crear el disco de emergencia.

   Si es la primera vez que crea un disco de emergencia, aparecerá un mensaje que indica que la utilidad Disco de emergencia necesita descargar su archivo de imagen. Haga clic en **Aceptar** para descargar el componente ahora o en **Cancelar** para hacerlo más adelante.

   Un mensaje de advertencia le indicará que perderá el contenido actual del disquete.

4 Haga clic en **Sí** para crear el disco de emergencia.

El cuadro de diálogo **Crear disco de emergencia** mostrará el progreso del estado de creación.

5 Cuando aparezca un mensaje que indica que se ha creado el disco de emergencia, haga clic en **Aceptar** y cierre el cuadro de diálogo **Crear disco de emergencia**.

6 Extraiga el disco de emergencia de la unidad, protéjalo contra escritura y guárdelo en un lugar seguro.

Protección de un disco de emergencia contra escritura

Para proteger un disco de emergencia contra escritura:

1 Dé la vuelta al disquete (debería ver el círculo metálico del disquete).

2 Busque la pestaña de protección contra escritura. Deslice la pestaña de manera que se vea el orificio.

Utilización de un disco de emergencia

Para usar un disco de emergencia:

1 Apague el equipo infectado.

2 Inserte el disco de emergencia en la unidad.

3 Encienda el equipo.

Aparecerá una ventana de color gris con varias opciones.

4 Elija la opción que mejor se adapte a sus necesidades pulsando las teclas de función (por ejemplo, F2, F3).

NOTA
El disco de emergencia se iniciará automáticamente en 60 segundos si no pulsa ninguna de las teclas.

Actualización de un disco de emergencia

Es conveniente actualizar periódicamente el disco de emergencia. Para ello, siga las mismas instrucciones indicadas para crear un disco de emergencia nuevo.

Información automática sobre virus

Puede enviar información de rastreo de virus de manera anónima para su inclusión en el World Virus Map. Participe automáticamente en esta función de protección gratuita durante la instalación de VirusScan (en el cuadro de diálogo **Informes de Mapa de virus**) o en cualquier otro momento en la ficha **Informes de Mapa de virus** del cuadro de diálogo **VirusScan - Opciones**.

Envío de información al World Virus Map

Para enviar automáticamente información sobre virus al World Virus Map:

1 Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y, a continuación, haga clic en **Opciones**.

Se abrirá el cuadro de diálogo **VirusScan - Opciones**.

2 Haga clic en la ficha **Informes de Mapa de virus** (figura 3-14).

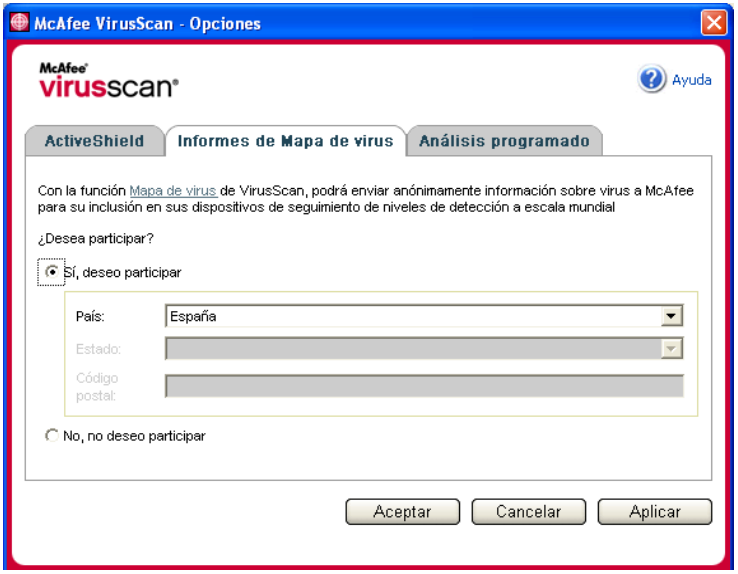


Figura 3-14. Opciones - Informes de Mapa de virus

3 Acepte la opción predeterminada **Sí, deseo participar** para enviar información sobre virus de manera anónima a McAfee para incorporarla al World Virus Map que incluye los niveles de detección a escala mundial. En caso contrario, seleccione **No, no deseo participar** para no enviar ninguna información.

4 Si reside en Estados Unidos, seleccione el estado y escriba el código postal correspondiente a la ubicación física del equipo. En caso contrario, VirusScan tratará de seleccionar automáticamente el país en el que se encuentra el equipo.

5 Haga clic en **Aceptar**.

Visualización del World Virus Map

Independientemente de si participa en el World Virus Map, puede consultar los últimos índices de detecciones a escala mundial por medio del icono de McAfee situado en la bandeja del sistema de Windows.

Para ver el World Virus Map:

- Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y, a continuación, haga clic en **World Virus Map**.

  Aparecerá la página Web de **World Virus Map** (figura 3-15).

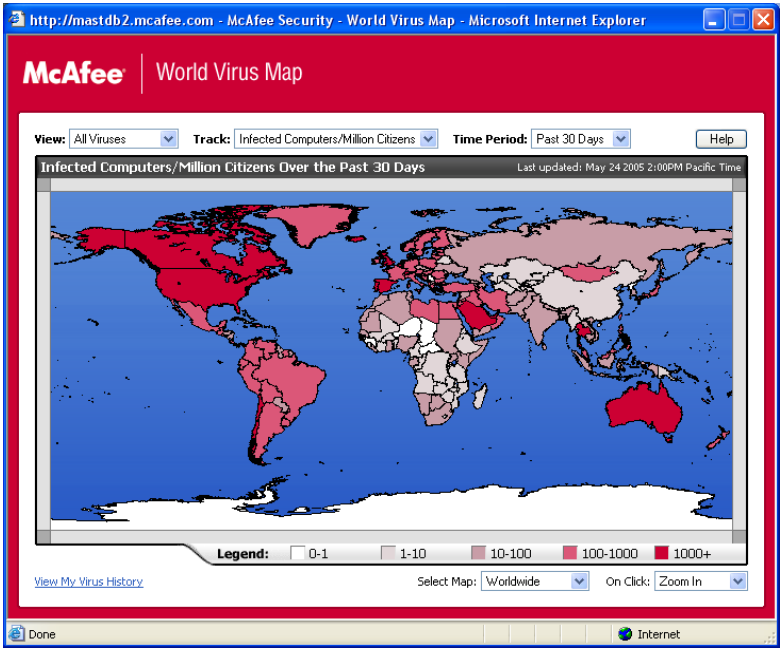


Figura 3-15. World Virus Map

De manera predeterminada, el World Virus Map muestra un conjunto de equipos detectados en todo el mundo en los últimos 30 días y en el momento en el que se actualizó la última información. Puede cambiar la vista del mapa para mostrar el número de archivos detectados o cambiar el período de tiempo para mostrar únicamente los resultados de los últimos 7 días o de las pasadas 24 horas.

La sección de rastreo de virus enumera los totales acumulados correspondientes a los archivos examinados y a los archivos y equipos detectados sobre los que se ha recibido información desde la fecha indicada.

Actualización de VirusScan

Mientras está conectado a Internet, VirusScan comprueba automáticamente cada cuatro horas si hay alguna actualización disponible y se encarga de descargar e instalar automáticamente las actualizaciones de definición de virus sin interrumpir su trabajo.

Los archivos de definición de virus suelen tener unos 100 KB y su descarga apenas afecta al rendimiento del sistema.

Si se ha actualizado un producto o se ha producido un brote de virus, aparecerá una alerta. Tras recibir la alerta, puede elegir actualizar VirusScan para eliminar la amenaza de un virus.

Comprobación automática de actualizaciones

McAfee SecurityCenter está configurado para buscar automáticamente actualizaciones de todos sus servicios de McAfee cada cuatro horas mientras haya conexión a Internet para, a continuación, notificarlo mediante alertas y sonidos. De forma predeterminada, SecurityCenter descarga e instala automáticamente cualquier actualización disponible.

NOTA
En algunos casos, se le pedirá que reinicie el equipo para completar la actualización. Asegúrese de guardar todo el trabajo y de cerrar las aplicaciones antes de reiniciar el equipo.

Comprobación manual de actualizaciones

Además de comprobar automáticamente las actualizaciones cada cuatro horas cuando esté conectado a Internet, también puede comprobar actualizaciones manualmente cuando así lo desee.

Para comprobar manualmente la existencia de actualizaciones de VirusScan:

1. Asegúrese de que el equipo está conectado a Internet.
2. Haga clic con el botón derecho del ratón en el icono de McAfee y seleccione **Actualizaciones**.

   Se abrirá el cuadro de diálogo **Actualizaciones de SecurityCenter**.
3. Haga clic en **Comprobar**.

   Si existiese una actualización, se abriría el cuadro de diálogo **Actualizaciones de VirusScan** (figura 3-16 en la página 79). Haga clic en **Actualizar** para continuar.

Si no hay actualizaciones disponibles, aparecerá un cuadro de diálogo que le indicará que VirusScan está actualizado. Haga clic en **Aceptar** para cerrar el cuadro de diálogo.

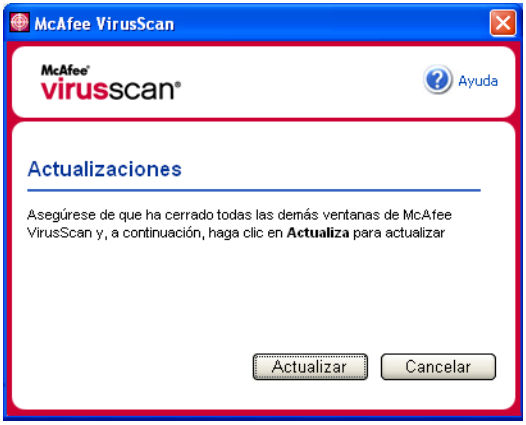


Figura 3-16. Cuadro de diálogo Actualizaciones

4 Regístrese en el sitio Web si así se le pide. El **Asistente para actualizaciones** instalará la actualización automáticamente.

5 Haga clic en **Finalizar** cuando la actualización haya terminado de instalarse.

NOTA
En algunos casos, se le pedirá que reinicie el equipo para completar la actualización. Asegúrese de guardar todo el trabajo y de cerrar las aplicaciones antes de reiniciar el equipo.

McAfee Personal Firewall Plus 4

Bienvenido a McAfee Personal Firewall Plus.

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

Gracias a él, disfrutará de las funciones siguientes:

- Protección contra ataques e intentos de ataque de los piratas informáticos
- Complemento de defensas antivirus
- Control de la actividad de Internet y de la red
- Alertas contra eventos potencialmente hostiles
- Información detallada sobre tráfico de Internet sospechoso
- Integración con la funcionalidad Hackerwatch.org, que incluye la elaboración de informes de eventos, herramientas de autocomprobación y la posibilidad de enviar a las autoridades en línea los sucesos recibidos.
- Funciones de rastreo y búsqueda de eventos detalladas

Funciones nuevas

- **Compatibilidad para juegos mejorada**
  McAfee Personal Firewall Plus protege su equipo de intentos de intrusión y actividades sospechosas durante juegos a toda pantalla, pero puede ocultar alertas si detecta intentos de intrusión o actividades sospechosas. Las alertas rojas aparecen después de salir del juego.

- **Gestión de acceso mejorada**
  McAfee Personal Firewall Plus permite a los usuarios conceder a las aplicaciones acceso temporal a Internet. El acceso queda restringido al tiempo que transcurre desde que se inicia la aplicación hasta que se cierra. Cuando Personal Firewall detecta un programa desconocido que trata de conectarse a Internet, una Alerta roja ofrece la opción de conceder a la aplicación acceso temporal a Internet.

- **Control de la seguridad mejorado**
  La función de bloqueo de McAfee Personal Firewall Plus permite bloquear de manera instantánea todo el tráfico entrante y saliente entre su equipo e Internet. Los usuarios pueden activar o desactivar la función de bloqueo desde tres lugares diferentes de Personal Firewall.

- **Opciones de recuperación mejoradas**
  La función Restablecer opciones permite restablecer automáticamente la configuración predeterminada de Personal Firewall. Si Personal Firewall se comporta de un modo no deseado que no se puede controlar, puede anular la configuración actual y recuperar la configuración predeterminada del producto.

- **Protección contra las conexiones a Internet**
  Para impedir que un usuario desactive de manera accidental su conexión a Internet, la opción para prohibir una dirección de Internet se excluye mediante una Alerta azul cuando Personal Firewall detecta una conexión a Internet que se origina en un servidor DHCP o DNS. Si el tráfico entrante no se origina en un servidor DHCP o DNS, aparece la opción.

- **Integración mejorada con HackerWatch.org**
  Ahora resulta más fácil que nunca informar acerca de posibles piratas informáticos. McAfee Personal Firewall Plus mejora la funcionalidad de HackerWatch.org, que incluye el envío de eventos potencialmente malintencionados a la base de datos.

- **Gestión inteligente de aplicaciones mejorada**
  Cuando una aplicación pretende acceder a Internet, Personal Firewall comprueba en primer lugar si la reconoce como fiable o malintencionada. Si Personal Firewall considera que la aplicación es de confianza, permite automáticamente su acceso a Internet sin necesidad de la intervención del usuario.

- **Detección avanzada de troyanos**
  McAfee Personal Firewall Plus combina la gestión de la conexión entre las aplicaciones con una base de datos mejorada para detectar y bloquear el acceso a Internet y la posible transmisión de sus datos personales a las aplicaciones potencialmente más peligrosas, como los troyanos.

- **Rastreo visual mejorado**
  Visual Trace incluye mapas gráficos de fácil lectura que muestran el origen del tráfico y de los ataques hostiles en todo el mundo, junto con información detallada sobre contactos y propietarios de las direcciones IP de origen.

- **Mayor facilidad de uso**
  McAfee Personal Firewall Plus incluye un Asistente para la configuración y un tutorial para guiar a los usuarios durante la configuración y utilización del cortafuegos. Aunque el producto está diseñado para su uso sin necesidad de intervención del usuario, McAfee ofrece a los usuarios un amplio número de recursos para comprender y valorar lo que el cortafuegos puede hacer por ellos.

- **Detección de intrusiones mejorada**
  El sistema de detección de intrusiones (IDS, Intrusion Detection System) de Personal Firewall detecta los patrones comunes de ataque y otras actividades sospechosas. La detección de intrusiones controla todos los paquetes de datos en busca de transferencias de datos o métodos de transferencia que resulten sospechosos, y los incluye en el registro de eventos.

- **Análisis del tráfico mejorado**
  McAfee Personal Firewall Plus permite que los usuarios vean tanto los datos que entran como los que salen de su equipo, y, además, muestra las conexiones de las aplicaciones, incluidas las que están "escuchando" conexiones abiertas. Esto permite a los usuarios ver las aplicaciones que pueden ser susceptibles de intrusión y actuar en consecuencia.

Eliminación de otros cortafuegos

Antes de instalar McAfee Personal Firewall Plus, es necesario desinstalar cualquier otro programa cortafuegos que se encuentre instalado en el equipo. Para ello, siga las instrucciones de desinstalación del programa cortafuegos que tenga instalado.

NOTA
Si utiliza Windows XP, no es necesario que desactive la función de cortafuegos incorporada antes de instalar el McAfee Personal Firewall Plus. No obstante, recomendamos que la desactive. En caso contrario, no recibirá eventos en el registro **Eventos de entrada** de McAfee Personal Firewall Plus.

Configuración del cortafuegos predeterminado

McAfee Personal Firewall Plus puede gestionar permisos y tráfico para las aplicaciones de Internet de su equipo, aún cuando se detecta que en éste se está ejecutando Firewall de Windows.

Una vez instalado, McAfee Personal Firewall desactiva automáticamente Firewall de Windows y se establece como cortafuegos predeterminado. Entonces sólo podrá utilizar la funcionalidad y los mensajes de McAfee Personal Firewall. Si posteriormente activa Firewall de Windows a través del Centro de seguridad o del Panel de control de Windows, tenga en cuenta que el funcionamiento simultáneo los dos cortafuegos en el equipo puede provocar una pérdida parcial del registro de McAfee Firewall, así como la duplicación de los mensajes de estado y de alerta.

NOTA
Si están activados los dos cortafuegos, McAfee Personal Firewall no muestra todas las direcciones IP bloqueadas en la ficha **Eventos entrantes**. Firewall de Windows intercepta la mayor parte de estos eventos y los bloquea, evitando que McAfee Personal Firewall detecte o registre dichos eventos. Sin embargo, es posible que McAfee Personal Firewall bloquee tráfico adicional en función de otros factores de seguridad, y quedará un registro de dicho tráfico.

El registro está desactivado en Firewall de Windows de forma predeterminada, pero si decide activar los dos cortafuegos, puede activarlo. El registro predeterminado de Firewall de Windows es C:\Windows\pfirewall.log

Para asegurarse de que el equipo está protegido al menos por un cortafuegos, Firewall de Windows se vuelve a activar automáticamente cuando se desinstala McAfee Personal Firewall.

Si desactiva McAfee Personal Firewall o establece el ajuste de seguridad como **Abierto** sin activar manualmente Firewall de Windows, se eliminará completamente la protección del cortafuegos excepto en el caso de las aplicaciones bloqueadas anteriormente.

Configuración del nivel de seguridad

Puede configurar las opciones de seguridad para indicar el modo en que Personal Firewall responderá cuando detecte tráfico no deseado. De forma predeterminada, se activa el nivel de seguridad **Estándar**. En el nivel de seguridad **Estándar**, cuando una aplicación solicita acceso a Internet y se le concede, le está otorgando Acceso pleno a la aplicación. El Acceso pleno permite a la aplicación enviar y recibir datos no solicitados desde un puerto que no sea del sistema.

Para definir la configuración de seguridad:

1. Haga clic con el botón derecho del ratón en el icono de McAfee de la bandeja del sistema de Windows, elija **Personal Firewall** y, a continuación, seleccione **Utilidades**.
2. Haga clic en el icono **Configuración de seguridad**.
3. Configure el nivel de seguridad moviendo el control deslizante hasta el valor deseado.

   El rango de niveles de seguridad abarca desde Bloqueado a Abierto:

   - **Bloqueado:** se cierran todas las conexiones a Internet del equipo. Puede utilizar esta opción para bloquear puertos que haya configurado para que estén abiertos en la página **Servicios del sistema**.

- **Seguridad estricta:** cuando una aplicación solicita un tipo de acceso a Internet específico (por ejemplo, Sólo acceso saliente), puede permitir o no que la aplicación se conecte a Internet. Si la aplicación solicita más adelante Acceso pleno, puede concedérselo o restringirlo a Sólo acceso saliente.
- **Seguridad estándar (recomendado):** cuando una aplicación solicita y se le concede acceso a Internet, la aplicación disfruta de acceso pleno a Internet para gestionar el tráfico entrante y saliente.
- **Seguridad fiable:** se confía automáticamente en todas las aplicaciones cuando intentan acceder por primera vez a Internet. Sin embargo, puede configurar Personal Firewall para utilizar alertas que le notifiquen sobre nuevas aplicaciones en su equipo. Utilice este valor si percibe que algunos juegos o transferencias de vídeo/audio en tiempo real no funcionan.
- **Abierto:** el cortafuegos está desactivado. Este valor de configuración permite todo el tráfico a través de Personal Firewall sin ningún tipo de filtro.

  NOTA
  Las aplicaciones previamente bloqueadas siguen bloqueadas cuando el cortafuegos se configura con el valor de seguridad **Abierto** o **Bloqueado**. Para evitar esto, puede cambiar los permisos de las aplicaciones a **Permitir acceso pleno** o simplemente eliminar la regla del permiso **Bloqueado** en la lista **Aplicaciones de Internet**.

4 Seleccione parámetros de seguridad adicionales:

  NOTA
  Si su equipo dispone de Windows XP y se han agregado varios usuarios de XP, estas opciones están disponibles únicamente si se inicia la sesión como Administrador.

- **Registrar eventos de detección de intrusiones (IDS) en registro de eventos entrantes:** si selecciona esta opción, los eventos detectados por IDS aparecerán en el registro **Eventos entrantes**. El sistema de detección de intrusiones detecta tipos de ataques comunes y otras actividades sospechosas. La detección de intrusiones controla todos los paquetes de datos entrantes y salientes en busca de transferencias de datos o métodos de transferencia sospechosos. Los compara con una base de datos de “firmas” y se deshace de los paquetes procedentes del equipo infractor.

  IDS busca patrones de tráfico específicos utilizados por los agresores. Comprueba cada paquete que recibe el equipo para detectar tráfico sospechoso o de ataques conocidos. Por ejemplo, si Personal Firewall detecta paquetes de ICMP, los analiza en busca de patrones de tráfico sospechoso comparando el tráfico de ICMP con los patrones de los ataques conocidos.

- **Aceptar solicitudes de ping ICMP**: el tráfico de ICMP se usa principalmente para llevar a cabo seguimientos y realizar solicitudes de ping. Las solicitudes de ping se utilizan habitualmente para llevar a cabo una comprobación rápida antes de iniciar las comunicaciones. Si utiliza o ha utilizado un programa de intercambio de archivos de igual a igual, es posible que el equipo reciba numerosas solicitudes de ping. Si selecciona esta opción, Personal Firewall permite todas las solicitudes de ping sin incluirlas en el registro **Eventos entrantes**. Si no selecciona esta opción, Personal Firewall bloquea todas las solicitudes de ping y las registra en el registro **Eventos entrantes**.
- **Permitir a usuarios restringidos cambiar la configuración de Personal Firewall**: si el equipo dispone de Windows XP o Windows 2000 Professional con varios usuarios de XP, seleccione esta opción para permitir que los usuarios de XP restringidos modifiquen la configuración de Personal Firewall.

5 Haga clic en **Aceptar** cuando haya terminado de realizar cambios.

Comprobación de McAfee Personal Firewall Plus

Puede comprobar si la instalación de Personal Firewall presenta posibles puntos vulnerables frente a intrusiones o actividades sospechosas.

Para comprobar la instalación de Personal Firewall desde el icono de la bandeja del sistema de McAfee:

- Haga clic con el botón derecho del ratón en el icono de McAfee  de la bandeja del sistema de Windows y seleccione **Comprobar cortafuegos**.

Personal Firewall abre Internet Explorer y se dirige a http://www.hackerwatch.org/, un sitio Web que mantiene McAfee. Siga las instrucciones de la página Hackerwatch.org para comprobar Personal Firewall.

Acerca de la página Resumen

El Resumen de Personal Firewall contiene cuatro páginas de resumen:

- Resumen principal
- Resumen de aplicaciones
- Resumen de eventos
- Resumen de HackerWatch

Las páginas de resumen contienen una serie de informes sobre los eventos entrantes recientes, el estado de las aplicaciones y la actividad de intrusión mundial recogida por HackerWatch.org. También encontrará vínculos sobre tareas comunes realizadas en Personal Firewall.

Para abrir la página **Resumen principal** en Personal Firewall:

- Haga clic con el botón derecho del ratón en el icono de McAfee de la bandeja del sistema de Windows, elija **Personal Firewall** y, a continuación, seleccione **Ver resumen** (figura 4-1).

Figura 4-1. Página Resumen principal

Haga clic en los siguientes vínculos para desplazarse a las páginas de **Resumen**:

Elemento	Descripción
Cambiar vista	Haga clic en **Cambiar vista** para abrir una lista de páginas de resumen. Seleccione en la lista la página Resumen que desea ver.
 Flecha derecha	Haga clic en el icono de flecha derecha para ver la siguiente página Resumen.
 Flecha izquierda	Haga clic en el icono de flecha izquierda para ver la página Resumen anterior.
 Inicio	Haga clic en el icono de inicio para volver a la página **Resumen principal**.

