McAfee

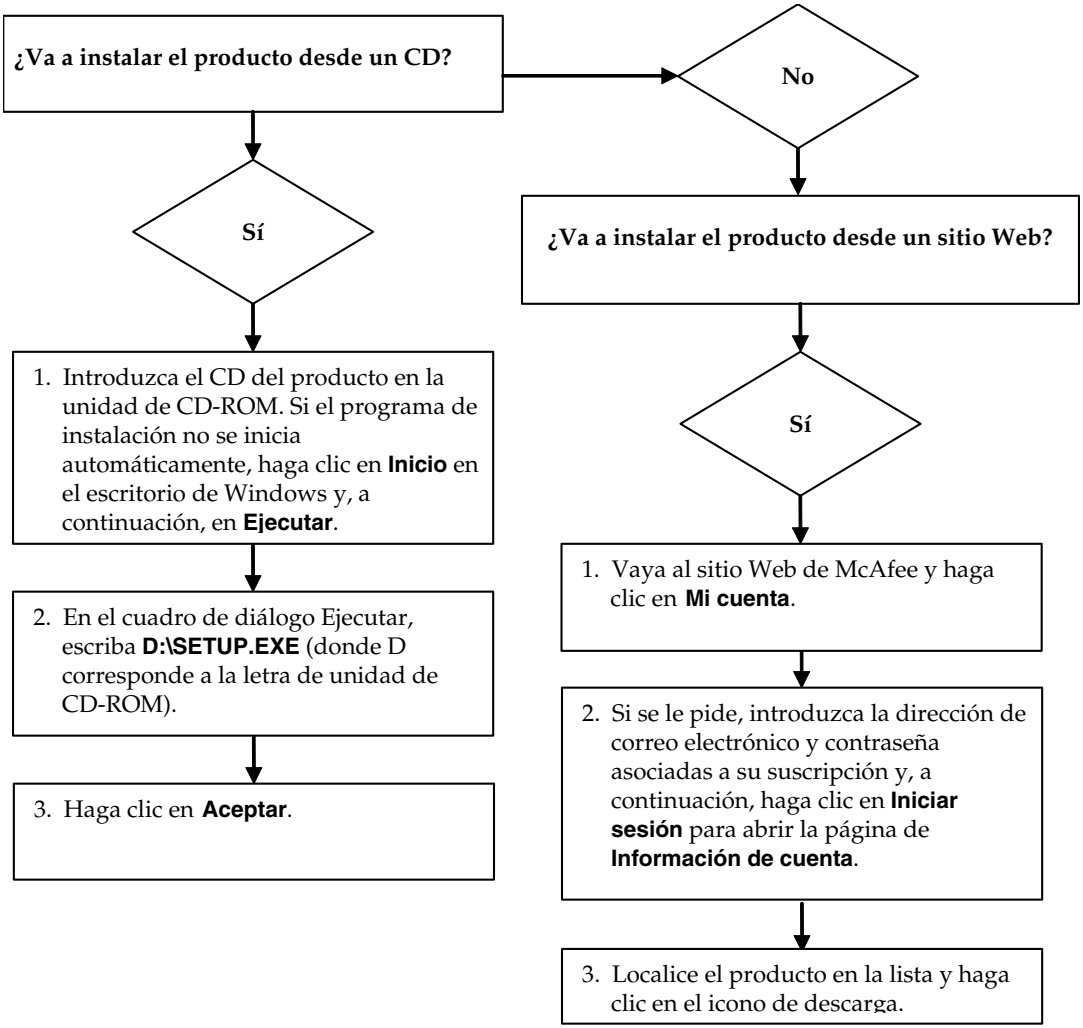
wirelesshomenetworksecurity suite

Guía del usuario

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 los manuales 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

Tarjeta de inicio rápido iii

1 Introducción 9

Requisitos del sistema 9
Utilización de McAfee SecurityCenter 10

2 McAfee Wireless Home Network Security 11

Utilización de McAfee Wireless Home Network Security 11
Protección de su red 11
McAfee Wireless Home Network Security 12
Con Wireless Home Network Security es fácil 12
Características 13
Instalación de McAfee Wireless Home Network Security 14
Instalación desde un CD 14
Instalación desde el sitio Web 15
Instalación desde el archivo 15
Utilización del asistente de configuración 15
Utilización de la página Resumen 16
Visualización de su conexión 16
Visualización de su red inalámbrica protegida 17
Gestión de redes inalámbricas 18
Conexión a una red 19
Desconexión de una red 19
Utilización de las opciones avanzadas 19
Configuración de opciones 20
Visualización de eventos 20
Configuración de opciones avanzadas 21
Definición de la configuración de seguridad 21
Configuración de los parámetros de alerta 21
Configuración de otros parámetros 22
Denegación de acceso a la red 22
Reparación de la configuración de seguridad 23
Protección de otros equipos 23

Rotación de claves 24
Protección de redes inalámbricas 24
Desprotección de redes inalámbricas 24
Actualización de McAfee Wireless Home Network Security 25
Comprobación automática de actualizaciones 25
Comprobación manual de actualizaciones 25
Información sobre alertas 26
Acceso denegado 26
Cambio de nombre de red 26
Clave de seguridad rotada 26
Configuración de red modificada 26
Configuración de seguridad de red modificada 27
Contraseña modificada 27
Equipo conectado 27
Equipo desconectado 27
Equipo protegido 27
Frecuencia de rotación de clave de seguridad modificada 27
PA/enrutador inalámbrico no protegido 27
PA/enrutador inalámbrico protegido 27
Red reparada 28
Rotación de clave interrumpida 28
Rotación de clave no realizada 28
Rotación de clave reanudada 28
Solución de problemas 29
Instalación 29
Equipos en los que se instala este software 29
No se ha detectado el adaptador inalámbrico 29
Varios adaptadores inalámbricos 29
No se puede descargar en los equipos inalámbricos porque la red ya está protegida 30
Protección o configuración de la red 30
Punto de acceso o enrutador no admitido 30
Actualización del firmware del punto de acceso o enrutador 30
Error de administrador duplicado 31
La red aparece como no segura 31
No se puede reparar 31
Conexión de equipos a la red 32
Esperando autorización 32
Concesión de acceso a un equipo desconocido 32

Conexión a una red o a Internet 32
Conexión a Internet defectuosa 32
La conexión se interrumpe por momentos 33
Dispositivos (no su equipo) que pierden la conexión 33
Se le ha pedido introducir la clave WEP o WPA 33
No es posible realizar la conexión 33
Actualización del adaptador inalámbrico 34
Nivel de señal débil 35
Windows no puede configurar su conexión inalámbrica 35
Windows no muestra ninguna conexión 35
Otros problemas 36
El nombre de la red es distinto al utilizar otros programas 36
Problemas al configurar los puntos de acceso o enrutadores inalámbricos 36
Sustitución de equipos 37
El software no funciona tras ampliar los sistemas operativos 37
Glosario 38

