McAfee®

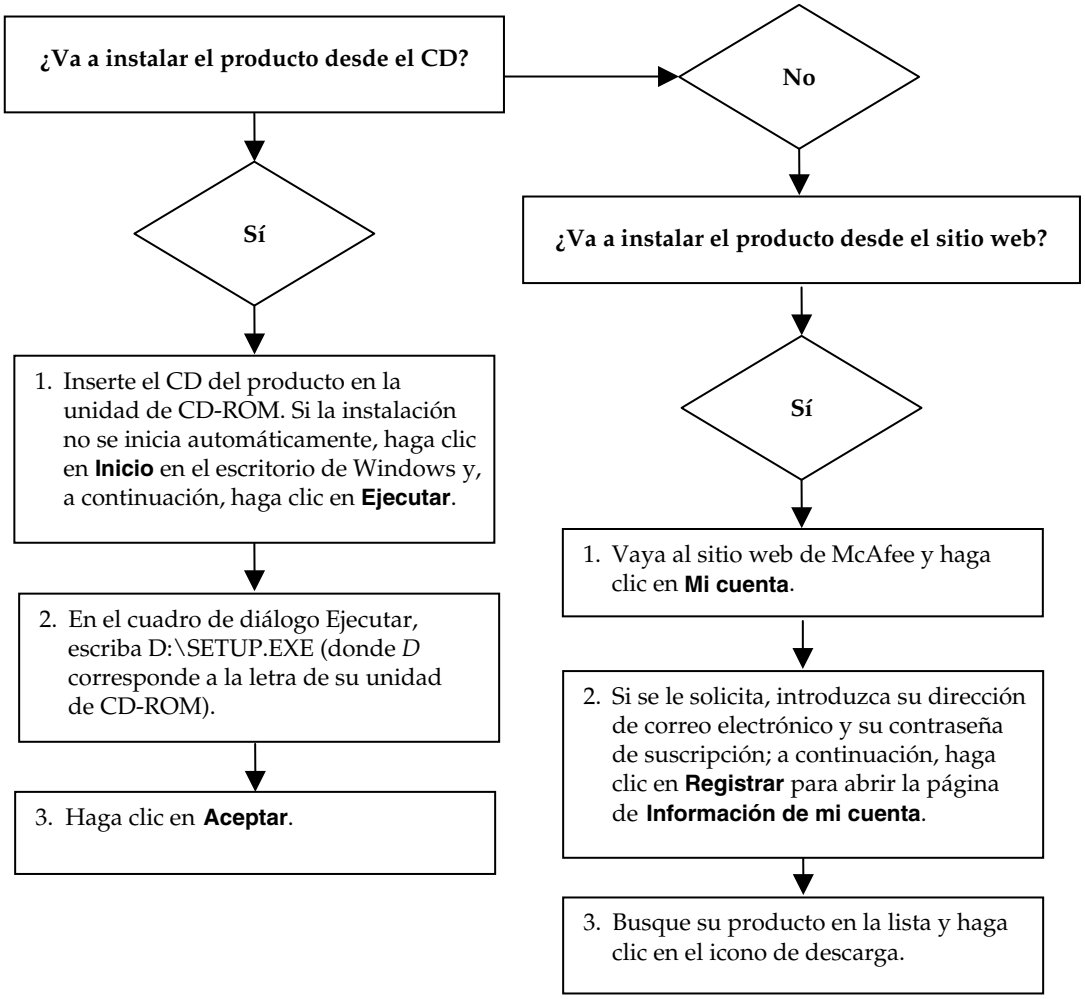
internet security suite

Manual del usuario

McAfee®

Tarjeta de inicio rápido

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



Si desea obtener más información

Para ver los manuales de usuario en el CD del producto, asegúrese de que tiene Acrobat Reader instalado; en caso contrario, 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. Busque la carpeta Manuales y haga doble clic en el Manual del usuario en formato .PDF que desee abrir.

Ventajas del registro

Es recomendable que siga los sencillos pasos en el producto para transmitirnos su registro directamente. Gracias al registro, podrá disfrutar de asistencia técnica especializada 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 cuando adquirió el software de VirusScan.

  Visite http://es.mcafee.com para obtener información sobre el precio de un año adicional de definiciones de virus.
- Una garantía de 60 días que le asegura la sustitución del software o CD si está defectuoso o dañado.
- El filtro de SpamKiller se actualiza durante un año después de instalarlo cuando adquirió el software SpamKiller

  Visite 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 cuando adquirió el software MIS.

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

Soporte técnico

Si desea obtener soporte técnico, visite la página http://www.mcafeeayuda.com/. Nuestro sitio de soporte permite acceder durante las 24 horas del día al sencillo Asistente de respuestas para obtener soluciones sobre las preguntas de soporte 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 nuestro servicios GRATUITOS Chat Now! y Email Express! Estas opciones le ayudan ponerse en contacto rápidamente con nuestros cualificados ingenieros de soporte técnico a través de Internet sin coste alguno. También puede obtener información de soporte en http://www.mcafeeayuda.com/.

Contenido

Presentación 1

Internet pone a nuestro alcance una ingente cantidad de información y posibilidades de entretenimiento. Sin embargo, tan pronto como se conecta, el equipo queda expuesto a un sinnúmero de amenazas para la privacidad y la seguridad. Proteja la privacidad y la seguridad de su equipo y los datos que contiene con McAfee Internet Security Suite. Gracias a la incorporación de las galardonadas tecnologías de McAfee, Internet Security Suite proporciona uno de los conjuntos más amplios de herramientas de privacidad y seguridad disponibles en la actualidad. McAfee Internet Security Suite destruye virus; se anticipa a los piratas informáticos; asegura su información personal; privatiza su navegación por la Web; bloquea anuncios y ventanas emergentes; gestiona los cookies y las contraseñas; bloquea los archivos, carpetas y unidades; filtra los contenidos objetables, y le concede el control de las comunicaciones entrantes y salientes de su equipo. McAfee Internet Security Suite facilita una potente protección a los usuarios de Internet en la actualidad.

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

Software McAfee Internet Security

- **McAfee SecurityCenter:** Evalúa, informa y protege la vulnerabilidad de su equipo. Cada índice de seguridad evalúa rápidamente su exposición a las amenazas de seguridad y a las existentes en Internet, y propone recomendaciones para proteger su equipo de manera rápida y segura.
- **McAfee VirusScan:** Trata los problemas relacionados con los virus que pueda encontrar en Internet. Usted puede especificar cómo realizar un análisis de virus, qué hacer si se encuentra un virus y cómo avisar cuando se ha detectado un virus. También puede hacer que VirusScan mantenga un registro de las acciones efectuadas en el equipo.
- **McAfee Personal Firewall Plus:** Protege su equipo mientras está conectado a Internet. Cuando se encuentre conectado a Internet, ya sea mediante DSL, módem por cable o marcación estándar, la comunicación bidireccional que se mantenga a través de Internet estará plenamente asegurada.
- **McAfee Privacy Service:** Combina la protección de la información personal identificable (PII) con el bloqueo de anuncios en línea y el filtrado de contenidos. Este servicio protege su información personal a la vez que facilita un mayor control sobre el uso de Internet por parte de su familia. Privacy Service de McAfee evita la exposición de información confidencial a amenazas en línea, además de protegerle a usted y a su familia de contenidos inadecuados.
- **McAfee SpamKiller:** A causa del gran número de mensajes de correo electrónico recibidos a diario por adultos, menores y empresas con contenidos fraudulentos, inapropiados u ofensivos, la protección contra el correo basura es un componente esencial de la estrategia de seguridad de su equipo.

Requisitos del sistema

- Microsoft® Windows 98, Me, 2000 o XP
- Ordenador personal con procesador
  - Windows 98 o Me: Pentium 150 MHz o superior
  - Windows 2000 o XP: Pentium 233 MHz o superior
- RAM
  - Windows 98: 32 MB (se recomienda 64 MB)
  - Windows Me, 2000 o XP: 64 MB (se recomienda 128 MB)
- 70 MB de espacio disco duro
- Microsoft® Internet Explorer 5.5 o superior.

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

Utilización de McAfee SecurityCenter

McAfee SecurityCenter es su estableciemiento de seguridad en línea, al que puede acceder desde el icono situado en la bandeja del sistema Windows o directamente desde el escritorio. Gracias a éste, puede realizar estas útiles tareas:

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

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

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

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

Para abrir McAfee SecurityCenter:

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

Para acceder al producto McAfee:

1. Haga clic con el botón derecho en el icono de McAfee  .
2. Elija el producto McAfee adecuado y seleccione la función que desee utilizar.

Desinstalación de Internet Security Suite

En algunas situaciones, es posible que desee desinstalar Internet Security Suite o algunos de sus programas.

> **NOTA**
> Los usuarios deben poseer los derechos del Administrador para poder desinstalar Internet Security Suite.

1. Guarde todo su trabajo y cierre todas las aplicaciones que se encuentren abiertas.
2. Abra el **Panel de control**.
   - Usuario de Windows 98, ME, y 2000: En la barra de tareas de Windows, seleccione **Inicio**, elija **Configuración** y haga clic en **Panel de control**.
   - Usuario de Windows XP: En la barra de tareas de Windows, seleccione **Inicio** y haga clic en **Panel de control**.
3. Haga clic en **Agregar o quitar programas**.

   > **NOTA**
   > Para desinstalar McAfee Internet Security Service, deberá desinstalar cada programa (McAfee Personal Firewall, McAfee Privacy Service, McAfee SpamKiller, McAfee VirusScan), además de McAfee SecurityCenter.

4. Seleccione un programa de McAfee en la lista de programas y haga clic en **Cambiar o quitar**.
5. Cuando se le pida que confirme la desinstalación, haga clic en **Sí**. Se iniciará la desinstalación.
6. Si se le solicita, haga clic en **Reiniciar** para reiniciar el equipo.
7. Si está desinstalando Internet Security Suite, repita los pasos de Paso 1 a Paso 6 para cada programa.
8. En el cuadro de diálogo Agregar o quitar programas, seleccione **McAfee SecurityCenter** y haga clic en **Cambiar o quitar**.
9. Si se le solicita, haga clic en **Reiniciar** para reiniciar el equipo.

McAfee VirusScan 2

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 malintencionadas y ataques híbridos.

Gracias a él, disfrutará de las funciones siguientes:

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

Análisis: detecta la existencia de virus y programas potencialmente no deseables en las unidades de disco duro, unidades de disquete y en cada una de las carpetas y archivos.

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

Detección de actividades hostiles: supervisa el equipo para detectar actividad semejante a la de los virus provocada por secuencias de comandos malintencionadas o gusanos.

Funciones nuevas

Esta versión de VirusScan incluye las siguientes funciones nuevas:

- **Análisis del correo electrónico**
  VirusScan analiza automáticamente el correo electrónico de entrada (POP3) y salida (SMTP) y sus archivos adjuntos de la mayoría de los clientes de correo electrónico más conocidos, como Microsoft Outlook, Netscape Mail, Eudora y Pegasus.

- **Análisis de mensajes instantáneos**
  VirusScan analiza de modo automático las transferencias de archivos recibidos de los clientes más conocidos de mensajes instantáneos, incluidos Yahoo Instant Messenger, AOL Instant Messenger y MSM Messenger.

- **Detección de actividades hostiles**
  VirusScan incluye ScriptStopper™ y WormStopper™ para detectar, notificar y bloquear actividades relacionadas con virus producidas por secuencias de comandos malintencionadas y gusanos.

- **Integración con el Explorador de Windows**
  VirusScan permite utilizar un menú con métodos abreviados para analizar los archivos, carpetas o unidades que se hayan seleccionado dentro del Explorador de Windows.

- **Integración con Microsoft Outlook**
  VirusScan permite utilizar un icono de la barra de herramientas para analizar los mensajes, carpetas o almacenes de mensajes en Microsoft Outlook.

- **Desinfección automática de archivos**
  VirusScan intenta limpiar de forma automática archivos infecciosos o sospechosos al detectarlos.

- **Análisis programados**
  Ahora puede programar el análisis automático a intervalos específicos para examinar exhaustivamente su equipo en busca de virus.

- **Integración con McAfee SecurityCenter**
  Su perfecta integración con McAfee SecurityCenter proporciona una visión general del estado de seguridad de su equipo y acceso a los últimos virus detectados y alertas de seguridad. Puede ejecutar SecurityCenter desde el icono de McAfee que se muestra en la bandeja del sistema de Windows o desde el escritorio.

- **Cuarentena de archivos**
  Puede utilizar la función de cuarentena para cifrar y aislar temporalmente archivos infectados o sospechosos en la carpeta de cuarentena hasta que se tome alguna medida. Una vez limpio, puede restablecer en su ubicación original el archivo que estaba en cuarentena.

- **Envío de archivos a AVERT**
  VirusScan incluye ahora la posibilidad de enviar los archivos sospechosos directamente desde la función de cuarentena a AVERT™ (McAfee AntiVirus Emergency Response Team, o Equipo de respuesta de emergencia antivirus de McAfee) para su investigación.

- **Informes del mapa de virus**
  Ahora puede enviar información de rastreo de virus de forma anónima para su inclusión en el World Virus Map. Puede registrarse de forma automática y gratuita para acceder a esta función de seguridad y ver los niveles de infección más recientes en todo el mundo mediante McAfee SecurityCenter.

Comprobación del funcionamiento de VirusScan

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

Comprobación del funcionamiento de ActiveShield

Para comprobar el funcionamiento de ActiveShield:

1. Diríjase a http://www.eicar.com/ en el navegador Web.
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 **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 los archivos infectados para comprobar el tratamiento que da ActiveShield a los virus. Consulte la sección *Acciones que ActiveShield lleva a cabo al descubrir un virus* en la página 29 para obtener información más detallada.

Comprobar la función analizar

Antes de poder comprobar la función de Análisis, debe desactivar ActiveShield para evitar que detecte los archivos infectados antes de que lo haga la función de Análisis y, a continuación, compruebe los archivos.

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 mencionado anteriormente:
   a. Diríjase 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 **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 primero de ellos. 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 archivos** 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 **Carpeta de análisis de VSO**.

f Haga doble clic en **Carpeta de análisis VSO** y, a continuación 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 Analizar:

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

2 Diríjase a la carpeta **Carpeta de análisis de VSO** en la que guardó los archivos mediante el árbol de directorios situado en el panel izquierdo del cuadro de diálogo:

a Haga clic en el signo **+** situado junto al icono.

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, la función de análisis sólo examinará dicha carpeta. Si desea obtener una demostración más convincente de la capacidad de detección de la función de análisis, coloque los archivos en distintas ubicaciones del disco duro de forma aleatoria.

3 En el área **Opciones de análisis** del cuadro de diálogo **Detectar virus**, 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 infectados**. Si es así, la función de análisis funciona correctamente.

Puede intentar eliminar o poner en cuarentena los archivos infectados para comprobar el tratamiento que da la función de exploración a los virus. Consulte la sección *Si el análisis encuentra un virus o un programa potencialmente no deseado* en la página 39 para obtener información más detallada.

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; su equipo queda protegido en todo momento. ActiveShield analiza los archivos cuando el usuario o el equipo tienen acceso a ellos. Cuando ActiveShield detecta un archivo infectado, automáticamente intenta limpiarlo. Si ActiveShield no puede limpiar el virus, el usuario puede eliminar el archivo o ponerlo en cuarentena.

Activación o desactivación de ActiveShield

De manera predeterminada, ActiveShield se inicia (se carga en la memoria del equipo) y se activa (así lo indica el icono en color rojo de la bandeja de Windows) al reiniciar el equipo tras el proceso de instalación.

Si se detiene ActiveShield (no se carga) o se desactiva (el icono en color negro así lo indica), puede ejecutarlo de modo manual y configurarlo para que se inicie automáticamente al abrir Windows.

Activación de ActiveShield

Para activar ActiveShield únicamente para la sesión de Windows en curso:

Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y haga clic en **Activar**. El icono de McAfee pasará a tener color rojo .

Si ActiveShield sigue configurado para iniciarse al abrir Windows, se mostrará un mensaje que indica que ya está protegido contra el ataque de virus. De lo contrario, aparecerá un cuadro de diálogo que le permitirá configurar ActiveShield para que se inicie al abrir Windows (figura 2-1 en la página 20).

Desactivación de ActiveShield

Para desactivar ActiveShield sólo durante la sesión actual de Windows:

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

   El icono de McAfee pasará a tener color negro .

Si ActiveShield sigue configurado para iniciarse al abrir Windows, se mostrará un mensaje que indica que ya está protegido contra el ataque de virus cuando reinicie su equipo.

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 2-1), a la que puede tener acceso a través del icono de McAfee situado en la bandeja del sistema de Windows.