La página **Resumen principal** proporciona la siguiente información:

Elemento	Descripción
Configuración de seguridad	El estado de la configuración de seguridad muestra el nivel de seguridad definido para el cortafuegos. Haga clic en el vínculo para cambiar el nivel de seguridad.
Eventos bloqueados	El estado de los eventos bloqueados muestra el número de eventos que se han bloqueado en el día actual. Haga clic en el vínculo para ver detalles de eventos procedentes de la página **Eventos entrantes**.
Cambios de reglas de aplicación	El estado de las reglas de aplicación muestra el número de reglas de aplicación que han cambiado recientemente. Haga clic en el vínculo para ver la lista de aplicaciones permitidas y bloqueadas, así como para modificar los permisos de las aplicaciones.
Novedades	**Novedades** muestra la última aplicación a la que se concedió acceso pleno a Internet.
Último evento	**Último evento** muestra los eventos entrantes más recientes. Haga clic en un vínculo para rastrear el evento o definir la dirección IP como fiable. Esta última acción permitirá que todo el tráfico procedente de esa dirección llegue hasta el equipo.
Informe diario	**Informe diario** muestra el número de eventos entrantes bloqueados por Personal Firewall en el día actual, esta semana y este mes. Haga clic en el vínculo para ver detalles de eventos procedentes de la página **Eventos entrantes**.
Aplicaciones activas	**Aplicaciones activas** permite ver qué aplicaciones están abiertas y con acceso a Internet en el equipo. Haga clic en una aplicación para consultar las direcciones IP a las que se está conectando.
Tareas comunes	Haga clic en un vínculo de **Tareas comunes** para ir a las páginas de Personal Firewall, donde podrá consultar la actividad del cortafuegos y llevar a cabo algunas tareas.

Para ver la página **Resumen de aplicaciones**:

1 Haga clic con el botón derecho del ratón en el icono de McAfee de la bandeja del sistema de Windows, elija **Personal Firewall** y, a continuación, seleccione **Ver resumen.**

2 Haga clic en **Cambiar vista** y, a continuación, seleccione **Resumen de aplicaciones**.

La página **Resumen de aplicaciones** incluye la siguiente información:

Elemento	Descripción
Control del tráfico	El **Control del tráfico** muestra el volumen de tráfico entrante y saliente en las conexiones de Internet durante los últimos quince minutos. Haga clic en el gráfico para ver los detalles de control del tráfico.
Aplicaciones activas	**Aplicaciones activas** muestra el uso de ancho de banda por parte de las aplicaciones con mayor actividad del equipo durante las últimas veinticuatro horas. **Aplicación**: aplicación que accede a Internet. **%**: porcentaje de ancho de banda utilizado por la aplicación. **Permiso**: tipo de acceso a Internet que se permite a la aplicación. **Regla creada**: fecha en que se creó la regla de la aplicación.
Novedades	**Novedades** muestra la última aplicación a la que se concedió acceso pleno a Internet.
Aplicaciones activas	**Aplicaciones activas** permite ver qué aplicaciones están abiertas y con acceso a Internet en el equipo. Haga clic en una aplicación para consultar las direcciones IP a las que se está conectando.
Tareas comunes	Haga clic en un vínculo de **Tareas comunes** para ir a las páginas de Personal Firewall, donde podrá consultar el estado de la aplicación y llevar a cabo algunas tareas.

Para ver la página **Resumen de eventos**:

1 Haga clic con el botón derecho del ratón en el icono de McAfee de la bandeja del sistema de Windows, elija **Personal Firewall** y, a continuación, seleccione **Ver resumen.**

2 Haga clic en **Cambiar vista** y, a continuación, seleccione **Resumen de eventos**.

La página **Resumen de eventos** contiene la siguiente información:

Elemento	Descripción
Comparación de puertos	**Comparación de puertos** muestra un gráfico circular de los puertos del equipo que se han intentado abrir con mayor frecuencia durante los últimos 30 días. Haga clic en el nombre de un puerto para ver detalles de la página **Eventos entrantes**. También puede situar el cursor sobre el número de puerto para ver una descripción del puerto.
Principales sospechosos	**Principales sospechosos** indica las direcciones IP bloqueadas con mayor frecuencia, cuándo se produjo el último evento entrante correspondiente a cada dirección y el número total de eventos entrantes en los últimos 30 días. Haga clic en un evento para ver detalles en la página **Eventos entrantes**.
Informe diario	**Informe diario** muestra el número de eventos entrantes bloqueados por Personal Firewall en el día actual, esta semana y este mes. Haga clic en un número para ver detalles de eventos procedentes del registro **Eventos entrantes**.
Último evento	**Último evento** muestra los eventos entrantes más recientes. Haga clic en un vínculo para rastrear el evento o definir la dirección IP como fiable. Esta última acción permitirá que todo el tráfico procedente de esa dirección llegue hasta el equipo.
Tareas comunes	Haga clic en un vínculo de **Tareas comunes** para ir a las páginas de Personal Firewall, donde podrá consultar los detalles de los eventos y llevar a cabo algunas tareas.

Para ver la página **Resumen de HackerWatch**:

1. Haga clic con el botón derecho del ratón en el icono de McAfee  de la bandeja del sistema de Windows, elija **Personal Firewall** y, a continuación, seleccione **Ver resumen.**
2. Haga clic en **Cambiar vista** y, a continuación, seleccione **Resumen de HackerWatch**.

La página **Resumen de HackerWatch** incluye la siguiente información**.**

Elemento	Descripción
Actividad mundial	**Actividad mundial** muestra un mapa mundial que identifica la actividad recién bloqueada que ha supervisado HackerWatch.org. Haga clic en el mapa para abrir el mapa de análisis de amenazas mundiales en HackerWatch.org.
Registro de eventos	**Registro de eventos** muestra el número de eventos entrantes enviados a HackerWatch.org.

Elemento	Descripción
Actividad mundial de puertos	**Actividad mundial de puertos** muestra los puertos que han recibido un mayor número de amenazas en los últimos cinco días. Haga clic en un puerto para ver su número y descripción.
Tareas comunes	Haga clic en un vínculo de **Tareas comunes** para ir a las páginas de HackerWatch.org, donde podrá obtener información adicional sobre las actividades de piratería a escala mundial.

Información acerca de la página Aplicaciones de Internet

En la página **Aplicaciones de Internet** podrá consultar una lista de las aplicaciones permitidas y bloqueadas.

Para iniciar la página **Aplicaciones de Internet**:

- Haga clic con el botón derecho del ratón en el icono de McAfee de la bandeja del sistema de Windows, elija **Personal Firewall** y, a continuación, seleccione **Aplicaciones de Internet** (figura 4-2).

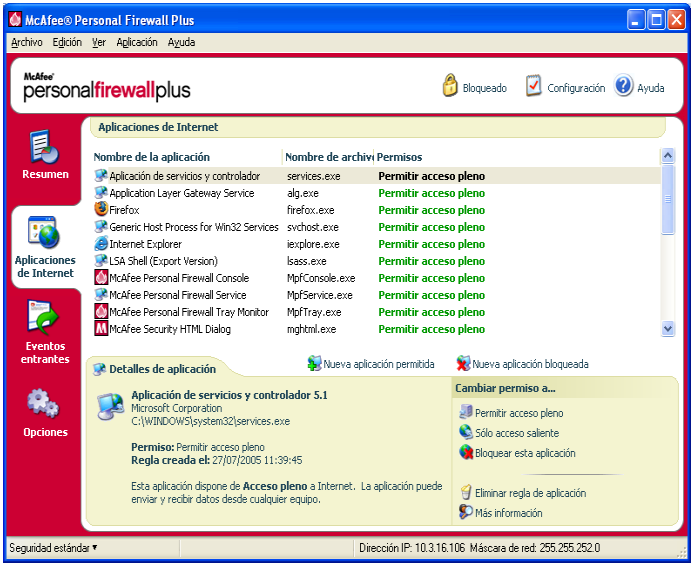


Figura 4-2. Página Aplicaciones de Internet

La página **Aplicaciones de Internet** incluye la siguiente información:

- Nombre de la aplicación
- Nombre de archivo
- Permisos
- Detalles de aplicación: nombre y versión de la aplicación, nombre de la compañía, nombre de la ruta, permiso, fechas y horas del evento y explicaciones de los tipos de permisos

Cambiar reglas de aplicación

Personal Firewall le permite cambiar las reglas de acceso de las aplicaciones.

Para cambiar una regla de aplicación:

1. Haga clic con el botón derecho en el icono de McAfee, elija **Personal Firewall** y, a continuación, seleccione **Aplicaciones de Internet**.
2. En la lista **Aplicaciones de Internet**, haga clic con el botón derecho del ratón en la regla de una aplicación y, a continuación, seleccione un nivel diferente:
   - **Permitir acceso pleno:** permite que la aplicación establezca conexiones de Internet entrantes y salientes.
   - **Sólo acceso saliente:** permite que la aplicación establezca sólo una conexión de Internet saliente.
   - **Bloquear esta aplicación:** prohíbe que la aplicación acceda a Internet.

     NOTA
     Las aplicaciones previamente bloqueadas siguen bloqueadas cuando el cortafuegos se configura con el valor de seguridad **Abierto** o **Bloqueado**. Para evitar esto, puede cambiar la regla de acceso de las aplicaciones a **Acceso pleno** o simplemente eliminar la regla del permiso **Bloqueado** en la lista **Aplicaciones de Internet**.

Para eliminar una regla de aplicación:

1. Haga clic con el botón derecho del ratón en el icono de McAfee de la bandeja del sistema de Windows, elija **Personal Firewall** y, a continuación, seleccione **Aplicaciones de Internet**.
2. En la lista **Aplicaciones de Internet**, haga clic con el botón derecho del ratón en la regla de la aplicación y, a continuación, seleccione **Eliminar regla de aplicación**.

La próxima vez que la aplicación solicite acceder a Internet, será posible establecer su nivel de permiso para que se vuelva a agregar a la lista.

Permitir y bloquear el acceso a aplicaciones de Internet

Para modificar la lista de las aplicaciones de Internet que se han bloqueado y a las que se ha permitido el acceso:

1. Haga clic con el botón derecho del ratón en el icono de McAfee de la bandeja del sistema de Windows, elija **Personal Firewall** y, a continuación, seleccione **Aplicaciones de Internet**.
2. En la página **Aplicaciones de Internet**, haga clic en una de las siguientes opciones:
   - **Nueva aplicación permitida**: concede a la aplicación acceso total a Internet.
   - **Nueva aplicación bloqueada**: impide a la aplicación acceder a Internet.
   - **Eliminar regla de aplicación**: elimina una regla de aplicación.

Información acerca de la página Eventos entrantes

La página **Eventos entrantes** permite consultar el registro **Eventos entrantes** generado cuando Personal Firewall bloquea las conexiones a Internet no solicitadas.

Para abrir la página **Eventos entrantes**:

- Haga clic con el botón derecho del ratón en el icono de McAfee de la bandeja del sistema de Windows, elija **Personal Firewall** y, a continuación, seleccione **Eventos de entrada** (figura 4-3).

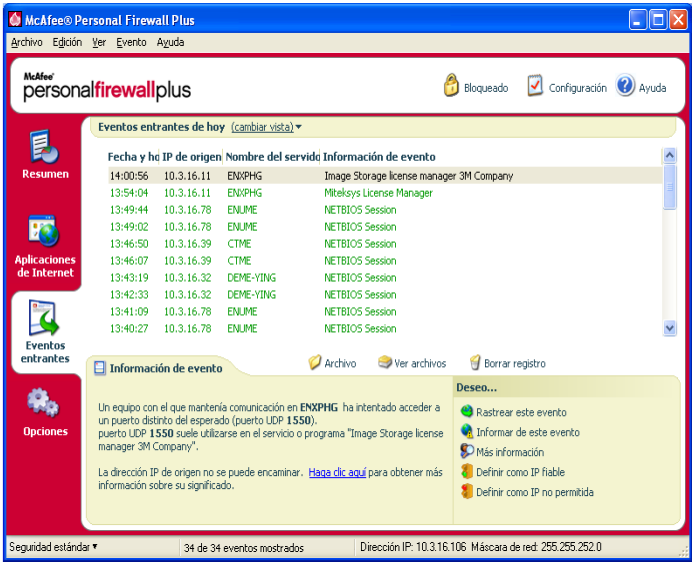


Figura 4-3. Página Eventos entrantes

La página **Eventos entrantes** incluye la siguiente información:

- Fechas y horas de los eventos
- IP de origen
- Nombre del servidor
- Nombres del servicio o de la aplicación
- Información del evento: tipos de conexión, puertos de conexión, nombre de host o IP y explicación sobre los eventos de los puertos

Explicación de los eventos

Información acerca de las direcciones IP

Las direcciones IP están compuestas por números: concretamente, cuatro números comprendidos entre 0 y 255. Estos números permiten identificar un lugar concreto al que dirigir el tráfico a través de Internet.

Tipos de direcciones IP

Existen varias direcciones IP que no se utilizan con demasiada frecuencia por diversas razones:

Direcciones IP que no se pueden enrutar: también se conocen como "espacio de IP privadas". Estas direcciones IP no se pueden utilizar en Internet. Los bloques de direcciones IP privadas son 10.x.x.x, 172.16.x.x - 172.31.x.x y 192.168.x.x.

Direcciones IP de bucle invertido: estas direcciones se utilizan para efectuar comprobaciones. El tráfico enviado a este grupo de direcciones IP se devuelve directamente al dispositivo que haya generado el paquete. Nunca abandona el dispositivo y se utiliza principalmente para realizar comprobaciones de hardware y software. El bloque de IP de bucle de invertido es 127.x.x.x.

Dirección IP nula: se trata de una dirección no válida. Cuando se detecta, Personal Firewall indica que el tráfico utilizó una dirección IP vacía. Esto indica con frecuencia que el emisor oculta deliberadamente el origen del tráfico. El emisor no podrá recibir ninguna respuesta de tráfico a no ser que el paquete lo reciba una aplicación que comprenda su contenido, que a su vez incluya instrucciones específicas para dicha aplicación. Las direcciones que empiezan por 0 (0.x.x.x) son direcciones nulas. Por ejemplo, 0.0.0.0 es una dirección IP nula.

Eventos desde 0.0.0.0

Si observa eventos procedentes de la dirección IP 0.0.0.0, existen dos causas probables. La primera, y más común, es que el equipo ha recibido un paquete defectuoso. Internet no es siempre fiable al 100%, por lo que puede que reciba paquetes dañados. Dado que Personal Firewall ve los paquetes antes de que se validen mediante TCP/IP, es posible que informe acerca de estos paquetes como un evento.

La otra situación se produce cuando la IP de origen se falsifica o simula. Los paquetes falsificados pueden ser signos de que alguien está buscando troyanos en el equipo. Personal Firewall bloquea este tipo de actividad, por lo que su equipo estará seguro.

Eventos de 127.0.0.1

En ocasiones, los eventos mostrarán 127.0.0.1 como IP de origen. Esto se conoce como dirección de bucle invertido o host local (localhost).

Muchos programas legítimos utilizan la dirección de bucle invertido para establecer la comunicación entre sus componentes. Por ejemplo, se pueden configurar muchos servidores Web o servidores personales de correo a través de una interfaz Web. Para acceder a la interfaz, escriba “http://localhost/” en el navegador Web.

Personal Firewall permite el tráfico procedente de dichos programas, de modo que si detectan eventos procedentes de 127.0.0.1; es probable que la dirección IP esté falsificada o simulada. Los paquetes falsificados normalmente indican que otro equipo está buscando troyanos en el suyo. Personal Firewall bloquea estos intentos de intrusión, por lo que su equipo estará seguro.

Algunos programas, principalmente Netscape 6.2 y versiones posteriores, requieren que agregue 127.0.0.1 a la lista de direcciones IP fiables. Los componentes de estos programas se comunican entre sí de tal forma que Personal Firewall no puede determinar si el tráfico es local o no.

En el ejemplo de Netscape 6.2, si no define la dirección 127.0.0.1 como fiable, no podrá utilizar la lista de contactos. Por lo tanto, si detecta tráfico procedente de 127.0.0.1 y todas las aplicaciones instaladas en su equipo funcionan con normalidad, resulta completamente seguro bloquear este tráfico. Pero si un programa (como Netscape) experimenta algún problema, agregue la dirección 127.0.0.1 a la lista **Direcciones IP fiables** de Personal Firewall y compruebe si se ha solucionado el problema.

Si de esta forma se soluciona el problema, debe sopesar las opciones siguientes: si confía en la dirección 127.0.0.1, el programa funcionará, pero estará más expuesto a sufrir ataques desde IP falsificadas. Si no confía en esta dirección, el programa no funcionará, pero permanecerá protegido frente a determinado tráfico malintencionado.

Eventos procedentes de equipos de la LAN

Los eventos pueden originarse en equipos situados en la red de área local (LAN). Para indicar que estos eventos se originan en su red, Personal Firewall los muestra en verde.

En la mayoría de las configuraciones de redes LAN empresariales, se debe seleccionar la opción **Confiar en todos los equipos de la LAN** en las opciones de direcciones IP fiables.

En algunas situaciones, su red "local" puede resultar tan peligrosa como Internet, especialmente si su equipo está en una red DSL de gran ancho de banda o de módem por cable. En este caso, no seleccione **Confiar en todos los equipos de la LAN**. En su lugar, agregue las direcciones IP de los equipos locales a la lista **Direcciones IP fiables**.

Eventos procedentes de direcciones IP privadas

Las direcciones IP con formato 192.168.xxx.xxx, 10.xxx.xxx.xxx y 172.16.0.0 - 172.31.255.255 suelen denominarse direcciones IP privadas o que no se pueden enrutar. Estas direcciones IP nunca deben abandonar la red, por lo que casi siempre resultan fiables.

El bloque 192.168.xxx.xxx se utiliza con Conexión compartida a Internet de Microsoft (ICS). Si utiliza una red ICS, y ve eventos con este bloque, tal vez le interese agregar la dirección IP 192.168.255.255 a la lista **Direcciones IP fiables**. De esta forma todo el bloque 192.168.xxx.xxx se convertirá en fiable.

Si no se encuentra en una red privada, y ve eventos con direcciones similares, es posible que la dirección IP de origen haya sido falsificada o simulada. Los paquetes falsificados normalmente indican que alguien está buscando troyanos. Es importante recordar que Personal Firewall ha bloqueado este intento de conexión, por lo que su equipo estará seguro.

Dado que las direcciones IP privadas se refieren a diferentes equipos en función de la red en que se encuentren, no se informará acerca de estos eventos, ya que no serviría de nada.

Visualización de eventos en el registro Eventos entrantes

El registro **Eventos entrantes** muestra los eventos de diferentes maneras. La vista predeterminada se limita a los eventos que han tenido lugar el día actual. También se pueden ver los eventos que se han producido durante la semana anterior, o incluso consultar el registro completo.

Personal Firewall también permite consultar los eventos entrantes producidos en un día concreto, los procedentes de determinadas direcciones IP o los que presentan la misma información.

Para obtener información acerca de un evento, haga clic en él y visualice la información que aparecerá en el panel **Información de evento**.

Visualización de los eventos del día actual

Utilice esta opción para consultar los eventos del día.

Para mostrar los eventos del día actual:

1. Haga clic con el botón derecho del ratón en el icono de McAfee de la bandeja del sistema de Windows, elija **Personal Firewall** y, a continuación, seleccione **Eventos de entrada**.
2. En el registro **Eventos entrantes**, haga clic con el botón derecho en una entrada y, a continuación, haga clic en **Mostrar eventos de hoy**.

Visualización de eventos de esta semana

Utilice esta opción para consultar los eventos de la semana.

Para mostrar los eventos de esta semana:

1. Haga clic con el botón derecho del ratón en el icono de McAfee de la bandeja del sistema de Windows, elija **Personal Firewall** y, a continuación, seleccione **Eventos de entrada**.
2. En el registro **Eventos entrantes**, haga clic con el botón secundario en una entrada y, a continuación, haga clic en **Mostrar eventos de esta semana**.

Visualización del registro completo de eventos entrantes

Utilice esta opción para consultar todos los eventos.

Para mostrar todos los eventos del registro **Eventos entrantes**:

1. Haga clic con el botón derecho en el icono de McAfee, elija **Personal Firewall** y, a continuación, haga clic en **Eventos de entrada**.
2. En el registro **Eventos entrantes**, haga clic con el botón derecho en una entrada y, a continuación, haga clic en **Mostrar registro completo**.

   El registro **Eventos entrantes** muestra todos los eventos del registro de eventos entrantes.

Visualización de los eventos de un día concreto

Utilice esta opción para consultar los eventos de un día concreto.

Para mostrar los eventos de un día concreto:

1. Haga clic con el botón derecho del ratón en el icono de McAfee de la bandeja del sistema de Windows, elija **Personal Firewall** y, a continuación, seleccione **Eventos de entrada**.
2. En el registro **Eventos entrantes**, haga clic con el botón derecho en una entrada y, a continuación, haga clic en **Mostrar sólo eventos de un día concreto**.

Visualización de los eventos de una dirección de Internet específica

Utilice esta opción para consultar otros eventos que se originen en una dirección de Internet determinada.

Para mostrar los eventos de una dirección de Internet:

1. Haga clic con el botón derecho del ratón en el icono de McAfee de la bandeja del sistema de Windows, elija **Personal Firewall** y, a continuación, haga clic en **Eventos de entrada**.
2. En el registro **Eventos entrantes**, haga clic con el botón derecho en una entrada y, a continuación, haga clic en **Mostrar sólo eventos de esta dirección de Internet**.

Visualización de eventos que comparten la misma información de evento

Utilice esta opción para comprobar si existen otros eventos en el registro **Eventos entrantes** que presenten la misma información que el evento seleccionado en la columna **Información de evento**. Podrá ver cuántas veces ha ocurrido el evento y si tienen el mismo origen. La columna **Información de evento** ofrece una descripción del evento y, si se conoce, el programa o servicio que utiliza el puerto.

Para mostrar eventos que comparten la misma información de evento:

1. Haga clic con el botón derecho del ratón en el icono de McAfee de la bandeja del sistema de Windows, elija **Personal Firewall** y, a continuación, haga clic en **Eventos de entrada**.
2. En el registro **Eventos entrantes**, haga clic con el botón secundario en una entrada y, a continuación, haga clic en **Mostrar sólo eventos con la misma información de evento**.

Respuesta a eventos entrantes

Además de visualizar detalles sobre los eventos del registro **Eventos entrantes**, puede efectuar un rastreo visual de las direcciones IP de un evento concreto o incluso obtener detalles en el sitio Web de la comunidad en línea contra la piratería informática HackerWatch.org.

Rastreo del evento seleccionado

Puede rastrear mediante Visual Trace las direcciones IP correspondientes a un evento del registro **Eventos entrantes**.

Para rastrear un evento seleccionado:

1. Haga clic con el botón derecho del ratón en el icono de McAfee de la bandeja del sistema de Windows, elija **Personal Firewall** y seleccione **Eventos de entrada**.

2 En el registro **Eventos entrantes**, haga clic con el botón derecho en el evento que desee rastrear y después haga clic en **Rastrear evento seleccionado**. También puede hacer doble clic en un evento para iniciar el rastreo.

De forma predeterminada, Personal Firewall inicia el rastreo mediante el programa Visual Trace integrado en Personal Firewall.

Obtención de consejos de HackerWatch.org

Para obtener consejos de HackerWatch.org:

1 Haga clic con el botón derecho en el icono de McAfee, elija **Personal Firewall** y, a continuación, seleccione **Eventos de entrada**.

2 Seleccione la entrada del evento en la página **Eventos entrantes** y, a continuación, haga clic en **Más información**. En el panel **Deseo**.

Se iniciará el navegador de Web predeterminado y se abrirá el sitio de HackerWatch.org donde podrá obtener detalles sobre el tipo de evento y consejos sobre si debe informar sobre el mismo.