3 McAfee VirusScan 49

Funciones nuevas 49
Comprobación de VirusScan 50
Comprobación de ActiveShield 50
Comprobación de Analizar 51
Utilización de McAfee VirusScan 53
Utilización de ActiveShield 53
Activación o desactivación de ActiveShield 53
Configuración de las opciones de ActiveShield 54
Descripción de las alertas de seguridad 65
Análisis manual del equipo 68
Análisis manual para detectar virus y otras amenazas 68
Análisis automático en busca de virus y otras amenazas 73
Descripción de las detecciones de amenazas 75
Gestión de archivos en cuarentena 76
Creación de un disco de emergencia 77
Protección de un disco de emergencia contra escritura 79
Utilización de un disco de emergencia 79
Actualización de un disco de emergencia 79

Información automática sobre virus 79
Envío de información al World Virus Map 79
Visualización del World Virus Map 81
Actualización de VirusScan 82
Comprobación automática de actualizaciones 82
Comprobación manual de actualizaciones 82

4 McAfee Personal Firewall Plus 85

Funciones nuevas 85
Desinstalación de otros cortafuegos 87
Configuración del cortafuegos predeterminado 88
Configuración del nivel de seguridad 88
Comprobación de McAfee Personal Firewall Plus 91
Utilización de McAfee Personal Firewall Plus 91
Acerca de la página Resumen 91
Acerca de la página Aplicaciones de Internet 96
Cambio de reglas de las aplicaciones 97
Permiso y bloqueo de aplicaciones de Internet 97
Acerca de la página Eventos entrantes 98
Explicación de los eventos 99
Visualización de eventos en el registro de eventos entrantes 101
Respuesta a eventos entrantes 103
Gestión del registro de eventos entrantes 107
Acerca de las alertas 109
Alertas rojas 110
Alertas verdes 116
Alertas azules 117

Índice 119

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, los datos y la red inalámbrica quedan expuestos a un sinnúmero de amenazas para la privacidad y la seguridad. Proteja la red inalámbrica y la seguridad del equipo y los datos que contiene con McAfee Wireless Home Network Security Suite. Gracias a la incorporación de las galardonadas tecnologías de McAfee Wireless Home Network Security, McAfee VirusScan y McAfee Personal Firewall Plus, Wireless Home Network Security Suite proporciona uno de los conjuntos más completos de herramientas de privacidad y seguridad disponibles en el mercado.

Para obtener más información sobre cada producto de McAfee, consulte los capítulos siguientes:

- *McAfee Wireless Home Network Security* en la página 11
- *McAfee VirusScan* en la página 49
- *McAfee Personal Firewall Plus* en la página 85

Requisitos del sistema

- Microsoft® Windows 98SE, Windows Me, Windows 2000 o Windows XP
- Equipo personal con procesador Pentium o compatible

  Windows 98 o 2000: 133 MHz o superior

  Windows Me: 150 MHz o superior

  Windows XP (Home y Pro): 300 MHz o superior
- RAM

  Windows 98SE, Me o 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 ampliar a la última versión de Internet Explorer, visite el sitio Web de Microsoft en http://www.microsoft.com/.

Red inalámbrica

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

Programas de correo electrónico compatibles

- POP3 (Outlook Express, Outlook, Eudora o Netscape)

Programas de mensajería instantánea compatibles

- 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 versión posterior

Utilización de McAfee SecurityCenter

McAfee SecurityCenter es su centro integral de seguridad. La perfecta integración con McAfee SecurityCenter ofrece una visión general del estado de seguridad de su equipo, además de las últimas alertas sobre seguridad y virus. Puede ejecutar SecurityCenter desde el icono de McAfee que se muestra en la bandeja del sistema de Windows o desde el escritorio de Windows.

> **NOTA**
> Para obtener más información sobre sus funciones, haga clic en **Ayuda** en el cuadro de diálogo **SecurityCenter**.

Cuando SecurityCenter se encuentra en ejecución y todas las funciones de McAfee están instaladas en el equipo, aparece un icono rojo con una **M** en la bandeja del sistema de Windows (área de notificación de Windows XP).

Si una o varias de las aplicaciones de McAfee instaladas en el equipo se encuentra desactivadas, el icono de McAfee se mostrará de color negro: .

Para abrir McAfee SecurityCenter:

1. Haga clic con el botón derecho en el icono de McAfee .
2. Seleccione **Abrir SecurityCenter**.

Para acceder al producto de McAfee:

1. Haga clic con el botón derecho en el icono de McAfee .
2. Elija el producto de McAfee adecuado y, a continuación, haga clic en la función que desea utilizar.

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 38.

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 McAfee Wireless Home Network Security* en la página 14.

4 Proteja la red desde uno de los equipos inalámbricos. Consulte *Protección de redes inalámbricas* en la página 24.

5 Incorpórese a la red desde otros equipos inalámbricos. Consulte *Protección de otros equipos* en la página 23.

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 de McAfee Wireless Home Network Security

En esta sección se explica cómo instalar Wireless Home Network Security y se indican los primeros procedimientos para proteger la red.

Al instalar Wireless Home Network Security, tenga en cuenta lo siguiente:

- Instale el software en todos los equipos inalámbricos.
- No tiene que instalar el software en equipos que se conecten mediante un cable.

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 15.

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 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 de red** 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 15.

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 24.

  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**.

- Incorporar a una red protegida (este paso no es necesario si sólo hay un equipo inalámbrico). Para obtener más información, consulte *Gestión de redes inalámbricas* en la página 18.
- Conectarse a una red. Para obtener más información, consulte *Conexión a una red* en la página 19.

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

Utilización de la página Resumen

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 20.

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.

Gestión de redes inalámbricas

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, a continuación, seleccione **Redes inalámbricas disponibles**. Aparece la página **Redes inalámbricas** (figura 2-2).

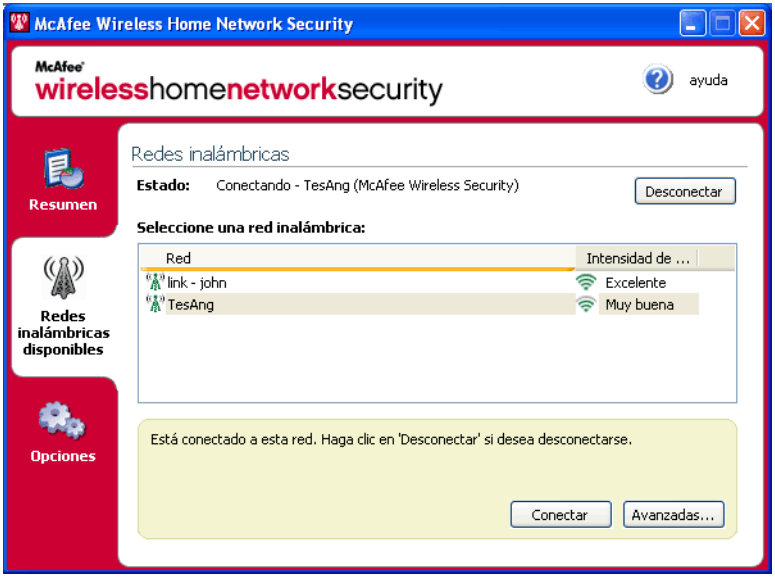


Figura 2-2. Página Redes inalámbricas

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).

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.

Configuración de opciones

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).