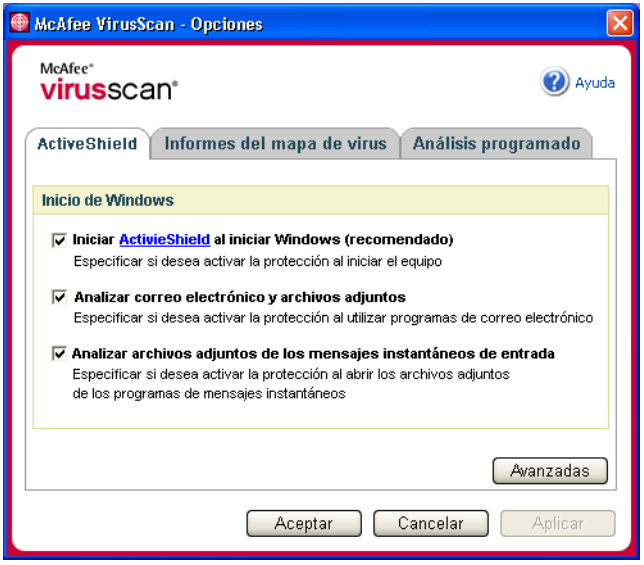


Figura 2-1. Opciones de ActiveShield

Inicio de ActiveShield

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

Si ActiveShield se detiene (así lo indica el icono en color negro), puede configurarlo para que se inicie automáticamente al abrir Windows (opción recomendada).

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

Para iniciar ActiveShield 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 2-1 en la página 20).

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 contra virus. Si necesita detener ActiveShield para realizar otra tarea que no sea la actualización de VirusScan, asegúrese de no estar conectado a Internet.

Para detener ActiveShield al iniciar 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 2-1 en la página 20).

2. Desactive 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**.

Exploración del correo electrónico y los archivos adjuntos

De forma predeterminada, el análisis del correo electrónico y la limpieza automática se activan mediante las opciones **Analizar correo electrónico y archivos adjuntos** (figura 2-1 en la página 20) y **Limpiar automáticamente los archivos adjuntos infectados (recomendado)** (figura 2-2 en la página 24).

Cuando estas dos opciones se encuentran activadas, ActiveShield analiza y trata de limpiar automáticamente todos los mensajes de correo electrónico de entrada (POP3) y salida (SMTP), así como los archivos adjuntos infectados de los clientes de correo electrónico más conocidos, incluidos los siguientes:

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

NOTA

El análisis del correo electrónico no es posible para los siguientes clientes: correo electrónico basado en la 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 opciones de Análisis de correo electrónico (figura 2-2 en la página 24) y la opción de WormStopper (figura 2-5 en la página 29) se desactivan automáticamente. Si desactiva el análisis de correo electrónico saliente, las opciones de WormStopper se desactivan automáticamente.

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

Correo electrónico de entrada

Si un mensaje de correo electrónico o un archivo adjunto de entrada están infectados, ActiveShield lleva a cabo el procedimiento siguiente:

- Intenta limpiar el mensaje infectado.
- Intenta poner en cuarentena el mensaje o eliminarlo si no lo puede limpiar.
- Incluye un archivo de alerta en el mensaje de entrada que contiene información sobre las acciones realizadas para eliminar la infección.

Correo electrónico de salida

Si un mensaje de correo electrónico o un archivo adjunto de salida están infectados, ActiveShield lleva a cabo el procedimiento siguiente:

- Intenta limpiar el mensaje infectado.
- Intenta poner en cuarentena el mensaje o eliminarlo si no lo puede limpiar.
- Incluye un archivo de alerta en un mensaje nuevo que contiene información sobre las acciones realizadas para eliminar la infección.

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

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

Para desactivar la exploración de 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 **Análisis del correo electrónico** (figura 2-2 en la página 24).
3. Desactive la selección **Mensajes de correo electrónico entrantes** o **Mensajes de correo electrónico salientes** y, a continuación, haga clic en **Aceptar**.

Si el servidor de correo electrónico está configurado de modo que sólo se reciba y envíe correo electrónico mientras el usuario está utilizando su equipo, puede desactivar la limpieza automática para que aparezcan alertas que le pidan que limpie los mensajes infectados. Siga el procedimiento siguiente para desactivar la limpieza automática y, a continuación, consulte *Gestión del correo electrónico infectado* en la página 30 para obtener más información sobre la forma de responder a las alertas.

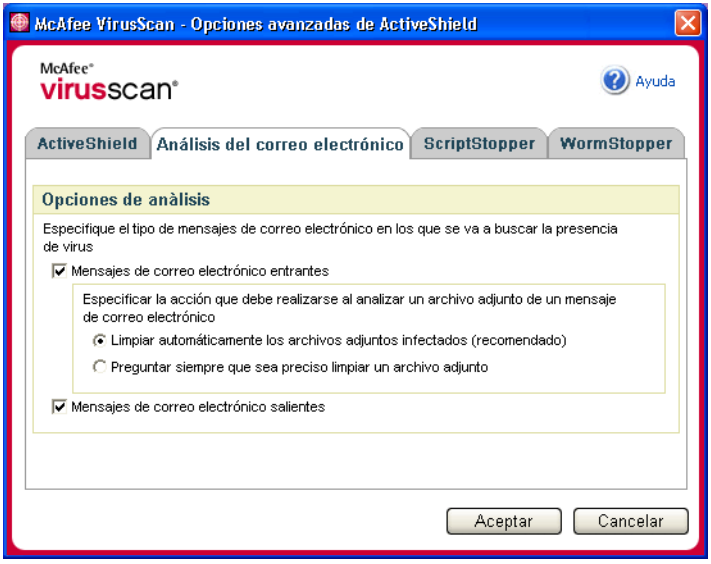


Figura 2-2. Opciones de análisis del correo electrónico

Para desactivar la limpieza automática del correo electrónico infectado:

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 del correo electrónico** (figura 2-2).
3. Haga clic en **Preguntar siempre que sea preciso limpiar un archivo adjunto** y, a continuación, en **Aceptar**.

Análisis de archivos adjuntos de los 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 2-1 en la página 20).

Cuando esta opción está activada, VirusScan analiza y trata de limpiar automáticamente los archivos adjuntos de los mensajes instantáneos de entrada de los clientes de mensajes instantáneos más conocidos, incluidos los siguientes:

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

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

Si un mensaje instantáneo o un archivo adjunto de entrada están infectados, VirusScan lleva a cabo el procedimiento siguiente:

- Intenta limpiar el mensaje infectado.
- Pregunta al usuario si lo pone en cuarentena o si lo suprime en caso de no poder limpiarlo.

Exploración 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 de la exploración.

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 **ActiveShield** (figura 2-3 en la página 26).
3. Haga clic en **Todos los archivos (recomendado)** y, a continuación, en **Aceptar**.

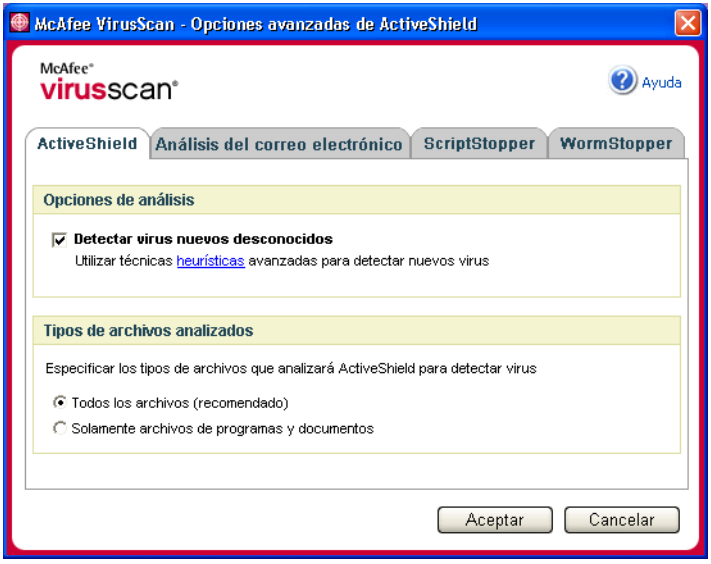


Figura 2-3. Opciones avanzadas de ActiveShield

Exploración exclusiva de los archivos de programas y documentos

Si configura ActiveShield para que utilice la opción **Solamente archivos de programas y documentos**, se analizarán únicamente los archivos de programas y documentos pero no se analizará ningún otro 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 **ActiveShield** (figura 2-3).
3. Haga clic en **Solamente archivos de programas y documentos** y, a continuación, en **Aceptar**.

Exploración de virus nuevos desconocidos

Si configura ActiveShield de modo que utilice la opción predeterminada **Analizar virus nuevos desconocidos (recomendado)**, se emplearán técnicas heurísticas que comparan los archivos con las definiciones de nuevos virus y, al mismo tiempo, 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 **ActiveShield** (figura 2-3 en la página 26).
3. Haga clic en **Analizar virus nuevos desconocidos (recomendado)** y, a continuación, en **Aceptar**.

Exploración de secuencias de comandos y 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, ScriptStopper™ y WormStopper™ evitan la proliferación de virus, gusanos y archivos troyanos.

Los mecanismos de protección de ScriptStopper y WormStopper detectan, notifican y bloquean la actividad perjudicial. La actividad sospechosa puede incluir las acciones siguientes en el equipo:

- Ejecución de una secuencia de comandos o archivo de comandos que provoque la creación, copia o supresión de archivos, o bien la apertura del registro de Windows.
- Intento de reenviar mensajes de correo electrónico a una parte importante de la agenda.
- Intentos de reenviar varios mensajes de correo electrónico en rápida sucesión.

Si configura ActiveShield de modo que utilice las opciones predeterminadas **Activar ScriptStopper (recomendado)** y **Activar WormStopper (recomendado)** en el cuadro de diálogo **Opciones avanzadas**, ScriptStopper y WormStopper supervisarán la ejecución de secuencias de comandos y la actividad del correo electrónico para detectar pautas sospechosas y le avisarán en el momento en que se supere un número determinado de mensajes o destinatarios dentro del intervalo especificado.

Para configurar ActiveShield de modo que detecte actividades parecidas a las de las secuencias de comandos y 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 **ScriptStopper**.

3 Haga clic en **Activar ScriptStopper (recomendado)** (figura 2-4).

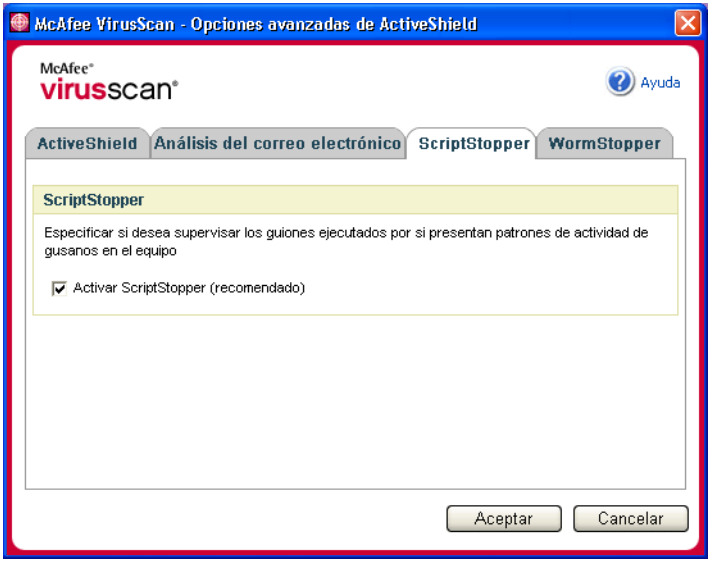


Figura 2-4. Opciones de ScriptStopper

4 Haga clic en la ficha **WormStopper**, y en **Activar WormStopper (recomendado)** y, a continuación, en **Aceptar** (figura 2-5 en la página 29).

De forma predeterminada están activadas las siguientes opciones detalladas:

- Coincidencia de patrones, para detectar la actividad sospechosa.
- Alerta al usuario cuando se envía correo electrónico a 40 o más destinatarios.
- Alerta al usuario cuando se envían 5 mensajes de correo electrónico o más en un lapso de 30 segundos.

NOTA
Si modifica el número de destinatarios o segundos para controlar los mensajes de correo enviados, es posible que se realicen detecciones no válidas. McAfee recomienda que haga clic en **No** para conservar el valor predeterminado. De lo 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 31 para obtener información detallada):

- Bloqueo automático de mensajes sospechosos de correo electrónico de salida

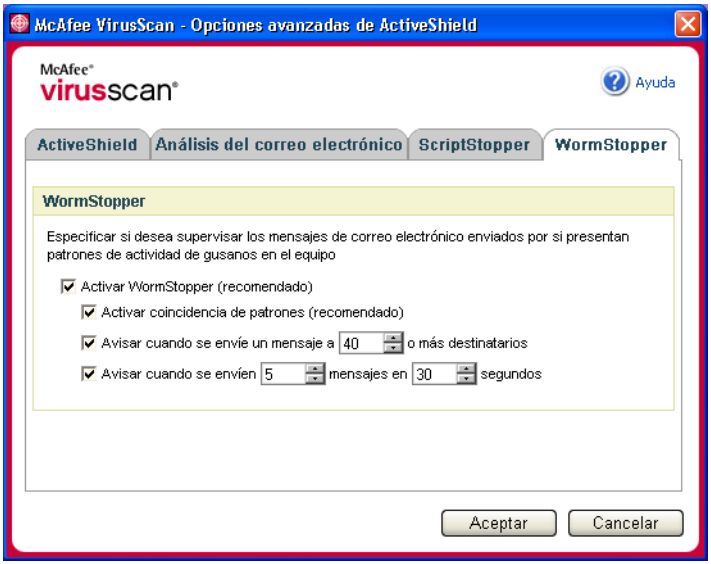


Figura 2-5. Opciones de WormStopper

Acciones que ActiveShield lleva a cabo al descubrir un virus

Si ActiveShield descubre un virus, aparecerá una alerta similar a la de la figura 2-6 en la página 30. ActiveShield intenta limpiar automáticamente la mayor parte de los virus, archivos troyanos y gusanos. A continuación, puede elegir cómo desea tratar los archivos infectados, el correo electrónico infectado, las secuencias de comandos sospechosas y los posibles gusanos; si lo desea, también puede enviar los archivos infectados a los laboratorios de McAfee AVERT para su investigación.

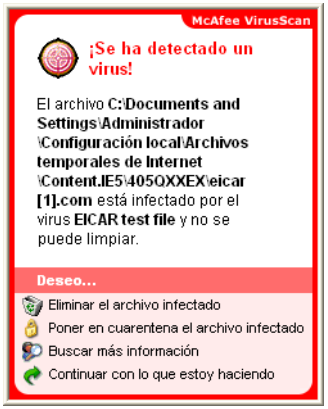


Figura 2-6. Alerta de virus

Gestión de archivos infectados

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 infectado.
- 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 infectado** para cifrar y aislar temporalmente los archivos infectados y sospechosos en el directorio de cuarentena hasta que se pueda tomar una medida conveniente.

Aparecerá un mensaje de confirmación y se le pedirá que examine su equipo en busca de virus. 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 infectado** para intentar eliminar el archivo.

Gestión del correo electrónico infectado

1 Si ha desactivado la limpieza automática del correo electrónico, puede obtener más información y limpiar el mensaje:

a Haga clic en **Buscar más información** para ver el nombre del archivo, el nombre del virus, el estado de la infección, el remitente y el asunto asociados al mensaje infectado.

b Haga clic en **Limpiar los archivos adjuntos infectados**.

2 Si ActiveShield no puede limpiar el mensaje de correo electrónico, haga clic en **Poner en cuarentena los archivos adjuntos infectados** para cifrar y aislar temporalmente los archivos infectados y sospechosos en el directorio de cuarentena hasta que pueda tomar una medida conveniente.

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

3 Si ActiveShield no puede poner el mensaje de correo electrónico en cuarentena, haga clic en **Eliminar los archivos adjuntos infectados** para intentar eliminar el archivo.

Administración de secuencias de comandos sospechosas

1 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:

   a 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.

   b Haga clic en **Detener esta secuencia de comandos** para evitar la ejecución de la secuencia de comandos sospechosa.

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

   a Haga clic en **Permitir la secuencia de comandos completa esta vez** para dejar que todas las secuencias de comandos contenidas en un archivo concreto se ejecuten una vez.

   b Haga clic en **Continuar con lo que estaba haciendo** para hacer caso omiso de la alerta y dejar que se ejecute la secuencia de comandos.

Gestión de gusanos potenciales

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

   a 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 infectado.

   b Haga clic en **Detener este mensaje de correo electrónico** para evitar que el mensaje sospechoso se envíe y elimínelo de la cola de mensajes.