Informar sobre un evento

Para informar sobre un evento que considere un ataque a su equipo:

1 Haga clic con el botón derecho del ratón en el icono de McAfee de la bandeja del sistema de Windows, elija **Personal Firewall** y seleccione **Eventos de entrada**.

2 Haga clic en el evento sobre el que desea informar y, a continuación, seleccione **Informar de este evento** en el panel **Deseo**.

Personal Firewall informa sobre el evento en el sitio Web HackerWatch.org utilizando su ID exclusivo.

Registro en HackerWatch.org

Al abrir la página **Resumen** por primera vez, Personal Firewall se pondrá en contacto con HackerWatch.org para generar la identificación exclusiva del usuario. Si ya es usuario, su registro se validará automáticamente. Si es un usuario nuevo, deberá introducir un nombre de usuario y una dirección de correo electrónico y, a continuación, hacer clic en el vínculo de validación del mensaje de correo electrónico de confirmación remitido por HackerWatch.org para poder utilizar las funciones de filtro y correo electrónico de su sitio Web.

Puede informar sobre eventos a HackerWatch.org sin validar su identificación de usuario. Sin embargo, para filtrar eventos y mandarlos por correo electrónico a un amigo, debe registrarse en el servicio.

Si se registra en el servicio, se podrán rastrear sus envíos y podremos avisarle si HackerWatch.org necesita que haga algo más o que envíe algún tipo de información adicional. También necesitamos que se registre porque debemos confirmar toda la información recibida para que resulte de utilidad.

HackerWatch.org se compromete a mantener la confidencialidad de todas las direcciones de correo electrónico que se le proporcionen. Si un proveedor de servicios de Internet realiza una solicitud para obtener información adicional, dicha solicitud se enrutará a través de HackerWatch.org, por lo que su dirección de correo electrónico nunca se verá comprometida.

Confianza en una dirección

Puede utilizar la página **Eventos entrantes** para agregar una dirección IP a la lista **Direcciones IP fiables** con el fin de permitirle la conexión permanente.

Si detecta un evento en la página **Eventos entrantes** que contenga una dirección IP que necesite autorizar, puede configurar Personal Firewall para que permita todas las conexiones procedentes de ella en todo momento.

Para agregar una dirección IP a la lista **Direcciones IP fiables**:

1. Haga clic con el botón derecho del ratón en el icono de McAfee de la bandeja del sistema de Windows, elija **Personal Firewall** y seleccione **Eventos de entrada**.
2. Haga clic con el botón derecho del ratón en el evento en cuya dirección IP desee confiar y, a continuación, en **Definir IP de origen como fiable**.

Verifique que la dirección IP que se muestra en el cuadro de diálogo **Definir como IP fiable** es correcta y haga clic en **Aceptar**. La dirección IP se agregará a la lista **Direcciones IP fiables**.

Para verificar que la dirección IP se ha agregado:

1. Haga clic con el botón derecho del ratón en el icono de McAfee de la bandeja del sistema de Windows, elija **Personal Firewall** y, a continuación, seleccione **Utilidades**.
2. Haga clic en el icono **IP fiables y prohibidas** y, a continuación, en la ficha **Direcciones IP fiables**.

La dirección IP aparecerá marcada en la lista **Direcciones IP fiables**.

Prohibición de una dirección

Si aparece una dirección IP en el registro **Eventos entrantes**, indica que se ha bloqueado el tráfico procedente de esa dirección. Por lo tanto, la prohibición de una dirección no incrementa la protección a menos que el equipo tenga abiertos intencionadamente determinados puertos a través de la función Servicios del sistema o que incluya una aplicación con permiso para recibir tráfico.

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

Si detecta un evento en la página **Eventos entrantes** que contenga una dirección IP que desee prohibir, puede configurar Personal Firewall para que rechace todas las conexiones procedentes de dicha dirección.

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

Para agregar una dirección IP a la lista **Direcciones IP no permitidas**:

1. Haga clic con el botón derecho del ratón en el icono de McAfee de la bandeja del sistema de Windows, elija **Personal Firewall** y, a continuación, seleccione **Eventos de entrada**.
2. La página **Eventos entrantes** muestra las direcciones IP de todo el tráfico de Internet entrante. Seleccione una dirección IP y realice una de las acciones siguientes:
   - Haga clic con el botón derecho en la dirección IP y, a continuación, seleccione **Definir IP de origen como no permitida**.
   - En el menú **Deseo**, haga clic en **Definir como IP no permitida**.
3. En el cuadro de diálogo Agregar regla de dirección IP prohibida, utilice uno o más de los siguientes parámetros para configurar la dirección de IP prohibida:
   - **Una sola dirección IP**: la dirección IP que desea prohibir. La entrada predeterminada corresponde a la dirección IP que se haya seleccionado en la página **Eventos entrantes**.
   - **Una serie de direcciones IP**: las direcciones IP entre la dirección especificada en De dirección IP y la dirección IP especificada en A dirección IP.
   - **Caducidad de la regla**: la fecha y la hora en la que desea que caduque la regla de dirección IP no permitida. Seleccione los menús desplegables adecuados para establecer la fecha y la hora.

- **Descripción**: permite introducir una descripción opcional para la nueva regla.
- Haga clic en **Aceptar**.

4 En el cuadro de diálogo, haga clic en **Sí** para confirmar la configuración. Haga clic en **No** para volver al cuadro de diálogo **Agregar regla de direcciones IP no permitidas**.

Si Personal Firewall detecta un evento de una conexión de Internet prohibida, le avisará según el método especificado en la página **Configuración de alertas**.

Para verificar que la dirección IP se ha agregado:

1 Haga clic en la ficha **Utilidades**.

2 Haga clic en el icono **IP fiables y prohibidas** y, a continuación, en la ficha **Direcciones IP no permitidas**.

La dirección IP aparecerá marcada en la lista **Direcciones IP no permitidas**.

Gestión del registro de eventos entrantes

Puede utilizar la página **Eventos entrantes** para gestionar los eventos del registro **Eventos entrantes** que se generan cuando Personal Firewall bloquea tráfico no solicitado de Internet.

Archivado del registro de eventos entrantes

Puede archivar el registro **Eventos entrantes** actual para guardar todos los eventos entrantes registrados, incluidas fechas y horas, IP de origen, nombres de host, puertos e información de eventos. Archive el registro **Eventos entrantes** periódicamente para evitar que se haga demasiado grande.

Para archivar el registro **Eventos entrantes**:

1 Haga clic con el botón derecho del ratón en el icono de McAfee de la bandeja del sistema de Windows, elija **Personal Firewall** y, a continuación, seleccione **Eventos de entrada**.

2 En la página **Eventos entrantes**, haga clic en **Archivo**.

3 En el cuadro de diálogo **Archivar registro**, haga clic en **Sí** para continuar con la operación.

4 Haga clic en **Guardar** para guardar el archivo en la ubicación predeterminada o bien diríjase a la ubicación en la que desea guardarlo.

> **NOTA:**
> De manera predeterminada, Personal Firewall archiva automáticamente el registro **Eventos entrantes**. Active o desactive **Archivar automáticamente los eventos registrados** en la página **Configuración de registro de eventos** para activar o desactivar la opción.

Visualización del registro de eventos entrantes archivado

Puede ver todos los registros **Eventos entrantes** previamente archivados. El archivo guardado contiene fechas y horas, direcciones IP de origen, nombres de host, puertos e información de cada evento.

Para ver un registro **Eventos entrantes** archivado:

1. Haga clic con el botón derecho del ratón en el icono de McAfee de la bandeja del sistema de Windows, elija **Personal Firewall** y, a continuación, seleccione **Eventos de entrada**.
2. En la página **Eventos entrantes**, haga clic en **Ver archivos**.
3. Seleccione o busque el nombre del archivo archivado y haga clic en **Abrir**.

Eliminación del registro de eventos entrantes

Puede borrar toda la información del registro **Eventos entrantes**.

> **ADVERTENCIA**
> Una vez borrado, el registro de eventos entrantes no podrá recuperarse. Si cree que va a necesitar el registro de eventos en el futuro, es mejor que lo guarde en un archivo.

Para eliminar el registro **Eventos entrantes**:

1. Haga clic con el botón derecho del ratón en el icono de McAfee, elija **Personal Firewall** y, a continuación, seleccione **Eventos de entrada**.
2. En la página **Eventos entrantes**, haga clic en **Borrar registro**.
3. Haga clic en **Sí** en el cuadro de diálogo para borrar el registro.

Copia de un evento en el portapapeles

Puede copiar un evento en el portapapeles para pegarlo en un archivo de texto con el Bloc de notas.

Para copiar un evento en el portapapeles:

1. Haga clic con el botón derecho del ratón en el icono de McAfee, elija **Personal Firewall** y, a continuación, seleccione **Eventos de entrada**.
2. Haga clic con el botón derecho del ratón en el evento del registro **Eventos entrantes**.
3. Haga clic en **Copiar evento seleccionado en el portapapeles**.

4 Abra el Bloc de notas.

- Escriba `notepad` en la línea de comandos o haga clic en el botón **Inicio** de Windows, elija **Programas** y, a continuación, seleccione **Accesorios**. Seleccione **Bloc de notas**.

5 Haga clic en **Editar** y, a continuación, en **Pegar**. El texto de evento se mostrará en el Bloc de notas. Repita este paso hasta que tenga todos los eventos necesarios.

6 Guarde el archivo del Bloc de notas en un lugar seguro.

Eliminación del evento seleccionado

Puede eliminar eventos del registro **Eventos entrantes**.

Para eliminar eventos del registro **Eventos entrantes**:

1 Haga clic con el botón derecho del ratón en el icono de McAfee de la bandeja del sistema de Windows, elija **Personal Firewall** y, a continuación, seleccione **Eventos de entrada**.

2 Haga clic en la entrada del evento de la página **Eventos entrantes** que desee eliminar.

3 En el menú **Editar**, haga clic en **Eliminar evento seleccionado**. El evento se borra del registro **Eventos entrantes**.

Acerca de las alertas

Se recomienda familiarizarse con los distintos tipos de alertas que aparecerán al utilizar Personal Firewall. Revise los siguientes tipos de alerta que aparecen y las posibles respuestas para poder responder con seguridad a una alerta.

NOTA
Las recomendaciones sobre las alertas ayudan a decidir cómo reaccionar en cada situación. Para que las alertas incluyan recomendaciones, haga clic en la ficha **Utilidades**, a continuación, en el icono **Configuración de alertas** y seleccione **Usar recomendaciones inteligentes** (valor predeterminado) o **Mostrar sólo recomendaciones inteligentes** en la lista **Recomendaciones inteligentes**.

Alertas rojas

Las alertas rojas contienen información importante que requiere atención inmediata:

- **Aplicación de Internet bloqueada**: esta alerta aparece cuando Personal Firewall bloquea el acceso a Internet de una aplicación. Por ejemplo, si aparece una alerta sobre un programa troyano, McAfee denegará automáticamente el acceso del programa a Internet y recomendará que se analice el equipo en busca de virus.
- **La aplicación desea tener acceso a Internet:** esta alerta aparece cuando Personal Firewall detecta tráfico procedente de una red o de Internet para aplicaciones nuevas.
- **Se ha modificado la aplicación:** esta alerta aparece cuando Personal Firewall detecta que se ha modificado una aplicación a la que previamente autorizó el acceso a Internet. Si no ha actualizado recientemente la aplicación, tenga cuidado a la hora de concederle permiso de acceso a Internet.
- **La aplicación desea tener acceso de servidor:** esta alerta aparece cuando Personal Firewall detecta que una aplicación a la que previamente se le concedió permiso para acceder a Internet solicita acceder a Internet como servidor.

NOTA
La configuración predeterminada de Actualizaciones automáticas de Windows XP SP2 descarga e instala actualizaciones para el sistema operativo de Windows y para otros programas de Microsoft que estén instalados en su equipo sin que reciba ningún mensaje de advertencia. Cuando se actualiza una aplicación mediante una de las actualizaciones silenciosas de Windows, aparecerá una alerta de McAfee Personal Firewall la próxima vez que se ejecute la aplicación de Microsoft.

IMPORTANTE
Debe conceder acceso a las aplicaciones que necesiten acceder a Internet para obtener actualizaciones en línea del programa (como ocurre con los servicios de McAfee) para mantenerlos al día.

Alerta Aplicación de Internet bloqueada

Si aparece una alerta sobre un programa troyano (figura 4-4), Personal Firewall denegará automáticamente el acceso del programa a Internet y recomendará que se analice el equipo en busca de virus. Si McAfee VirusScan no se ha instalado, puede iniciar McAfee SecurityCenter.

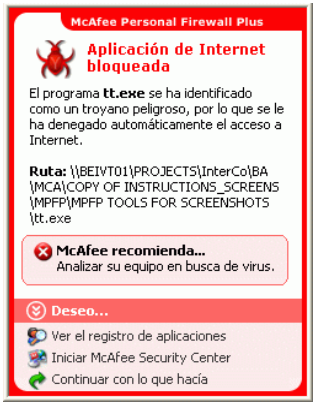


Figura 4-4. Alerta Aplicación de Internet bloqueada

Consulte una breve descripción del evento y seleccione una de las opciones siguientes:

- Haga clic en **Más información** para obtener detalles sobre el evento del registro **Eventos entrantes** (consulte *Información acerca de la página Eventos entrantes* en la página 93 para obtener información detallada al respecto).
- Haga clic **Iniciar McAfee VirusScan** para analizar el equipo en busca de virus.
- Haga clic en **Continuar con lo que hacía** si no desea aplicar otra medida aparte de la que tome Personal Firewall.
- Haga clic en **Conceder acceso saliente** para permitir una conexión saliente (Seguridad **Estricta**).

Alerta La aplicación desea tener acceso a Internet

Si selecciona el nivel de seguridad **Estándar** o **Estricta** en las opciones de Configuración de seguridad, Personal Firewall mostrará una alerta (figura 4-5) cuando detecte conexiones de red o de acceso a Internet procedente de aplicaciones nuevas o modificadas.

Figura 4-5. Alerta La aplicación desea tener acceso a Internet

Si aparece una alerta que recomienda precaución a la hora de permitir el acceso a Internet a la aplicación, elija **Haga clic aquí para obtener más información** para conocer más detalles sobre la aplicación. Esta opción aparece en la alerta sólo cuando Personal Firewall está configurado para utilizar recomendaciones inteligentes.

McAfee podría no reconocer la aplicación que intenta obtener acceso a Internet (figura 4-6).

Figura 4-6. Alerta Aplicación no reconocida

Por lo tanto, McAfee no puede dar una recomendación sobre cómo gestionar la aplicación. Puede informar sobre la aplicación a McAfee haciendo clic en **Informar a McAfee sobre este programa**. Aparecerá una página Web que solicitará información relacionada con la aplicación. Rellene tanta información como sea posible.

La información enviada la emplean los operadores de HackerWatch con otras herramientas de investigación para determinar si una aplicación garantiza su aparición en nuestra base de datos de aplicaciones conocidas y, si es así, el modo en que debe tratarla Personal Firewall.

Consulte una breve descripción del evento y seleccione una de las opciones siguientes:

- Haga clic en **Conceder acceso** para permitir que la aplicación establezca una conexión de Internet entrante y saliente.
- Haga clic en **Conceder acceso una vez** para permitir que la aplicación se conecte a Internet de manera temporal. El acceso se limita al tiempo desde el momento en el que se inicia la aplicación hasta cuando se cierra.
- Haga clic en **Bloquear todo acceso** para prohibir la conexión a Internet.
- Haga clic en **Conceder acceso saliente** para permitir una conexión saliente (Seguridad **Estricta**).
- Haga clic en **Ayuda para elegir** para ver la Ayuda en línea sobre los permisos de acceso de aplicaciones.

Alerta Se ha modificado la aplicación

Si selecciona **Fiable**, **Estándar** o **Estricta** en las opciones de Configuración de seguridad, Personal Firewall mostrará una alerta (figura 4-7) cuando detecte que se ha modificado una aplicación a la que se había concedido permiso de acceso a Internet. Si ha actualizado recientemente la aplicación en cuestión, debe tener cuidado a la hora de concederle permiso de acceso a Internet.

Figura 4-7. Alerta Se ha modificado la aplicación

Consulte una breve descripción del evento y seleccione una de las opciones siguientes:

- Haga clic en **Conceder acceso** para permitir que la aplicación establezca una conexión de Internet entrante y saliente.
- Haga clic en **Conceder acceso una vez** para permitir que la aplicación se conecte a Internet de manera temporal. El acceso se limita al tiempo desde el momento en el que se inicia la aplicación hasta cuando se cierra.
- Haga clic en **Bloquear todo acceso** para prohibir la conexión a Internet.
- Haga clic en **Conceder acceso saliente** para permitir una conexión saliente (Seguridad **Estricta**).
- Haga clic en **Ayuda para elegir** para ver la Ayuda en línea sobre los permisos de acceso de aplicaciones.

Alerta La aplicación desea tener acceso de servidor

Si selecciona el nivel de seguridad **Estricta** en las opciones de Configuración de seguridad, Personal Firewall mostrará una alerta (figura 4-8) al detectar que una aplicación a la que se había concedido permiso de acceso a Internet solicita acceso a Internet como servidor.

Figura 4-8. Alerta La aplicación desea tener acceso de servidor

Por ejemplo, aparecerá una alerta cuando MSN Messenger solicite acceso de servidor para enviar un archivo durante una sesión de chat.

Consulte una breve descripción del evento y seleccione una de las opciones siguientes:

- Haga clic en **Conceder acceso una vez** para permitir el acceso temporal a Internet de la aplicación. El acceso se limita al tiempo desde el momento en el que se inicia la aplicación hasta cuando se cierra.
- Haga clic en **Conceder acceso al servidor** para permitir que la aplicación establezca una conexión de Internet entrante y saliente.
- Haga clic en **Restringir a acceso mensajes salientes** para prohibir una conexión a Internet entrante.
- Haga clic en **Bloquear todo acceso** para prohibir la conexión a Internet.
- Haga clic en **Ayuda para elegir** para ver la Ayuda en línea sobre los permisos de acceso de aplicaciones. Alertas verdes.

Alertas verdes

Las alertas verdes le notifican eventos en Personal Firewall, tales como aplicaciones a las que se les haya concedido automáticamente acceso a Internet.

Programa con permiso de acceso a Internet: esta alerta aparece cuando Personal Firewall concede acceso a Internet automáticamente a todas las aplicaciones nuevas y lo notifica con posterioridad (Seguridad **Fiable**). Un ejemplo de aplicación modificada sería la que tuviera reglas modificadas que permitieran acceder automáticamente a Internet.

Alerta Programa con permiso de acceso a Internet

Si selecciona el nivel de seguridad **Fiable** en las opciones de Configuración de seguridad, Personal Firewall concederá acceso a Internet de forma automática a todas las aplicaciones nuevas y se lo notificará mediante una alerta (figura 4-9).

Figura 4-9. Programa con permiso de acceso a Internet

Consulte una breve descripción del evento y seleccione una de las opciones siguientes:

- Haga clic en **Ver el registro de aplicaciones** para obtener detalles sobre el evento a través del registro de aplicaciones de Internet (consulte *Información acerca de la página Aplicaciones de Internet* en la página 91 para obtener información detallada al respecto).
- Haga clic en **Desactivar este tipo de alertas** para impedir que aparezca de este tipo de alertas.
- Haga clic en **Continuar con lo que hacía** si no desea aplicar otra medida aparte de la que tome Personal Firewall.
- Haga clic en **Bloquear todo acceso** para prohibir la conexión a Internet.

Alerta de modificación de aplicación

Si selecciona el nivel de seguridad **Fiable** en las opciones de Configuración de seguridad, Personal Firewall concederá acceso a Internet de forma automática a todas las aplicaciones modificadas. Consulte una breve descripción del evento y seleccione una de las opciones siguientes:

- Haga clic en **Ver el registro de aplicaciones** para obtener detalles sobre el evento a través del registro **Aplicaciones de Internet** (consulte *Información acerca de la página Aplicaciones de Internet* en la página 91 para obtener información detallada al respecto).
- Haga clic en **Desactivar este tipo de alertas** para impedir que aparezca de este tipo de alertas.
- Haga clic en **Continuar con lo que hacía** si no desea aplicar otra medida aparte de la que tome Personal Firewall.
- Haga clic en **Bloquear todo acceso** para prohibir la conexión a Internet.

Alertas azules

Las alertas azules contienen información, pero no requieren ninguna acción por parte del usuario.

- **Intento de conexión bloqueado:** esta alerta aparece cuando Personal Firewall bloquea tráfico no deseado procedente de una red o de Internet. (Seguridad Fiable, Estándar o Estricta)

Alerta Intento de conexión bloqueado

Si ha seleccionado la seguridad **Fiable**, **Estándar** o **Estricta**, Personal Firewall muestra una alerta (figura 4-10) al bloquear el tráfico de red o de Internet no deseado.

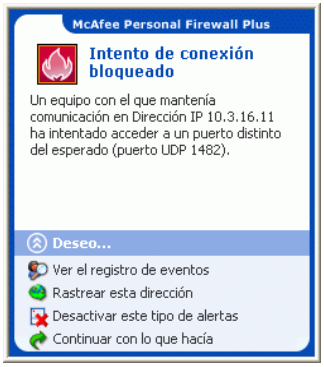


Figura 4-10. Alerta Intento de conexión bloqueado

Consulte una breve descripción del evento y seleccione una de las opciones siguientes:

- Haga clic en **Ver el registro de eventos** para obtener detalles sobre el evento a través del registro **Eventos entrantes** de Personal Firewall (consulte *Información acerca de la página Eventos entrantes* en la página 93 para obtener información detallada al respecto).
- Haga clic en **Rastrear esta dirección** para realizar un rastreo visual de las direcciones IP correspondientes al evento.
- Haga clic en **Definir como IP no permitida** para evitar que se acceda al equipo desde esta dirección. La dirección se agregará a la lista **Direcciones IP no permitidas**.
- Haga clic en **Definir como IP fiable** para permitir que se acceda al equipo desde esta dirección.
- Haga clic en **Continuar con lo que hacía** si no desea aplicar otra medida aparte de la que tome Personal Firewall.

McAfee Privacy Service 5

Bienvenido a McAfee® Privacy Service™. El software McAfee Privacy Service ofrece protección avanzada para usted, su familia, sus datos personales y su equipo.

Funciones

Esta versión de McAfee Privacy Service incluye las siguientes funciones:

- Reglas de horario de uso de Internet: especifique los días y horas en los que los usuarios pueden acceder a Internet.
- Filtros personalizados mediante palabras clave: cree reglas de palabras clave que permitan o bloqueen a los usuarios el acceso a sitios Web.
- Copia de seguridad y restauración de Privacy Service: se puede guardar y restaurar la configuración de Privacy Service en cualquier momento.
- Bloqueador de Web bugs: bloquea Web bugs (objetos que se obtienen en sitios Web potencialmente peligrosos) para que no se carguen dentro las páginas Web exploradas.
- Bloqueador de elementos emergentes: evita que aparezcan elementos emergentes mientras navega por Internet.
- Shredder: McAfee Shredder protege la privacidad de manera rápida y segura mediante la eliminación de archivos no deseados.

Administrador

El Administrador especifica qué usuarios pueden acceder a Internet, cuándo pueden utilizarlo y qué pueden realizar en Internet.

NOTA
Se considera que el Administrador es adulto y que por tanto puede acceder a todos los sitios Web, pero debe permitir o impedir la transmisión de información personal identificable (PII, del inglés Personal Identifiable Information) añadida.

Configuración de Privacy Service

El Asistente para la configuración permite crear el Administrador, gestionar las opciones globales, introducir información personal y agregar usuarios.