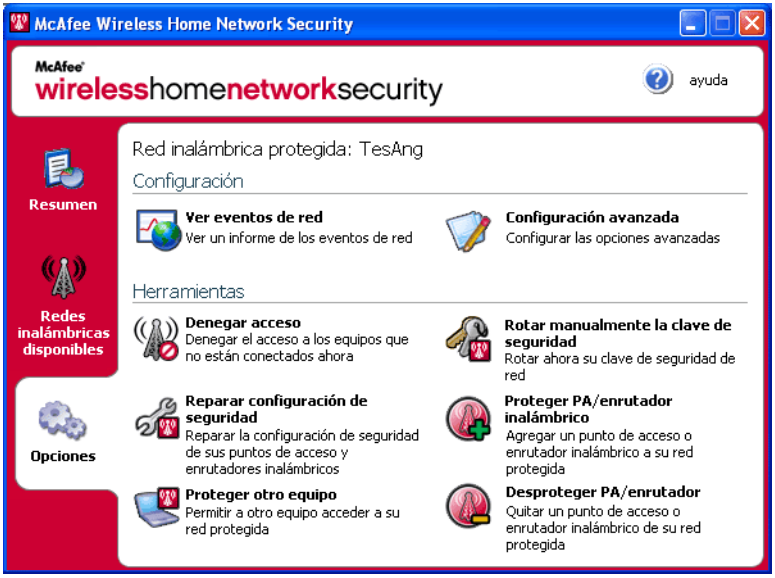


Figura 2-3. Página de opciones

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. Para obtener más información sobre las alertas, consulte *Información sobre alertas* en la página 26.

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. Consulte *Gestión de redes inalámbricas* en la página 18.
- 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 34.
- 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 17.
- 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 desprotegidas 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 McAfee Wireless Home Network Security* en la página 14), volver a conectarse a la red protegida e incorporarse a ella (consulte *Conexión a una red* en la página 19).

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 33.

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 disponibles.
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 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 desproteger y haga clic en **Desproteger**.

Actualización de McAfee Wireless Home Network Security

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, 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. 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.

Información sobre alertas

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 22.

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 19.

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.

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

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 21.

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 21.

Equipo conectado

Un usuario se ha conectado a la red. Para obtener más información, consulte *Conexión a una red* en la página 19.

Equipo desconectado

Un usuario se ha desconectado de la red. Para obtener más información, consulte *Desconexión de una red* en la página 19.

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'.

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 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 24.

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 24.

Red reparada

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

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.

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 23.
- 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 33.
- 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 31.

Si tiene problemas para conectarse a la red, consulte *Reparación de la configuración de seguridad* en la página 23.

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.

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 24) 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. Anule selección de 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 34.

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 24). 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 24).
- Vea la clave de red (consulte *Visualización de su red inalámbrica protegida* en la página 17). 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 23).
- 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 33 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 24). 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 38) 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 30.

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 23).

  Si no funciona la reparación, consulte *No se puede reparar* en la página 31.

- Reinicie el equipo.
- Actualice el adaptador inalámbrico o compre uno nuevo. Para actualizar el adaptador, consulte *Actualización del adaptador inalámbrico* en la página 34. 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.

Glosario

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 itinerancia, 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

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 y de publicidad**
  VirusScan identifica y elimina software espía, de publicidad 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 (spyware), de publicidad (adware) 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 de 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 proporcionan 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 65.

Comprobación de 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 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**, después en el botón **Crear carpeta nueva** y, a continuación, 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, seleccione **VirusScan** y haga clic en **Activar**.

Para comprobar el funcionamiento de la función de análisis:

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 75.

Utilización de McAfee VirusScan

Esta sección describe cómo utilizar VirusScan.

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 junto con Windows (figura 3-1 en la página 54).

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, seleccione **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.

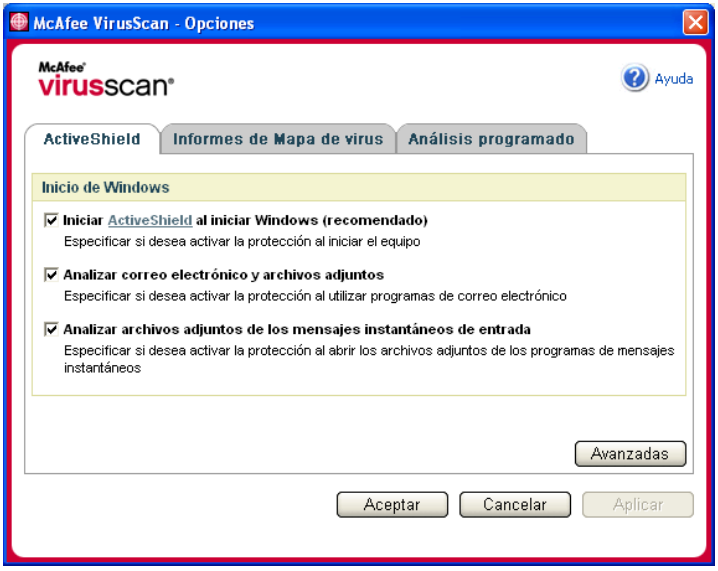


Figura 3-1. VirusScan - Opciones

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 (como indica 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 haga clic en **Opciones**.

   Se abrirá el cuadro de diálogo **VirusScan - Opciones** (figura 3-1 en la página 54).

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, 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 evitar que ActiveShield se inicie al abrir Windows:

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

   Se abrirá el cuadro de diálogo **VirusScan - Opciones** (figura 3-1 en la página 54).

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, 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 54).

Cuando esta opción está activada, ActiveShield analiza y trata de limpiar automáticamente todos los mensajes de correo electrónico entrante (POP3) y saliente (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 57) 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 entrantes 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 de 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**.

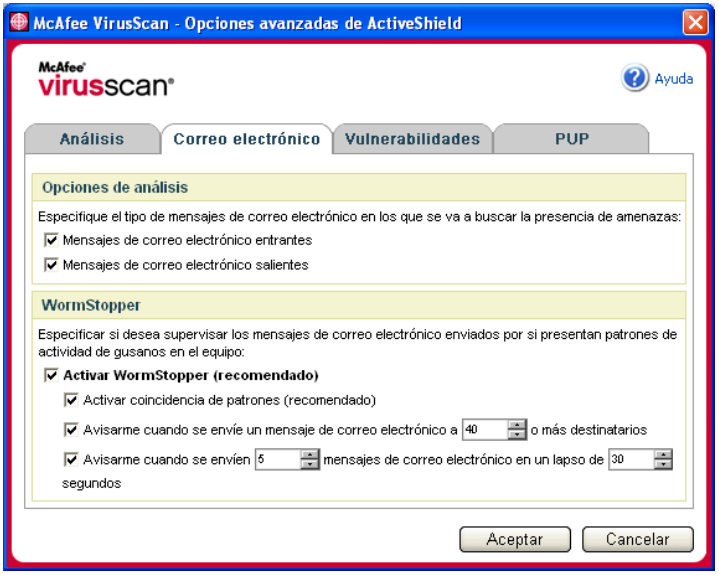


Figura 3-2. Opciones avanzadas de ActiveShield: ficha Correo electrónico

Análisis en busca de gusanos

VirusScan supervisa el equipo para analizar la actividad sospechosa que pueda indicar la presencia de una amenaza en él. 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 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 en la página 59).