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

Análisis manual del equipo

La función de análisis permite seleccionar discos duros, disquetes, y archivos y carpetas individuales para detectar virus y programas potencialmente no deseados en ellos. Cuando el proceso de análisis localiza un archivo infectado, automáticamente intenta limpiar el archivo, a menos que se trate de un programa no deseado. Si ActiveShield no puede limpiar el archivo, puede eliminar el archivo o ponerlo en cuarentena.

Análisis manual de virus y programas potencialmente no deseados

Para analizar su equipo:

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

Se abrirá el cuadro de diálogo **Análisis de virus** (figura 2-7).

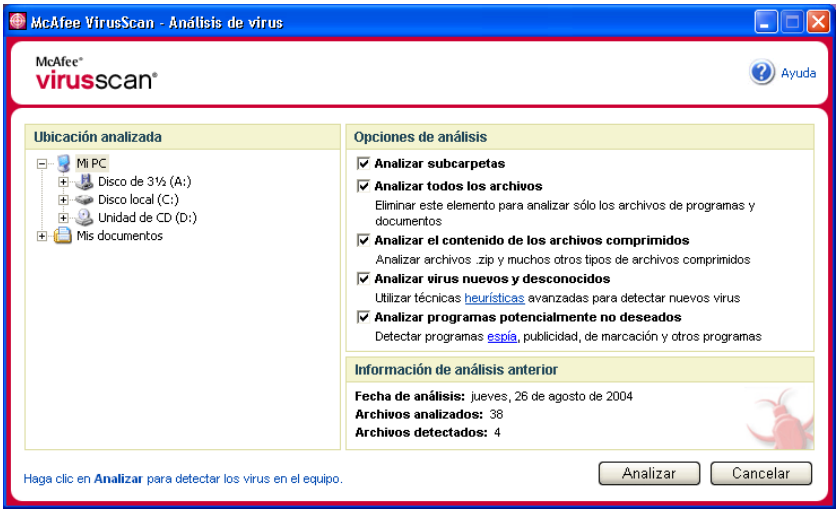


Figura 2-7. Análisis de virus

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 2-7):

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

Ejemplo: Los archivos de la figura 2-8 son los únicos que se analizarán si se desactiva la casilla de verificación **Analizar subcarpetas**. Las carpetas y sus contenidos no se analizarán. Para analizar dichas carpetas y sus contenidos, debe dejar la casilla activada.

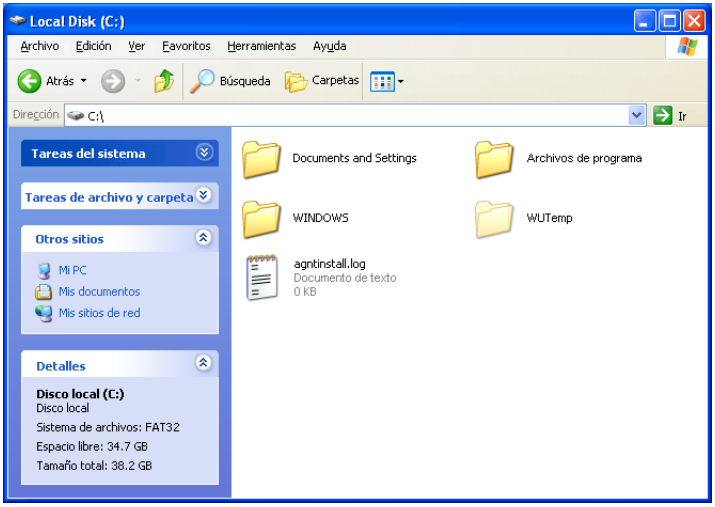


Figura 2-8. Contenido del disco local

- **Analizar todos los archivos**: utilice esta opción para realizar un análisis completo de todos los tipos de archivos. Desactive 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 los archivos infectados ocultos en los archivos.ZIP y otros archivos comprimidos. Desactive esta casilla de verificación para no analizar ningún archivo, ya esté 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 de análisis los puede detectar si esta opción está activada.

- **Analizar virus nuevos desconocidos**: utilice esta opción para encontrar los virus más recientes, para los que puede suceder que no se haya desarrollado aún la "vacuna". 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, por regla general, puedan descartar la existencia de virus. De esta manera, se minimizan las posibilidades de que la función de análisis genere una falsa alarma. No obstante, si un análisis heurístico detecta un virus, el archivo se debería tratar con la misma precaución que cualquier otro archivo que contenga un virus con certeza.

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

- **Analizar si hay programas potencialmente no deseados**: esta opción se utiliza para detectar programas espía, publicidad, de marcación y otros programas que no tenga intención de instalarse en su equipo.

  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 realizarse. Cuanto mayor sea el tamaño del disco duro y mayor sea el número de archivos que contiene, más tiempo llevará la operación de análisis.

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

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

5 Haga clic en **Aceptar** para cerrar el resumen y visualice la lista de cualquier archivo infectado en el cuadro de diálogo **Análisis de virus** (figura 2-9 en la página 35).

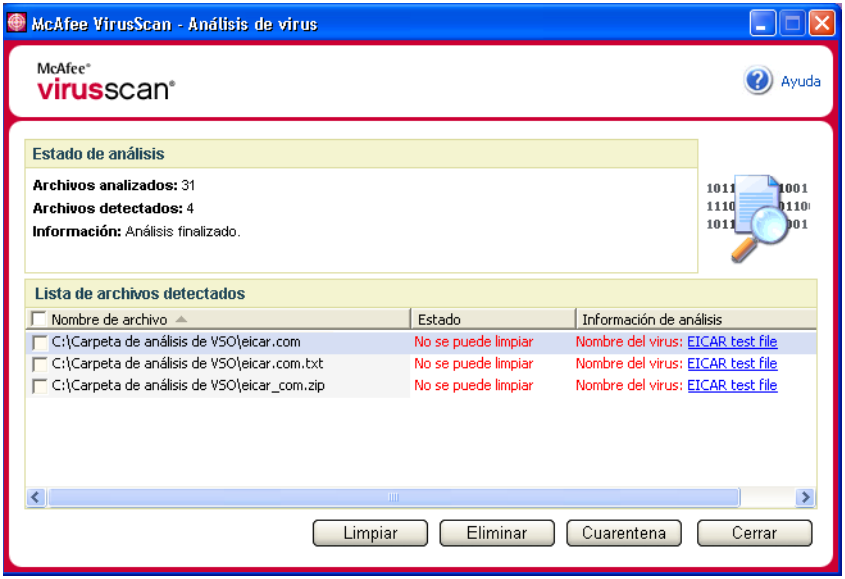


Figura 2-9. Resultados del análisis

NOTA
La función de análisis computa cada archivo comprimido (.ZIP, .CAB, etc.) como un solo archivo en el recuento de **Archivos analizados**. Asimismo, el número de archivos analizados puede variar si ha suprimido los archivos temporales de Internet desde el último análisis.

6 Si no se detecta ningún virus ni ningún programa potencialmente no deseado, haga clic en **Atrás** para seleccionar otra unidad o carpeta que analizar, o bien en **Cerrar** para cerrar el cuadro de diálogo. En cualquier otro caso, consulte *Si el análisis encuentra un virus o un programa potencialmente no deseado* en la página 39.

Análisis desde 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 programas potencialmente no deseados desde dentro del Explorador de Windows.

Análisis de archivos en el Explorador de Windows:

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

   Se abrirá el cuadro de diálogo **Análisis de virus** 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 2-7 en la página 32).

Análisis desde Microsoft Outlook

VirusScan proporciona un icono de la barra de herramientas para analizar la presencia de virus o de programas potencialmente no deseados en los almacenes de mensajes seleccionados y sus subcarpetas, las carpetas de correo o los mensajes de correo electrónico que contengan archivos adjuntos en el seno de 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, a continuación, haga clic en el icono de análisis de correo electrónico de la barra de herramientas  .

   Aparecerá 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 2-7 en la página 32).

Análisis manual de virus y programas potencialmente no deseados

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 programas potencialmente no deseados 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 2-10).

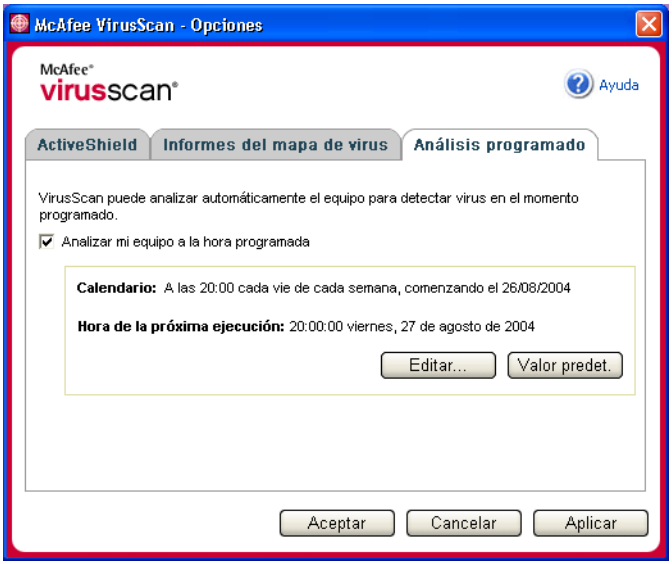


Figura 2-10. Opciones del análisis programado

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

4 Especifique un programa 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 desee 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 el nombre del día o 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**.

  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 varias programaciones**. El último programa admitido permanecerá activado hasta que seleccione otra opción válida.

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

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

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

  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** si desea guardar los cambios y cerrar el cuadro de diálogo. De lo contrario, haga clic en **Cancelar**.

5. Haga clic en **Aceptar** si desea guardar los cambios y cerrar el cuadro de diálogo. De lo contrario, haga clic en **Cancelar**.

6. Si desea restablecer la programación predeterminada, haga clic en **Establecer valores predeterminados**. De lo contrario, haga clic en **Aceptar**.

Si el análisis encuentra un virus o un programa potencialmente no deseado

Scan intenta limpiar automáticamente la mayor parte de los virus, archivos troyanos y gusanos. A continuación, puede elegir la forma de administrar los archivos infectados, incluso si desea enviarlos a los laboratorios de McAfee AVERT para su investigación. Si el análisis 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 infectados**, 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 virus 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 de análisis no consigue limpiar el archivo, haga clic en **Cuarentena** para cifrar y aislar temporalmente los archivos infectados y sospechosos en el directorio de cuarentena hasta que se pueda tomar una medida conveniente. (Consulte *Gestión de archivos en cuarentena* para obtener más información.)

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

Si el archivo infectado no permite utilizar su conexión a Internet o impide el acceso al equipo, pruebe a utilizar el disco de emergencia para iniciarlo. En muchos casos, el disco de emergencia permite iniciar un equipo inutilizado por un archivo infectado. Consulte la sección *Creación de un disco de emergencia* en la página 41 para obtener información más detallada.

Si desea obtener ayuda adicional, consulte al servicio de asistencia técnica de McAfee en http://www.mcafeeayuda.com/.

Gestión de archivos en cuarentena

La función Cuarentena cifra y aísla temporalmente los archivos infectados y 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, a continuación, haga clic en **Gestionar archivos en cuarentena**.

Aparecerá una lista de archivos en cuarentena (figura 2-11).

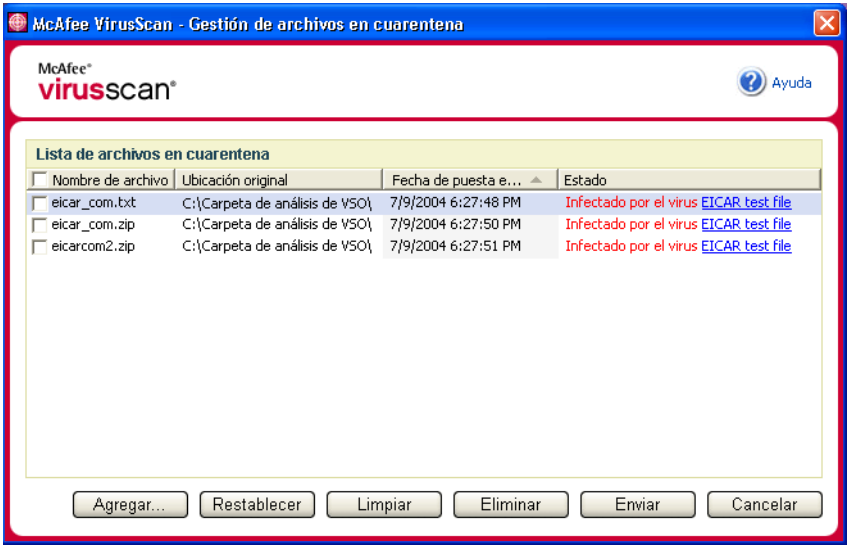


Figura 2-11. Gestión de archivos en cuarentena

2 Marque la casilla de verificación situada junto al archivo o los archivos que desee 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 **Restablecer** 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 a AVERT™ (siglas del inglés de McAfee AntiVirus Emergency Response Team, o Equipo de respuesta de emergencia antivirus de McAfee) para su investigación:

   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 envía el archivo en cuarentena 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 y el nombre original del archivo y su ubicación. El volumen máximo que puede enviar es 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

La utilidad del disco de emergencia crea un disquete de arranque que puede utilizar para iniciar su equipo y detectar los virus que contenga en caso de que un virus no permita su inicio con normalidad.

> **NOTA**
> Debe estar conectado a Internet para descargar la imagen del disco de emergencia. El disco de emergencia sólo está disponible para equipos con particiones FAT (FAT 16 y FAT 32) de disco duro. No se puede utilizar 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 de análisis para asegurarse de que el equipo y el disquete están libres de virus. (Consulte *Análisis manual de virus y programas potencialmente no deseados* en la página 32 para obtener más información.)

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 2-12).

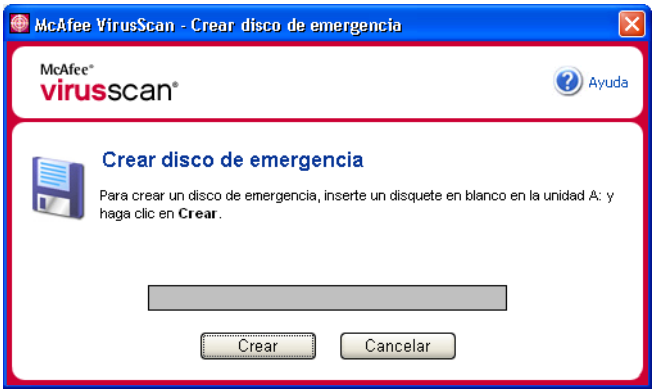


Figura 2-12. Creación de un disco de emergencia

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 del disco de emergencia necesita descargar su archivo 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 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 su 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 agujero.

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 de disquete.
3. Encienda el equipo.

   Aparecerá una ventana de color gris con varias opciones.
4. Seleccione la opción que mejor se adapte a sus necesidades con ayuda de 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

Conviene actualizar el disco de emergencia periódicamente. 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. Regístrese automáticamente en esta función de protección gratuita durante la instalación de VirusScan (en el cuadro de diálogo **Informes del mapa de virus**) o en cualquier otro momento en la ficha **Informes del 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 del mapa de virus** (figura 2-13).

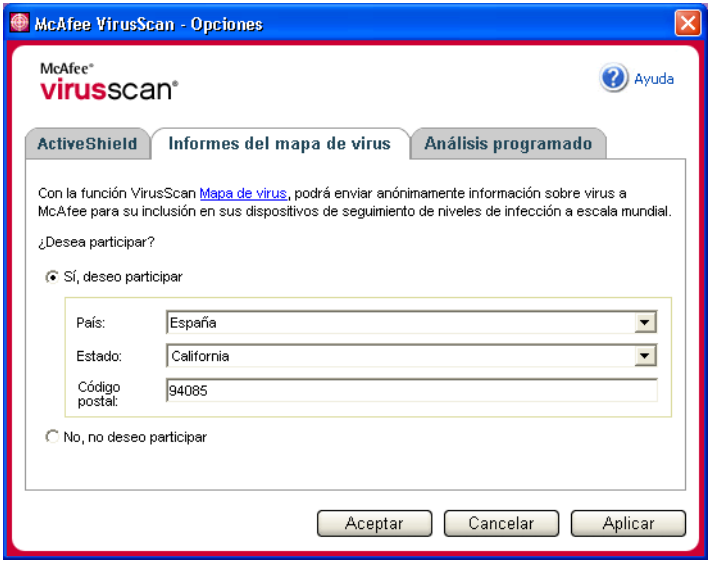


Figura 2-13. Opciones de informes del mapa de virus

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 infección a escala mundial. En caso contrario, seleccione **No, no deseo participar** para no enviar ninguna información.