Recuerde su contraseña de Administrador y la respuesta de seguridad para poder iniciar la sesión en Privacy Service. Si no puede iniciar la sesión, no podrá utilizar Privacy Service ni Internet. Mantenga su contraseña en secreto de manera que sólo usted pueda cambiar la configuración de Privacy Service. Para funcionar correctamente, algunos sitios Web necesitan que las cookies estén activadas. Privacy Service siempre acepta cookies de McAfee.com.

Recuperación de la contraseña del Administrador

Si olvida la contraseña del Administrador, podrá acceder a ella mediante la información de seguridad introducida al crear el perfil del Administrador.

Para recuperar la contraseña del Administrador:

1. Haga clic con el botón derecho del ratón en el icono de McAfee, en la bandeja del sistema de Windows, seleccione **McAfee Privacy Service** y, a continuación, elija **Iniciar sesión**.
2. Seleccione **Administrador** en el menú desplegable **Nombre de usuario**.
3. Haga clic en **¿Olvidó su contraseña?**
4. Introduzca la respuesta a la pregunta de seguridad que aparece y, a continuación, haga clic en **Obtener contraseña**. Aparecerá un mensaje con la contraseña. Si olvida la respuesta a la pregunta de seguridad, deberá desinstalar McAfee Privacy Service en modo a prueba de fallos (sólo en Windows 2000 y Windows XP).

Desinstalación de Privacy Service en modo a prueba de fallos

Para desinstalar Privacy Service en modo a prueba de fallos:

1. Haga clic en **Inicio** y elija **Apagar**. Aparecerá el cuadro de diálogo **Salir de Windows**.
2. Seleccione **Apagar** en el menú y haga clic en **Aceptar**.
3. Espere a que aparezca el mensaje **Ahora puede apagar su equipo con seguridad** y apague el equipo.
4. Vuelva a encender el equipo.
5. Empiece a pulsar inmediatamente la tecla **F8** cada segundo hasta que aparezca el menú **Inicio de Windows**.
6. Seleccione **Modo a prueba de fallos** y pulse **Intro**.

7 Cuando se inicie Windows, se mostrará un mensaje describiendo el modo a prueba de fallos. Haga clic en **Aceptar**.

8 Vaya **Agregar o quitar programas** en el Panel de control de Windows. Cuando haya terminado, reinicie el PC.

9 Vuelva a instalar McAfee Privacy Service y especifique la contraseña de administrador. Anote la contraseña que especifique.

NOTA
Puede desinstalar Privacy Service en el modo a prueba de fallos únicamente en Windows 2000 o Windows XP.

Usuario de inicio

El Usuario de inicio inicia la sesión automáticamente en Privacy Service al encender el equipo.

Por ejemplo, si un usuario utiliza el equipo o Internet más que los demás (incluido el Administrador), podrá definirlo como Usuario de inicio. Cuando el Usuario de inicio utiliza el equipo, no se requiere que inicie la sesión en Privacy Service.

Si tiene niños, puede definir al más pequeño como Usuario de inicio. De este modo, cuando un usuario mayor utilice el equipo, podrá cerrar la cuenta del usuario más pequeño e iniciar una nueva sesión utilizando su propio nombre de usuario y contraseña. Así se protege a los usuarios más jóvenes de las visitas a sitios Web inadecuados.

Configuración del Administrador como Usuario de inicio

Para configurar el Administrador como Usuario de inicio:

1 En el cuadro de diálogo **Pulse Inicio de sesión**, seleccione su nombre en el menú desplegable **Nombre del usuario**.

2 Escriba su contraseña en el campo **Contraseña**.

3 Seleccione **Definir como Usuario de inicio** e inicie la sesión.

Apertura de McAfee Privacy Service

Cuando se instala McAfee Privacy Service, el icono de McAfee aparece en la bandeja del sistema de Windows, junto al reloj del sistema. Con el icono de McAfee, puede acceder a McAfee Privacy Service, McAfee SecurityCenter y otros productos de McAfee instalados en el equipo.

Apertura e inicio de sesión en Privacy Service

1. Haga clic con el botón derecho del ratón en el icono de McAfee, en la bandeja del sistema de Windows, seleccione **McAfee Privacy Service** y, a continuación, elija **Iniciar sesión**.
2. Seleccione su nombre de usuario en el menú desplegable **Nombre del usuario**.
3. Escriba su contraseña en el campo **Contraseña**.
4. Haga clic en **Iniciar sesión**.

Desactivación de Privacy Service

Debe tener una sesión iniciada en Privacy Service como administrador si desea desactivarlo.

Para desactivar Privacy Service:

- Haga clic con el botón derecho en el icono de McAfee , elija **McAfee Privacy Service** y seleccione **Cerrar sesión**.

  NOTA
  Si **Iniciar sesión** aparece en lugar de **Cerrar sesión**, significa que ya ha cerrado la sesión.

Actualización de McAfee Privacy Service

McAfee SecurityCenter comprueba regularmente la existencia de actualizaciones de Privacy Service mientras el equipo está encendido y conectado a Internet. Si hay actualizaciones disponibles, McAfee SecurityCenter le preguntará si desea actualizar Privacy Service.

Para comprobar manualmente la existencia de actualizaciones:

- Haga clic en el icono **Actualizaciones** situado en el panel superior.

Desinstalación y reinstalación de Privacy Service

Para desinstalar Privacy Service debe haber iniciado la sesión como Administrador.

NOTA
Cuando se desinstala Privacy Service se eliminan todos los datos del programa.

Desinstalación de Privacy Service

Para desinstalar Privacy Service:

1. Guarde su trabajo y cierre todas las aplicaciones que se encuentren abiertas.
2. Abra el Panel de control:

- Usuario de Windows 98, Windows Me y Windows 2000: seleccione **Inicio**, elija **Configuración** y haga clic en **Panel de control**.
- Usuario de Windows XP: en la barra de tareas de Windows, seleccione **Inicio** y haga clic en **Panel de control**.

3. Abra el cuadro de diálogo **Agregar o quitar programas**:

- Usuario de Windows 98, Me y 2000: haga doble clic en **Agregar o quitar programas**.
- Usuario de Windows XP: haga clic en **Agregar o quitar programas**.

4. Seleccione McAfee Privacy Service en la lista de programas y haga clic en **Cambiar o quitar**.
5. Cuando se le pida que confirme la operación, haga clic en **Sí**.
6. Cuando se le pida que reinicie el sistema, haga clic en **Cerrar**. El equipo se reinicia para completar el proceso de desinstalación.

Instalación de Privacy Service

Para instalar Privacy Service:

1. Vaya al sitio Web de McAfee y diríjase a la página **Privacy Service**.
2. Haga clic en el enlace **Descargar** de la página de **Privacy Service**.
3. Haga clic en **Sí** en todos los mensajes que aparezcan preguntando si desea descargar archivos del sitio Web de McAfee.
4. Haga clic en **Iniciar la instalación** en la ventana de instalación de Privacy Service.
5. Cuando finalice la descarga, haga clic en **Reiniciar** para reiniciar el equipo. O haga clic en **Cerrar** si necesita guardar cualquier trabajo o salir de cualquier programa y, a continuación, reinicie el equipo como de costumbre. Debe reiniciar el equipo para que Privacy Service funcione correctamente.

Después de reiniciar el equipo, tendrá que volver a establecer un administrador.

Para agregar usuarios, deberá iniciar la sesión en Privacy Service como Administrador.

1. Haga clic con el botón derecho del ratón en el icono de McAfee , en la bandeja del sistema de Windows.
2. Seleccione **McAfee Privacy Service** y, a continuación, **Gestión de usuarios**. Aparecerá el cuadro de diálogo **Seleccionar a un usuario**.
3. Haga clic en **Agregar** e introduzca el nombre del nuevo usuario en el campo **Nombre de usuario**.

Definición de la contraseña

1. Escriba una contraseña en el campo **Contraseña**. La contraseña puede tener hasta 50 caracteres, que pueden ser mayúsculas, minúsculas y números.
2. Escriba de nuevo la contraseña en el campo **Confirmar contraseña**.
3. Seleccione **Definir como Usuario de inicio** si desea que este usuario sea el Usuario de inicio.
4. Haga clic en **Siguiente**.

Al asignar las contraseñas deberá tener en cuenta la edad de la persona. Por ejemplo, si asigna una contraseña a un niño, ésta deberá ser sencilla. Si asigna una contraseña a un joven o a un adulto, podrá ser más compleja.

Definición del grupo de edad

Seleccione la configuración adecuada basada en la edad y haga clic en **Siguiente**.

Configuración del bloqueador de cookies

Seleccione la opción adecuada y haga clic en **Siguiente**.

- **Rechazar todos los cookies**: devuelve cookies ilegibles a los sitios Web que los han enviado. Para funcionar correctamente, algunos sitios Web requieren que tenga los cookies activados.
- **Preguntar si acepta cookies**: permite al usuario decidir si desea aceptar o rechazar cada cookie de manera individual. Privacy Service notifica al usuario si el sitio Web que está a punto de visitar desea enviar cookies a su equipo. Después de haber tomado la decisión, ya no se le volverá a preguntar sobre dichos cookies.
- **Aceptar todos los cookies**: permite a los sitios Web leer los cookies que envían al equipo.

  NOTA
  Para funcionar correctamente, algunos sitios Web necesitan que los cookies estén activados.

  Privacy Service acepta siempre cookies de McAfee.

Establecimiento de límites de tiempo de acceso a Internet

Para permitir el uso de Internet sin restricciones:

1. Seleccione **Puede utilizar Internet en todo momento**.
2. Haga clic en **Crear**. El nuevo usuario aparecerá en la lista **Seleccionar a un usuario**.

Para permitir el uso de Internet restringido:

1. Seleccione **Restringir el uso de Internet** y haga clic en **Editar**.

2 En la página **Límites de tiempo de Internet**, arrastre el cuadrante temporal para seleccionar las horas y los días que el usuario puede acceder a Internet. Puede especificar límites temporales en intervalos de treinta minutos. Las partes verdes del cuadrante corresponden a los períodos en los que un usuario puede acceder a Internet. Las partes rojas indican cuando un usuario no puede acceder a Internet. Si un usuario intenta utilizar Internet cuando no tienen permiso para ello, Privacy Service muestra un mensaje advirtiendo al usuario que no tiene permiso para utilizar Internet en ese momento. Para modificar los períodos en los que un usuario puede acceder a Internet, arrastre las partes verdes del cuadrante.

3 Haga clic en **Realizado**.

4 Haga clic en **Crear**. El nuevo usuario aparecerá en la lista **Seleccionar a un usuario**. Si un usuario intenta utilizar Internet cuando no tienen permiso para ello, Privacy Service muestra un mensaje advirtiendo al usuario que no tiene permiso para utilizar Internet en ese momento.

Para prohibir el acceso a Internet:

Seleccione **Restringir el uso de Internet** y haga clic en **Crear**. Cuando el usuario utilice el equipo, se le solicitará que inicie una sesión en Privacy Service. El usuario podrá utilizar el equipo, pero no Internet.

Creación de permisos a sitios Web mediante palabras clave

Privacy Service tiene una lista predeterminada de palabras clave y reglas correspondientes que determinan si un usuario con cierta edad puede explorar un sitio Web en el que existe una palabra clave.

El Administrador puede agregar sus propias palabras clave permitidas a la base de datos de Privacy Service y asociarlas a ciertos tramos de edad. Las reglas de las palabras clave, agregadas por el Administrador, sobrescribirán la regla asociada con cualquier palabra clave coincidente de la base de datos predeterminada de Privacy Service. Un Administrador puede buscar palabras clave existentes, así como especificar nuevas palabras que podrá asociar con ciertos tramos de edad.

Para crear permisos a sitios Web mediante palabras clave:

1 Haga clic con el botón derecho en el icono de McAfee (en la bandeja del sistema de Windows), seleccione **Privacy Service** y, a continuación, **Opciones**.

2 Haga clic en la ficha **Palabras clave**.

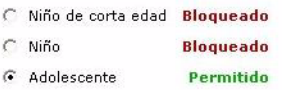
3 En el campo **Búsqueda de palabra**, escriba una palabra para un tramo de edad.

4 En el panel **Permisos**, seleccione el tramo de edad que desea asociar a la palabra. Los tramos de edad son los siguientes:

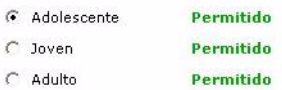
- Niño de corta edad
- Niño
- Adolescente
- Joven
- Adulto

La palabra clave y el grupo de edad seleccionado aparecen en el panel **Lista de palabras**.

Los tramos de edad situados por encima del tramo asociado quedan bloqueados y no se les permite el acceso a los sitios Web que contengan la palabra.



El tramo de edad al que se ha asignado la palabra, así como los que aparecen por debajo del mismo, tienen permitido el acceso a los sitios Web que contengan la palabra.



Para modificar permisos a sitios Web mediante palabras clave:

1 Haga clic con el botón derecho en el icono de McAfee (en la bandeja del sistema de Windows), seleccione **Privacy Service** y, a continuación, **Opciones**.

2 Haga clic en la ficha **Palabras clave**.

3 En el campo **Búsqueda de palabra**, escriba la palabra que desea modificar y haga clic en **Búsqueda**. La palabra aparece si existe en la base de datos de Privacy Service.

Para editar usuarios, deberá iniciar una sesión en Privacy Service como Administrador.

Cambio de contraseñas

1. Seleccione el usuario cuya información desee modificar y haga clic en **Editar**.
2. Seleccione **Contraseña** e introduzca la nueva contraseña del usuario en el campo **Nueva contraseña**. La contraseña puede tener hasta 50 caracteres, así como mayúsculas, minúsculas y números.
3. Escriba la misma contraseña en el campo **Confirmar contraseña** y haga clic en **Aplicar**.
4. Haga clic en **Aceptar** en el cuadro de dialogo de confirmación.

NOTA
Un Administrador puede cambiar la contraseña de un usuario sin necesidad de conocer su contraseña actual.

Cambio de la información de usuario

1. Seleccione el usuario cuya información desee modificar y haga clic en **Editar**.
2. Seleccione **Información de usuario**.
3. Escriba el nuevo nombre de usuario en el campo **Nombre de usuario nuevo**.
4. Haga clic en **Aplicar** y después en **Aceptar**, en el cuadro de diálogo de confirmación.
5. Para restringir el acceso de un usuario a los sitios Web de la lista **Sitios Web aceptados**, seleccione **Restringir el acceso de este usuario a los sitios Web de la lista "Sitios Web aceptados"**.

Modificación de la configuración del bloqueador de cookies

1. Seleccione el usuario cuya información desee modificar y haga clic en **Editar**.
2. Seleccione **Cookies** y, a continuación, la opción adecuada.
   - **Rechazar todos los cookies**: devuelve cookies ilegibles a los sitios Web que los han enviado. Para funcionar correctamente, algunos sitios Web requieren que tenga los cookies activados.
   - **Preguntar si acepta cookies**: permite al usuario decidir si desea aceptar o rechazar cada cookie de manera individual. Privacy Service notifica al usuario si el sitio Web que está a punto de visitar desea enviar cookies a su equipo. Después de haber tomado la decisión, ya no se le volverá a preguntar sobre dichos cookies.
   - **Aceptar todos los cookies**: permite a los sitios Web leer los cookies que envían al equipo.
3. Haga clic en **Aplicar** y después en **Aceptar**, en el cuadro de diálogo de confirmación.

Edición de la lista de aceptación o rechazo de cookies

1. Seleccione **Preguntar si acepta cookies** y haga clic en **Editar** para especificar los sitios Web que pueden leer cookies.
2. Especifique la lista que desea modificar seleccionando **Sitios Web que pueden establecer cookies** o **Sitios Web que no pueden establecer cookies**.
3. En el campo **http://**, introduzca la dirección del sitio Web del que vaya a aceptar o rechazar cookies.
4. Haga clic en **Agregar**. El sitio Web aparecerá en la lista de sitios Web.
5. Haga clic en **Realizado** cuando haya terminado de realizar los cambios.

NOTA
Para funcionar correctamente, algunos sitios Web necesitan que los cookies estén activados.

Privacy Service acepta siempre cookies de McAfee.

Cambio del grupo de edad

1. Seleccione el usuario cuya información desee modificar y haga clic en **Editar**.
2. Seleccione **Grupo de edad**.
3. Seleccione un nuevo grupo de edad para el usuario y haga clic en **Aplicar**.
4. Haga clic en **Aceptar** en el cuadro de dialogo de confirmación.

Modificación de los límites de tiempo de acceso a Internet

1. Seleccione el usuario cuya información desee modificar y haga clic en **Editar**.
2. Seleccione **Límites de tiempo** y haga lo siguiente:

Para permitir acceso ilimitado a Internet:

1. Seleccione **Puede utilizar Internet en todo momento** y haga clic en **Aplicar**.
2. Haga clic en **Aceptar** en el cuadro de dialogo de confirmación.

Para restringir el acceso a Internet:

1. Seleccione **Restringir el uso de Internet** y haga clic en **Editar**.
2. En la página **Límites de tiempo**, seleccione un cuadrado verde o rojo y arrástrelo en el cuadrante para cambiar las horas y los días definidos y permitir a un usuario acceder a Internet.
   Puede especificar límites temporales en intervalos de treinta minutos. Las partes verdes del cuadrante corresponden a los períodos en los que un usuario puede acceder a Internet. Las partes rojas indican cuando un usuario no puede acceder a Internet. Si un usuario intenta utilizar Internet cuando no tienen permiso para ello, Privacy Service muestra un mensaje advirtiendo al usuario que no tiene permiso para utilizar Internet en ese momento.
3. Haga clic en **Aplicar**.
4. En la página **Límites de tiempo**, haga clic en **Aceptar**.
5. En el cuadro de diálogo de confirmación de McAfee Privacy Service, haga clic en **Aceptar**.

Cambio del Usuario de inicio

El Administrador puede cambiar el Usuario de inicio en cualquier momento. Si ya existe un Usuario de inicio, no tendrá que desactivarlo como tal.

1. Seleccione el usuario que desee establecer como Usuario de inicio y haga clic en **Editar**.
2. Seleccione **Información de usuario**.
3. Seleccione **Definir como Usuario de inicio**.
4. Haga clic en **Aplicar** y después en **Aceptar**, en el cuadro de diálogo de confirmación.

> **NOTA**
> También puede asignar un Usuario de inicio en el cuadro de diálogo **Pulse Inicio de sesión**. Para obtener más información, consulte: *Usuario de inicio* en la página 117.

Eliminación de usuarios

1. Seleccione el usuario que desee eliminar y haga clic en **Quitar**.
2. Haga clic en **Sí** en el cuadro de diálogo de confirmación.
3. Cierre la ventana Privacy Service cuando haya terminado de realizar los cambios.

Para configurar las opciones de Privacy Service, deberá iniciar una sesión como Administrador.

Bloqueo de sitios Web

1. Haga clic en **Opciones** y seleccione **Lista bloquear**.
2. En el campo **http://**, introduzca la URL del sitio Web que desee bloquear y, a continuación, haga clic en **Agregar**. El sitio Web aparecerá en la lista **Sitios Web bloqueados**.

> **NOTA**
> Los usuarios (incluidos los administradores) que pertenezcan a un grupo de edad de adultos podrán acceder a todos los sitios Web, incluso si éstos aparecen en la lista **Sitios Web bloqueados**. Para probar los sitios Web bloqueados, los administradores deberán registrarse como usuarios no adultos.

Permiso de acceso a sitios Web

El Administrador puede permitir a todos los usuarios que vean sitios Web específicos. Esto sobrescribe la configuración predeterminada de Privacy Service y los sitios Web agregados a la lista de sitios bloqueados.

1. Haga clic en **Opciones** y seleccione **Lista permitir**.
2. En el campo **http://**, introduzca la URL del sitio Web que desee permitir y, a continuación, haga clic en **Agregar**. El sitio Web aparecerá en la lista **Sitios Web permitidos**.

Bloqueo de información

El Administrador puede impedir que otros usuarios envíen determinados datos personales a través de Internet (sin embargo, el Administrador puede enviar dicha información).

Cuando Privacy Service detecta información personal identificable (PII) en algún documento que vaya a enviarse, ocurre lo siguiente:

- Si usted es el Administrador, se le preguntará y podrá decidir si desea enviar la información.
- Si el usuario que ha iniciado la sesión no es el Administrador, la información bloqueada será reemplazada por *MFEMFEMFE*. Por ejemplo, si envía el mensaje *Lance Armstrong gana el Tour* y Armstrong está establecido como información personal que debe bloquearse, se enviará el siguiente mensaje: *Lance MFEMFEMFE gana el Tour*.

Adición de información

1. Haga clic en **Opciones** y seleccione **Información para bloquear**.
2. Haga clic en **Agregar**. Aparece el menú desplegable **Seleccionar tipo**.
3. Seleccione el tipo de información que desee bloquear.
4. Introduzca la información en los campos adecuados y haga clic en **Aceptar**. La información introducida aparece en la lista.

Edición de información

1. Haga clic en **Opciones** y seleccione **Información para bloquear**.
2. Seleccione la información que desee modificar y haga clic en **Editar**.
3. Realice los cambios adecuados y haga clic en **Aceptar**. Si no es necesario modificar la información, haga clic en **Cancelar**.

Eliminación de información personal

1. Haga clic en **Opciones** y seleccione **Información para bloquear**.
2. Seleccione la información que desee eliminar y haga clic en **Quitar**.
3. Haga clic en **Sí** en el cuadro de diálogo de confirmación.

Bloqueo de Web bugs

Los Web bugs son pequeños archivos gráficos que pueden enviar mensajes a terceros, realizar un seguimiento de los hábitos de navegación en Internet o transmitir información personal a una base de datos externa. Esa información puede usarse por parte de terceros para crear perfiles de usuario.

Para evitar que se carguen Web bugs en las páginas Web a las que se accede, seleccione **Bloquear Web Bugs en este equipo**.

Bloqueo de anuncios

Los anuncios son normalmente gráficos procedentes de dominios de terceros que se insertan en páginas Web o ventanas emergentes. Privacy Service no bloquea los anuncios procedentes del mismo dominio que la página Web del host.

Los elementos emergentes son ventanas secundarias del navegador que contienen anuncios no deseados que se muestran automáticamente al visitar un sitio Web. Privacy Service únicamente bloquea los elementos emergentes que se cargan automáticamente al abrir una página Web. Privacy Service no bloquea los elementos emergentes que se inician al hacer clic en un vínculo. Para mostrar un elemento emergente bloqueado, mantenga pulsada la tecla CTRL mientras actualiza la página.

Configure Privacy Service para bloquear anuncios y elementos emergentes mientras esté utilizando Internet.

1. Haga clic en **Opciones** y seleccione **Bloquear anuncios**.
2. Seleccione la opción adecuada.
   - **Bloquear anuncios en este equipo**: bloquea anuncios mientras se está utilizando Internet.
   - **Bloquear ventanas emergentes en este equipo**: bloquea las ventanas emergentes mientras se está utilizando Internet.
3. Haga clic en **Aplicar** y después en **Aceptar**, en el cuadro de diálogo de confirmación.

Para desactivar el bloqueo de elementos emergentes, haga clic con el botón derecho en la página Web, elija **Bloqueo de mensaje emergentes de McAfee** y desactive **Activar Bloqueo de mensajes emergentes**.

Admisión de cookies de sitios Web específicos

Si bloquea cookies o prefiere que le pregunten antes de aceptarlos y encuentra ciertos sitios Web que no funcionan correctamente, configure Privacy Service para permitir que el sitio lea dichos cookies.

1. Haga clic en **Opciones** y seleccione **Cookies**.
2. En el campo **http://**, introduzca la dirección del sitio Web que necesite leer los cookies y, a continuación, haga clic en **Agregar**. La dirección aparecerá en la lista **Aceptar cookies de sitios Web**.