   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 67 para obtener información detallada):

- Bloqueo automático de mensajes de correo electrónico saliente sospechosos

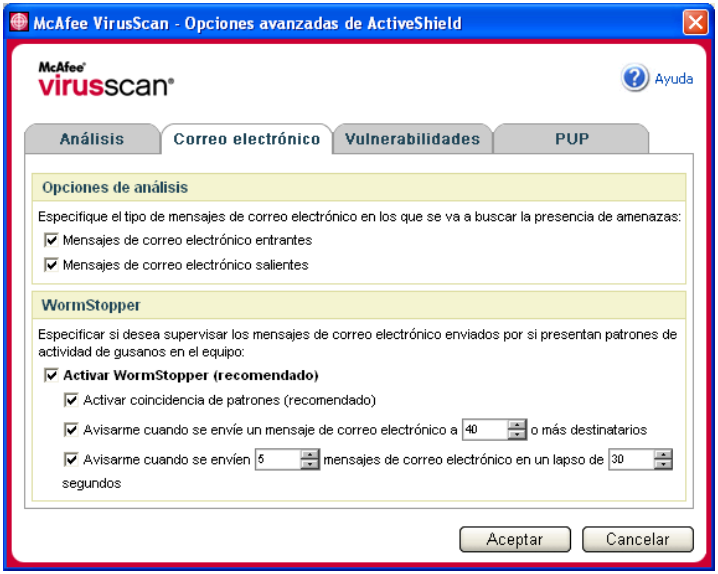


Figura 3-3. Opciones avanzadas de ActiveShield: ficha Correo electrónico

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 54).

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 ha configurado ActiveShield para utilizar la opción **Todos los archivos (recomendado),** 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 haga clic en **Opciones**.
2. Haga clic en **Avanzadas** y, a continuación, en la ficha **Análisis** (figura 3-4 en la página 61).

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

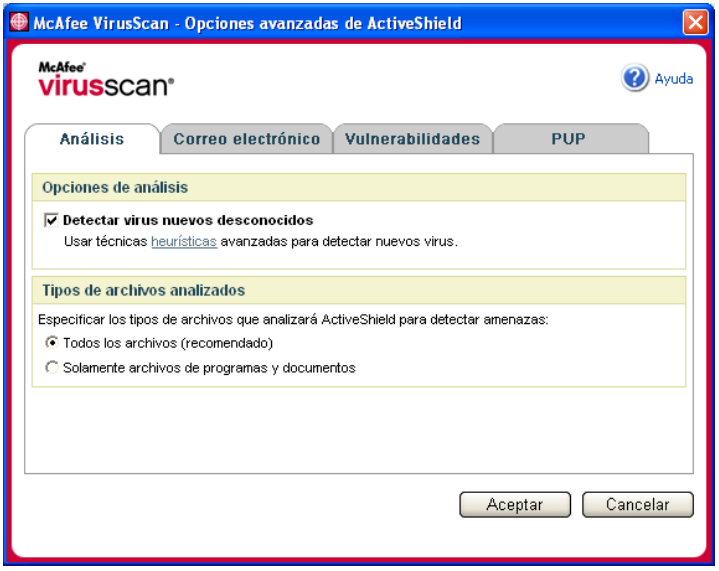


Figura 3-4. Opciones avanzadas de ActiveShield: ficha Análisis

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 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**.

Análisis 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 haga clic en **Opciones**.
2. Haga clic en **Avanzadas** y, a continuación, en la ficha **Análisis** (figura 3-4 en la página 61).
3. Haga clic en **Detectar virus nuevos desconocidos** y, a continuación, en **Aceptar**.

Análisis en busca 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 hacer proliferar más los 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 de ActiveShield**, 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 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**.

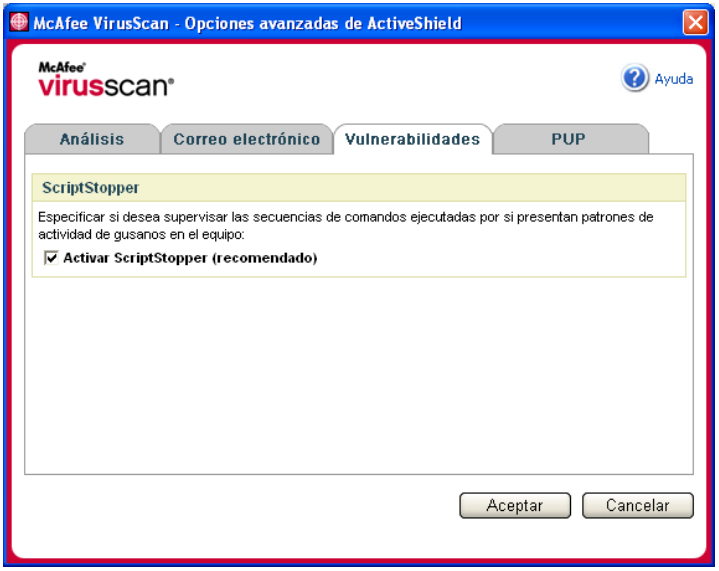


Figura 3-5. Opciones avanzadas de ActiveShield: ficha Vulnerabilidades

Análisis en busca 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 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**.

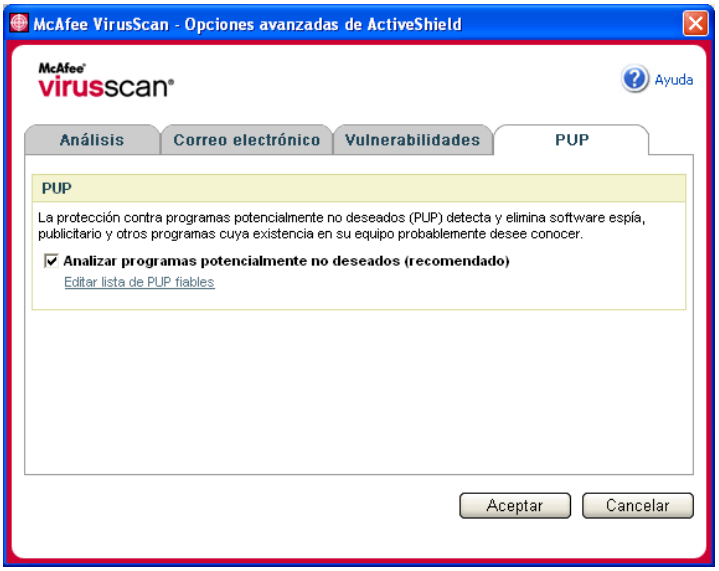


Figura 3-6. Opciones avanzadas de ActiveShield: ficha PUP

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.

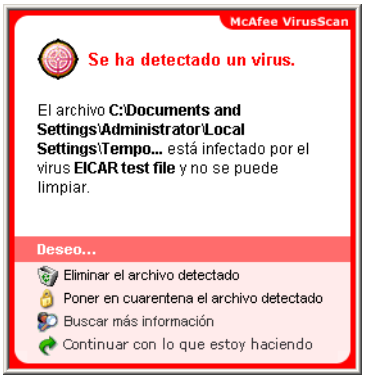


Figura 3-7. Alerta de virus

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 los 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 la 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.