4. Si reside en los Estados Unidos, seleccione el estado y el código postal correspondiente a la ubicación física del equipo. En caso contrario, VirusScan tratará de seleccionar automáticamente el país en el que se encuentre su 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 infecciones 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 **World Virus Map** (figura 2-14).

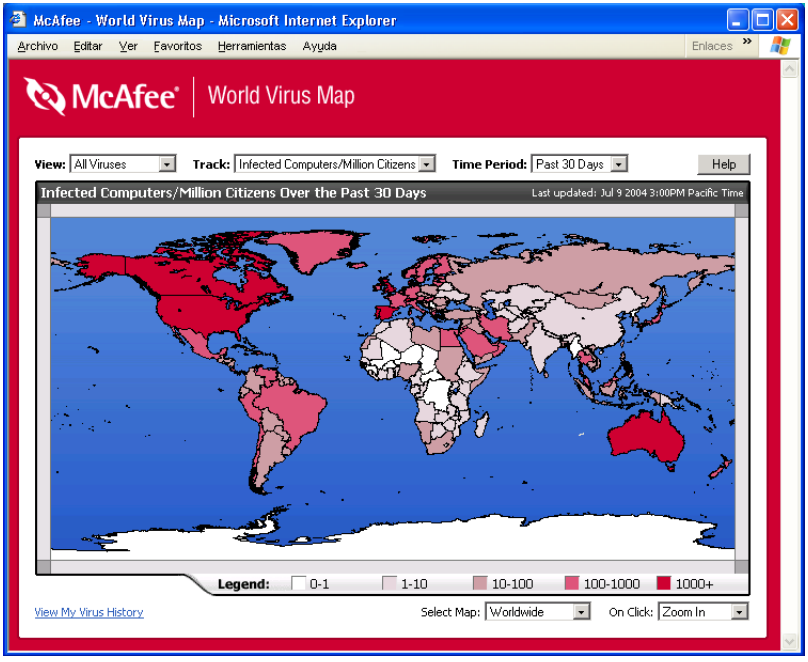


Figura 2-14. World Virus Map

De manera predeterminada, el World Virus Map muestra un conjunto de equipos infectados 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 infectados o cambiar el período de tiempo para mostrar únicamente los resultados de los últimos 7 días o de las pasadas 24 horas.

La sección **Virus Tracking** enumera los totales acumulados correspondientes a los archivos examinados y a los archivos y equipos infectados 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, por consiguiente, su descarga no afecta prácticamente 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 actualizar VirusScan para eliminar la amenaza de un virus.

Comprobación automática de actualizaciones

McAfee SecurityCenter está configurado para automáticamente buscar actualizaciones de todos los servicios de McAfee de los que disponga cada cuatro horas mientras está conectado a Internet para, a continuación, notificárselo 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 todos sus trabajos 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 su 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 ahora**.

   Si existiese una actualización, se abriría el cuadro **Actualizaciones de VirusScan** (figura 2-15 en la página 47). 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.

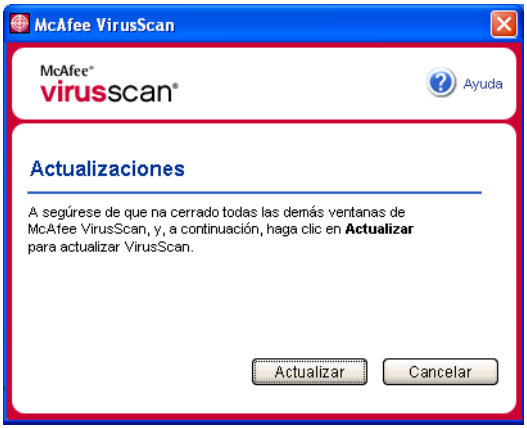


Figura 2-15. Cuadro de diálogo Actualizaciones

4 Regístrese en el sitio Web si se le pide que lo haga. 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 todos sus trabajos y de cerrar las aplicaciones antes de reiniciar el equipo.

McAfee Personal Firewall Plus 3

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 resultan sospechosas.

Gracias a él, disfrutará de las funciones siguientes:

- Protección contra ataques e intentos de ataque de los piratas informáticos.
- Complemento de defensas antivirus.
- Vigilancia de la actividad de Internet y de la red.
- Alerta 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 informes recibidos.
- Funciones de rastreo y búsqueda de eventos.

Funciones nuevas

- **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.

- **Mejoras en la gestión inteligente de las aplicaciones**
  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. Esta base de datos se ha mejorado para proporcionar a los usuarios más información sobre las aplicaciones que se conectan a Internet.

- **Detección avanzada de troyanos**
  McAfee Personal Firewall Plus combina la administración 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.

- **Mejoras en el rastreo visual**
  McAfee Personal Firewall Plus incluye una herramienta actualizada para rastrear intrusiones conocida comoVisual Trace. 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 y todas las escalas siguientes hasta llegar a su equipo. McAfee Personal Firewall Plus ha añadido más datos geográficos a la función Visual Trace que mejoran los detalles de ubicaciones, además de facilitar las ubicaciones de los intrusos con una señalización más visual. Visual Trace permite que los usuarios rastreen de modo visual en dónde se originan las intrusiones, por lo que con estos nuevos datos pueden disponer de una mejor representación gráfica de sus búsquedas.

- **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 buen número de recursos para comprender y apreciar lo que el cortafuegos puede hacer por ellos.

- **Mejoras en la detección de intrusiones**
  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 supervisa 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.

- **Mejoras en el análisis del tráfico**
  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 “a la escucha” de conexiones abiertas. Esto permite a los usuarios ver y actuar con las aplicaciones que pudieran mostrarse susceptibles de intrusión.

Desinstalación de otros cortafuegos

Antes de instalar McAfee Personal Firewall, 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 desactive la función de cortafuegos incorporada. De no hacerlo, 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 detecta que se está ejecutando Windows Firewall en éste.

Una vez instalado, McAfee Personal Firewall desactiva automáticamente Windows Firewall y se establece como cortafuegos predeterminado. Entonces sólo podrá utilizar la funcionalidad y los mensajes de McAfee Personal Firewall. Si posteriormente activa Windows Firewall mediante Windows Security Center o el Panel de Control de Windows, al permitir que los dos cortafuegos se ejecuten en el equipo puede provocar una pérdida parcial del registro de McAfee Firewall, así como la duplicación del estado y de los mensajes de alerta.

NOTA
Si están activados los dos cortafuegos, McAfee Personal Firewall no muestra todas las direcciones IP bloqueadas en la ficha Eventos entrantes. Windows Firewall intercepta la mayor parte de estos eventos y los bloquea, evitando que McAfee Personal Firewall detecte o inicie 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 Windows Firewall de forma predeterminada, pero si decide activar los dos cortafuegos, puede activar el registro de Windows Firewall. El registro predeterminado de Windows Firewall es C:\Windows\pfirewall.log

Para asegurarse de que el equipo está protegido al menos por un cortafuegos, Windows Firewall 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 Windows Firewall, 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**. Utilice este valor si es un usuario novel de cortafuegos. Si tiene experiencia en el uso de cortafuegos, puede utilizar otros valores de configuración. 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 configurar los ajustes de seguridad:

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

   Si es un usuario de cortafuegos inexperto, acepte el valor de configuración predeterminado **Estándar**. El rango de valores de seguridad abarca desde Bloqueado a Abierto

   - **Conexión bloqueada:** se detiene todo el tráfico. En esencia es lo mismo que desconectar la conexión a Internet. Puede utilizar esta opción para bloquear puertos que configuró para estar abiertos en la página Servicios del sistema.
   - **Seguridad estricta:** una aplicación sólo solicita el tipo de acceso a Internet que necesita de forma explícita (por ejemplo, Sólo acceso saliente), y puede concedérselo o bloquearlo. Si la aplicación solicita más adelante Acceso Pleno, puede concedérselo o mantenerlo limitado a Sólo acceso saliente. Utilice este valor si es un usuario de cortafuegos experimentado.
   - **Seguridad estándar (recomendado):** cuando una aplicación solicita acceso a Internet y se le concede, le está concediendo Acceso Pleno. El Acceso Pleno permite a la aplicación enviar y recibir datos no solicitados desde un puerto que no sea del sistema. Utilice este valor si es un usuario novel de cortafuegos.
   - **Seguridad Fiable:** se confía automáticamente en todas las aplicaciones cuando intentan acceder por primera vez a Internet. Sin embargo, puede elegir que se le notifique acerca de nuevas aplicaciones en el equipo mediante alertas. Utilice este valor si percibe que algunos juegos o medios de transferencia no funcionan.
   - **Abierto:** el cortafuegos está realmente 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 **Desactivado**. Para que esto no ocurra, puede cambiar los permisos de las aplicaciones a **Acceso Pleno** o simplemente eliminar la regla del permiso **Bloqueado** en la lista **Permisos**.

4 Seleccione configuración de seguridad adicional:

NOTA
El 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 Eventos entrantes. El sistema de detección de intrusiones detecta los 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 "definición" y se deshace de los paquetes procedentes del equipo infractor.

  IDS busca patrones de tráfico específicos utilizados por los que efectúan el ataque. IDS 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. Los ping se hacen habitualmente para realizar una comprobación rápida antes de intentar iniciar las comunicaciones. Si utiliza o ha utilizado un programa de intercambio de archivos, es posible que su equipo reciba numerosas solicitudes de ping. Si selecciona esta opción, Personal Firewall permite todas las solicitudes de ping sin registrarlas en el registro de eventos entrantes. Si selecciona esta opción, Personal Firewall permite todas las solicitudes de ping sin registrarlas en el registro de eventos entrantes.

- **Permitir a usuarios restringidos cambiar la configuración de Personal Firewall:** si el equipo dispone de Windows XP y se han agregado varios usuarios de XP, asegúrese de que esta casilla de selección está marcada si quiere 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

Para comprobar Personal Firewall:

1. Haga clic con el botón derecho en el icono de McAfee, seleccione **Personal Firewall** y, a continuación, haga clic en **Probar Firewall**.
2. 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.

NOTA
Si se conecta a Internet mediante un servidor proxy o un servidor NAT (del inglés Network Address Translation, conversión de direcciones de red), como ocurre con la mayoría de redes de las oficinas (LAN), la lectura que obtendrá no será la correcta. La herramienta de comprobación de cortafuegos de Hackerwatch.org buscará el equipo que solicitó la comprobación y efectuará una prueba de dicho equipo. Si se conecta a través de un proxy o un servidor NAT, simplemente transmite la solicitud de comprobación, por lo que Hackerwatch.org comprobará un equipo distinto del que realiza la solicitud. Los resultados obtenidos serían los del servidor proxy, no los del equipo del usuario.

Uso de McAfee Personal Firewall Plus

Para abrir Personal Firewall:

Haga clic con el botón derecho en el icono de McAfee, seleccione **Personal Firewall** y haga clic en **Ver resumen**, **Aplicaciones de Internet**, **Eventos entrantes**, o **Utilidades**.

Información acerca de la página Resumen

El Resumen de Personal Firewall incluye cuatro páginas de resumen: Resumen principal, Resumen de aplicaciones, Resumen de eventos y 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 las páginas de resumen de Personal Firewall, haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall** y haga clic en **Ver resumen**. Aparecerá la página Resumen principal (figura 3-1 en la página 55).

Figura 3-1. 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 de resumen que desea ver.
Flecha derecha	Haga clic en el icono de flecha derecha para ver la siguiente página de resumen.
Flecha izquierda	Haga clic en el icono de flecha izquierda para ver la página de resumen anterior.
Inicio	Haga clic en el icono de inicio para volver a la página **Resumen principal**.

La página Resumen principal incluye los datos siguientes:

Elemento	Descripción
Configuración de seguridad	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	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.

Elemento	Descripción
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 dicha dirección llegue hasta su 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, haga clic en **Cambiar vista** y, a continuación, seleccione **Resumen de aplicaciones**. La página Resumen de aplicaciones incluye los datos siguientes:

Elemento	Descripción
Control del tráfico	**Control del tráfico** muestra el volumen de tráfico entrante y saliente en la conexión de Internet durante los últimos diez 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 24 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 de creación de la regla de aplicación.
Novedades	**Novedades** muestra la última aplicación a la que se concedió acceso pleno a Internet.

Elemento	Descripción
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, haga clic en **Cambiar vista** y, a continuación, seleccione **Resumen de eventos**. La página Resumen de eventos incluye los datos siguientes:

Elemento	Descripción
Comparación de puertos	**Comparación de puertos** muestra un gráfico de sectores 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 de dicho puerto.
Principales sospechosos	**Principales sospechosos** indica las direcciones IP bloqueadas con mayor frecuencia, cuándo se produjo el último evento entrante de cada dirección y el número total de eventos entrantes registrados de cada dirección en los últimos 30 días. Haga clic en un evento para ver detalles de la página Eventos entrantes.
Informe diario	**Informe diario** muestra el número de eventos entrantes bloqueados por Personal Firewall en el día actual, esta semana y este mes. Haga clic en un número para ver detalles de eventos procedentes del registro 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 dicha dirección llegue hasta su 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, haga clic en **Cambiar vista** y, a continuación, seleccione **Resumen de HackerWatch**. La página Resumen de HackerWatch incluye los datos siguientes:

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.
Volumen de eventos	**Volumen 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.

Información acerca de la página Aplicaciones de Internet

La página Aplicaciones de Internet permite consultar una lista de las aplicaciones permitidas y bloqueadas.

Haga clic con el botón derecho en el icono de McAfee, seleccione **Personal Firewall** y, después, haga clic en **Aplicaciones de Internet**. Aparecerá la página Aplicaciones de Internet (figura 3-2).

Figura 3-2. Página Aplicaciones de Internet

La página Aplicaciones de Internet incluye los datos siguientes:

- Nombres de aplicaciones
- Nombres de archivos
- Niveles de permiso actuales
- Detalles de aplicaciones: rutas, fechas y horas de los permisos y explicaciones de los tipos de permisos

Cambio de permisos

Personal Firewall permite establecer el nivel de permiso para cada una de las aplicaciones que solicite acceder a Internet.

Para cambiar un nivel de permiso:

1. Haga clic con el botón derecho en el icono de McAfee, seleccione **Personal Firewall** y, después, haga clic en **Aplicaciones de Internet**.
2. En la lista **Permisos**, haga clic con el botón derecho en el nivel de permiso de una aplicación y, a continuación, seleccione un nivel diferente:
   - Seleccione **Permitir acceso pleno** para permitir que la aplicación envíe y reciba datos.
   - Haga clic en **Sólo acceso saliente** para evitar que la aplicación reciba datos.
   - Haga clic en **Bloquear esta aplicación** para evitar que la aplicación envíe y reciba datos.

NOTA
Las aplicaciones previamente bloqueadas siguen bloqueadas cuando el cortafuegos se configura con el valor de seguridad **Abierto** o **Desactivado**. Para que esto no ocurra, puede cambiar los permisos de las aplicaciones a **Acceso Pleno** o simplemente eliminar la regla del permiso **Bloqueado** en la lista **Permisos**.

Para eliminar un nivel de permiso:

1. Haga clic con el botón derecho en el icono de McAfee, seleccione **Personal Firewall** y, después, haga clic en **Aplicaciones de Internet**.
2. En la lista **Permisos**, haga clic con el botón derecho en el nivel de permiso para 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.

Cambio de aplicaciones

Para modificar la lista de aplicaciones a las que se permite y bloquea el acceso a Internet:

1. Haga clic con el botón derecho en el icono de McAfee, seleccione **Personal Firewall** y, después, haga clic en **Aplicaciones de Internet**.
2. Agregue o elimine aplicaciones de la lista **Nombre de la aplicación**:
   - Para agregar una nueva aplicación a la que se permite el acceso, haga clic en **Nueva aplicación permitida**, seleccione la aplicación y, a continuación, haga clic en **Abrir**.

- Para agregar una nueva aplicación bloqueada, haga clic en **Nueva aplicación bloqueada**, seleccione la aplicación que desea bloquear y, a continuación, haga clic en **Abrir**.
- Para eliminar una aplicación de la lista, pulse en **Eliminar regla de aplicación**.

Información acerca de la página Eventos entrantes

La página Eventos entrantes permite consultar el registro de eventos entrantes generado cuando Personal Firewall bloquea el tráfico de Internet no solicitado.

Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall** y, a continuación, haga clic en **Eventos entrantes**. Aparecerá la página Eventos entrantes (figura 3-3).