Para ver el registro de eventos, deberá iniciar una sesión en Privacy Service como administrador. Seleccione **Registro de eventos** y haga clic en cualquier entrada de registro para visualizar los detalles. Para guardar un registro o ver un registro guardado, seleccione la ficha **Registros guardados**.

Fecha y hora

De manera predeterminada, el registro de eventos muestra la información en orden cronológico, con los eventos más recientes en la parte superior. Si las entradas del registro de eventos no aparecen en orden cronológico, haga clic en el encabezado Fecha y hora.

La fecha se muestra en formato mes/día/año y la hora, en formato A.M./P.M.

Usuario

El usuario es la persona que ha iniciado la sesión y ha utilizado Internet en el momento en que Privacy Service ha registrado el evento.

Resumen

Los resúmenes muestran una descripción breve y concisa de qué hace Privacy Service para proteger a los usuarios y qué hacen los usuarios en Internet.

Información de evento

El campo **Información de evento** muestra los detalles de la entrada.

Grabación del registro actual

La página **Registro actual** muestra información acerca de acciones administrativas y de usuarios recientes. Puede guardar esta información para verla más adelante.

Para guardar el registro de eventos actual:

1. Inicie una sesión en Privacy Service como administrador.
2. Seleccione **Registro de eventos**.
3. En la página **Registro actual**, haga clic en **Guardar registro**.
4. En el campo **Nombre**, escriba el nombre del archivo de registro.
5. Haga clic en **Guardar**.

Visualización de registros guardados

La página **Registro actual** muestra información acerca de acciones administrativas y de usuarios recientes. Puede guardar esta información para verla más adelante.

Para ver un registro guardado:

1. Inicie una sesión en Privacy Service como administrador.
2. Seleccione **Registro de eventos**.
3. En la página **Registro actual**, haga clic en **Abrir registro**.
4. En el cuadro de diálogo **Seleccione el registro guardado que desee consultar**, seleccione el archivo de registro y haga clic en **Abrir**.

Para acceder a las utilidades, deberá iniciar la sesión en Privacy Service como Administrador y hacer clic en **Utilidades**.

Para eliminar archivos, carpetas o el contenido completo de un disco, haga clic en **McAfee Shredder**. Para guardar la configuración de la base de datos de Privacy Service, haga clic en **Copia de seguridad**. Para restablecer la configuración, haga clic en **Restaurar**.

Eliminación de archivos de manera permanente mediante McAfee Shredder

McAfee Shredder protege su privacidad borrando de forma rápida y segura los archivos no deseados.

Los archivos eliminados se pueden recuperar de su equipo incluso después de haber vaciado la Papelera de reciclaje. Cuando se elimina un archivo, Windows sólo marca ese espacio en la unidad de disco como espacio que ya no está en uso, pero el archivo sigue ahí.

Por qué Windows conserva restos de archivos

Para eliminar permanentemente un archivo, deberá sobrescribir varias veces el archivo existente con datos nuevos. Si Microsoft Windows eliminara los archivos totalmente, cada operación con un archivo sería muy lenta. La purga de un documento mediante Shredder no siempre evita que se recupere, ya que algunos programas crean copias temporales ocultas de los documentos abiertos. Si sólo purga los documentos que se ven en el Explorador, puede que tenga todavía copias temporales de ellos. Le recomendamos que purgue periódicamente el espacio libre de la unidad de disco para asegurarse de que se eliminan de manera permanente esas copias temporales.

NOTA
Mediante herramientas forenses informáticas, se pueden recuperar registros tributarios, currículos u otros documentos que haya eliminado.

Qué borra McAfee Shredder

Con McAfee Shredder, puede borrar de manera segura y permanente lo siguiente:

- Uno o más archivos o carpetas
- Un disco completo
- Los rastros dejados al navegar por la Web

Eliminación permanente de los archivos del Explorador de Windows

Para purgar archivos mediante el Explorador de Windows:

1. Abra el Explorador de Windows, seleccione los archivos que desee purgar.
2. Haga clic con el botón derecho en la selección, elija **Enviar a** y seleccione **McAfee Shredder**.

Vaciado de la Papelera de reciclaje de Windows

Si hay archivos en la Papelera de reciclaje, McAfee Shredder le ofrece un método más seguro para vaciarla.

Para purgar el contenido de la Papelera de reciclaje:

1. En el escritorio de Windows, haga clic con el botón derecho en la Papelera de reciclaje.
2. Seleccione **Vaciar Papelera de reciclaje** y siga las instrucciones que aparezcan en la pantalla.

Personalización de la configuración de Shredder

Puede realizar lo siguiente:

- Especificar el número de pasadas de purga.
- Mostrar un mensaje de advertencia cuando se purguen los archivos.
- Comprobar el disco duro en busca de errores antes de realizar la purga.
- Agregar McAfee Shredder al menú **Enviar a**.
- Colocar un icono de Shredder en el escritorio de Windows.

Para personalizar la configuración de Shredder, abra McAfee Shredder, haga clic en **Propiedades** y siga las instrucciones que aparezcan en la pantalla.

Copia de seguridad de la base de datos de Privacy Service

Puede restaurar la base de datos de Privacy Service de dos formas. Si su base de datos está dañada o se elimina, Privacy Service le pide que restaure la base de datos de Privacy Service. También puede restaurar la configuración de la base de datos mientras se esté ejecutando Privacy Service.

1. Haga clic en **Utilidades** y seleccione **Copia de seguridad**.
2. Haga clic en **Examinar** para seleccionar la ubicación del archivo de la base de datos y haga clic en **Aceptar**.
3. Escriba una contraseña en el campo **Contraseña**.
4. Introduzca de nuevo la contraseña en el campo **Confirmar contraseña** y haga clic en **Copia de seguridad**.

5 Haga clic en **Aceptar** en el cuadro de dialogo de confirmación.

6 Cierre la ventana Privacy Service cuando haya terminado.

NOTA
Mantenga en secreto esta contraseña y no la olvide. No podrá restaurar la configuración de Privacy Service sin esta contraseña.

Restauración de la base de datos desde la copia de seguridad

1 Puede restaurar la configuración original de Privacy Service de dos formas:

- Cargando el archivo de copia de seguridad de la base de datos cuando Privacy Service le solicite que restaure la configuración porque la base de datos está dañada o se ha eliminado.
- Cargando el archivo de copia de seguridad de la base de datos mientras se esté ejecutando Privacy Service.

Para restaurar la configuración de Privacy Service cuando se le solicite:

1 Haga clic en **Examinar** para localizar el archivo.

2 Escriba la contraseña en el campo **Contraseña**.

3 Haga clic en **Restaurar**.
Si no ha realizado una copia de seguridad de la base de datos de Privacy Service, si ha olvidado la contraseña de la copia de seguridad o si la restauración de la base de datos no funciona, deberá desinstalar y volver a instalar Privacy Service.

Para restaurar la configuración de Privacy Service mientras está en ejecución:

1 Haga clic en la ficha **Utilidades**.

2 Haga clic en **Restaurar**.

3 Haga clic en **Examinar** y escriba la ruta y el nombre del archivo de copia de seguridad.

4 Haga clic en **Abrir**.

5 Escriba la contraseña en el campo **Contraseña**.

6 Haga clic en **Restaurar** y después en **Aceptar** en el cuadro de diálogo de confirmación de McAfee Privacy Service.

Estas instrucciones no se aplican al Administrador.

Puede cambiar su contraseña y nombre de usuario. Le recomendamos que cambie su contraseña después de que el Administrador se la haya dado. También recomendamos que cambie la contraseña una vez al mes o cuando crea que alguien la conoce. De este modo, se evita que otras personas utilicen Internet con su nombre de usuario.

Cambio de la contraseña

1 Haga clic con el botón derecho en el icono de McAfee, elija **McAfee Privacy Service** y seleccione **Opciones**.

2 Haga clic en **Contraseña** e introduzca su contraseña en el campo **Contraseña antigua**.

3 Escriba la contraseña nueva en el campo **Nueva contraseña**.

4 Vuelva a escribir la nueva contraseña en el campo **Confirmar contraseña** y haga clic en **Aplicar**.

5 Haga clic en **Aceptar** en el cuadro de dialogo de confirmación. Ahora ya tiene una nueva contraseña.

Cambio del nombre de usuario

1 Haga clic con el botón derecho en el icono de McAfee, elija **McAfee Privacy Service** y seleccione **Opciones**.

2 Haga clic en **Información de usuario**.

3 Escriba un nombre de usuario nuevo en el campo **Nombre de usuario nuevo** y haga clic en **Aplicar**.

4 Haga clic en **Aceptar** en el cuadro de dialogo de confirmación. Ahora ya tiene un nuevo nombre de usuario.

Vaciado de la caché

Recomendamos vaciar la caché para que los niños no puedan acceder a las páginas Web que haya visitado recientemente. Para vaciar la caché, haga lo siguiente:

1. Abra Internet Explorer.
2. En el menú **Herramientas**, haga clic en **Opciones de Internet**. De este modo se abrirá el cuadro de diálogo **Opciones de Internet**.
3. En la sección **Archivos temporales de Internet**, haga clic en **Eliminar archivos**. Aparecerá el cuadro de diálogo **Eliminar archivos**.
4. Seleccione **Eliminar todo el contenido sin conexión** y haga clic en **Aceptar**.
5. Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Opciones de Internet**.

Admisión de cookies

Esta opción sólo está disponible si el administrador le permite aceptar o rechazar cookies al interceptarlos.

Si accede a sitios Web que requieran cookies, puede permitir que dichos sitios lean los cookies.

1. Haga clic con el botón derecho en el icono de McAfee, elija **McAfee Privacy Service** y seleccione **Opciones**.
2. Haga clic en **Cookies aceptados**.
3. Introduzca la URL del sitio Web en el campo **http://** y haga clic en **Agregar**. El sitio Web aparecerá en la lista de sitios Web.

Si necesita eliminar un sitio Web de la lista:

1. Seleccione la URL del sitio en la lista de sitios Web.
2. Haga clic en **Quitar** y después en **Sí**, en el cuadro de diálogo de confirmación.

Rechazo de cookies

Esta opción sólo está disponible si el administrador le permite aceptar o rechazar cookies al interceptarlos.

Si accede a sitios Web que no requieran cookies, puede rechazar las cookies sin que se le solicite hacerlo.

1. Haga clic con el botón derecho en el icono de McAfee, elija **McAfee Privacy Service** y seleccione **Opciones**.
2. Haga clic en **Cookies rechazados**.
3. Introduzca la URL del sitio Web en el campo **http://** y haga clic en **Agregar**. El sitio Web aparecerá en la lista **Sitio Web**.

Si necesita eliminar un sitio Web de la lista:

1. Seleccione la URL del sitio en la lista de sitios Web.
2. Haga clic en **Quitar** y después en **Sí**, en el cuadro de diálogo de confirmación.

McAfee SpamKiller 6

Bienvenido a McAfee SpamKiller.

El software McAfee SpamKiller contribuye a evitar que llegue spam a su bandeja de entrada. Gracias a él, disfrutará de las funciones siguientes:

Opciones de usuario

- Bloquear el spam con filtros y ponerlo en cuarentena fuera de la bandeja de entrada.
- Ver los mensajes bloqueados y aceptados.
- Supervisar y filtrar varias cuentas de correo electrónico.
- Importar las direcciones de confianza a una lista de amigos.
- Luchar contra los remitentes de spam (informar de su existencia, quejarse del spam, crear filtros personalizados).
- Proteger a los menores de los mensajes de spam.
- Bloquear y recuperar los mensajes con un solo clic.
- Compatibilidad con conjuntos de caracteres de doble byte.
- Soporte de varios usuarios (Windows 2000 y Windows XP).

Filtrado

- Actualizar filtros automáticamente.
- Crear filtros personalizados para bloquear los correos electrónicos que contengan principalmente imágenes, texto oculto o formato no válido.
- Motor central de filtrado de varios niveles.
- Filtro de ataques de diccionario.
- Filtrado adaptable de varios niveles.
- Filtros de seguridad.

Funciones

Esta versión de SpamKiller incluye las siguientes funciones:

- Filtrado: las opciones avanzadas de filtrado proporcionan nuevas técnicas de filtrado, incluido soporte para filtrado por metacaracteres e identificación de texto basura.
- Phishing: complemento AntiPhishing de navegador a través de la barra de herramientas de Internet Explorer que identifica con facilidad los sitios Web potenciales de phishing y los bloquea.
- Integración con Microsoft Outlook y Outlook Express: barra de herramientas que proporciona una carpeta en el cliente de correo para bloquear directamente el spam.
- Instalación: configuración e instalación mejoradas. La detección automática de cuentas asegura una instalación, configuración e integración sin problemas con las cuentas de correo electrónico existentes.
- Actualizaciones: actualizaciones automáticas que se ejecutan en segundo plano, siempre alerta para reducir riesgos de exposición a nuevas amenazas de spam.
- Interfaz: una interfaz de usuario intuitiva para mantener al equipo libre de spam.
- Soporte técnico: gratuito y en directo por correo electrónico y mensajería instantánea, para ofrecer una atención al cliente directa, fácil y rápida.
- Procesamiento de mensajes de spam: de forma predeterminada, los mensajes de spam son etiquetados como [SPAM] y se colocan en la carpeta SpamKiller en Outlook y Outlook Express, o en la bandeja de entrada. Los mensajes etiquetados también aparecen en la página **Correos aceptados**.

Descripción del panel superior

Los iconos siguientes aparecen en el panel superior de todas las páginas de SpamKiller:

- Haga clic en **Cambiar usuario**  para iniciar una sesión como otro usuario diferente.

  NOTA
  Cambiar usuario sólo está disponible si el equipo utiliza Windows 2000 o Windows XP, se han agregado varios usuarios a SpamKiller y usted ha iniciado una sesión como Administrador en SpamKiller.

- Haga clic en **Soporte**  para abrir la página de soporte en línea de McAfee, donde encontrará temas útiles sobre SpamKiller y sobre otros productos de McAfee, respuestas a preguntas frecuentes y mucho más. Debe estar conectado a Internet para acceder a la página de soporte.
- Haga clic en **Ayuda**  para abrir la ayuda en línea, donde encontrará instrucciones detalladas sobre la configuración y el uso de SpamKiller.

Descripción de la página Resumen

Haga clic en la ficha **Resumen** para abrir la página **Resumen** (figura 6-1).

- **Información general sobre el estado de SpamKiller**: indica si está activado el filtrado, cuando se activó por última vez una lista de amigos y el número de mensajes de spam que ha recibido hoy. Desde aquí puede activar y desactivar el filtrado de SpamKiller, actualizar las listas de amigos y abrir la página **Correos bloqueados**.
- **Correos más recientes identificados como correos basura y bloqueados**: los mensajes de spam que SpamKiller ha bloqueado más recientemente (mensajes eliminados de la bandeja de entrada).
- **Información general sobre el correo electrónico**: número total de mensajes de correo electrónico, mensajes de spam (mensajes bloqueados) y el porcentaje total de spam recibido.
- **Correo basura reciente**: desglose del tipo de correo spam que ha recibido en los últimos 30 días.

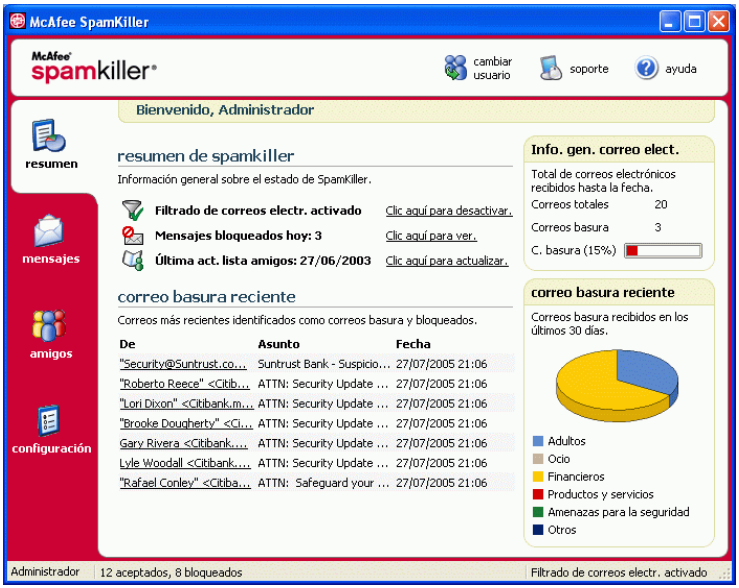


Figura 6-1. Página Resumen

Integración con Microsoft Outlook y Outlook Express

Puede acceder a las funciones fundamentales de SpamKiller desde Outlook Express 6.0, Outlook 98, Outlook 2000 y Outlook XP seleccionando el menú o la barra de herramientas de SpamKiller.

La barra de herramientas de SpamKiller aparece a la derecha de las barras de herramientas estándar de Outlook y Outlook Express. Si la barra de herramientas no es visible, debe ampliar la ventana de la aplicación de correo electrónico o hacer clic en las flechas para ver más barras de herramientas.

Cuando la barra de herramientas aparezca por primera vez en la aplicación de correo electrónico, únicamente podrá utilizar las instrucciones de la barra de herramientas con los nuevos mensajes. El correo spam existente debe eliminarse manualmente.

Desactivación de SpamKiller

Puede desactivar SpamKiller y evitar que se filtren los mensajes de correo electrónico.

Para desactivar el filtrado:

Haga clic con el botón derecho sobre el icono de McAfee  , seleccione **SpamKiller** y haga clic en **Desactivar**. O haga clic en la ficha **Resumen** y, a continuación, en **Clic aquí para desactivar**.

Para activar el filtrado:

Haga clic con el botón derecho sobre el icono de McAfee, seleccione **SpamKiller** y, a continuación, haga clic en **Activar**. O haga clic en la ficha **Resumen** y, a continuación, en **Clic aquí para activar**.

Adición de cuentas de correo electrónico

Puede agregar los siguientes tipos de cuentas de correo electrónico:

- Cuenta de correo electrónico estándar (POP3): la mayoría de usuarios particulares disponen de este tipo de cuenta.
- Cuenta de MSN/Hotmail: cuentas de Internet MSN/Hotmail.

> **NOTA**
> Si su equipo utiliza Windows 2000 o Windows XP y desea agregar varios usuarios a SpamKiller, deberá añadir los usuarios antes de agregar las cuentas de correo electrónico a sus perfiles de usuario. Para obtener más información, consulte *Adición de usuarios* en la página 151. Si agrega varios usuarios a SpamKiller, la cuenta se agregará al perfil del usuario que tiene una sesión iniciada en SpamKiller en este momento.

Adición de una cuenta de correo electrónico

1. Haga clic en la ficha **Configuración** para abrir la página **Configuración** (figura 6-2) y, a continuación, haga clic en **Cuentas de correo electrónico**. Aparece el cuadro de diálogo **Cuentas de correo electrónico**, que muestra todas las cuentas de correo electrónico que se han agregado a SpamKiller.

   > **NOTA**
   > Si se han agregado varios usuarios a SpamKiller, la lista mostrará las cuentas de correo electrónico del usuario que tiene una sesión iniciada en SpamKiller.

2. Haga clic en **Agregar**. Aparecerá el asistente para cuentas de correo electrónico.
3. Siga las instrucciones de los cuadros de diálogo que aparezcan.

Si agrega una cuenta de MSN/Hotmail, SpamKiller buscará una libreta de direcciones MSN/Hotmail de la que poder importar la **Lista personal de amigos**.

Figura 6-2. Página Configuración

Orientación del cliente de correo electrónico a SpamKiller

Si agrega una cuenta y SpamKiller no la detecta (la cuenta no aparece en el cuadro de diálogo **Seleccionar cuenta**) o si desea leer su correo MSN/Hotmail como una cuenta POP3 en SpamKiller, oriente su cliente de correo electrónico a SpamKiller modificando el servidor de correo entrante.

Por ejemplo, si el servidor de mensajes entrantes es “mail.mcafee.com”, cámbielo a “localhost”.

Eliminación de cuentas de correo electrónico

Si desea que SpamKiller deje de filtrar una cuenta de correo electrónico, bórrela.

Eliminación de una cuenta de correo electrónico de SpamKiller

1. Haga clic en la ficha **Configuración** y, a continuación, en **Cuentas de correo electrónico**. Aparece el cuadro de diálogo **Cuentas de correo electrónico**, que muestra todas las cuentas de correo electrónico que se han agregado a SpamKiller.

   NOTA
   Si se han agregado varios usuarios a SpamKiller, la lista mostrará las cuentas de correo electrónico del usuario que tiene una sesión iniciada en SpamKiller.

2. Seleccione una cuenta y haga clic en **Eliminar**.

Edición de las propiedades de la cuenta de correo electrónico

Puede editar información de las cuentas de correo electrónico que haya agregado a SpamKiller. Por ejemplo, es posible cambiar la dirección de correo electrónico, la descripción de la cuenta, la información del servidor, la frecuencia con la que SpamKiller debe comprobar la presencia de spam y el modo en que el equipo se conecta a Internet.

Cuentas POP3

Edición de cuentas POP3

1. Haga clic en la ficha **Configuración** y, a continuación, en **Cuentas de correo electrónico**. Aparece el cuadro de diálogo **Cuentas de correo electrónico**, que muestra todas las cuentas de correo electrónico que se han agregado a SpamKiller.

   NOTA
   Si se han agregado varios usuarios a SpamKiller, la lista mostrará las cuentas de correo electrónico del usuario que tiene una sesión iniciada en SpamKiller.

2. Seleccione una cuenta POP3 y haga clic en **Editar**.

3 Haga clic en la ficha **General** para editar la descripción de la cuenta y la dirección de correo electrónico.

- **Descripción**: descripción de la cuenta. En este cuadro puede escribir la información que desee.
- **Dirección electrónica**: dirección de correo electrónico de la cuenta.

4 Haga clic en la ficha **Servidores** para editar la información del servidor.

- **Entrante**: nombre del servidor que recibe el correo electrónico entrante.
- **Nombre de usuario**: nombre de usuario utilizado para acceder a la cuenta. También conocido como Nombre de cuenta.
- **Contraseña**: contraseña que utiliza para acceder a la cuenta.
- **Saliente**: nombre del servidor que envía el correo electrónico saliente. Haga clic en **Más** para modificar los requisitos de autenticación del servidor de correo electrónico saliente.

5 Haga clic en la ficha **Comprobación** para modificar la frecuencia con la que SpamKiller comprueba la presencia de mensajes de spam en la cuenta:

a Seleccione **Comprobar cada** o **Comprobar a diario a las**; a continuación, seleccione o especifique una hora en el cuadro correspondiente. Si especifica el número cero, SpamKiller sólo comprueba la cuenta cuando se conecta.

b Seleccione otras horas para que SpamKiller filtre la cuenta:

Comprobar al inicio: seleccione esta opción si dispone de conexión directa y desea que SpamKiller compruebe la cuenta cada vez que arranque el equipo.

Comprobar al establecer una conexión: seleccione esta opción sólo si dispone de una conexión telefónica y desea que SpamKiller compruebe la cuenta cada vez que se conecte a Internet.

6 Haga clic en la ficha **Conexión** para especificar el modo en que SpamKiller debe establecer la conexión a Internet para que pueda comprobar su bandeja de entrada en busca de nuevos mensajes que filtrar.

- **No marcar nunca una conexión**: SpamKiller no establece automáticamente ninguna conexión. Primero debe iniciar una conexión manual.
- **Marcar cuando sea necesario**: cuando no hay ninguna conexión a Internet disponible, SpamKiller intenta conectarse automáticamente mediante la conexión predeterminada a Internet.