Gestión 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.

  Consulte la sección *Gestión de PUP fiables* para obtener información más detallada.

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 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).

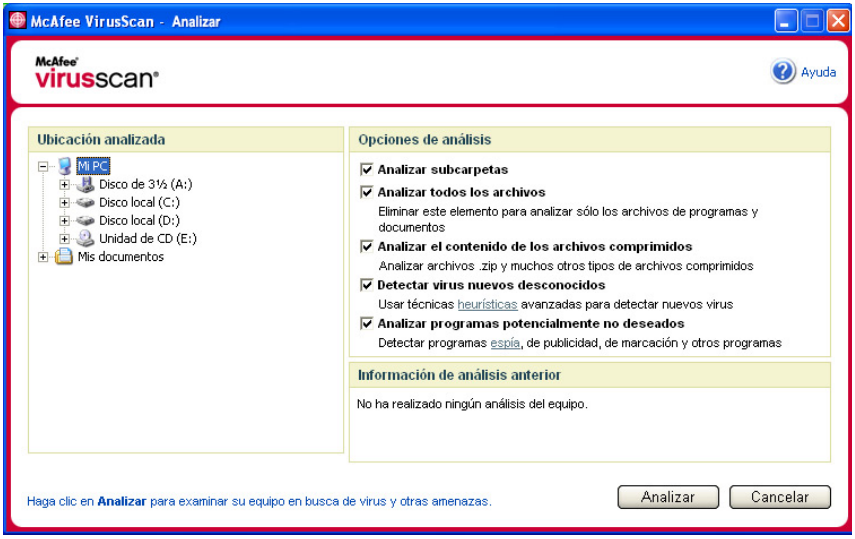


Figura 3-8. Cuadro de diálogo Analizar

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 en la página 70 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.

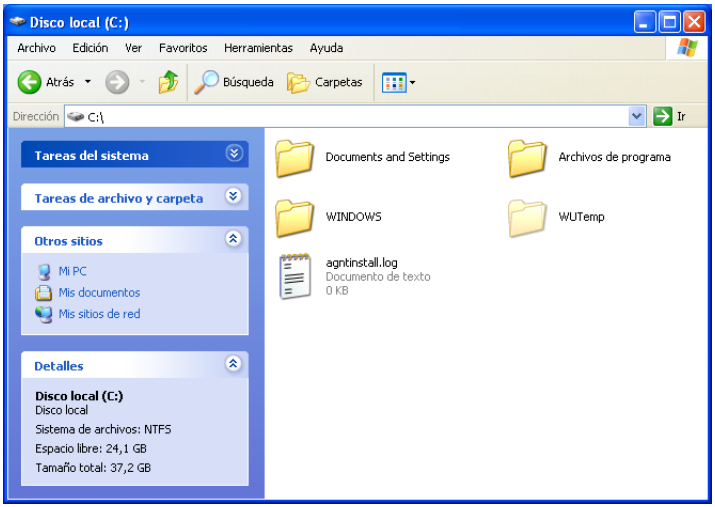


Figura 3-9. Contenido del disco local

- **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.

- **Detectar 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).

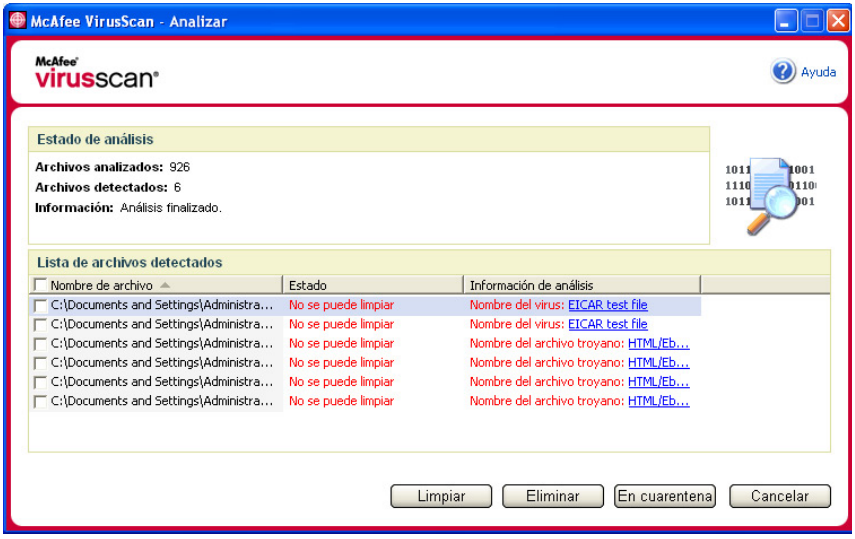


Figura 3-10. Resultados del análisis

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 75.

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 Windows Explorer.

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 69).

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 69).

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 haga clic en **Opciones**.

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

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

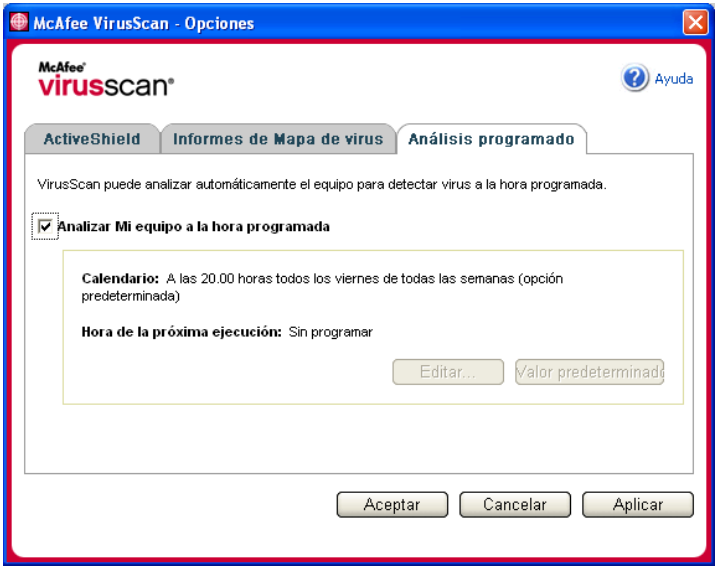


Figura 3-11. Opciones - Análisis programado

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. (Consulte *Gestión de archivos en cuarentena* en la página 76 para obtener más detalles.)

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 77.

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 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).