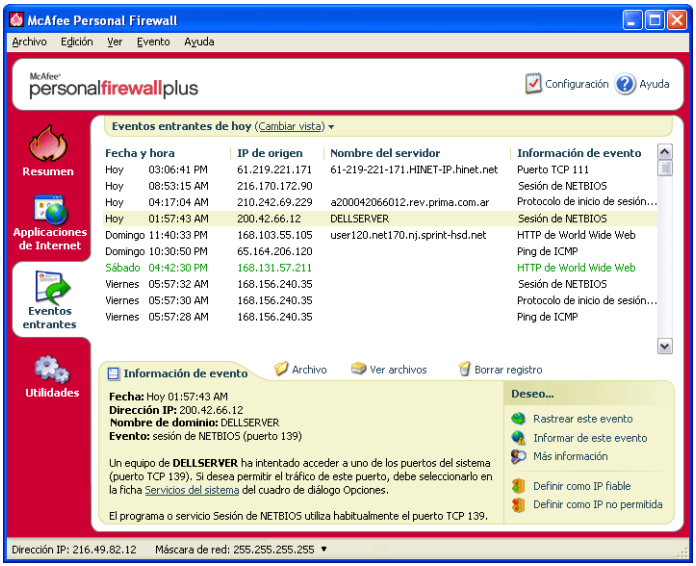


Figura 3-3. Página Eventos entrantes

La página Eventos entrantes incluye los datos siguientes:

- Fechas y horas de los eventos
- IP de origen
- Nombres de servidores
- Nombres de servicio o de aplicaciones
- Detalles del evento: tipos de conexión, puertos de conexión y explicación sobre los eventos de los puertos

Explicación de los eventos

Información acerca de las direcciones IP

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

Direcciones IP especiales

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 ve, indica que el tráfico presenta una dirección IP vacía. Obviamente, esto no es normal, e 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 sería una dirección IP nula.

Eventos desde 0.0.0.0

Si observa eventos procedentes de la dirección IP 0.0.0.0, existen dos causas probables. La primera, y más común, es que por algún motivo 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 está trucada o simulada. Los paquetes trucados pueden ser un indicio de que alguien realiza una exploración en busca de troyanos y, por casualidad, ha llegado a su equipo. Personal Firewall ya ha bloqueado esta dirección, 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. Es importante recordar que esta IP es especial y suele llamarse IP de bucle invertido.

En términos generales, 127.0.0.1 siempre se refiere al usuario, independientemente del equipo en que se encuentre. Esta dirección también suele llamarse "localhost" (servidor local), pues el nombre de equipo "localhost" siempre se remitirá a la dirección IP 127.0.0.1.

¿Significa eso que el equipo intenta un ataque a sí mismo? ¿Hay algún troyano o software espía intentando manipular el equipo? No es probable. Muchos programas habituales utilizan la dirección de bucle invertido para la comunicación entre sus componentes. Por ejemplo, muchos servidores Web o servidores personales de correo permiten configurarlos a través de una interfaz Web a la que se accede normalmente a través de una dirección similar a http://localhost/.

Sin embargo, Personal Firewall permite el tráfico procedente de dichos programas, de modo que si detecta eventos procedentes de 127.0.0.1, lo más probable es que la dirección IP sea simulada o trucada. Los paquetes trucados suelen presentar signos de que alguien está buscando troyanos. Personal Firewall ya ha bloqueado esta dirección, por lo que su equipo estará seguro. Obviamente, presentar un informe sobre eventos procedentes de 127.0.0.1 no tiene ninguna utilidad, por lo que no se hará.

Dicho esto, algunos programas, el más destacado es Netscape 6.2 y superiores, requieren que agregue 127.0.0.1 a la lista 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 confía en la dirección 127.0.0.1, no podrá utilizar su 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, coloque la dirección 127.0.0.1 en la lista de 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 simuladas. Si no confía en esta dirección, el programa no funcionará, pero permanecerá protegido frente al 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 proceden de un lugar cercano, Personal Firewall los muestra en verde.

En la mayoría de las configuraciones de redes de área local (LAN) empresariales, normalmente se selecciona la opción **Confiar en todos los equipos de la LAN** en las opciones de IP fiables.

No obstante, debe recordar que, en algunas situaciones, la red local puede resultar tan peligrosa, o incluso más, que la red externa. Esto es especialmente probable en redes públicas de gran ancho de banda, como DSL o módems por cable. En este caso, se recomienda no seleccionar la opción **Confiar en todos los equipos de la LAN**.

Si se encuentra en una red de banda ancha, agregue manualmente las direcciones IP de los equipos locales a la lista de direcciones IP fiables. Recuerde que puede utilizar direcciones del tipo .255 para confiar en un bloque entero. Por ejemplo, puede confiar en toda una red ICS (uso compartido de conexión a Internet, del inglés Internet Connection Sharing) definiendo como fiable la dirección IP 192.168.255.255.

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 llamarse 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 se utiliza con Microsoft Internet Connection Sharing (ICS). Si utiliza una red ICS, y ve eventos con este bloque, es posible que desee agregar la dirección IP 192.168.255.255 a la lista de direcciones IP fiables. De esta forma confiará en todo el bloque 192.168.xxx.xxx.

Si no se encuentra en una red privada, y ve eventos con direcciones similares, es posible que la dirección IP de origen haya sido trucada o simulada. Los paquetes trucados normalmente presentan signos de que alguien está buscando troyanos. Personal Firewall ya ha bloqueado esta dirección, 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 sirve de nada informar acerca de estos eventos, por lo que no se hará.

Visualización de eventos en el registro de eventos entrantes

El registro de eventos entrantes permite consultar cómodamente los eventos de varias formas. La vista predeterminada se limita a los eventos del 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; la información aparecerá en el área **Información de evento** situada en la parte inferior de la página Eventos entrantes.

Visualización de los eventos del día actual

Para mostrar sólo los eventos que se han producido en el día en curso:

1. Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall** y, a continuación, haga clic en **Eventos entrantes**.
2. En el menú **Ver**, haga clic en **Mostrar los eventos de hoy**.

   El registro de eventos entrantes muestra sólo los eventos que se han producido en el día actual.

Visualización de eventos de esta semana

Para mostrar los eventos que se han producido durante la semana pasada:

1. Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall** y, a continuación, haga clic en **Eventos entrantes**.
2. En el menú **Ver**, haga clic en **Mostrar eventos de esta semana**.

   El registro de eventos entrantes muestra sólo los eventos que se han producido en la semana actual.

Visualización del registro completo de eventos entrantes

Para mostrar todos los eventos del registro de eventos entrantes:

1. Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall** y haga clic en **Eventos entrantes**.
2. En el menú **Ver**, haga clic en **Mostrar registro completo**.

   El registro de eventos entrantes muestra todos los eventos del registro, sin incluir los archivos comprimidos.

Visualización sólo de los eventos de un día concreto

Esta función resulta de gran utilidad cuando desea consultar los eventos que se produjeron un determinado día. Se ocultarán todos los eventos que no se hayan producido el día seleccionado.

Para visualizar todos los eventos de un determinado día:

1. Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall** y, a continuación, haga clic en **Eventos entrantes**.
2. En el menú **Ver**, haga clic en **Mostrar sólo eventos de un día concreto**.

   Los eventos que se hayan producido en el día actual se mostrarán en el registro de eventos entrantes.

Visualización sólo de los eventos de una dirección de Internet concreta

Esta opción resulta de gran utilidad para consultar los eventos procedentes de una dirección de Internet concreta. El resto de los eventos no se muestra.

Para visualizar todos los eventos de una dirección de Internet determinada:

1. Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall** y, a continuación, haga clic en **Eventos entrantes**.
2. En el menú **Ver**, haga clic en **Mostrar sólo eventos de una dirección de Internet concreta.**

   Los eventos originados en la dirección de Internet seleccionada se mostrarán en el registro de eventos entrantes.

Visualización sólo de eventos con la misma información de evento

Esta opción resulta de gran utilidad cuando se necesita comprobar si existen otros eventos en el registro que presenten la misma información en la columna **Información de evento** que el evento seleccionado. Podrá consultar cuántas veces ha ocurrido dicho 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 suele utilizar dicho puerto.

Para mostrar todos los eventos con la misma información de evento:

1. Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall** y haga clic en **Eventos entrantes**.
2. En el menú **Ver**, haga clic en **Mostrar sólo eventos con la misma información de evento**.

   Los eventos cuya información coincida aparecerán en el registro de eventos entrantes.

Respuesta a eventos entrantes

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

Rastreo del evento seleccionado

Puede intentar un rastreo visual de las direcciones IP correspondientes a un evento del registro de eventos entrantes:

1. Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall** y haga clic en **Eventos entrantes**.
2. Pulse con el botón derecho en el evento que desea rastrear y, a continuación, seleccione **Rastrear evento seleccionado**.

   También puede hacer doble clic en el evento para iniciar el rastreo.

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

Obtención de consejos de HackerWatch.org

También puede intentar obtener más información sobre un evento en la comunidad en línea contra la piratería HackerWatch.org:

1. Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall** y haga clic en **Eventos entrantes**.
2. Busque el evento sobre el que desea obtener más información y haga clic en él.
3. En el menú **Evento**, haga clic en **Más información sobre evento**.

Se abrirá el navegador Web y se dirigirá al sitio Web de HackerWatch.org en http://www.hackerwatch.org/ para obtener detalles sobre el tipo de eventos y consejos sobre si debe informar al respecto.

Informes sobre un evento

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

1. Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall** y haga clic en **Eventos entrantes**.
2. Haga clic en el evento sobre el que desea informar y, a continuación, seleccione **Informar de este evento** en el panel inferior derecho.

   Personal Firewall informa sobre el evento al sitio Web HackerWatch.org mediante su identificación exclusiva.

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 de inmediato. 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 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 este servicio, sus envíos serán rastreados y nos permitirá notificarle 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 petición se encaminará a través de HackerWatch.org, por lo que su dirección de correo electrónico nunca se verá expuesta.

Confianza en una dirección

Si detecta un evento en el registro de eventos que contenga una dirección IP que necesite autorizar, puede configurar Personal Firewall para que permita todas las conexiones procedentes de ella en todo momento:

1. Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall** y haga clic en **Eventos entrantes**.
2. Haga clic con el botón derecho del ratón en el evento en cuya dirección IP desee confiar y, después, en **Confiar en la dirección IP de origen**.
3. Verifique que la dirección IP que muestra el mensaje de confirmación de confianza en esta dirección 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 en la ficha **Utilidades**.
2. Haga clic en el icono **IP fiables y prohibidas**, a continuación, haga clic en la ficha **Direcciones IP fiables**.

   La dirección IP aparecerá 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 dicha dirección. Por lo tanto, la prohibición de una dirección no incrementa la protección del sistema a menos que su equipo tenga abiertos, intencionadamente, determinados puertos a través de la función de 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 más puertos abiertos intencionadamente y tiene razones para creer que debe bloquear el acceso a los puertos abiertos por parte de dicha dirección.

Si detecta un evento del registro de eventos entrantes que contenga una dirección IP que desee prohibir, puede configurar Personal Firewall para que rechace todas las conexiones procedentes de ella:

1. Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall** y haga clic en **Eventos entrantes**.
2. Haga clic con el botón derecho en el evento cuya dirección IP desee prohibir y haga clic en **Prohibir dirección IP de origen**.
3. Verifique que la dirección IP que muestra el mensaje de confirmación de prohibición de esta dirección es correcta y haga clic en **Aceptar**.

   La dirección IP se agregará a la lista **Direcciones IP prohibidas**.

Para verificar que la dirección IP se ha agregado:

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

   La dirección IP se agregará a 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.

Compresión del registro de eventos entrantes

Puede archivar el registro de eventos entrantes actual en un archivo comprimido dentro del disco duro. Es aconsejable comprimir el registro de eventos de manera regular porque puede alcanzar un tamaño considerable.

Para comprimir el registro de eventos entrantes:

1. Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall** y, a continuación, haga clic en **Eventos entrantes**.
2. En el menú **Archivo**, haga clic en **Comprimir registro**.
3. Haga clic en **Sí** en el mensaje de confirmación.
4. Haga clic en **Guardar** para guardar el archivo comprimido en la ubicación predeterminada, o bien diríjase a la ubicación en la que desea guardarlo.

Visualización del registro de eventos entrantes comprimido

Puede ver todos los registros de eventos entrantes previamente comprimidos.

> **NOTA**
> Para consultar los archivos comprimidos, deberá comprimir el registro actual de eventos entrantes. De lo contrario, el registro de eventos entrantes se borrará cuando visualice un archivo comprimido.

1. Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall** y haga clic en **Eventos entrantes**.
2. En el menú Archivo, haga clic en **Ver registros comprimidos**.
3. Haga clic en el nombre del archivo comprimido (puede que necesite buscarlo primero) y, después, en **Abrir**.

   Los datos comprimidos se mostrarán en el registro de eventos entrantes.

Eliminación del registro de eventos entrantes

Puede borrar toda la información del registro de eventos entrantes.

> **NOTA**
> 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 comprimido.

1. Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall** y haga clic en **Eventos entrantes**.
2. En el menú **Archivo**, seleccione **Borrar registro**.
3. Haga clic en **Sí** en el cuadro de confirmación para borrar el registro.

   El registro de eventos quedará vacío.

Exportación de eventos mostrados

Puede exportar el registro de eventos a un archivo de texto en caso de que necesite compartirlo con su proveedor de servicios de Internet (ISP), con el servicio de asistencia técnica o con las autoridades públicas pertinentes.

1. Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall** y haga clic en **Eventos entrantes**.
2. En el menú Archivo, haga clic en **Exportar eventos mostrados**.
3. Busque la ubicación en la que desea guardar los eventos.
4. Cambie el nombre del archivo si lo cree necesario, y haga clic en **Guardar**.

   Los eventos se guardarán en un archivo .txt en la ubicación escogida.

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.

1. Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall** y haga clic en **Eventos entrantes**.
2. Haga clic en el evento del registro de eventos entrantes que quiere exportar.
3. En el menú **Edición**, haga clic en **Copiar evento seleccionado en el portapapeles**.
4. Abra el Bloc de notas:

   Haga clic en el botón Inicio de Windows, seleccione Programas, Accesorios y finalmente Bloc de notas.
5. En el menú **Edición**, haga clic en **Pegar**. El 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.

1. Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall** y haga clic en **Eventos entrantes**.
2. Haga clic en el evento del registro de eventos entrantes que desee eliminar.
3. En el menú **Edición**, haga clic en **Eliminar evento seleccionado**.

   El evento quedará eliminado del registro de eventos entrantes.

Acerca de las alertas

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

NOTA
Las recomendaciones sobre las alertas ayudan a decidir cómo reaccionar en cada situación. Para que las alertas incluyan recomendaciones, haga clic en la ficha **Utilidades**, 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 explore 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. (Seguridad estándar o estricta)
- **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 ha actualizado recientemente la aplicación en cuestión, debería tener cuidado a la hora de concederle permiso de acceso a Internet. (Seguridad Fiable, Estándar o Estricta)
- **La aplicación desea tener acceso de servidor:** esta alerta aparece cuando Personal Firewall detecta que una aplicación con permiso para acceder a Internet solicita acceder a Internet como servidor. (Seguridad estricta)

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 de aplicación de Internet bloqueada

Si aparece una alerta sobre un programa troyano (figura 3-4), Personal Firewall denegará automáticamente el acceso del programa a Internet y recomendará que se explore el equipo en busca de virus.

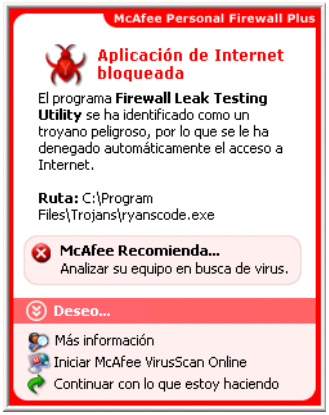


Figura 3-4. Alerta de aplicación de Internet bloqueada

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

- Haga clic en **Más información** para obtener detalles sobre el evento del registro de eventos entrantes (consulte *Información acerca de la página Eventos entrantes en la página 61* para obtener información detallada al respecto).
- Pulse en **Iniciar McAfee VirusScan Online** para analizar el equipo en busca de virus.
- Haga clic en **Continuar con lo que estaba haciendo** si no desea aplicar otra medida aparte de la que tome Personal Firewall.

Aplicación que desea obtener acceso a la alerta de Internet

Si selecciona el nivel de seguridad **Estándar** o **Estricta** en las opciones de Configuración de seguridad, Personal Firewall mostrará una alerta (figura 3-5 en la página 74) cuando detecte tráfico de red o de acceso a Internet procedente de aplicaciones nuevas o modificadas.