- **Marcar siempre**: SpamKiller intenta conectar automáticamente con la conexión de acceso telefónico que se haya especificado.
- **Permanecer conectado después de realizar el filtrado**: su equipo permanece conectado a Internet después de finalizar el filtrado.

7 Haga clic en la ficha **Avanzada** para editar las opciones avanzadas.

- **Dejar correos basura en el servidor**: seleccione esta casilla de selección si desea conservar una copia de los mensajes bloqueados en el servidor de correo electrónico. Puede ver mensajes desde el cliente de correo electrónico y desde la página **Correos bloqueados** de SpamKiller. Si la casilla de activación no está seleccionada, sólo podrá ver los mensajes bloqueados desde la página **Correos bloqueados**.
- **Puerto POP3**: (número de puerto POP3) el servidor POP3 gestiona los mensajes entrantes.
- **Puerto SMTP**: (número de puerto SMTP) el servidor SMTP gestiona los mensajes salientes.
- **Tiempo de espera del servidor**: el tiempo que esperará SpamKiller para recibir mensajes de correo antes de agotar el tiempo de espera y detenerse.

  Aumente el valor del tiempo de espera del servidor si tiene problemas para recibir correo. Es posible que su conexión de correo electrónico sea lenta, por lo que aumentar el tiempo de espera del servidor permite que SpamKiller espere más tiempo antes de desconectarse.

8 Haga clic en **Aceptar**.

Cuentas MSN/Hotmail

Edición de las cuentas MSN/Hotmail

1 Haga clic en la ficha **Configuración** y, a continuación, en **Cuentas de correo electrónico**.

Aparece el cuadro de diálogo **Cuentas de correo electrónico**, que muestra todas las cuentas de correo electrónico que se han agregado a SpamKiller.

> **NOTA**
> Si se han agregado varios usuarios a SpamKiller, la lista mostrará las cuentas de correo electrónico del usuario que tiene una sesión iniciada en SpamKiller.

2 Seleccione una cuenta MSN/Hotmail y haga clic en **Editar**.

3 Haga clic en la ficha **General** para editar la descripción de la cuenta y la dirección de correo electrónico.

- **Descripción**: descripción de la cuenta. En este cuadro puede escribir la información que desee.
- **Dirección electrónica**: dirección de correo electrónico de la cuenta.

4 Haga clic en la ficha **Servidores** para editar la información del servidor.

- **Entrante**: nombre del servidor que recibe el correo electrónico entrante.
- **Contraseña**: contraseña que utiliza para acceder a la cuenta.
- **Saliente**: nombre del servidor que envía el correo electrónico saliente.
- **Utilizar un servidor SMTP para los correos salientes**: seleccione esta opción si desea enviar mensajes de error sin que aparezca la línea de firma MSN. La línea de firma MSN permite a los remitentes de correo basura saber que el mensaje de error es falso.

  Haga clic en **Más** para cambiar los requisitos de autenticación del servidor de correo electrónico saliente.

5 Haga clic en la ficha **Comprobación** para especificar con qué frecuencia SpamKiller debe comprobar la presencia de mensajes de spam en la cuenta:

a Seleccione **Comprobar cada** o **Comprobar a diario a las**; a continuación, seleccione o especifique una hora en el cuadro correspondiente. Si especifica el número cero, SpamKiller sólo comprueba la cuenta cuando se conecta.

b Seleccione otras horas para que SpamKiller filtre la cuenta:

Comprobar al inicio: seleccione esta opción si dispone de conexión directa y desea que SpamKiller compruebe la cuenta cada vez que inicie SpamKiller.

Comprobar al establecer una conexión: seleccione esta opción sólo si dispone de una conexión telefónica y desea que SpamKiller compruebe la cuenta cada vez que se conecte a Internet.

6 Haga clic en la ficha **Conexión** para especificar el modo en que SpamKiller debe establecer la conexión a Internet para que pueda comprobar su bandeja de entrada en busca de nuevos mensajes que filtrar.

- **No marcar nunca una conexión**: SpamKiller no establece automáticamente ninguna conexión. Primero debe iniciar una conexión manual.
- **Marcar cuando sea necesario**: cuando no hay ninguna conexión a Internet disponible, SpamKiller intenta conectarse automáticamente con la conexión predeterminada a Internet.

- **Marcar siempre**: SpamKiller intenta conectar automáticamente con la conexión de acceso telefónico que se haya especificado.
- **Permanecer conectado después de realizar el filtrado**: su equipo permanece conectado a Internet después de finalizar el filtrado.

7 Haga clic en **Aceptar**.

Configuración de una cuenta de Hotmail de modo que bloquee el spam en Outlook o Outlook Express

SpamKiller puede filtrar directamente cuentas de Hotmail. Consulte la ayuda en línea para obtener más información. Sin embargo, no podrá bloquear mensajes ni agregar amigos con la barra de herramientas de SpamKiller en Outlook o Outlook Express hasta que configure la cuenta de Hotmail.

1 Configure la cuenta de Hotmail en MSK.

2 Si ya tiene una cuenta de Hotmail en Outlook o Outlook Express, debe eliminarla antes.

3 Agregue la cuenta de Hotmail a Outlook o Outlook Express. Asegúrese de que selecciona **POP3** para el tipo de cuenta y el tipo de servidor de correo electrónico entrante.

4 Llame al servidor entrante `localhost`.

5 Escriba el nombre del servidor saliente SMTP disponible (obligatorio).

6 Complete el proceso de configuración de la cuenta. A partir de ese momento ya podrá bloquear el spam nuevo en Hotmail o agregar amigos.

Cuentas MAPI

Las condiciones siguientes son necesarias para que SpamKiller se integre con éxito con MAPI en Outlook:

- Sólo para Outlook 98: Outlook debe haber sido instalado inicialmente con soporte para empresas/grupos de trabajo.
- Sólo para Outlook 98: la primera cuenta de correo electrónico debe ser una cuenta MAPI.
- El equipo debe haber iniciado una sesión en el dominio.

Edición de cuentas MAPI

1. Haga clic en la ficha **Configuración** y, a continuación, en **Cuentas de correo electrónico**. Aparece el cuadro de diálogo **Cuentas de correo electrónico**, que muestra todas las cuentas de correo electrónico que se han agregado a SpamKiller.

   NOTA
   Si se han agregado varios usuarios a SpamKiller, la lista mostrará las cuentas de correo electrónico del usuario que tiene una sesión iniciada en SpamKiller.

2. Seleccione una cuenta MAPI y haga clic en **Editar**.

3. Haga clic en la ficha **General** para editar la descripción de la cuenta y la dirección de correo electrónico.

   - **Descripción**: descripción de la cuenta. En este cuadro puede escribir la información que desee.
   - **Dirección electrónica**: dirección de correo electrónico de la cuenta.

4. Haga clic en la ficha **Perfil** para editar la información del perfil.

   - **Perfil**: perfil MAPI de la cuenta.
   - **Contraseña**: la contraseña que se corresponde con el perfil MAPI si ha configurado uno (no necesariamente la contraseña de la cuenta de correo electrónico).

5. Haga clic en la ficha **Conexión** para especificar el modo en que SpamKiller debe establecer la conexión a Internet para que pueda comprobar su bandeja de entrada en busca de nuevos mensajes que filtrar.

   - **No marcar nunca una conexión**: SpamKiller no establece automáticamente ninguna conexión. Primero debe iniciar una conexión manual.
   - **Marcar cuando sea necesario**: cuando no hay ninguna conexión a Internet disponible, SpamKiller intenta conectarse automáticamente con la conexión predeterminada a Internet.
   - **Marcar siempre**: SpamKiller intenta conectar automáticamente con la conexión de acceso telefónico que se haya especificado.
   - **Permanecer conectado después de realizar el filtrado**: su equipo permanece conectado a Internet después de finalizar el filtrado.

6. Haga clic en **Aceptar**.

Adición de usuarios

SpamKiller puede configurar diferentes usuarios, correspondientes a los que se hayan configurado en el sistema operativo Windows 2000 o Windows XP.

Cuando se instala SpamKiller en el equipo, se crea automáticamente un perfil de administrador para el usuario de Windows que tenía iniciada la sesión. Si agrega cuentas de correo electrónico a SpamKiller durante la instalación, se añadirán a ese perfil de usuario de administrador.

Antes de agregar otras cuentas de correo electrónico a SpamKiller, decida si necesita agregar otros usuarios de SpamKiller. La adición de usuarios supone una ventaja cuando hay varias personas que usan el mismo equipo y que disponen de sus propias cuentas de correo electrónico. Cada una de las cuentas de correo electrónico se agrega a su propio perfil de usuario, de modo que los usuarios puedan gestionar sus cuentas, configuración personal, filtros personales y **Lista personal de amigos**.

Los tipos de usuario definen las tareas que puede realizar cada usuario en SpamKiller. La siguiente tabla resume los permisos de cada tipo de usuario. Los administradores pueden realizar todas las tareas; los usuarios restringidos sólo pueden realizar tareas adecuadas para sus perfiles personales. Por ejemplo, los administradores pueden ver todo el contenido de los mensajes bloqueados, mientras que los usuarios restringidos sólo pueden ver la línea referente al asunto.

Tareas	Administrador	Usuario restringido
Gestionar cuentas personales de correo electrónico, **Filtros personales**, **Lista personal de amigos** y configuración personal de sonido.	X	X
Gestionar las páginas personales **Correos bloqueados** y **Correos aceptados**.	X	X
Ver el texto de mensaje de los mensajes bloqueados.	X	
Ver el texto de mensaje de los mensajes aceptados.	X	X
Gestionar los filtros globales y la **Lista global de amigos**.	X	
Informar del spam a McAfee.	X	X
Enviar quejas y mensajes de error.	X	X
Gestionar quejas y mensajes de error (crear, modificar y eliminar plantillas de mensajes).	X	
Gestionar usuarios (crear, modificar y eliminar usuarios).	X	

Tareas	Administrador	Usuario restringido
Realizar copias de seguridad y restaurar SpamKiller.	X	
Ver la página **Resumen** del spam recibido.	X	X

Cuando un usuario inicie la sesión en su equipo una vez agregado, se le pedirá que agregue una cuenta de correo a su perfil de usuario.

Para agregar y gestionar usuarios, es necesario lo siguiente:

- Debe haber iniciado la sesión en SpamKiller como administrador.
- Su equipo debe tener Windows 2000 o Windows XP.
- Los usuarios que está agregando o administrando deben tener cuentas de usuario de Windows.

Contraseñas de usuario y protección contra el spam para menores

Si crea una contraseña de usuario mejorará el nivel de privacidad. A la configuración personal de un usuario, a la lista de amigos y a la lista **Correos aceptados** no pueden acceder otros usuarios que no dispongan de la contraseña de inicio de sesión. La creación de contraseñas resulta útil también para evitar que los niños accedan a SpamKiller y vean el contenido de los mensajes de spam.

Creación de una contraseña para un usuario existente de SpamKiller

1. Haga clic en la ficha **Configuración** y, a continuación, en **Usuarios**.
2. Seleccione un usuario y haga clic en **Editar**.
3. Escriba una contraseña en el cuadro **Contraseña**. Cuando un usuario accede a SpamKiller, debe usar la contraseña de inicio de sesión.

IMPORTANTE
Si la olvida, no podrá recuperarla. Sólo los administradores de SpamKiller pueden crear una nueva contraseña para usted.

Adición de un usuario a SpamKiller

1 Haga clic en la ficha **Configuración** y, a continuación, en **Usuarios**.

2 Haga clic en **Agregar**.

Aparecerá una lista de usuarios de Windows. Para agregar a un usuario que no aparezca en la lista, cree una cuenta de usuario de Windows para esa persona. Después, el nuevo usuario debe iniciar una sesión en el equipo al menos una vez. Finalmente, se podrá agregar el usuario a SpamKiller.

NOTA
Los usuarios de Windows con derechos de administrador tienen derechos de administrador de SpamKiller.

3 Seleccione un usuario y haga clic en **Aceptar**. El usuario se agrega a SpamKiller y el nombre de usuario aparece en la lista de usuarios de SpamKiller.

4 Haga clic en **Cerrar** cuando termine de agregar usuarios.

Para crear una contraseña para un usuario, consulte *Creación de una contraseña para un usuario existente de SpamKiller* en la página 152.

La próxima vez que el usuario inicie una sesión en el equipo, se le pedirá que agregue una cuenta de correo electrónico a su perfil de usuario de SpamKiller. Puede agregar cuentas de correo electrónico al perfil de usuario si ha iniciado una sesión en SpamKiller como ese usuario y dispone de la información necesaria sobre la cuenta de correo electrónico. Para obtener más información, consulte *Adición de cuentas de correo electrónico* en la página 143.

Edición de perfiles de usuario de SpamKiller

1 Haga clic en la ficha **Configuración** y, a continuación, en **Usuarios**. Aparecerá una lista de usuarios de SpamKiller.

2 Seleccione un usuario y haga clic en **Editar**.

3 Escriba una contraseña y un nombre nuevos.

Eliminación de un perfil de usuario de SpamKiller

ADVERTENCIA
Cuando se elimina un perfil de usuario, se eliminan también las cuentas de correo electrónico de ese usuario de SpamKiller.

1 Haga clic en la ficha **Configuración** y, a continuación, en **Usuarios**. Aparecerá una lista de usuarios de SpamKiller.

2 Seleccione un usuario de la lista y haga clic en **Eliminar**.

Inicio de sesión en SpamKiller en un entorno de varios usuarios

Cuando los usuarios inician una sesión en el equipo y abren SpamKiller, inician automáticamente una sesión de SpamKiller con sus perfiles de usuario. Si se han asignado contraseñas de SpamKiller a los usuarios, deben introducirlas en el cuadro de diálogo **Inicio de sesión** que aparece.

Cambio de usuario

Debe haber iniciado la sesión en SpamKiller como administrador.

1. Haga clic en **Cambiar usuario**, en la parte superior de la página. Aparecerá el cuadro de diálogo **Cambiar usuario**.
2. Seleccione un usuario y haga clic en **Aceptar**. Si el usuario dispone de contraseña, aparecerá el cuadro de diálogo **Inicio de sesión**. Escriba la contraseña de usuario en el cuadro **Contraseña** y, a continuación, haga clic en **Aceptar**.

Le recomendamos que agregue los nombres y direcciones de correo electrónico de sus amigos a la lista de amigos. SpamKiller no bloquea los mensajes que envían las personas incluidas en la lista. De este modo se puede tener la certeza de que le llegan los mensajes que desea recibir.

SpamKiller permite agregar nombres, direcciones de correo electrónico, dominios y listas de correo a la lista de amigos. Puede agregar direcciones de forma individual o todas a la vez mediante la importación de la libreta de direcciones de su programa de correo electrónico.

Hay dos tipos de listas en SpamKiller:

- **Lista global de amigos**: esta lista afecta a todas las cuentas de correo de los usuarios de SpamKiller. Si se agregaron varios usuarios, debe haber iniciado la sesión en SpamKiller como Administrador para poder gestionar esta lista.
- **Lista personal de amigos**: afecta a todas las cuentas de correo electrónico asociadas a un usuario específico. Si se agregaron varios usuarios, debe haber iniciado la sesión en SpamKiller como usuario para poder gestionar esta lista.

Puede agregar amigos a una lista de amigos para que no se bloquee su correo. La página de amigos muestra los nombres y direcciones que se han agregado a la lista de amigos. Esta página también muestra la fecha en que se agregó un amigo y el número total de mensajes que ha recibido.

Haga clic en la ficha **Direcciones** para ver las direcciones de correo electrónico de la lista de amigos. Haga clic en la ficha **Dominios** para ver las direcciones de dominio de la lista. Haga clic en la ficha **Listas de correo** para ver las listas de correo de la lista de amigos.

Para pasar de la **Lista global de amigos** a la **Lista personal de amigos**, haga clic en la flecha abajo situada en las fichas **Direcciones**, **Dominios** o **Listas de correo** y seleccione **Lista personal de amigos**.

Apertura de una lista de amigos

1 Para abrir una lista de amigos, haga clic en la ficha **Amigos**. Aparecerá la página de **Amigos** (figura 6-3).

2 Haga clic en la ficha **Direcciones**, **Dominios** o **Lista de correo**. Aparecerá la **Lista global de amigos**. Para ver la **Lista personal de amigos**, haga clic en la flecha abajo de una de las fichas y, a continuación, seleccione **Lista personal de amigos**.

NOTA
Si el sistema operativo de su equipo es Windows 2000 o Windows XP y se han agregado varios usuarios a SpamKiller, los usuarios limitados sólo podrán acceder a la **Lista personal de amigos**.

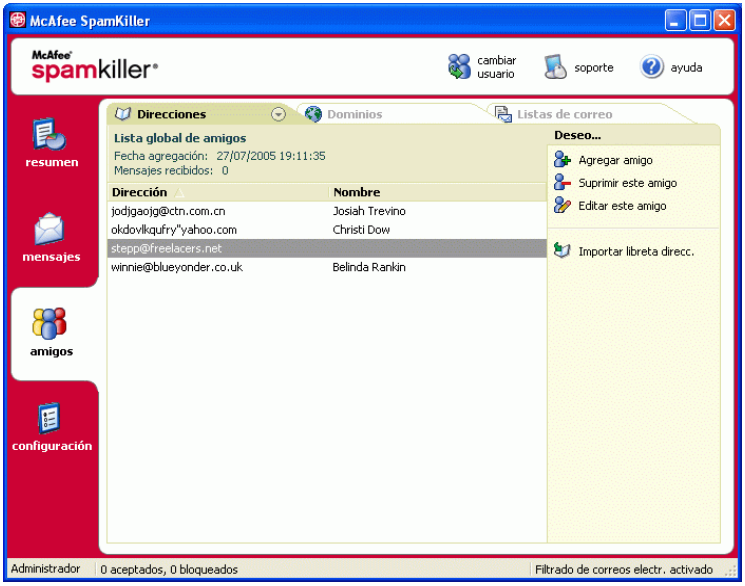


Figura 6-3. Página Amigos

Importación de libretas de direcciones

La importación de libretas de direcciones a una lista de amigos puede realizarse manual o automáticamente. La importación automática permite que SpamKiller compruebe con regularidad sus libretas de direcciones, para verificar si existen nuevas direcciones e importarlas a una lista de amigos.

Puede importar libretas de direcciones de los siguientes programas de correo electrónico:

- Microsoft Outlook (versión 98 y posterior)
- Microsoft Outlook Express (todas las versiones)
- Netscape Communicator (versión 6 y anteriores, si se exportan como archivo LDIF)
- Qualcomm Eudora (versión 5 y posterior)
- IncrediMail Xe
- MSN/Hotmail
- Cualquier programa que pueda exportar su libreta de direcciones en formato de texto normal

Importación automática de una libreta de direcciones

Puede actualizar con regularidad la lista personal de amigos, mediante la creación de un calendario de importación de direcciones de las libretas.

1. Haga clic en la ficha **Configuración** y, a continuación, en **Libreta de direcciones**. Aparece el cuadro de diálogo **Importar libretas de direcciones** que muestra una lista de libretas de direcciones que SpamKiller comprueba con regularidad y desde las cuales importa nuevas direcciones.
2. Haga clic en **Agregar**. Aparecerá el cuadro de diálogo **Importar calendario**.
3. Seleccione el **Tipo** de libreta de direcciones que desea importar y su **Origen**.
4. En el cuadro **Calendario**, seleccione la frecuencia con la que SpamKiller debe comprobar la libreta de direcciones en busca de nuevas direcciones.
5. Haga clic en **Aceptar**. Después de realizar una actualización, las direcciones nuevas se incluyen en la **Lista personal de amigos**.

Importación manual de una libreta de direcciones

Puede importar manualmente libretas de direcciones a la **Lista personal de amigos** o a la **Lista global de amigos**.

> **NOTA**
> Si utiliza el sistema operativo Windows 2000 o Windows XP y ha agregado varios usuarios a SpamKiller, debe iniciar una sesión como Administrador para agregar amigos a la **Lista global de amigos**.

1. Haga clic en la ficha **Amigos** y después en **Importar libreta de direcciones**.

   El cuadro de diálogo **Importar libreta de direcciones** muestra una lista de tipos de libretas de direcciones que se pueden importar.

2. Seleccione el tipo de libreta de direcciones que desee importar o haga clic en **Examinar** para importar direcciones almacenadas en un archivo.

   Para importar una libreta de direcciones solamente a la **Lista personal de amigos**, asegúrese de que la casilla de verificación **Agregar a la lista personal de amigos** está seleccionada. Para importar la libreta de direcciones solamente a la **Lista global de amigos**, asegúrese de que la casilla de verificación no está seleccionada.

3. Haga clic en **Siguiente**. Aparecerá una página de confirmación que le indicará el número de direcciones que ha agregado SpamKiller.

4. Haga clic en **Finalizar**. Las direcciones aparecen en la **Lista global de amigos** o en la **Lista personal de amigos**.

Edición de la información de la libreta de direcciones

Edición de la información de una libreta de direcciones importada de forma automática.

1. Haga clic en la ficha **Configuración** y, a continuación, en **Libreta de direcciones**.
2. Seleccione una libreta de direcciones y haga clic en **Editar**.
3. Modifique la información de la libreta de direcciones y haga clic en **Aceptar**.

Eliminación de libretas de direcciones de la lista de importación automática

Cuando no desee que SpamKiller siga importando automáticamente direcciones de una libreta, elimine la entrada correspondiente.

1. Haga clic en la ficha **Configuración** y, a continuación, en **Libreta de direcciones**.
2. Seleccione una libreta de direcciones y, a continuación, haga clic en **Eliminar**. Aparece un cuadro de diálogo de confirmación.
3. Haga clic en **Sí** para eliminar la libreta de direcciones de la lista.

Adición de amigos

Para asegurarse de que recibe los mensajes de correo electrónico de todos sus amigos, agregue sus nombres y direcciones a una lista de amigos. Puede agregar amigos desde la página **Amigos**, **Correos bloqueados**, **Correos aceptados** y desde Microsoft Outlook o Outlook Express.

NOTA
Si utiliza el sistema operativo Windows 2000 o Windows XP y ha agregado varios usuarios a SpamKiller, debe iniciar una sesión como Administrador para agregar amigos a la **Lista global de amigos**.

Adición de amigos desde las páginas Correos bloqueados o Correos aceptados

1. Haga clic en la ficha **Mensajes** y, a continuación, en la ficha **Correos bloqueados** o **Correos aceptados**.

   O

   En el menú SpamKiller de Microsoft Outlook o Outlook Express, seleccione **Ver correos bloqueados** para abrir la página **Correos bloqueados** correspondiente a esa cuenta.

   Aparece la página **Correos bloqueados** o **Correos aceptados**.

2. Seleccione un mensaje de un remitente que desee agregar a una lista de amigos y haga clic en **Agregar amigo**.

3. En el cuadro **Dirección** escriba la dirección que desee agregar a la lista de amigos. Es posible que el cuadro **Dirección** contenga ya la dirección del mensaje seleccionado.

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

5. Seleccione el tipo de dirección que desea agregar en el cuadro **Tipo de amigo**:

   - **Una dirección de correo electrónico**: la dirección de correo electrónico del remitente se agrega a la sección Dominios de la lista de amigos.
   - **Todos los del dominio**: el nombre de dominio se agrega a la sección **Dominios** de la lista de amigos. SpamKiller acepta todos los mensajes de correo electrónico procedentes del dominio.
   - **Lista de correo**: la dirección se agrega a la sección **Lista de correo** de la lista de amigos.

Para agregar la dirección solamente a la **Lista personal de amigos**, asegúrese de que la casilla de verificación **Agregar a la lista personal de amigos** está seleccionada. Para agregar la dirección solamente a la **Lista global de amigos**, asegúrese de que la casilla de verificación no está seleccionada.

6 Haga clic en **Aceptar**. Todos los mensajes de amigos se marcan como tal y aparecen en la página de **Correos aceptados**.