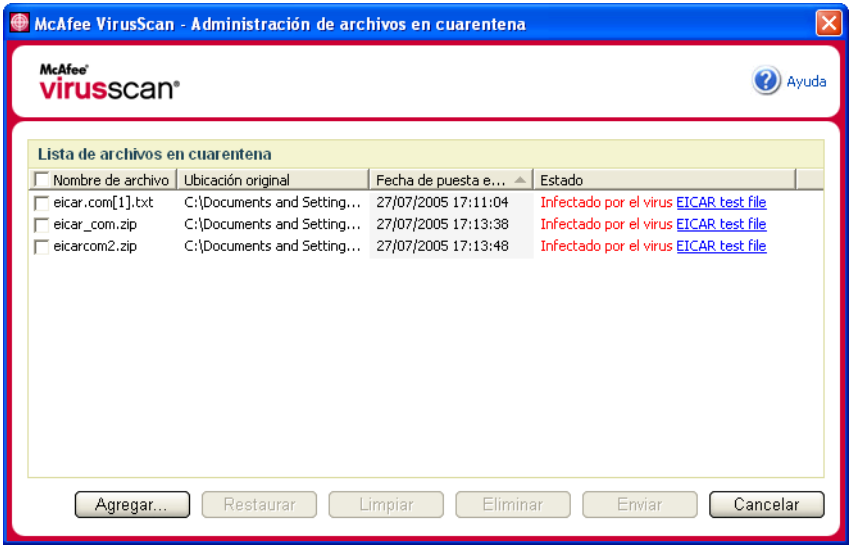


Figura 3-12. Cuadro de diálogo Administración de archivos en cuarentena

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 libres de virus. (Consulte *Análisis manual para detectar virus y otras amenazas* en la página 68 para obtener más detalles.)

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 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).

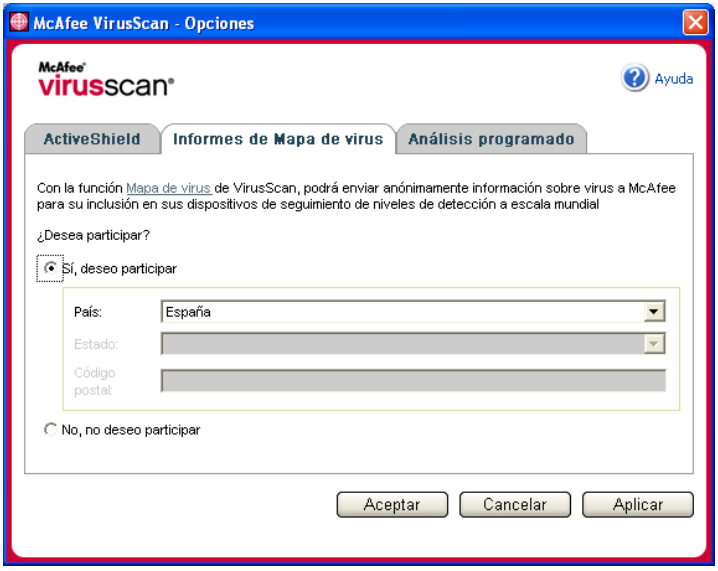


Figura 3-14. Opciones - Informes de mapa de virus

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

Participe o no 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 haga clic en **World Virus Map**.

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

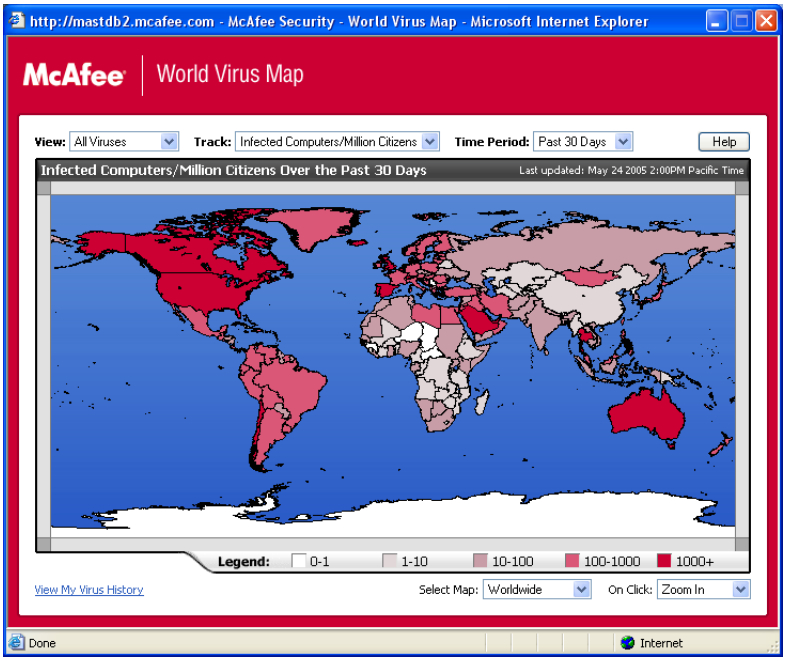


Figura 3-15. World Virus Map

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 83). 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.

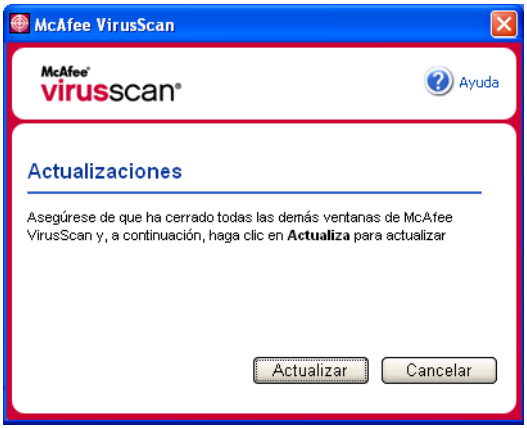


Figura 3-16. Cuadro de diálogo Actualizaciones

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 reconoce la aplicación como fiable, permitirá 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.

Desinstalación 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 de eventos entrantes de McAfee Personal Firewall Plus.

Configuración del cortafuegos predeterminado

McAfee Personal Firewall 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 de 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 **Opciones**.
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.

- **Eventos de detección de intrusión (IDS) en Registro de eventos entrantes**: si selecciona esta opción, los eventos detectados por IDS aparecerán en el registro de 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 hacer 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 de 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.

Utilización de McAfee Personal Firewall Plus

Para abrir 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 seleccione una tarea.

Acerca de la página Resumen

El Resumen de Personal Firewall contiene cuatro páginas de resumen:

- Resumen principal
- Resumen de la aplicación
- Resumen de evento
- 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 de la página **Eventos entrantes**.

Elemento	Descripción
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 de 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.
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.

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).

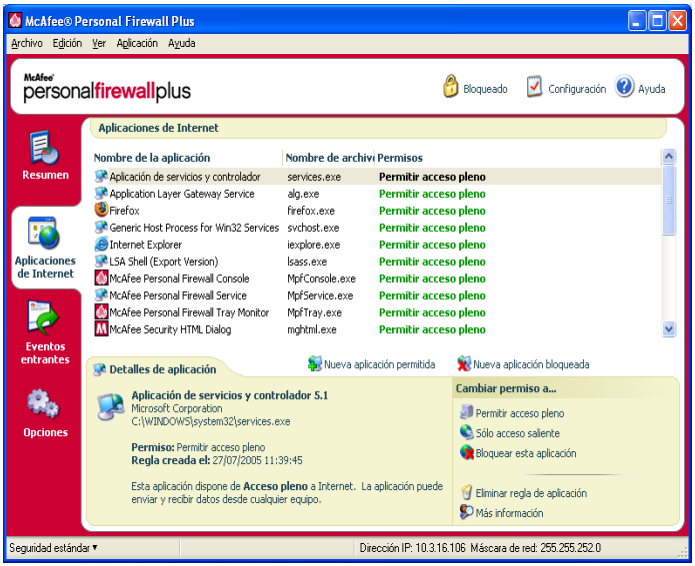


Figura 4-2. Página Aplicaciones de Internet

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

Cambio de reglas de las aplicaciones

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.