Figura 3-5. Aplicación que desea obtener acceso a la alerta de Internet

Si aparece una alerta que recomienda precaución a la hora de permitir el acceso a Internet a la aplicación, haga clic en **Haga clic aquí para obtener más información** para ver información adicional de 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 el acceso a Internet (figura 3-6).

Figura 3-6. Alerta Aplicación no reconocida

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

La información enviada la emplean con otras herramientas de investigación los operadores de HackerWatch 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 envíe y reciba datos no solicitados desde un puerto que no sea del sistema.
- Haga clic en **Bloquear todo acceso** para impedir que la aplicación envíe o reciba datos.

Alerta de modificación de aplicación

Si selecciona **Fiable**, **Estándar** o **Estricta** en las opciones de Configuración de seguridad, Personal Firewall mostrará una alerta (figura 3-7) 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 3-7. Alerta de modificación de aplicación

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

- Haga clic en **Conceder acceso** para permitir que la aplicación envíe y reciba datos no solicitados desde un puerto que no sea del sistema.
- Haga clic en **Bloquear todo acceso** para impedir que la aplicación envíe o reciba datos.

Alerta “La aplicación desea tener acceso al servidor”

Si selecciona el nivel de seguridad **Estricta** en las opciones de Configuración de seguridad, Personal Firewall mostrará una alerta (figura 3-8) al detectar que una aplicación con permiso de acceso a Internet solicita acceso a Internet como servidor.

Figura 3-8. Alerta “La aplicación desea tener acceso al 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 al servidor** para permitir que la aplicación envíe y reciba datos.
- Haga clic en **Restringir a acceso mensajes salientes** para impedir que la aplicación reciba datos.
- Haga clic en **Bloquear todo acceso** para impedir que la aplicación envíe o reciba datos.

Alertas verdes

Las alertas verdes informan de cambios que se han realizado en Personal Firewall. Por ejemplo, pueden informar de las aplicaciones a las que Personal Firewall ha concedido acceso automático a Internet, o informar de nuevas reglas de aplicación.

El programa tiene permiso para acceder a Internet: esta alerta aparece cuando Personal Firewall concede acceso a Internet automáticamente a todas las aplicaciones nuevas o modificadas 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 "La aplicación tiene permiso para acceder 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 o modificadas, y se lo notificará mediante una alerta (figura 3-9).

Figura 3-9. El programa tiene permiso para acceder 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 *Información acerca de la página Aplicaciones de Internet* en la página 59 para obtener información detallada al respecto).
- Haga clic en **Desactivar este tipo de alertas** para evitar la activación de alertas de este tipo.
- Haga clic en **Continuar con lo que estoy haciendo** si no desea aplicar otra medida aparte de la que tome Personal Firewall.

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 el tráfico no deseado procedente de una red o de Internet. (Seguridad Fiable, Estándar o Estricta)

Alerta de intento de conexión bloqueado

Si ha seleccionado la seguridad **Fiable**, **Estándar** o **Estricta**, Personal Firewall muestra una alerta (figura 3-10) al bloquear el tráfico de red o de Internet no deseado.

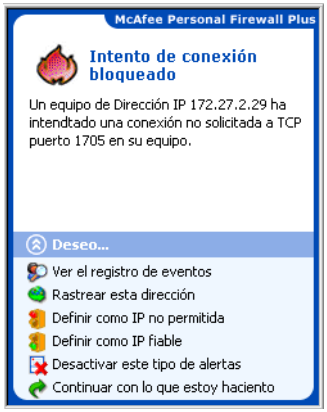


Figura 3-10. Alerta de intento de conexión bloqueado

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 del registro de eventos entrantes de Personal Firewall (consulte *Información acerca de la página Eventos entrantes* en la página 61 para obtener información detallada al respecto).
- Haga clic en **Rastrear esta dirección** para realizar un rastreo visual de las direcciones IP correspondientes al evento.
- Haga clic en **Definir como IP no permitida** para evitar que se acceda al equipo desde esta dirección. La dirección se agregará a la lista de 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.

McAfee Privacy Service 4

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

Funciones

Esta versión de McAfee Privacy Service incluye las siguientes funciones:

- Bloqueador de Web bug: Bloquea Web bugs (objetos que se obtienen en sitios Web potencialmente peligrosos) para que no se carguen desde las páginas exploradas.
- Bloqueador de ventanas emergentes: Evita que aparezcan ventanas emergentes mientras explora en Internet.
- Triturador: McAfee Shredder protege la privacidad de manera rápida y segura mediante la eliminación de archivos no deseados.

Administrador

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

NOTA
El Administrador se considera adulto y por lo tanto puede acceder a todos los sitios Web pero debe permitir o impedir la transmisión de información personal identificable añadida (PII).

Asistente para la configuración

El Asistente para la configuración le permite crear al Administrador (si no lo ha hecho previamente), gestionar los ajustes globales, introducir información personal y agregar usuarios.

NOTA
Recuerde su contraseña de Administrador y la respuesta de seguridad para que pueda iniciar sesión en Privacy Service. Si no puede iniciar sesión, no puede utilizar ni Privacy Service ni Internet. Mantenga su contraseña en secreto de manera que sólo usted pueda cambiar la configuración de Privacy Service.

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

Privacy Service siempre acepta cookies de McAfee.com.

Recuperación de la contraseña del Administrador

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

1. Haga clic con el botón derecho en el icono de McAfee  , elija **McAfee Privacy Service** y seleccione **Iniciar la sesión**.
2. Seleccione **Administrador** en el menú desplegable **Nombre de usuario**.
3. Haga clic en **¿Olvidó su contraseña?**

NOTA
Introduzca la respuesta a la pregunta de seguridad que aparece y, a continuación, haga clic en **Obtener contraseña**. Aparecerá un mensaje con la contraseña. Si olvida la respuesta a la pregunta de seguridad, póngase en contacto con el servicio de Atención al cliente.

Usuario de inicio

Al encender el equipo, se iniciará la sesión automáticamente en Privacy Service mediante el usuario de inicio.

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

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

Apertura de McAfee Privacy Service

Cuando instale McAfee Privacy Service, el icono de McAfee aparecerá en la bandeja del sistema de Windows, cerca del reloj del sistema  . Con el icono de McAfee, puede acceder a McAfee Privacy Service, McAfee SecurityCenter y otros productos McAfee instalados en su equipo.

Apertura e inicio de sesión en Privacy Service

Para abrir Privacy Service:

1. Haga clic con el botón derecho en el icono de McAfee, elija **McAfee Privacy Service** y seleccione **Inicio de sesión**.
2. Seleccione su nombre de usuario en el menú desplegable **Nombre de usuario**.
3. Introduzca la contraseña en el campo **Contraseña**.
4. Haga clic en **Inicio de sesión**.

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

Desactivación de Privacy Service

Debe haber iniciado la sesión en Privacy Service como Administrador si desea desactivarlo.

Para desactivar Privacy Service

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

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

Actualización de McAfee Privacy Service

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

Para comprobar manualmente la existencia de actualizaciones, haga clic en el icono Actualizaciones situado en el panel superior.

Desinstalación y reinstalación de Privacy Service

Debe haber iniciado Privacy Service como Administrador para desinstalarlo.

NOTA
Al desinstalar Privacy Service, puede eliminar todos los datos de Privacy Service.

Desinstalación de Privacy Service

1. Guarde su trabajo y cierre todas las aplicaciones que se encuentren abiertas.
2. Abra el Panel de control:
   - Usuario de Windows 98, Windows Me y Windows 2000: Seleccione **Inicio**, **Configuración** y haga clic en **Panel de control**.
   - Usuario de Windows XP: En la barra de tareas de Windows, seleccione **Inicio** y haga clic en **Panel de control**.
3. Abra el cuadro de diálogo **Agregar o quitar programas**:
   - Usuario de Windows 98, Me y 2000: Haga doble clic en **Agregar o quitar programas**.
   - Usuario de Windows XP: Haga clic en **Agregar o quitar programas**.

4 Seleccione McAfee Privacy Service en la lista de programas y haga clic en **Cambiar o quitar**.

5 Cuando se le pida que confirme la desinstalación, haga clic en **Sí**. Privacy Service comenzará a desinstalarse.

6 Cuando se le pida que reinicie el sistema, haga clic en **Cerrar**. El equipo se reiniciará para completar el proceso de desinstalación.

Instalación de Privacy Service

1 Diríjase al sitio Web de McAfee y vaya a la página de Privacy Service.

2 Haga clic en el enlace **Descargar** en la página Privacy Service.

3 Haga clic en **Sí** en cualquiera de los mensajes que aparecen preguntando si desea descargar archivos del sitio Web de McAfee.

4 Haga clic en **Iniciar la instalación** en la ventana de instalación de Privacy Service.

5 Al finalizar la descarga, haga clic en **Reiniciar** para reiniciar el equipo. O, haga clic en **Cerrar** si necesita guardar cualquier trabajo o salir de cualquier programa y, a continuación, reinicie el equipo como de costumbre. Debe reiniciar el equipo para que Privacy Service funcione correctamente.

Después de reiniciar el equipo, necesitará volver a establecer un Administrador.

Agregación de usuarios

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

1 Haga clic con el botón derecho en el icono de McAfee  .

2 Seleccione **McAfee Privacy Service** y, a continuación, **Gestionar usuarios**. Aparecerá el cuadro de diálogo **Seleccionar un usuario**.

3 Haga clic en **Agregar** e introduzca el nuevo nombre de usuario en el campo **Nombre de usuario**.

Configuración de la contraseña

1. Escriba una contraseña en el campo **Contraseña**. La contraseña puede ser de hasta 50 caracteres y contener letras en mayúscula y minúscula así como números.
2. Escriba de nuevo la contraseña en el campo **Confirmar contraseña**.
3. Seleccione **Convertir a este usuario en Usuario de inicio** si desea que este usuario sea el Usuario de inicio.
4. Haga clic en **Siguiente**.

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

Establecimiento de la clasificación de contenido

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

Configuración del bloqueador de cookies

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

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

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

  Privacy Service acepta siempre cookies de McAfee.

Establecimiento de límites de tiempo de acceso a Internet

Para permitir que un nuevo usuario utilice Internet sin ninguna restricción de tiempo

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

Para establecer límites de tiempo para el nuevo usuario

1. Seleccione **Restringir el uso de Internet** y haga clic en **Editar**.
2. En el menú desplegable **Día** seleccione los días en los que desee que el nuevo usuario utilice Internet.
3. Seleccione la **Hora de inicio** y la **Hora de finalización** en los campos respectivos y haga clic en **Agregar**.
4. Haga clic en **Aceptar** en el cuadro de dialogo de confirmación. Los días y las horas seleccionados aparecerán en el área día. Para eliminar un horario de acceso, seleccione el día y haga clic en **Eliminar**.
5. Haga clic en **Listo** cuando haya terminado de agregar los horarios.
6. Haga clic en **Crear**. El nuevo usuario aparecerá en la lista Seleccionar a un usuario. Si un usuario intenta utilizar Internet sin permiso, Privacy Service mostrará un mensaje advirtiendo al usuario que no tiene permiso para utilizar Internet en ese momento.

Para evitar que un nuevo usuario acceda a Internet

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

Edición de usuarios

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

Cambio de contraseñas

1. Seleccione el usuario cuya información desee modificar y haga clic en **Editar**.
2. Seleccione **Contraseña** e introduzca la nueva contraseña del usuario en el campo **Nueva contraseña**. La contraseña puede ser de hasta 50 caracteres y contener letras en mayúscula y minúscula así como números.
3. Introduzca otra vez la nueva contraseña en el campo **Confirmar contraseña** y haga clic en **Aplicar**.
4. Haga clic en **Aceptar** en el cuadro de dialogo de confirmación.

NOTA
Un administrador puede cambiar la contraseña de un usuario sin necesidad de conocer la contraseña actual de éste.

Cambio de la información de usuario

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

Modificación de la configuración del bloqueador de cookies

1. Seleccione el usuario cuya información desee modificar y haga clic en **Editar**.
2. Seleccione **Cookies** y, a continuación, la opción adecuada.
   - **Rechazar todos los cookies:** Devuelve los cookies ilegibles a los sitios Web que los han enviado. Para funcionar correctamente, algunos sitios Web requieren que tenga los cookies activados.
   - **Preguntar al usuario si desea aceptar cookies:** Le permite decidir si desea aceptar o rechazar cada cookie de manera individual. Privacy Service le notifica si el sitio Web que está a punto de visitar desea enviar cookies a su equipo. Después de haber realizado la elección, no se le volverá a preguntar acerca de dicho cookie.

- **Aceptar todos los cookies:** Permite a los sitios Web leer los cookies que envían a su equipo.

3 Haga clic en **Aplicar** y, a continuación, en **Aceptar** en el cuadro de diálogo de confirmación.

Edición de la lista para aceptar y rechazar cookies

1 Seleccione **Preguntar al usuario si desea aceptar cookies** y haga clic en **Editar** para especificar que sitios Web pueden leer cookies.

2 Especifique la lista que esté modificando mediante la selección de **Sitios Web que pueden establecer cookies** o **Sitios Web que no pueden establecer cookies**.

3 En el campo **http://**, introduzca la dirección del sitio Web del que vaya a aceptar o rechazar cookies.

4 Haga clic en **Agregar**. El sitio Web aparecerá en la lista de sitios Web.

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

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

Privacy Service acepta siempre cookies de McAfee.

Cambio del grupo de edad

1 Seleccione el usuario cuya información desee modificar y haga clic en **Editar**.

2 Seleccione **Grupo de edad**.

3 Seleccione un nuevo Grupo de edad para el usuario y haga clic en **Aplicar**.

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

Modificación de los límites de tiempo de acceso a Internet

1 Seleccione el usuario cuya información desee modificar y haga clic en **Editar**.

2 Seleccione **Límites de tiempo** y haga lo siguiente:

Para permitir siempre el acceso a Internet del usuario

1 Seleccione **Puede utilizar Internet en todo momento** y haga clic en **Aplicar**.

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

Para restringir el acceso del usuario a Internet

1. Seleccione **Restringir el uso de Internet** y haga clic en **Editar**.
2. En el menú desplegable **Día**, seleccione los días en los que desee permitir el acceso a Internet.
3. Seleccione la **Hora de inicio** y la **Hora de finalización** y haga clic en **Agregar**.
4. Haga clic en **Aceptar** en el cuadro de dialogo de confirmación. Los días y las horas seleccionados aparecerán en el área situada debajo de las listas.
5. Haga clic en **Listo** cuando haya terminado de agregar los horarios.

Modificación del usuario de inicio

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

> **NOTA**
> Si ya existe un usuario de inicio, no tendrá que desactivarlo como usuario de inicio.

Eliminación de usuarios

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

Opciones

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

Bloqueo de sitios Web

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

> **NOTA**
> Los usuarios que pertenezcan a un nivel de grupo Adulto podrán acceder a todos los sitios Web, incluso si éstos aparecen en la lista Sitios Web bloqueados.

Permiso de sitios Web

El Administrador puede permitir a todos los usuarios que visiten sitios Web específicos. Esto sobrescribe la configuración predeterminada de Privacy Service y de los sitios Web agregados a la Lista para bloquear.

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

Bloqueo de información

El Administrador puede impedir que otros usuarios envíen información personal específica a través de Internet (el Administrador podrá enviar esta información).

Cuando Privacy Service detecta información personal identificable (PII) que vaya a ser enviada, sucederá lo siguiente:

- Si usted es el Administrador, se le solicitará y podrá decidir si desea enviar o no la información.
- Si el usuario que ha iniciado la sesión no es el Administrador, la información bloqueada será reemplazada por *mcgdog*. Por ejemplo, si envía el correo electrónico *Lance Armstrong gana el Tour* y Armstrong está establecido como información personal para bloquear; entonces el correo electrónico que se envía es el siguiente *Lance mcgdogmcg gana el Tour*.

Agregación de información

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

Edición de información

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

Eliminación de información personal

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

Bloqueo de Web bugs

Los Web bugs son pequeños archivos gráficos que pueden enviar mensajes a terceros, realizar el seguimiento de los hábitos de navegación en Internet o transmitir información personal a una base de datos externa. Los terceros pueden utilizar esta información para crear perfiles de usuario.

Para evitar que se descarguen Web bugs desde las páginas Web exploradas, seleccione **Bloquear Web Bugs en este equipo**.

Bloqueo de anuncios

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

Las ventanas emergentes son ventanas secundarias del navegador que contienen anuncios no deseados que se muestran automáticamente al visitar el sitio Web. Privacy Service únicamente bloquea las ventanas emergentes que se cargan automáticamente al abrir una página Web. Privacy Service no bloquea las ventanas emergentes que se inician al hacer clic en un enlace. Para mostrar una ventana emergente bloqueada, mantenga pulsada la tecla CTRL mientras actualiza la página Web.