Adición de amigos desde la página de amigos

1 Haga clic en la ficha **Amigos** y, a continuación, en **Agregar amigo**. Aparecerá el cuadro de diálogo **Propiedades de amigos**.

2 En el cuadro **Dirección** escriba la dirección que desee agregar a la lista de amigos.

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

4 Seleccione el tipo de dirección que desea agregar en el cuadro **Tipo de amigo**:

- **Una dirección de correo electrónico**: la dirección de correo electrónico del remitente se agrega a la sección Dominios de la lista de amigos.
- **Todos los del dominio**: el nombre de dominio se agrega a la sección **Dominios** de la lista de amigos. SpamKiller acepta todos los mensajes de correo electrónico procedentes del dominio.
- **Lista de correo**: la dirección se agrega a la sección **Lista de correo** de la lista de amigos.

Para agregar la dirección solamente a la **Lista personal de amigos**, asegúrese de que la casilla de verificación **Agregar a la lista personal de amigos** está seleccionada. Para agregar la dirección solamente a la **Lista global de amigos**, asegúrese de que la casilla de verificación no está seleccionada.

5 Haga clic en **Aceptar**. Todos los mensajes de amigos se marcan como tal y aparecen en la página de **Correos aceptados**.

Adición de amigos desde Microsoft Outlook

1 Abra su cuenta de correo electrónico en Microsoft Outlook o Outlook Express.

2 Seleccione un mensaje de un remitente que desee agregar a una lista de amigos.

3 Haga clic en  en la barra de herramientas de Microsoft Outlook. Todos los mensajes de amigos se marcan como tal y aparecen en la página de **Correos aceptados**.

Edición de amigos

1. Haga clic en la ficha **Amigos** y, a continuación, en la ficha **Direcciones**, **Dominios** o **Listas de correo**.

   Aparecerá la **Lista global de amigos**. Para ver la **Lista personal de amigos**, haga clic en la flecha abajo de una de las fichas y, a continuación, seleccione **Lista personal de amigos**.

   NOTA
   Si el sistema operativo de su equipo es Windows 2000 o Windows XP y se han agregado varios usuarios a SpamKiller, sólo podrá acceder a la **Lista global de amigos** si dispone de derechos de Administrador.

2. Seleccione una dirección de la lista y, a continuación, haga clic en **Editar**.
3. Modifique la información adecuada y haga clic en **Aceptar**.

Eliminación de amigos

Elimine las direcciones que no desee tener en la lista de amigos.

1. Haga clic en la ficha **Amigos** y, a continuación, en la ficha **Direcciones**, **Dominios** o **Listas de correo**.

   Aparecerá la **Lista global de amigos**. Para ver la **Lista personal de amigos**, haga clic en la flecha abajo de una de las fichas y, a continuación, seleccione **Lista personal de amigos**.

   NOTA
   Si el sistema operativo de su equipo es Windows 2000 o Windows XP y se han agregado varios usuarios a SpamKiller, sólo podrá acceder a la **Lista global de amigos** si dispone de derechos de Administrador.

2. Seleccione una dirección de la lista y, a continuación, haga clic en **Eliminar amigo**. Aparece un cuadro de diálogo de confirmación.
3. Haga clic en **Sí** para eliminar la dirección del amigo.

Haga clic en la ficha **Mensajes** para abrir la página **Mensajes** (figura 6-4) y acceder a los mensajes de correo electrónico bloqueados y aceptados. Las páginas **Correos bloqueados** y **Correos aceptados** tienen funciones similares.

Figura 6-4. Página Mensajes

Página Correos bloqueados

Haga clic en la ficha **Correos bloqueados** de la página **Mensajes** para ver los mensajes bloqueados.

> **NOTA**
> También puede acceder a los mensajes bloqueados desde su cuenta de Microsoft Outlook, seleccionando el menú de SpamKiller y haciendo clic en **Ver mensajes bloqueados**.

Los mensajes bloqueados son mensajes que SpamKiller ha identificado como spam, ha sacado de la bandeja de entrada y ha puesto en la página **Correos bloqueados**.

La página **Correos bloqueados** muestra todos los mensajes de spam eliminados de las cuentas de correo electrónico. Para ver los correos electrónicos bloqueados de una cuenta concreta, haga clic en la flecha abajo de la ficha **Correos bloqueados** y seleccione la cuenta que desee ver.

El panel superior de mensajes muestra los mensajes de spam, organizados por fechas. El mensaje más reciente aparece en primer lugar. El panel inferior de la vista previa contiene el texto del mensaje seleccionado en ese momento.

NOTA
Si el equipo funciona con Windows 2000 o Windows XP, se han agregado varios usuarios a SpamKiller y ha iniciado una sesión de usuario restringido en SpamKiller, en el panel de vista previa no se mostrará el contenido del mensaje.

El panel central muestra detalles del mensaje. Haga clic en las flechas abajo  para ampliar el panel de detalles y ver el texto del mensaje y el encabezado en formato original, incluidas las etiquetas del formato HTML. El panel de detalles del mensaje muestra lo siguiente:

- **Acción**: describe el modo en que SpamKiller ha procesado el mensaje de spam. Acción está asociada a la acción del filtro que bloqueó el mensaje.
- **Razón**: explica por qué SpamKiller ha bloqueado el mensaje. Puede hacer clic sobre la razón para abrir el editor de filtros y ver el filtro. El editor de filtros muestra lo que se busca en los mensajes y la acción que SpamKiller debe realizar cuando encuentre mensajes que respondan al filtro.
- **De**: muestra el remitente del mensaje.
- **Fecha**: muestra la fecha en que se envió el mensaje.
- **Para**: muestra el destinatario del mensaje.
- **Asunto**: muestra el tema que aparece en la línea del asunto del mensaje.

En la columna de la izquierda aparecen iconos que se sitúan junto a los mensajes si se han enviado quejas o mensajes de error manuales:

- Queja enviada  : se ha enviado una queja acerca del mensaje.
- Mensaje de error enviado  : se ha enviado un mensaje de error a la dirección de respuesta del mensaje de spam.
- Queja y mensaje de error enviados  : se han enviado una queja y un mensaje de error.

Para obtener más información acerca de dónde se encuentran los mensajes bloqueados, consulte *¿Dónde se encuentran los mensajes bloqueados?* en la página 167.

Página Correos aceptados

Haga clic en la ficha **Correos aceptados** de la página **Mensajes** para ver los mensajes aceptados.

La página **Correos aceptados** muestra todos los mensajes de la bandeja de entrada de cada una de sus cuentas de correo electrónico. Sin embargo, para las cuentas MAPI, la página **Correos aceptados** no contiene mensajes de correo internos. Para ver los mensajes de correo electrónico aceptados de una cuenta concreta, haga clic en la flecha abajo de la ficha **Correos aceptados** y seleccione la cuenta que desee ver.

> **NOTA**
> SpamKiller está diseñado para aceptar los mensajes de correo electrónico legítimos. Sin embargo, si hay correos electrónicos legítimos en la lista **Correos bloqueados**, puede devolverlos a la bandeja de entrada (y la lista **Correos aceptados**) seleccionando los mensajes y haciendo clic en **Recuperar este mensaje**.

Al igual que en la página **Correos bloqueados**, el panel superior de mensajes muestra los mensajes ordenados por fecha. El panel inferior de vista previa contiene el texto del mensaje seleccionado.

El panel central explica si un mensaje ha sido enviado por un remitente incluido en la lista de amigos o si el mensaje cumple los criterios del filtro, pero la acción de filtrado se ha definido como **Aceptar** o **Marcar como posible correo basura**. Haga clic en las flechas abajo para ampliar el panel de detalles y ver el texto del mensaje y el encabezado en formato original, incluidas las etiquetas de formato HTML.

El panel de detalles del mensaje muestra lo siguiente:

- **Acción**: describe el modo en que SpamKiller ha procesado el mensaje.
- **Razón**: si se ha etiquetado un mensaje, este valor explica el motivo de que SpamKiller lo etiquetara.
- **De**: muestra el remitente del mensaje.
- **Fecha**: muestra la fecha en que se envió el mensaje.
- **Para**: muestra el destinatario del mensaje.
- **Asunto**: muestra el tema que aparece en la línea del asunto del mensaje.

Al lado del mensaje puede aparecer uno de los iconos siguientes:

- Correo electrónico de un amigo : SpamKiller ha detectado que el remitente está en una lista de amigos. Este es un mensaje que usted desea conservar.

- Posible correo basura  : este mensaje coincide con un filtro cuya acción está definida como Marcar como posible spam.
- Queja enviada  : se ha enviado una queja acerca del mensaje.
- Mensaje de error enviado  : se ha enviado un mensaje de error a la dirección de respuesta del mensaje de spam.
- Queja y mensaje de error enviados  : se han enviado una queja y un mensaje de error.

Tareas relativas a los correos electrónicos bloqueados y aceptados

El panel de la derecha de las páginas **Correos bloqueados** y **Correos aceptados** muestra las tareas que se pueden realizar.

- **Bloquear este mensaje**: elimina un mensaje de la bandeja de entrada y lo sitúa en la página **Correos bloqueados** de SpamKiller. (Esta opción sólo aparece en la página **Correos aceptados**.)
- **Recuperar este mensaje**: vuelve a poner este mensaje en la bandeja de entrada (esta opción aparece únicamente en la página **Correos bloqueados**) y abre el cuadro de diálogo **Opciones de recuperación**. Puede agregar automáticamente al remitente a la lista de amigos y recuperar todos los mensajes de este remitente.
- **Suprimir mensaje**: elimina un mensaje seleccionado.
- **Agregar amigo**: agrega el nombre del remitente, la dirección de correo electrónico, el dominio o una lista de correo a una lista de amigos.
- **Agregar un filtro**: crea un filtro.
- **Notificar a McAfee**: informa a McAfee sobre mensajes de spam específicos que ha recibido.
- **Enviar una queja**: envía una queja sobre spam al administrador del dominio del remitente o a otra dirección de correo electrónico que introduzca.
- **Enviar un error**: envía un mensaje de error a la dirección de respuesta de un mensaje de spam.

Recuperación de mensajes

Si la página **Correos bloqueados** o la carpeta SpamKiller de Microsoft Outlook y Outlook Express contienen mensajes de correo electrónico legítimos, puede hacer que vuelvan a colocarse en la bandeja de entrada.

Desde la página Correos bloqueados

1. Haga clic en la ficha **Mensajes** y, a continuación, en la ficha **Correos bloqueados**.

   O

   En el menú SpamKiller de Microsoft Outlook o Outlook Express, seleccione **Ver correos bloqueados** para abrir la página **Correos bloqueados** correspondiente a esa cuenta.

2. Seleccione un mensaje y haga clic en **Recuperar este mensaje**  . Aparecerá el cuadro de diálogo **Opciones de recuperación**.

   - **Agregar amigo**: agrega al remitente a la lista de amigos.
   - **Rescatar todos los mensajes del mismo remitente**: recupera todos los mensajes bloqueados del remitente que envió el mensaje seleccionado.

3. Haga clic en **Aceptar**. El mensaje se vuelve a colocar en la bandeja de entrada y en la página **Correos aceptados**.

Desde la carpeta SpamKiller de Microsoft Outlook o Outlook Express

Seleccione los mensajes y haga clic en **Recuperar selección** en el menú o barra de herramientas de SpamKiller. La selección se vuelve a colocar en el buzón de entrada y se elimina la etiqueta de mensaje ([SPAM] de forma predeterminada).

Bloqueo de mensajes

Bloquea los mensajes de spam que están actualmente en la bandeja de entrada. Cuando se bloquea un mensaje, SpamKiller crea automáticamente un filtro para eliminar ese mensaje de la bandeja de entrada. Puede bloquear mensajes de la bandeja de entrada en la página **Correos aceptados**, en Microsoft Outlook o en Outlook Express.

Desde la página Correos aceptados

1. Haga clic en la ficha **Mensajes** y, a continuación, en la ficha **Correos aceptados**. Aparece la página **Correos aceptados** con los mensajes que se encuentran actualmente en la bandeja de entrada.
2. Seleccione un mensaje y haga clic en **Bloquear este mensaje**. El mensaje se elimina de la bandeja de entrada y de la página **Correos aceptados** y aparece una copia en la carpeta **Correos bloqueados**.

Desde Microsoft Outlook

En Microsoft Outlook, los mensajes de miembros de un servidor de Exchange se consideran seguros y SpamKiller no los filtra. Sólo se filtran los mensajes de origen externo.

1. Abra la bandeja de entrada de Microsoft Outlook o de Outlook Express.
2. Seleccione un mensaje y haga clic en  . En la página **Correos bloqueados** se coloca una copia del mensaje.

¿Dónde se encuentran los mensajes bloqueados?

De modo predeterminado, los mensajes de spam se etiquetan como [SPAM] y se colocan en la carpeta SpamKiller de Outlook y Outlook Express, o en la bandeja de entrada. Los mensajes etiquetados también aparecen en la página **Correos aceptados**.

Eliminación manual de mensajes

1. Haga clic en la ficha **Mensajes** y, a continuación, en la ficha **Correos bloqueados**.

   O

   En el menú SpamKiller de Microsoft Outlook o Outlook Express, seleccione **Ver correos bloqueados** para abrir la página **Correos bloqueados** correspondiente a esa cuenta.

2. Seleccione el mensaje que desea eliminar.

3. Haga clic en **Suprimir este mensaje**. Aparece un cuadro de diálogo de confirmación.

4. Haga clic en **Sí** para eliminar el mensaje.

Modificación del modo en que se procesa el spam

Cuando se detectan mensajes de spam, dichos mensajes se marcan o se bloquean. Los mensajes de spam se eliminan del servidor cada vez que SpamKiller se conecta a él.

Etiquetado

La línea del asunto del mensaje de correo se etiqueta como [SPAM] y el mensaje pasa la bandeja de entrada o a la carpeta SpamKiller, si dispone de Microsoft Outlook u Outlook Express.

Bloqueo

El mensaje se elimina y se coloca en la página **Correos bloqueados** de SpamKiller. Si por error se bloquean mensajes de correo electrónico legítimos, pueden recuperarse (consulte Recuperación de mensajes).

SpamKiller elimina automáticamente los mensajes bloqueados de la página **Correos bloqueados** cuando transcurren 15 días. Es posible configurar la frecuencia con la que se eliminan los mensajes bloqueados.

SpamKiller no elimina automáticamente los mensajes de la página **Correos aceptados**, dado que ésta refleja los mensajes que están actualmente en la bandeja de entrada.

Modificación del modo en que SpamKiller procesa el spam

1. Haga clic en la ficha **Configuración** y, a continuación, en el icono **Opciones de filtrado**.
2. Haga clic en la ficha **Procesamiento**.
   - **Poner el correo basura en una bandeja de mensajes bloqueados**: el spam se eliminará de la bandeja de entrada y se enviará a la página **Correos bloqueados** de SpamKiller.
   - **Etiquetar el correo basura y conservar en el buzón de entrada**: éste es el valor predeterminado. El spam se conserva en la bandeja de entrada, pero en la línea del asunto se añade la indicación [SPAM].

     Conservar los mensajes bloqueados durante ____ días: los mensajes bloqueados permanecen en la página **Correos bloqueados** durante el tiempo que se especifique.

     Conservar los mensajes aceptados durante ____ días: los mensajes aceptados permanecen en la página **Correos aceptados** durante el tiempo que se especifique.
3. Haga clic en **Aceptar**.

Configuración del filtro McAfee AntiPhishing

Los mensajes no solicitados pueden ser de tipo spam, mensajes de correo electrónico que solicitan que el usuario compre productos, o phishing, mensajes que solicitan que el usuario proporcione información personal en un sitio Web falsificado.

El filtro McAfee AntiPhishing proporciona protección contra sitios Web incluidos en una lista negra (con actividades de phishing confirmadas o sospechosos de falsificar sitios Web), o bien una lista gris (incluyen contenidos parciales peligrosos o enlaces a sitios Web incluidos en la lista negra).

Si accede a un sitio Web cuyas actividades de phishing son conocidas o del que se sospecha que es una página Web falsificada, será redirigido a la página del filtro McAfee AntiPhishing.

Para modificar la configuración del filtro AntiPhishing, lleve a cabo los siguientes pasos.

1. Abra Internet Explorer.
2. En el menú **Herramientas**, seleccione **McAfee AntiPhishing Filter**.

- **Activar filtrado de sitio Web**: activado de forma predeterminada. Para desactivar el filtro AntiPhishing, desactive esta casilla de verificación.
- **Permitir acceso a los sitios Web de la lista negra**: coloca un vínculo en la página de redireccionamiento que permite acceder a los sitios de la lista negra. Al hacer clic en dicho vínculo, accederá al sitio Web.
- **Permitir acceso a los sitios Web de la lista gris**: coloca un vínculo en la página de redireccionamiento que permite acceder a los sitios de la lista gris. Al hacer clic en dicho vínculo, accederá al sitio Web.

3. Cuando haya terminado, haga clic en **Aceptar**.

Adición de amigos a una lista de amigos

Consulte *Adición de amigos desde las páginas Correos bloqueados o Correos aceptados* en la página 158.

Adición de filtros

Si desea información sobre los filtros, consulte *Trabajo con filtros*, en la ayuda en línea.

1. Para crear un filtro global, haga clic en la ficha **Configuración**, seleccione **Filtros globales** y haga clic en **Agregar**.

   O

   Para crear un filtro personal, haga clic en la ficha **Configuración**, seleccione **Filtros personales** y haga clic en **Agregar**.

   O

   Haga clic en la ficha **Mensajes**, en **Correos bloqueados** o **Correos aceptados** y haga clic en **Agregar un filtro**.

2. Haga clic en **Agregar** para empezar a crear una condición de filtrado. Aparecerá el cuadro de diálogo **Condición de filtrado**.

3. Cree una condición de filtrado mediante los pasos siguientes.

   Una condición de filtrado es una declaración que indica a SpamKiller lo que debe buscar en un mensaje. En el ejemplo, "El texto del mensaje contiene hipoteca", el filtro busca mensajes que contienen la palabra "hipoteca". Para obtener más información, consulte *Condiciones de filtrado* en la ayuda en línea.

   a. Seleccione un tipo de condición en el primer cuadro.

   b. Seleccione o introduzca valores en los cuadros siguientes.

   c. Si aparecen las siguientes opciones, selecciónelas para definir mejor la condición de filtrado.

      Buscar también en los códigos de formato: esta opción aparece sólo si la condición de filtrado está configurada para buscar en el texto del mensaje. Si selecciona esta casilla de verificación, SpamKiller busca en el texto y en los códigos de formato del mensaje correspondientes al texto que se haya indicado.

      Hacer coincidir variaciones: permite a SpamKiller detectar errores de escritura utilizados habitualmente por los remitentes de spam. Por ejemplo, la palabra “común” se puede escribir de forma incorrecta como “c0mVn” para eludir los filtros.

Expresiones regulares (RegEx): permite especificar patrones de caracteres empleados en las condiciones de filtrado. Para comprobar un patrón de caracteres, haga clic en **Probar RegEx**.

Diferencia entre mayúsculas y minúsculas: esta opción aparece sólo para las condiciones en las que se introduce un valor de condición. Si selecciona esta casilla de verificación, SpamKiller distinguirá entre las letras mayúsculas y minúsculas del valor que haya introducido.

d Haga clic en **Aceptar**.

4 Cree otra condición de filtrado como se indica a continuación o vaya al paso 5 para seleccionar una acción de filtrado:

a Haga clic en **Agregar** y cree la condición de filtrado. Haga clic en **Aceptar** cuando haya terminado de crear la condición de filtrado.

Las dos condiciones aparecerán en la lista **Condiciones de filtrado** unidas por el operador **y**. El operador **y** indica que SpamKiller buscará mensajes que coincidan con *ambas* condiciones de filtrado. Si desea que SpamKiller busque mensajes que coincidan al menos con una de las dos condiciones, cambie **y** por **o** haciendo clic en **y** y seleccionando **o** en el cuadro que aparece.

b Haga clic en **Agregar** para crear otra condición, o vaya al paso 5 para seleccionar una acción de filtrado.

Si crea tres o más condiciones de filtrado, puede agruparlas para formar cláusulas. Si desea ver ejemplos de agrupaciones, consulte *Trabajo con filtros* en la ayuda en línea.

Para agrupar condiciones de filtrado, seleccione una condición y haga clic en **Agrupar**. Para desagrupar condiciones de filtrado, seleccione una condición agrupada y haga clic en **Desagrupar**.

5 Seleccione una acción de filtrado en el cuadro **Acción**. La acción de filtrado le indica a SpamKiller cómo debe procesar los mensajes que encuentre ese filtro. Para obtener más información, consulte *Acciones de filtrado* en la ayuda en línea.

6 Haga clic en **Avanzadas** para seleccionar opciones avanzadas de filtrado (la selección de opciones avanzadas no es obligatoria). Para obtener más información, consulte *Opciones de filtros avanzadas* en la ayuda en línea.

7 Haga clic en **Aceptar** cuando haya terminado de crear el filtro.

NOTA
Para modificar una condición, selecciónela y haga clic en **Editar**. Para suprimir una condición, selecciónela y haga clic en **Eliminar**.

Expresiones regulares

Las expresiones regulares sólo están disponibles para las siguientes condiciones de filtrado: **El asunto**, **El texto del mensaje**, **Al menos una de las frases siguientes**.

Las secuencias y los caracteres especiales descritos a continuación se pueden emplear como expresiones regulares al definir condiciones de filtrado. Por ejemplo:

- La expresión regular **[0-9]*\,[0-9]+** coincide con los números con coma flotante siempre que no se utilice una notación de ingeniería. La expresión regular coincide con: “12.12”, “0.1212” y “12.0”, pero no con “12” y “12”.
- La expresión regular **\D*[0-9]+\D*** coincide con todas las palabras que incluyan números: “SpamKi11er” y V1AGRA”, pero no “SpamKiller” ni “VIAGRA”.

****

Marca el siguiente carácter como especial o literal. Por ejemplo, “n“ coincide con el carácter “n”. “\n” coincide con un carácter de nueva línea. La secuencia “\\” coincide con “\” y “\(” con “(”.

^

Coincide con el comienzo de la introducción de datos.

$

Coincide con el fin de la introducción de datos.

*

Coincide con el carácter anterior cero o más veces. Por ejemplo, “zo*” coincide con el carácter “z” o con “zoo”.

+

Coincide con el carácter anterior una o más veces. Por ejemplo, “zo+” coincide con “zoo”, pero no con “z”.

?

Coincide con el carácter anterior cero veces o una vez. Por ejemplo, “e?ca?” coincide con “ca“ en “nunca”.

.

Coincide con cualquier carácter individual excepto un carácter de nueva línea.

(patrón)

Coincide con un patrón y recuerda la coincidencia. La cadena secundaria que coincide se puede recuperar del conjunto de resultados, empleando la expresión [0]...[n]. Para hacer coincidir los caracteres de paréntesis ( ), utilice “\(” o “\)”.

x|y

Coincide con x o y. Por ejemplo, “z|loco” busca “z” o “loco”. “(z|l)oco” busca “zoco” o “loco”.

{n}

La n es un número entero no negativo. Coincide exactamente n veces. Por ejemplo, “o{2}” no coincide con la “o” de “Bob”, pero sí con las primeras dos de “cooooomida”.

{n,}

La n es un número entero no negativo. Coincide al menos n veces. Por ejemplo, “u{2,}“ no coincide con la “u“ de “Juan“ pero coincide con todas las u de “¡cuuuuuuidado!“. La expresión “o{1,}“ equivale a “o+“. La expresión “o{0,}“ equivale a “o*“.