Permiso y bloqueo de 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.

Acerca de la página Eventos entrantes

La página **Eventos entrantes** permite consultar el registro de 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).

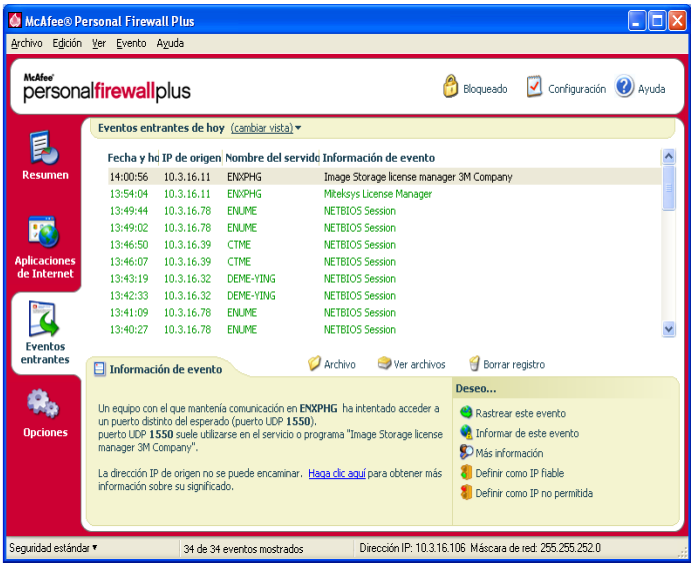


Figura 4-3. Página Eventos entrantes

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

- Fechas y horas de los eventos
- IP de origen
- Nombre del servidor

- Nombres del servidor 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

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 retorno 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 de 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 en 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 de eventos entrantes

El registro de 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 de eventos entrantes, haga clic con el botón derecho en una entrada y, a continuación, haga clic en **Mostrar los 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 entrantes**.
2. En el registro de eventos entrantes, haga clic con el botón derecho 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 de 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 de eventos entrantes, haga clic con el botón derecho en una entrada y, a continuación, haga clic en **Mostrar registro completo**.

   El registro de 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 de 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 entrantes**.
2. En el registro de 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 de 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 de eventos entrantes, haga clic con el botón derecho 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 de 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 de 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 de eventos entrantes, haga clic con el botón derecho en el evento que desee rastrear y, a continuación, 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.

Informes 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.

Definición de una dirección como fiable

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 de 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 prohibidas sólo si su equipo tiene uno o varios puertos abiertos intencionadamente y tiene razones para creer que debe bloquearla.

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 de 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 direcciones IP no permitidas**, 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 prohibida. 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 **Opciones**.

2 Haga clic en el icono **IP fiables y prohibidas** y, a continuación, en la ficha **Direcciones IP prohibidas**.

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

Gestión del registro de eventos entrantes

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

Archivado del registro de eventos entrantes

Puede archivar el registro de 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 los registros de eventos entrantes periódicamente para evitar que el registro de eventos entrantes se haga demasiado grande.

Para archivar el registro de 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 **Archivar**.

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 de 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 de 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 de 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 entrantes**.
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 de 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 de eventos entrantes:

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

Para eliminar eventos del registro de 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 entrantes**.

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 de 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 **Opciones**, después 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.

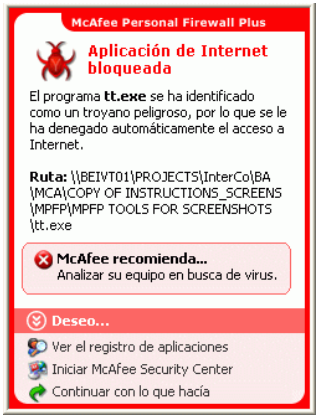


Figura 4-4. Alerta Aplicación de Internet bloqueada

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

- Haga clic en **Más información** para obtener detalles sobre el evento a través del registro de eventos entrantes (consulte *Acerca de la página Eventos entrantes* en la página 98 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 estoy haciendo** 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).

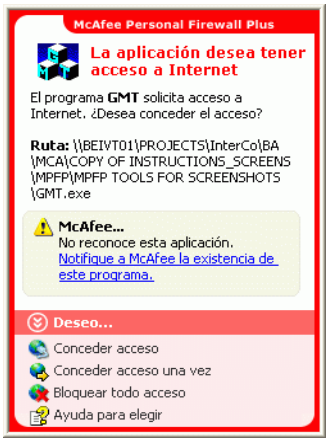


Figura 4-6. Alerta Aplicación no reconocida

Por lo tanto, McAfee no puede dar una recomendación sobre cómo gestionar la aplicación. Puede informar sobre la aplicación a McAfee haciendo clic en **Notifique a McAfee la existencia de 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 seguridad **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.

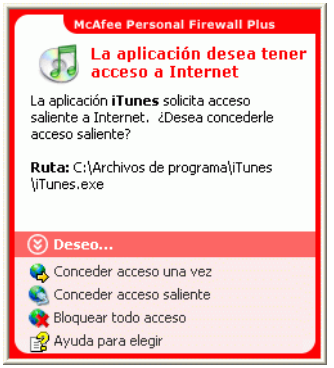


Figura 4-8. Alerta La aplicación desea tener acceso de servidor

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

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 del registro de aplicaciones de Internet (consulte *Acerca de la página Aplicaciones de Internet* en la página 96 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 estoy haciendo** 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 La aplicación ha cambiado

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 del registro de aplicaciones de Internet (consulte *Acerca de la página Aplicaciones de Internet* en la página 96 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 estoy haciendo** 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.

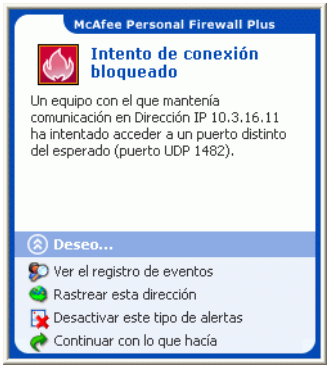


Figura 4-10. Alerta Intento de conexión bloqueado

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 de eventos entrantes de Personal Firewall (consulte *Acerca de la página Eventos entrantes* en la página 98 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 **Prohibir esta dirección** 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 estoy haciendo** si no desea aplicar otra medida aparte de la que tome Personal Firewall.