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

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

Para desactivar el bloqueo de ventanas emergentes, haga clic con el botón derecho en la página Web, elija **Bloqueador de ventanas emergentes McAfee** y desactive **Activar bloqueador de ventanas emergentes**.

Permiso de cookies desde sitios Web específicos

Si bloquea los cookies o si se le solicita hacerlo antes de que sean aceptados y encuentra ciertos sitios Web que no funcionan correctamente, deberá configurar Privacy Service para que le permita leer dichos cookies.

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

Copia de seguridad de la base de datos de Privacy Service

El archivo de copia de seguridad de la base de datos sólo podrá utilizarse si la base de datos original está dañada o se ha eliminado. Cuando esto ocurre, Privacy Service le solicita que restaure la base de datos de Privacy Service.

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

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

Utilización de la base de datos de copia de seguridad

1. Introduzca la ruta del archivo de copia de seguridad en el campo **Ubicación del archivo de copia de seguridad** o haga clic en **Examinar** para ubicar el archivo.
2. Escriba su contraseña en el campo **Contraseña**.
3. Haga clic en **Restaurar**.

Si no ha realizado la copia de seguridad de la base de datos de Privacy Service, si ha olvidado la contraseña de la copia de seguridad o si la restauración de la base de datos no funciona, deberá desinstalar y reinstalar Privacy Service.

Registro de eventos

Para visualizar el registro de eventos deberá iniciar sesión en Privacy Service como Administrador. Seleccione **Registro de eventos** y haga clic en cualquier entrada de registro para visualizar los detalles.

Fecha y hora

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

La fecha se muestra en formato mes/día/año y el tiempo en formato A.M./P.M.

Usuario

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

Resumen

Los resúmenes muestran una descripción breve y concisa de lo que realiza Privacy Service para proteger a los usuarios y lo que los usuarios realizan en Internet.

Detalles del evento

El campo Detalles del evento muestra los detalles de la entrada.

Opciones de usuario

Estas instrucciones no se aplican al Administrador.

Puede cambiar su contraseña y nombre de usuario. Le recomendamos que cambie su contraseña después de que el Administrador se la haya dado. También le recomendamos que cambie la contraseña una vez al mes o cuando crea que alguien la conoce. Esto ayuda a evitar que otras personas utilicen Internet con su nombre de usuario.

Cambio de la contraseña

1. Haga clic con el botón derecho en el icono de McAfee, elija **McAfee Privacy Service** y seleccione **Opciones**.
2. Haga clic en **Contraseña** e introduzca su antigua contraseña en el campo **Contraseña antigua**.
3. Escriba una contraseña en el campo **Nueva contraseña**.

4 Introduzca otra vez la nueva contraseña en el campo **Confirmar contraseña** y haga clic en **Aplicar**.

5 Haga clic en **Aceptar** en el cuadro de dialogo de confirmación. Ya dispone de una nueva contraseña.

Cambio del nombre de usuario

1 Haga clic con el botón derecho en el icono de McAfee, elija **McAfee Privacy Service** y seleccione **Opciones**.

2 Haga clic en **Información de usuario**.

3 Introduzca el nuevo nombre de usuario en el campo **Nuevo nombre de usuario** y haga clic en **Aplicar**.

4 Haga clic en **Aceptar** en el cuadro de dialogo de confirmación. Ahora ya tiene un nuevo nombre de usuario.

Vaciado de la caché

Le recomendamos que vacíe la memoria caché para evitar que un niño acceda a las páginas Web que haya visitado recientemente. Para vaciar la caché, haga lo siguiente.

1 Abra Internet Explorer.

2 En el menú **Herramientas**, haga clic en **Opciones de Internet**. Aparece el cuadro de diálogo Opciones de Internet.

3 En la sección **Archivos temporales de Internet**, haga clic en **Eliminar archivos**. Aparecerá el cuadro de diálogo Eliminar archivos.

4 Seleccione **Eliminar todo el contenido sin conexión** y haga clic en **Aceptar**.

5 Haga clic en **Aceptar** para cerrar el cuadro de diálogo Opciones de Internet.

Aceptación de cookies

Esta opción está sólo disponible si el Administrador le permite aceptar o rechazar cookies al interceptarlos.

Si accede a sitios Web que requieran cookies, puede permitir que dichos sitios los lean.

1. Haga clic con el botón derecho en el icono de McAfee, elija **McAfee Privacy Service** y seleccione **Opciones**.
2. Haga clic en **Cookies aceptados**.
3. Introduzca la URL del sitio Web en el campo **http://** y haga clic en **Agregar**. El sitio Web aparecerá en la lista **Sitio Web**.

Si necesita eliminar un sitio Web de la lista

1. Seleccione la URL del sitio Web en la lista **Sitio Web**.
2. Haga clic en **Eliminar** y, a continuación, en **Sí** en el cuadro de diálogo de confirmación.

Rechazo de cookies

Esta opción está sólo disponible si el Administrador le permite aceptar o rechazar cookies al interceptarlos.

Si accede a sitios Web que no requieran cookies, puede rechazar los cookies sin que se lo soliciten.

1. Haga clic con el botón derecho en el icono de McAfee, elija **McAfee Privacy Service** y seleccione **Opciones**.
2. Haga clic en **Cookies rechazados**.
3. Introduzca la URL del sitio Web en el campo **http://** y haga clic en **Agregar**. El sitio Web aparecerá en la lista **Sitio Web**.

Si necesita eliminar un sitio Web de la lista

1. Seleccione la URL del sitio Web en la lista **Sitio Web**.
2. Haga clic en **Eliminar** y, a continuación, en **Sí** en el cuadro de diálogo de confirmación.

Utilidades

Para acceder a las utilidades, deberá iniciar sesión en Privacy Service como Administrador. Haga clic en **Utilidades** y seleccione **McAfee Shredder**.

Eliminación de archivos de manera permanente mediante McAfee Shredder

McAfee Shredder  protege la privacidad eliminando de forma rápida y segura los archivos no deseados.

Puede recuperar los archivos eliminados incluso después de haber vaciado la Papelera de reciclaje. Cuando elimine un archivo, Windows marcará ese espacio en la unidad de disco como espacio no utilizado, aunque el archivo sigue ahí.

Por qué Windows conserva restos de archivos

Para eliminar permanentemente un archivo, deberá sobrescribir varias veces el archivo existente con datos nuevos. Si Microsoft Windows elimina archivos, cada operación será muy lenta. La destrucción de un documento no siempre evita que se recupere un documento ya que algunos programas crean copias temporales ocultas de los documentos abiertos. Si sólo destruye documentos visualizados en el Explorador, aún podrá conservar copias temporales de dichos documentos. Le recomendamos que destruya periódicamente el espacio libre de la unidad de disco para asegurarse de que se eliminan de manera permanente las copias temporales.

NOTA
Mediante las herramientas forenses de equipo, podrá conseguir registros tributarios, reanudaciones de trabajo u otros documentos que haya eliminado.

Qué elimina McAfee Shredder

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

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

Los archivos del Explorador de Windows

Para destruir archivos mediante el Explorador de Windows:

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

Vaciado de la Papelera de reciclaje de Windows

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

Para destruir el contenido de la Papelera de reciclaje:

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

Personalización de la configuración del triturador

Puede realizar lo siguiente:

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

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

McAfee SpamKiller 5

Bienvenido a McAfee SpamKiller.

El software McAfee SpamKiller contribuye a evitar que llegue correo basura a su buzón de entrada. Gracias a él, disfrutará de las funciones siguientes:

Opciones de usuario

- Bloquear el correo basura con filtros y ponerlo en cuarentena fuera del buzón de entrada.
- Visualizar los mensajes bloqueados y aceptados.
- Supervisar y filtrar varias cuentas de correo electrónico.
- Importar las direcciones de amigos a una lista de amigos.
- Luchar contra los remitentes de correo basura (informar de su existencia, quejarse de los correos basura, crear filtros personalizados).
- Proteger a los menores de los mensajes de correo basura.
- Bloquear y recuperar los mensajes con un solo clic.
- Admitir juegos de caracteres de doble byte.
- Utilizar un soporte de varios usuarios (Windows 2000 y Windows XP).

Filtrado

- Actualizar filtros automáticamente.
- Crear filtros personalizados para bloquear los correos electrónicos que contengan en su mayoría imágenes, texto oculto o formato no válido.
- Motor central de filtrado de varios niveles.
- Filtro de ataques de diccionario.
- Filtrado adaptable de varios niveles.
- Filtros de seguridad.

Funciones

McAfee SpamKiller impide que el correo basura contamine el buzón de entrada.

Información general

Los iconos siguientes aparecen en el panel superior de todas las páginas de SpamKiller:

- Cambiar usuario: haga clic en **Cambiar usuario** para iniciar la sesión como usuario diferente.

  Nota: La opción **Cambiar usuario** sólo estará disponible si el equipo funciona con Windows 2000 o Windows XP, se han agregado varios usuarios a SpamKiller y usted ha iniciado una sesión como Administrador en SpamKiller.

- Soporte: haga clic en **Soporte** para abrir la página en línea Soporte de McAfee, donde encontrará temas útiles sobre SpamKiller y sobre otros productos de McAfee, respuestas a preguntas frecuentes y mucho más. Debe estar conectado a Internet para acceder a la página de soporte.

- Ayuda: haga clic en **Ayuda** para abrir la ayuda en línea, donde encontrará instrucciones detalladas sobre la configuración y el uso de SpamKiller.

Página Resumen

Haga clic en la ficha **Resumen** para abrir la página Resumen, donde encontrará la siguiente información:

- **Estado:** indica si está activado el filtrado, cuando se activó por última vez una lista de amigos y el número de correos basura que ha recibido hoy. Desde aquí puede activar y desactivar el filtrado de SpamKiller, actualizar las listas de amigos y abrir la página de correos electrónicos bloqueados.

- **Correo basura reciente:** muestra los últimos mensajes de correo basura bloqueados por SpamKiller (mensajes eliminados del buzón de entrada). Para devolver un mensaje a la bandeja de entrada, haga clic en el icono **Recuperar** situado al lado del mensaje.

- **Información general sobre el correo electrónico:** muestra el número total de correos electrónicos, correos basura (mensajes bloqueados) y el porcentaje de todos los correos basura recibidos.

- **Correos basura recientes:** le ofrece un desglose del tipo de correo basura que ha recibido en los últimos 30 días.

Integración con Microsoft Outlook y Outlook Express

Puede acceder a las funciones fundamentales de SpamKiller directamente desde dentro de Outlook Express 6.0, Outlook 98, Outlook 2000 y Outlook XP. Los usuarios pueden bloquear el correo basura, agregar personas a la lista de amigos y ver los mensajes en cuarentena con sólo hacer clic en los botones que se integran en la barra de herramientas de Outlook y de Outlook Express.

Barra de herramientas de Microsoft Outlook

En la barra de herramientas de Microsoft Outlook Express 6.0, Outlook 98, Outlook 2000 y Outlook XP puede llevar a cabo las tareas siguientes.

- Bloquear mensaje: haga clic en el icono **Bloquear mensaje** para eliminar el mensaje seleccionado del buzón de entrada de Microsoft Outlook y poner el mensaje en la carpeta de correos electrónicos bloqueados de SpamKiller.
- Ver mensajes bloqueados: haga clic en el icono **Ver mensajes bloqueados** para ver los mensajes bloqueados desde su cuenta de Microsoft Outlook y movidos a la carpeta de correo bloqueado de SpamKiller.
- Haga clic en el icono **Agregar amigo** para agregar la dirección de correo electrónico del remitente a su lista personal de amigos.

Aparece una barra de herramientas de SpamKiller a la derecha de las barras de herramientas predeterminadas en Outlook y Outlook Express. Si la barra de herramientas no es visible, debe ampliar la ventana de la aplicación de correo electrónico o hacer clic en las flechas para ver más barras de herramientas.

Cuando la barra de herramientas aparezca por primera vez en la aplicación de correo electrónico, únicamente podrá utilizar las instrucciones de la barra de herramientas con los nuevos mensajes. El correo basura existente debe eliminarse.

Gestión de cuentas de correo electrónico y de usuarios

Esta sección describe cómo gestionar cuentas y usuarios.

Agregación de cuentas de correo electrónico

SpamKiller filtra los siguientes tipos de cuentas de correo electrónico:

- Cuenta de correo electrónico estándar (POP3): la mayoría de usuarios particulares disponen de este tipo de cuenta.
- Cuenta de MSN/Hotmail: cuentas de Internet MSN/Hotmail.

- Cuenta de correo electrónico MAPI: cuentas de correo electrónico de redes locales. Muchos usuarios empresariales disponen de este tipo de cuentas cuando sus empresas utilizan Microsoft® Exchange Server. Tenga en cuenta que para agregar la cuenta a SpamKiller, debe haber configurado un perfil MAPI válido.

  NOTA
  Si su equipo utiliza Windows 2000 o Windows XP y desea agregar múltiples usuarios a SpamKiller, deberá añadir los usuarios antes de agregar las cuentas de correo electrónico a sus perfiles de usuario. Para obtener más información, consulte *Agregación de usuarios* en la página 108. Si agrega varios usuarios a SpamKiller, la cuenta se agregará al perfil del usuario que tiene una sesión iniciada en SpamKiller en este momento.

Para agregar una cuenta de correo electrónico

1. Haga clic en la ficha **Configuración** y después en **Cuentas de correo electrónico**. Aparece el cuadro de diálogo **Cuentas de correo electrónico** y muestra todas las cuentas de correo electrónico que se han agregado a SpamKiller.

   NOTA
   Si se han agregado varios usuarios a SpamKiller, la lista mostrará las cuentas de correo electrónico del usuario que tiene una sesión iniciada en SpamKiller.

2. Haga clic en **Agregar**. Aparecerá el asistente para cuentas de correo electrónico.
3. Siga las instrucciones de los cuadros de diálogo que aparezcan.

Si agrega una cuenta de MSN/Hotmail, SpamKiller buscará una libreta de direcciones MSN/Hotmail de la que poder importar la lista personal de amigos.

Para orientar su cliente de correo electrónico a SpamKiller

Si ha agregado una cuenta que SpamKiller no ha detectado (la cuenta no aparece en el cuadro de diálogo **Seleccionar cuenta**) o si desea leer su correo MSN/Hotmail como una cuenta POP3 en SpamKiller, oriente su cliente de correo electrónico a SpamKiller.

1. Cambie el servidor de correo electrónico entrante. Por ejemplo, si el servidor de mensajes entrantes es “mail.mcafee.com”, cámbielo a “localhost”.
2. Sólo para cuentas POP3, cambie el nombre de usuario y escriba su dirección de correo electrónico completa. Por ejemplo, si su dirección de correo electrónico es “nombre@ejemplo.com”, cambie el nombre de usuario por “nombre@ejemplo.com”.

Eliminación de cuentas de correo electrónico

Si desea que SpamKiller deje de filtrar una cuenta de correo electrónico, bórrela.

Para eliminar una cuenta de correo electrónico de SpamKiller

1 Haga clic en la ficha **Configuración** y, a continuación, en **Cuentas de correo electrónico**. Aparece el cuadro de diálogo **Cuentas de correo electrónico** y muestra todas las cuentas de correo electrónico que se han agregado a SpamKiller.

> **NOTA**
> Si se han agregado varios usuarios a SpamKiller, la lista mostrará las cuentas de correo electrónico del usuario que tiene una sesión iniciada en SpamKiller.

2 Seleccione una cuenta y haga clic en **Eliminar**.

Edición de las propiedades de la cuenta de correo electrónico

Puede editar información de las cuentas de correo electrónico que haya agregado a SpamKiller. Por ejemplo, es posible cambiar la dirección de correo electrónico, la descripción de la cuenta, la información del servidor, la frecuencia con la que SpamKiller debe comprobar la presencia de correos basura y el modo en que el equipo se conecta a Internet.

Cuentas POP3

Para editar cuentas POP3

1 Haga clic en la ficha **Configuración** y después en **Cuentas de correo electrónico**. Aparece el cuadro de diálogo **Cuentas de correo electrónico** y muestra todas las cuentas de correo electrónico que se han agregado a SpamKiller.

> **NOTA**
> Si se han agregado varios usuarios a SpamKiller, la lista mostrará las cuentas de correo electrónico del usuario que tiene una sesión iniciada en SpamKiller.

2 Seleccione una cuenta PO3 y haga clic en **Editar**.

3 Haga clic en la ficha **General** para editar la descripción de la cuenta y la dirección de correo electrónico.

- **Descripción:** Descripción de la cuenta. En este campo puede introducir la información que desee.
- **Dirección de correo electrónico:** dirección de correo electrónico de la cuenta.