{n,m}

Las letras m y n son números enteros no negativos. Coincide al menos n veces y como mucho m veces. Por ejemplo, “u{1,3}“ coincide con las primeras tres ues de “cuuuuuuidado“. La expresión “o{0,1,}“ equivale a “o?“.

[xyz]

Un conjunto de caracteres. Coincide con cualquiera de los caracteres incluidos. Por ejemplo, “[abc]” coincide con la “a” de “plano”.

[^xyz]

Un conjunto negativo de caracteres. Coincide con cualquiera de los caracteres no incluidos. Por ejemplo, “[^abc]” coincide con la “p” de “plano”.

[a-z]

Un intervalo de caracteres. Coincide con cualquiera de los caracteres incluidos en el intervalo especificado. Por ejemplo, “[a-z]” coincide con cualquier carácter alfabético en el intervalo de la “a” a la “z”.

[^m-z]

Un conjunto negativo de caracteres. Coincide con cualquiera de los caracteres no incluidos en el intervalo especificado. Por ejemplo, “[^m-z]” coincide con cualquier carácter que no se encuentre en el intervalo de la “m” a la “z”.

\b

Coincide con un límite de palabra, es decir, con la posición entre una palabra y un espacio. Por ejemplo, “ca\b” coincide con “ca” en “nunca”, pero no con “ca” en “casa”.

\B

Coincide con un límite que no sea el espacio entre palabras. “ta*r\B” coincide con “tar” en “nunca tarde”.

\d

Coincide con un carácter de dígito. Equivale a [0-9].

\D

Coincide con un carácter que no sea un dígito. Equivale a [^0-9].

\f

Coincide con un carácter de salto de página.

\n

Coincide con un carácter de nueva línea.

\r

Coincide con un carácter de retorno de carro.

\s

Coincide con cualquier espacio en blanco, incluidos espacios, tabulaciones, saltos de página, etc. Equivale a “[\f\n\r\t\v]”.

\S

Coincide con cualquier carácter que no sea un espacio en blanco. Equivale a “[^ \f\n\r\t\v]”.

\t

Coincide con un carácter de tabulación.

\v

Coincide con un carácter de tabulación vertical.

\w

Coincide con cualquier carácter de palabra, incluido el subrayado. Equivale a “[A-Za-z0-9_]”.

\W

Coincide con cualquier carácter que no forme parte de una palabra. Equivale a “[A-Za-z0-9_]”.

\núm

Coincide con núm, donde núm es un entero positivo. Referencia a las coincidencias recordadas. Por ejemplo, "(.)\1" coincide con dos caracteres idénticos consecutivos.

\n

Coincide con n, donde n es un valor de escape octal. Los valores de escape octales deben tener una longitud de 1, 2 o 3 dígitos. Por ejemplo, tanto "\11" como "\011" coinciden con un carácter de tabulación. "\0011" equivale a "\001" y "1". Los valores de escape octales no deben ser superiores a 256. Si lo son, sólo se tienen en cuenta los dos primeros dígitos para la expresión. Permite emplear los códigos ASCII en las expresiones regulares.

\xn

Coincide con n, donde n es un valor de escape hexadecimal. Los valores de escape hexadecimales deben tener una longitud de dos dígitos. Por ejemplo, "\x41" coincide con "A" "\x041" equivale a "\x04" y "1". Permite emplear los códigos ASCII en las expresiones regulares.

Notificación del spam a McAfee

Puede notificar acerca del spam a McAfee para que lo analice y actualice los filtros.

1. Haga clic en la ficha **Mensajes** y, a continuación, haga clic en la ficha **Correos bloqueados** o **Correos aceptados**. Aparece la página **Correos bloqueados** o **Correos aceptados**.
2. Seleccione un mensaje y haga clic en **Notificar a McAfee**. Aparece un cuadro de diálogo de confirmación.
3. Haga clic en **Sí**. El mensaje se envía automáticamente a McAfee.

Envío manual de quejas

Envíe una queja para que el remitente no le vuelva a enviar correo basura. Para obtener más información sobre el envío de quejas, consulte *Envío de quejas y mensajes de error* en la ayuda en línea.

1. Haga clic en la ficha **Mensajes** y, a continuación, en la ficha **Correos bloqueados** o **Correos aceptados**. Aparecerá una lista de mensajes.
2. Seleccione un mensaje sobre el que desea quejarse y haga clic en **Enviar queja**. Aparecerá el cuadro de diálogo **Enviar queja**.
3. Seleccione a quién desea enviarle la queja.

   ADVERTENCIA
   En la mayoría de los casos, no se debe seleccionar **Remitente**. Si se envía una queja al remitente del spam, éste puede confirmar su dirección de correo electrónico y enviarle aún más mensajes.

4. Haga clic en **Siguiente** y siga las instrucciones de los cuadros de diálogo que irán apareciendo.

Envío de mensajes de error

Para obtener más información sobre el envío de mensajes de error, consulte *Envío de quejas y mensajes de error* en la ayuda en línea.

Envíe un mensaje de error para que el remitente no le vuelva a enviar spam.

Envío manual de mensajes de error

1. Haga clic en la ficha **Mensajes** y, a continuación, en la ficha **Correos bloqueados** o **Correos aceptados**. Aparecerá una lista de mensajes.
2. Para enviar un mensaje de error sobre un mensaje de correo basura específico, seleccione el mensaje y haga clic en **Enviar error**. Se envía un mensaje de error a la dirección de respuesta del spam.

SpamKiller no puede comunicarse con su servidor

Si el servidor de SpamKiller no se inicia o lo está bloqueando otra aplicación, no puede comunicarse con su servidor.

Inicio del servidor de SpamKiller manualmente

Esta sección sólo se aplica a los usuarios de Microsoft Windows 2000 y XP.

1. Haga clic en **Inicio** y seleccione **Ejecutar**.
2. Escriba SERVICES.MSC y haga clic en **Aceptar**.
3. Haga clic con el botón derecho en Servidor de McAfee SpamKiller y seleccione **Iniciar**. El servicio del servidor se inicia.

El servidor de SpamKiller está bloqueado por cortafuegos o programas de filtrado de Internet

Si el servicio de servidor de SpamKiller ya se ha iniciado y está funcionando, siga estos pasos.

1. Compruebe que Servidor de SpamKiller y/o MSKSrvr.exe tienen acceso completo a todos los programas de cortafuegos que estén instalados, incluido McAfee Personal Firewall.
2. Compruebe que LocalHost y/o 127.0.0.1 no están bloqueados ni prohibidos en ningún programa de cortafuegos instalado, incluido McAfee Personal Firewall.
3. Desactive todos los programas de privacidad o filtrado de Internet.

No se puede conectar con el servidor de correo electrónico

Si el servidor de SpamKiller intenta conectar con el servidor POP3 y la conexión no se realiza con éxito, siga estos pasos.

Verificación de la conexión a Internet

Usuarios de acceso telefónico

1. Haga clic en **Continuar con lo que hacía** cuando aparezca el mensaje de error (en caso necesario).
2. Establezca una conexión con Internet.
3. Mantenga la conexión durante al menos 15 minutos para ver si el mensaje vuelve a aparecer.

Banda ancha (cable, DSL)

1. Haga clic en **Continuar con lo que hacía** cuando aparezca el mensaje de error (en caso necesario).
2. Compruebe que hay conexión a Internet navegando por algún sitio Web.

Comprobación de la dirección del servidor POP3 de SpamKiller

1. Haga clic con el botón derecho en el icono de McAfee en la bandeja del sistema (esquina inferior derecha), elija **SpamKiller** y seleccione **Configuración**.
2. Haga clic en **Cuentas de correo electrónico**.
3. Resalte la cuenta de correo electrónico en el mensaje de error.
4. Haga clic en **Editar**.
5. Seleccione la ficha **Servidores**.
6. Anote la dirección del servidor en el cuadro **Correo entrante** y compárela con la dirección del servidor de correo entrante que su proveedor de servicios de Internet (ISP) le haya indicado para su cuenta de correo electrónico. Ambas direcciones de servidor deberían coincidir.
7. Compruebe las contraseñas volviendo a introducir la que le asignó su ISP para su cuenta de correo electrónico.
8. Haga clic en **Aceptar**.
9. Haga clic en **Cerrar**.

Glosario 7

802.11

Conjunto de estándares IEEE para tecnología LAN inalámbrica. 802.11 especifica una interfaz a través de ondas entre un cliente inalámbrico y una estación base o entre dos clientes inalámbricos. Las distintas especificaciones de 802.11 incluyen: 802.11a, estándar que admite hasta 54 Mbps en la banda de 5 Ghz; 802.11b, estándar que admite hasta 11 Mbps en la banda de 2,4 Ghz; 802.11g, estándar que admite hasta 54 Mbps en la banda de 2,4 Ghz y 802.11i, un conjunto de estándares de seguridad para todas las redes Ethernet inalámbricas.

802.11a

Extensión de 802.11 que se aplica a redes LAN inalámbricas y envía 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 se aplica a redes LAN inalámbricas y que proporciona una velocidad de transmisión de 11 Mbps en la banda de 2,4 GHz. 802.11b se considera actualmente el estándar para redes inalámbricas.

802.11g

Extensión de 802.11 que se aplica a redes LAN inalámbricas y que proporciona una velocidad de transmisión de hasta 54 Mbps en la banda de 2,4 GHz.

802.1x

No admitido por Wireless Home Network Security. Estándar IEEE para la autenticación de redes con cable e inalámbricas, aunque se utiliza principalmente con redes inalámbricas 802.11. Este estándar proporciona sólida autenticación mutua entre un cliente y un servidor de autenticación. Además, 802.1x puede proporcionar claves WEP dinámicas por usuario y por sesión, eliminando el trabajo de administración y los riesgos de seguridad de las claves WEP estáticas.

A

adaptador inalámbrico

Contiene el sistema de circuitos que permiten a un equipo u otro dispositivo comunicarse con un enrutador inalámbrico (conectado una red inalámbrica). Los adaptadores inalámbricos pueden venir integrados en el sistema de circuitos principal de un dispositivo de hardware o bien como un complemento independiente que puede insertarse en un dispositivo a través del puerto apropiado.

ancho de banda

Cantidad de datos que pueden transmitirse en un período de tiempo fijo. En el caso de dispositivos digitales, el ancho de banda se expresa normalmente en bits por segundo (bps) o bytes por segundo. En el caso de dispositivos analógicos, se expresa en ciclos por segundo o hercios (Hz).

ataque de diccionario

Estos ataques consisten en probar gran cantidad de palabras de una lista para intentar averiguar la contraseña de un usuario. Los agresores no prueban todas las combinaciones de forma manual, sino que disponen de herramientas que intentan identificar automáticamente la contraseña de la víctima.

ataque de fuerza bruta

Se trata de un método de ensayo y eliminación de error utilizado por aplicaciones cuyo objetivo es descodificar datos cifrados, como contraseñas, realizando un esfuerzo contundente (mediante la fuerza bruta) en lugar de emplear estrategias intelectuales. Al igual que un delincuente que intentara abrir una caja fuerte probando con muchas combinaciones posibles, una aplicación de descifrado por fuerza bruta intenta todas las combinaciones posibles de caracteres legales por orden. La fuerza bruta se considera un método infalible, aunque lleva mucho tiempo.

ataque de intermediario

El agresor intercepta mensajes en un intercambio de clave pública y los retransmite, sustituyendo su propia clave pública por la solicitada, de manera que las dos partes originales continúan comunicándose entre sí directamente. El agresor utiliza un programa que simula ser el servidor para el cliente y el cliente para el servidor. El ataque puede utilizarse sencillamente para obtener acceso a los mensajes o para permitir al agresor modificarlos antes de transmitirlos de nuevo. El término en inglés (Man-in-the-Middle Attack) procede de un juego de pelota en el que un número de personas intentan lanzarse la pelota directamente entre ellos mientras que otra persona en el centro intenta interceptarla.

autenticación

Proceso de identificación de un individuo y que habitualmente consiste en un nombre de usuario y una contraseña. La autenticación garantiza que el individuo es quien dice ser, aunque no influye en sus derechos de acceso.

B

C

cifrado

Traducción de datos a un código secreto. El cifrado es la manera más eficaz de conseguir la seguridad de los datos. Para leer un archivo cifrado, una persona debe tener acceso a la clave o contraseña secreta que permite descifrarlo. Los datos que no están cifrados se denominan texto normal; a los datos cifrados se les conoce como texto cifrado o codificado.

clave

Serie de letras y/o números utilizados por dos dispositivos con objeto de autenticar sus comunicaciones. Ambos dispositivos deben disponer de la clave. Véase también WEP y WPA-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.

cortafuegos

Sistema diseñado para impedir el acceso no autorizado de entrada o salida de una red privada. Los cortafuegos pueden estar basados en hardware y en software, o en una combinación de ambos. Se utilizan con frecuencia para impedir que usuarios de Internet no autorizados accedan a redes privadas conectadas a Internet y particularmente a una intranet. Todos los mensajes que entran o salen de la intranet atraviesan el cortafuegos. Éste examina cada mensaje y bloquea los que no cumplen los criterios de seguridad especificados. Un cortafuegos se considera la primera línea de defensa para la protección de la información confidencial. Para conseguir un mayor nivel de seguridad, los datos pueden cifrarse.

D

denegación de servicio

En Internet, un ataque de denegación de servicio (DoS) es un incidente en el que a un usuario u organización se le priva de los servicios de un recurso del que dispondría en condiciones normales. Por lo general, la pérdida de servicio es la imposibilidad de utilizar un servicio de red concreto, como el correo electrónico, o la pérdida temporal de todos los servicios y conectividad de red. Un ejemplo de un caso grave sería el de un sitio Web al que acceden millones de personas y que podría verse forzado a cesar sus operaciones de forma temporal. Un ataque de denegación de servicio también puede destruir programas y archivos en un equipo informático. Aunque habitualmente se trata de ataques intencionados y agresivos, también pueden producirse en ocasiones de manera accidental. Es un tipo de ataque a la protección de un sistema informático que no resulta por lo general en el robo de información ni conlleva ninguna otra pérdida de seguridad. Sin embargo, estos ataques pueden suponer para la persona o compañía que los sufren una pérdida importante de tiempo y dinero.

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 cero y 255. Un ejemplo de dirección IP sería 192.168.1.100.

dirección MAC (Media Access Control Address)

Una dirección de nivel bajo asignada al dispositivo físico que accede a la red.

E

enrutador

Dispositivo de red que reenvía paquetes de una red a otra. Los enrutadores están basados en las tablas de enrutamiento internas, leen todos los paquetes entrantes y deciden cómo reenviarlos. La interfaz del enrutador a la que se envían los paquetes salientes viene determinada por cualquier combinación de direcciones de origen y destino, así como por las condiciones del tráfico actual, como la carga, los costes de la línea y las líneas defectuosas. También se le conoce como punto de acceso (PA).

ESS (Extended Service Set)

Conjunto de servicios ampliados. Un grupo de dos o más redes que forman una subred única.

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.

G

H

hotspot

Ubicación geográfica específica en la que un punto de acceso proporciona servicios públicos de red inalámbrica de banda ancha a visitantes móviles a través de una red inalámbrica. Los hotspots o zonas de cobertura inalámbrica se encuentran con frecuencia en lugares con gran afluencia de público, como aeropuertos, estaciones de tren, bibliotecas, puertos deportivos, palacios de congresos y hoteles. Generalmente, su alcance de acceso es corto.

I

itinerancia

También conocido como roaming, es la capacidad para moverse de una zona de cobertura de un punto de acceso a otra sin que se produzca una interrupción del servicio ni una pérdida de conectividad.

J

K

L

M

MAC (Media Access Control o Message Authenticator Code)

Para la primera acepción, véase dirección MAC. La segunda se refiere a un código que se utiliza para identificar un mensaje determinado (p.ej., un mensaje RADIUS). Se emplea un código hash criptográficamente fuerte del contenido del mensaje que incluye un valor exclusivo para protegerse contra transmisiones.

N

O

P

PPPoE

Acrónimo del inglés Point-to-Point Protocol Over Ethernet, Protocolo punto a punto en Ethernet. Utilizado por muchos proveedores de DSL, PPPoE admite las capas de protocolos y la autenticación que más se utilizan en PPP y permite que se establezca una conexión punto a punto en la arquitectura multipunto de Ethernet.

protocolo

Formato acordado para la transmisión de datos entre dos dispositivos. Desde la perspectiva de un usuario, el único aspecto interesante sobre los protocolos está en el hecho de que su equipo o dispositivo debe admitir los protocolos adecuados si quiere comunicarse con otros equipos. El protocolo se puede basar en hardware o en software.

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.

Punto de acceso (PA)

Dispositivo de red que permite a clientes 802.11 conectarse a una red de área local (LAN). Los puntos de acceso amplían el alcance de servicio físico de un usuario inalámbrico. También se conoce como enrutador inalámbrico.

punto de acceso no autorizado

Punto de acceso para el que una empresa no ha concedido autorización. El problema radica en que un punto de acceso no autorizado no cumple las directivas de seguridad de redes LAN (WLAN) inalámbricas. Un punto de acceso no autorizado permite la conexión abierta e insegura a una red corporativa desde el exterior del centro físico controlado.

En una red WLAN convenientemente protegida, los puntos de acceso no autorizados son más dañinos que los usuarios malintencionados. Los usuarios no autorizados que intentan acceder a una red WLAN tienen pocas posibilidades de llegar a recursos valiosos de la empresa si hay implantados mecanismos de autenticación eficaces. Sin embargo, los principales problemas aparecen cuando un empleado o pirata informático conecta un punto de acceso no autorizado. Estos puntos permiten el acceso a la red corporativa a cualquiera que disponga de un dispositivo equipado con 802.11. Esto les sitúa muy cerca de los recursos de vital importancia.

Q

R

RADIUS (Remote Access Dial-In User Service)

Protocolo que proporciona autenticación para usuarios, normalmente en el contexto del acceso remoto. Originalmente definido para el uso con servidores de acceso telefónico remoto, este protocolo 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. La información sobre esta red se mantiene en McAfee Wireless Home Network Security. Véase ESS.

red de área local (LAN)

Red de equipos informáticos que cubre un área relativamente pequeña. La mayoría de las redes LAN están limitadas a un edificio o un grupo de edificios. Sin embargo, una red LAN puede estar conectada a otras redes LAN sin límite de distancia a través del teléfono u ondas de radio. A los sistemas de redes LAN conectadas de esta forma se les llama redes de área extensa (WAN).

La mayoría de las redes LAN conectan estaciones de trabajo y equipos personales, habitualmente a través de concentradores o conmutadores sencillos. Cada nodo (equipo individual) de una red LAN dispone de su propia CPU con la que ejecuta los programas, pero también puede acceder a los datos y dispositivos (p. ej., impresoras) de cualquier parte de la red. Esto significa que muchos usuarios pueden compartir dispositivos costosos, como impresoras láser, además de datos. Los usuarios también pueden utilizar la red LAN para comunicarse entre sí; por ejemplo, a través del correo electrónico o mediante sesiones de chat.

red de área local inalámbrica (WLAN)

Véase también LAN. Red de área local que utiliza un medio inalámbrico para la conexión. Una WLAN utiliza ondas de radio de alta frecuencia en lugar de cables para la comunicación entre nodos.

red privada virtual (VPN)

Red que se configura utilizando una red pública para unir nodos. Por ejemplo, hay sistemas que permiten crear redes utilizando Internet como medio de transporte de los datos. Estos sistemas utilizan el cifrado y otros mecanismos de seguridad para garantizar que sólo los usuarios autorizados puedan acceder a la red y para impedir que se intercepten los datos.

S

secreto compartido

Véase también RADIUS. Protege partes importantes de los mensajes RADIUS. Este secreto compartido es una contraseña que se comparte entre el autenticador y el servidor de autenticación de manera segura.

SSID (Service Set Identifier)

Nombre de red de los dispositivos de un subsistema LAN inalámbrico. Se trata de una cadena de 32 caracteres de texto sin formato que se añade al encabezado de todos los paquetes WLAN. Los SSID diferencian una WLAN de otra, de manera que todos los usuarios de una red deben facilitar el mismo SSID para acceder a un determinado punto de acceso. Un SSID impide el acceso a cualquier dispositivo cliente que no disponga del SSID. Sin embargo, de manera predeterminada, un punto de acceso difunde su SSID en su señal. Incluso si se desactiva la difusión del SSID, un pirata informático puede detectarlo a través de interceptación (sniffing).

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. Tanto Netscape Navigator como Internet Explorer utilizan y admiten SSL; asimismo, muchos sitios Web utilizan este protocolo para obtener información confidencial del usuario, como números de tarjetas de crédito. Como norma general, las direcciones URL que requieren una conexión SSL empiezan por https: en lugar de por http:

T

tarjeta adaptadora inalámbrica PCI

Conecta un equipo de sobremesa a una red. La tarjeta se inserta en una ranura de expansión PCI dentro del equipo.

tarjeta adaptadora inalámbrica USB

Proporciona una interfaz serie Plug and Play ampliable. Esta interfaz proporciona una conexión inalámbrica estándar de bajo coste para dispositivos periféricos como teclados, ratones, joysticks, impresoras, escáneres, dispositivos de almacenamiento y cámaras de videoconferencia.

tarjeta de interfaz de red (NIC)

Acrónimo del inglés Network Interface Card. Tarjeta que se inserta en un portátil u otro dispositivo y que conecta el dispositivo a la red LAN.

texto cifrado

Datos que se han cifrado. El texto cifrado es ilegible hasta que se convierte en texto normal (se descifra) mediante una clave.

texto normal

Cualquier mensaje que no esté cifrado.

TKIP (Temporal Key Integrity Protocol)

Método rápido de superar el punto débil inherente a la seguridad WEP, en concreto la reutilización de 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 equipo 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. WEP también utiliza RC4.

U

V

W

Wardriver

Intrusos armados con equipos portátiles, software especial y hardware improvisado, que deambulan por ciudades, barrios periféricos y parques empresariales con el objetivo de interceptar tráfico de redes LAN inalámbricas.

WEP (Wired Equivalent Privacy)

Protocolo de cifrado y autenticación definido como parte del estándar 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)

Utilizado genéricamente para referirse a cualquier tipo de red 802.11, ya sea 802.11b, 802.11a, banda dual, etc. Es el término utilizado por la Wi-Fi Alliance.

Wi-Fi Alliance

Organización formada por los principales proveedores de software y equipos inalámbricos con el objetivo de (1) certificar la interoperabilidad de todos los productos basados en 802.11 y (2) promocionar el término Wi-Fi como marca global entre mercados para todos los productos LAN inalámbricos basados en 802.11. La organización sirve como consorcio, laboratorio de pruebas y centro de intercambio de información para proveedores que desean promocionar la interoperabilidad y el crecimiento de la industria.

Mientras que todos los productos 802.11a/b/g se conocen como Wi-Fi, sólo los productos que superan las pruebas de la Wi-Fi Alliance pueden denominarse Wi-Fi Certified (marca registrada). Los productos que superan dichas pruebas deben identificarse mediante un sello en el paquete con la leyenda Wi-Fi Certified y la banda de frecuencia de radio que utilizan. El grupo se denominaba anteriormente Wireless Ethernet Compatibility Alliance (WECA), pero cambió de nombre en octubre de 2002 para reflejar de una forma más precisa la marca Wi-Fi que desea crear.

Wi-Fi Certified

Cualquier producto probado y aprobado como Wi-Fi Certified (marca registrada) por la Wi-Fi Alliance tiene el certificado de interoperabilidad con otro producto, incluso si pertenecen a fabricantes distintos. 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. No obstante, en general cualquier producto Wi-Fi que utilice la misma frecuencia de radio (por ejemplo, 2,4 GHz para 802.11b o 11g, 5 GHz para 802.11a) funciona con cualquier otro, aunque no sea Wi-Fi Certified.

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 TKIP.

X

Y

Z

Índice

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W