Índice

A

ActiveShield
- activar, 53
- análisis de secuencias de comandos, 62
- analizar archivos adjuntos de mensajes instantáneos entrantes, 60
- analizar correo electrónico y archivos adjuntos, 56
- analizar gusanos, 58
- analizar programas potencialmente no deseados (PUP), 64
- analizar sólo archivos de programas y documentos, 61
- analizar todos los archivos, 60
- analizar todos los tipos de archivo, 60
- comprobar, 50
- configuración de análisis predeterminada, 55, 58, 60, 62 a 64
- desactivar, 54
- detectar virus nuevos desconocidos, 62
- detener, 55
- iniciar, 55
- limpiar un virus, 65
- opciones de análisis, 54

Actualizaciones automáticas de Windows, 110

actualizar
- un disco de emergencia, 79
- VirusScan
  - automáticamente, 82
  - manualmente, 82

actualizar McAfee Wireless Home Network Security
- búsqueda manual de actualizaciones, 25
- comprobación automática de actualizaciones, 25

agregar a lista blanca
- PUP, 67

alertas, 26
- Aplicación de Internet bloqueada, 110
- de archivos detectados, 65
- de correo electrónico detectado, 66
- de gusanos potenciales, 67
- de PUP, 67
- de secuencias de comandos sospechosas, 66
- de virus, 65
- Intento de conexión bloqueado, 117
- La aplicación desea tener acceso a Internet, 110
- La aplicación desea tener acceso de servidor, 110
- Nueva aplicación permitida, 116
- Se ha modificado la aplicación, 110

Análisis
- análisis automático, 73
- análisis manual, 68
- análisis manual desde el Explorador de Windows, 72
- analizar manualmente desde la barra de herramientas de Microsoft Outlook, 72
- comprobar, 51 a 52
- eliminar un virus o un programa potencialmente no deseado, 75
- limpiar un virus o un programa potencialmente no deseado, 75
- opción Analizar el contenido de los archivos comprimidos, 70
- opción Analizar programas potencialmente no deseados, 71
- opción Analizar subcarpetas, 69
- opción Analizar todos los archivos, 70
- opción Detectar virus nuevos desconocidos, 70
- poner en cuarentena un virus o un programa potencialmente no deseado, 75

analizar
- archivos comprimidos, 70
- desde el Explorador de Windows, 72
- desde la barra de herramientas de Microsoft Outlook, 72
- gusanos, 58
- programar análisis automáticos, 73

programas potencialmente no deseados (PUP), 64
secuencias de comandos, 62
sólo archivos de programas y documentos, 61
subcarpetas, 69
todos los archivos, 60, 70
virus nuevos desconocidos, 70
Analizar el contenido de los archivos comprimidos, opción (Analizar), 70
Analizar programas potencialmente no deseados, opción (Analizar), 71
Analizar subcarpetas, opción (Analizar), 69
Analizar todos los archivos, opción (Analizar), 70
aplicaciones de Internet
acerca de, 96
cambiar reglas, 97
permitir y bloquear, 97
archivos adjuntos de mensajes instantáneos entrantes
analizar, 60
limpiar automáticamente, 60
asistente de configuración, utilizar, 15
Asistente para la actualización, 55
AVERT, enviar archivos sospechosos, 77

C

características, 13
claves, rotar, 24
comprobar Personal Firewall, 91
comprobar VirusScan, 50
conexión, visualizar, 16
configuración, reparar, 23
configurar
VirusScan
ActiveShield, 53
Análisis, 68
correo electrónico y archivos adjuntos
analizar
activar, 56
desactivar, 57
errores, 57
limpiar automáticamente
activar, 56
cortafuegos predeterminado, configurar, 88
crear disco de emergencia, 77
Cuarentena
añadir archivos sospechosos, 76
eliminar archivos, 76
eliminar archivos sospechosos, 77
enviar archivos sospechosos, 77
gestión de archivos sospechosos, 76
limpiar archivos, 76 a 77
restablecer archivos limpiados, 76 a 77

D

desinstalar
otros cortafuegos, 87
Detectar virus nuevos desconocidos, opción (Analizar), 70
direcciones IP
acerca de, 99
confiar, 105
prohibir, 105
Disco de emergencia
actualizar, 79
crear, 77
proteger contra escritura, 79
utilizar, 75, 79

E

editar listas blancas, 68
enviar archivos sospechosos a AVERT, 77
eventos
acerca de, 98
archivar el registro de eventos, 107
borrar el registro de eventos, 108
bucle invertido, 100
consejos de HackerWatch.org, 104
copiar, 108
de 0.0.0.0, 99
de 127.0.0.1, 100
de direcciones IP privadas, 101
desde equipos de la LAN, 100
eliminar, 109
exportar, 108
información adicional, 104
informar, 104

mostrar
con la misma información de evento, 103
de una dirección concreta, 102
día actual, 101
esta semana, 102
todos, 102
un día concreto, 102
rastrear
explicación, 98
ver registros de eventos archivados, 108
responder, 103
eventos, ver, 20
Explorador de Windows, 72

F

Firewall de Windows, 88
funciones nuevas, 49, 85

G

gusanos
alertas, 65, 67
detectar, 65, 75
detener, 67

H

HackerWatch.org
consejos, 104
informar de un evento, 104
registrarse, 104

I

informar de un evento, 104
introducción a VirusScan, 49

L

lista de archivos detectados (Analizar), 71, 75
lista de PUP fiables, 68

M

McAfee SecurityCenter, 10
Microsoft Outlook, 72
mostrar eventos en el registro de eventos, 101

O

opciones
avanzadas, 19
configurar, 20
opciones avanzadas
alertas, 21
otras, 22
seguridad, 21
opciones de análisis
ActiveShield, 54, 60 a 61
Análisis, 68
opciones, página, 20

P

Personal Firewall
comprobar, 91
utilizar, 91
programar análisis, 73
programas agregados a lista blanca, 68
programas potencialmente no deseados (PUP), 64
alertas, 67
confiar, 67
detectar, 75
eliminar, 67, 75
limpiar, 75
poner en cuarentena, 75
proteger equipos, 23
proteger un disco de emergencia contra escritura, 79

R

rastrear un evento, 103
red
conectar, 19
denegar acceso, 22
desconectar, 19
desproteger, 24
proteger, 24
ver, 17
Redes inalámbricas disponibles, página, 18

Registro de eventos
acerca de, 98
gestionar, 107
ver, 108
requisitos del sistema, 9
Resumen, página, 16, 18, 91

S

ScriptStopper, 62
secuencias de comandos
alertas, 66
detener, 66
permitir, 66
solución de problemas, 29
soporte técnico, 75

T

tarjeta de inicio rápido, iii
troyanos
alertas, 65
detectar, 75

U

utilizar un disco de emergencia, 79

V

virus
alertas, 65
detectar, 75
detectar con ActiveShield, 65
detención de secuencias de comandos sospechosas, 66
detener gusanos potenciales, 67
eliminar, 65, 75
eliminar archivos detectados, 66
eliminar PUP, 67
informar automáticamente, 79, 81
limpiar, 65, 75
permitir secuencias de comandos sospechosas, 66
poner en cuarentena, 65, 75
poner en cuarentena archivos detectados, 66
VirusScan
actualizar automáticamente, 82
actualizar manualmente, 82
analizar desde el Explorador de Windows, 72
analizar desde la barra de herramientas de Microsoft Outlook, 72
comprobar, 50
informar automáticamente sobre virus, 79, 81
introducción, 49
programar análisis, 73

W

Wireless Home Network Security
introducción, 12
utilizar, 11
World Virus Map
informar, 79
ver, 81
WormStopper, 58