4 Haga clic en la ficha **Servidores** para editar la información del servidor.

- **Correo electrónico entrante:** nombre del servidor que recibe el correo electrónico entrante.
- **Nombre de usuario:** nombre de usuario utilizado para acceder a la cuenta. También conocido como Nombre de cuenta.
- **Contraseña:** contraseña que utiliza para acceder a la cuenta.
- **Correo electrónico saliente:** nombre del servidor que envía el correo electrónico saliente. Haga clic en **Más** para modificar los requisitos de autenticación del servidor de correo electrónico saliente.

5 Haga clic en la ficha **Comprobación** para modificar la frecuencia con la que SpamKiller comprueba la presencia de correos basura en la cuenta:

a Seleccione **Comprobar cada** o **Comprobar a diario a las**; a continuación, seleccione una hora en el campo correspondiente.

b Selección de otras horas para que SpamKiller filtre la cuenta:

Comprobar al inicio: seleccione esta opción si dispone de conexión directa y desea que SpamKiller compruebe la cuenta cada vez que arranque el equipo.

Comprobar al establecer una conexión: seleccione esta opción sólo si dispone de una conexión telefónica y desea que SpamKiller compruebe la cuenta cada vez que se conecta a Internet.

6 Haga clic en la ficha **Conexión** para especificar el modo en que SpamKiller debe establecer la conexión a Internet para que pueda comprobar su buzón de entrada en busca de los mensajes que se deben filtrar.

- **No marcar nunca una conexión:** SpamKiller no establece automáticamente ninguna conexión. Primero debe iniciar una conexión manual.
- **Marcar cuando sea necesario:** cuando no hay ninguna conexión de Internet disponible, SpamKiller intenta conectarse automáticamente con la conexión predeterminada de Internet.
- **Marcar siempre:** SpamKiller intenta conectar automáticamente con la conexión de marcado que se haya especificado.
- **Permanecer conectado después de realizar el filtrado:** su equipo permanece conectado a Internet después de finalizar el filtrado.

7 Haga clic en la ficha **Avanzadas** para editar las opciones avanzadas.

- **Dejar correos basura en el servidor:** seleccione esta casilla de selección si desea conservar una copia de los mensajes bloqueados en el servidor de correo electrónico.

  Si deja mensajes bloqueados en el servidor, podrá ver el correo en su cliente de correo electrónico y en la página de correos electrónicos bloqueados de SpamKiller. Si la casilla no está seleccionada, podrá ver los mensajes bloqueados sólo en la página de correos electrónicos bloqueados y no en su cliente de correo electrónico.

- **Puerto POP3:** (número de puerto POP3) el servidor POP3 gestiona los mensajes entrantes.

- **Puerto SMTP:** (número de puerto SMTP) el servidor SMTP gestiona los mensajes salientes.

- **Tiempo de espera del servidor:** el tiempo que esperará SpamKiller para recibir mensajes de correo antes de agotar el tiempo de espera y detenerse.

  Aumente el valor del tiempo de espera del servidor si tiene problemas para recibir correo. Es posible que su conexión de correo electrónico sea lenta, por lo que el tiempo de espera del servidor permite que SpamKiller espere más tiempo antes de desconectarse.

8 Haga clic en **Aceptar**.

Cuentas MSN/Hotmail

Para editar las cuentas MSN/Hotmail

1 Haga clic en la ficha **Configuración** y después en **Cuentas de correo electrónico**.

Aparece el cuadro de diálogo **Cuentas de correo electrónico** y muestra todas las cuentas de correo electrónico que se han agregado a SpamKiller.

> **NOTA**
> Si se han agregado varios usuarios a SpamKiller, la lista mostrará las cuentas de correo electrónico del usuario que tiene una sesión iniciada en SpamKiller.

2 Seleccione una cuenta MSN/Hotmail y haga clic en **Editar**.

3 Haga clic en la ficha **General** para editar la descripción de la cuenta y la dirección de correo electrónico.

- **Descripción:** Descripción de la cuenta. En este campo puede introducir la información que desee.

- **Dirección de correo electrónico:** dirección de correo electrónico de la cuenta.

4 Haga clic en la ficha **Servidores** para editar la información del servidor.

- **Correo electrónico entrante:** nombre del servidor que recibe el correo electrónico entrante.
- **Contraseña:** contraseña que utiliza para acceder a la cuenta.
- **Correo electrónico saliente:** nombre del servidor que envía el correo electrónico saliente.
- **Utilizar un servidor SMTP para el correo electrónico saliente:** seleccione esta opción si desea enviar mensajes de error sin que aparezca la línea de firma MSN. La línea de firma MSN permite a los remitentes de correo basura saber que el mensaje de error es falso.

  Haga clic en **Más** para cambiar los requisitos de autenticación del servidor de correo electrónico saliente.

5 Haga clic en la ficha **Comprobación** para especificar con qué frecuencia SpamKiller debe comprobar la presencia de correos basura en la cuenta:

a Seleccione **Comprobar cada** o **Comprobar a diario a las**; a continuación, seleccione una hora en el campo correspondiente.

b Selección de otras horas para que SpamKiller filtre la cuenta:

Comprobar al inicio: seleccione esta opción si dispone de conexión directa y desea que SpamKiller compruebe la cuenta cada vez que inicie SpamKiller.

Comprobar al establecer una conexión: seleccione esta opción sólo si dispone de una conexión telefónica y desea que SpamKiller compruebe la cuenta cada vez que se conecta a Internet.

6 Haga clic en la ficha **Conexión** para especificar el modo en que SpamKiller debe establecer la conexión a Internet para que pueda comprobar su buzón de entrada en busca de los mensajes que se deben filtrar.

- **No marcar nunca una conexión:** SpamKiller no establece automáticamente ninguna conexión. Primero debe iniciar una conexión manual.
- **Marcar cuando sea necesario:** cuando no hay ninguna conexión de Internet disponible, SpamKiller intenta conectarse automáticamente con la conexión predeterminada de Internet.
- **Marcar siempre:** SpamKiller intenta conectar automáticamente con la conexión de marcado que se haya especificado.
- **Permanecer conectado después de realizar el filtrado:** su equipo permanece conectado a Internet después de finalizar el filtrado.

7 Haga clic en **Aceptar**.

Para configurar una cuenta de Hotmail de modo que bloquee el correo basura en Outlook o Outlook Express

SpamKiller puede filtrar directamente cuentas de Hotmail. Consulte la ayuda en línea para obtener más información. Sin embargo, no podrá bloquear mensajes ni agregar amigos con la barra de herramientas de SpamKiller en Outlook o Outlook Express hasta que configure la cuenta de Hotmail.

1. Configure la cuenta de Hotmail en MSK.
2. Si ya tiene una cuenta de Hotmail en Outlook o Outlook Express, debe eliminarla antes.
3. Agregue la cuenta de Hotmail a Outlook o Outlook Express. Asegúrese de que selecciona **POP3** para el tipo de cuenta y el tipo de servidor de correo electrónico entrante.
4. Llame al servidor entrante `localhost`.
5. Escriba el nombre del servidor saliente SMTP disponible (obligatorio).
6. Complete el proceso de configuración de la cuenta. A partir de ese momento ya podrá bloquear el correo basura nuevo en Hotmail o agregar amigos.

Cuentas MAPI

Las condiciones siguientes son necesarias para que SpamKiller se integre con éxito con MAPI en Outlook:

- Sólo para Outlook 98, Outlook estaba instalado inicialmente con soporte para empresas/grupos de trabajo.
- Sólo para Outlook 98, la primera cuenta de correo electrónico debe ser una cuenta MAPI.
- El equipo debe estar conectado al dominio.

Para editar cuentas MAPI

1. Haga clic en la ficha **Configuración** y después en **Cuentas de correo electrónico**. Aparece el cuadro de diálogo **Cuentas de correo electrónico** y muestra todas las cuentas de correo electrónico que se han agregado a SpamKiller.

   NOTA
   Si se han agregado varios usuarios a SpamKiller, la lista mostrará las cuentas de correo electrónico del usuario que tiene una sesión iniciada en SpamKiller.

2. Seleccione una cuenta MAPI y haga clic en **Editar**.

3 Haga clic en la ficha **General** para editar la descripción de la cuenta y la dirección de correo electrónico.

- **Descripción:** Descripción de la cuenta. En este campo puede introducir la información que desee.
- **Dirección de correo electrónico:** dirección de correo electrónico de la cuenta.

4 Haga clic en la ficha **Perfil** para editar la información del perfil.

- **Perfil**: perfil MAPI de la cuenta.
- **Contraseña**: la contraseña que se corresponde con el perfil MAPI si ha configurado uno (no necesariamente la contraseña de la cuenta de correo electrónico).

5 Haga clic en la ficha **Conexión** para especificar el modo en que SpamKiller debe establecer la conexión a Internet para que pueda comprobar su buzón de entrada en busca de los mensajes que se deben filtrar.

- **No marcar nunca una conexión:** SpamKiller no establece automáticamente ninguna conexión. Primero debe iniciar una conexión manual.
- **Marcar cuando sea necesario:** cuando no hay ninguna conexión de Internet disponible, SpamKiller intenta conectarse automáticamente con la conexión predeterminada de Internet.
- **Marcar siempre:** SpamKiller intenta conectar automáticamente con la conexión de marcado que se haya especificado.
- **Permanecer conectado después de realizar el filtrado:** su equipo permanece conectado a Internet después de finalizar el filtrado.

6 Haga clic en **Aceptar**.

Agregación de usuarios

SpamKiller puede configurar diferentes usuarios, correspondientes a los que se hayan configurado en el sistema operativo Windows 2000 o Windows XP.

Cuando se instala SpamKiller en el equipo, se crea automáticamente un perfil de administrador para el usuario de Windows que tenía iniciada la sesión. Si agrega cuentas de correo electrónico a SpamKiller durante la instalación, se añadirán a ese perfil de usuario de administrador.

Antes de agregar otras cuentas de correo electrónico a SpamKiller, decida si necesita agregar otros usuarios de SpamKiller. La agregación de usuarios supone una ventaja cuando hay varias personas que usan el mismo equipo y que disponen de sus propias cuentas de correo electrónico. Cada una de las cuentas de correo electrónico se agrega a su propio perfil de usuario, de modo que los usuarios puedan gestionar sus cuentas, configuración personal, filtros personales y lista personal de amigos.

Los tipos de usuario definen las tareas que puede realizar cada usuario en SpamKiller. La siguiente tabla resume los permisos de cada tipo de usuario. Los administradores pueden realizar todas las tareas, en tanto que los usuarios restringidos sólo pueden realizar tareas adecuadas para sus perfiles personales. Por ejemplo, los administradores pueden ver todo el contenido de los mensajes bloqueados, mientras que los usuarios restringidos sólo pueden ver la línea referente al asunto.

Tareas	Administrador	Usuario restringido
Gestionar cuentas personales de correo electrónico, filtros personales, lista personal de amigos y configuración personal de sonido	X	X
Gestionar correos electrónicos personales bloqueados y las páginas de correos electrónicos aceptados	X	X
Ver el texto de mensaje de los mensajes bloqueados	X	
Ver el texto de mensaje de los mensajes aceptados	X	X
Gestionar los filtros globales y la lista global de amigos	X	
Informar del correo basura a McAfee	X	X
Enviar quejas y mensajes de error	X	X
Gestionar quejas y mensajes de error (crear, modificar y eliminar plantillas de mensajes)	X	
Gestionar usuarios (crear, modificar y eliminar usuarios)	X	
Realizar copia de seguridad y restaurar SpamKiller	X	
Ver la página de resumen de los correos basura recibidos	X	X

Cuando un usuario inicia la sesión en su equipo una vez que se le ha agregado, se le pedirá que agregue una cuenta de correo a su perfil de usuario.

Para agregar y administrar usuarios, es necesario lo siguiente:

- Debe haber iniciado la sesión en SpamKiller como administrador.
- Su equipo debe tener Windows 2000 o Windows XP.
- Los usuarios que está agregando o administrando deben tener cuentas de usuario de Windows.

Contraseñas de usuario y protección contra el correo basura para menores

Si crea una contraseña de usuario mejorará el nivel de privacidad. A la configuración personal de un usuario, a la lista de amigos y a la lista de correos electrónicos aceptados no pueden acceder otros usuarios que no dispongan de la contraseña de inicio de sesión. La creación de contraseñas resulta útil también para evitar que los niños accedan a SpamKiller y vean el contenido de los correos basura.

Para crear una contraseña de un usuario existente de SpamKiller

1. Haga clic en la ficha **Configuración** y después en **Usuarios**.
2. Seleccione un usuario y haga clic en **Editar**.
3. Escriba una contraseña en el campo **Contraseña**. Cuando un usuario accede a SpamKiller, debe usar la contraseña de inicio de sesión.

   IMPORTANTE
   Si la olvida, no podrá recuperarla. Sólo los administradores de SpamKiller pueden crear una nueva contraseña para usted.

Para agregar a un usuario a SpamKiller

1. Haga clic en la ficha **Configuración** y después en **Usuarios**.
2. Haga clic en **Agregar**.

   Aparecerá una lista de usuarios de Windows. Para agregar a un usuario que no aparezca en la lista, cree una cuenta de usuario de Windows para esa persona. Después, el nuevo usuario debe iniciar una sesión en el equipo al menos una vez. Finalmente, se podrá agregar el usuario a SpamKiller.

   NOTA
   Los usuarios de Windows con derechos de administrador tienen derechos de administrador de SpamKiller.

3. Seleccione un usuario y haga clic en **Aceptar**. El usuario se agrega a SpamKiller y el nombre de usuario aparece en la lista de usuarios de SpamKiller.
4. Haga clic en **Cerrar** cuando termine de agregar usuarios.

Para crear una contraseña para un usuario, consulte *Para crear una contraseña de un usuario existente de SpamKiller* en la página 110.

La próxima vez que el usuario inicie una sesión en el equipo, se le pedirá que agregue una cuenta de correo electrónico a su perfil de usuario de SpamKiller. Puede agregar cuentas de correo electrónico al perfil de usuario si ha iniciado una sesión en SpamKiller como ese usuario y dispone de la información necesaria sobre la cuenta de correo electrónico. Para obtener más información, consulte *Agregación de cuentas de correo electrónico* en la página 101.

Para editar un perfil de usuario de SpamKiller

1. Haga clic en la ficha **Configuración** y después en **Usuarios**. Aparecerá una lista de usuarios de SpamKiller.
2. Seleccione un usuario y haga clic en **Editar**.
3. Escriba una contraseña y un nombre nuevos.

Para eliminar un perfil de usuario de SpamKiller

> **ADVERTENCIA**
> Cuando se elimina un perfil de usuario, se eliminan también las cuentas de correo electrónico de ese usuario de SpamKiller.

1. Haga clic en la ficha **Configuración** y después en **Usuarios**. Aparecerá una lista de usuarios de SpamKiller.
2. Seleccione un usuario de la lista y haga clic en **Eliminar**.

Inicio de sesión en SpamKiller en un entorno de múltiples usuarios

Cuando los usuarios inician una sesión en el equipo y abren SpamKiller, inician automáticamente una sesión de SpamKiller con sus perfiles de usuario. Si se han asignado contraseñas de SpamKiller a los usuarios, deben introducirlas en el cuadro de diálogo **Inicio de sesión** que aparece.

Para cambiar de usuario

Debe haber iniciado la sesión en SpamKiller como administrador.

1. Haga clic en **Cambiar usuario**, en la parte superior de la página. Aparecerá el cuadro de diálogo **Cambiar usuario**.
2. Seleccione un usuario y haga clic en **Aceptar**. Si el usuario dispone de contraseña, aparecerá el cuadro de diálogo **Inicio de sesión**. Escriba la contraseña de usuario en el cuadro **Contraseña** y haga clic en **Aceptar**.

Utilización de la lista de amigos

Le recomendamos que agregue los nombres y direcciones de correo electrónico de sus amigos a la lista de amigos. SpamKiller no bloquea los mensajes que envían las personas incluidas en la lista. De este modo se puede tener la certeza de que le llegan los mensajes que desea recibir.

SpamKiller permite agregar nombres, direcciones de correo electrónico, dominios y listas de correo a la lista de amigos. Puede agregar direcciones de una en una o todas a la vez, mediante la importación de la libreta de direcciones de su programa de correo electrónico.

Hay dos tipos de listas en SpamKiller:

- **Lista global de amigos:** Esta lista afecta a todas las cuentas de correo de los usuarios de SpamKiller. Si se agregaron varios usuarios, debe haber iniciado la sesión en SpamKiller como Administrador para poder gestionar esta lista.
- **Lista personal de amigos:** Esta lista afecta a todas las cuentas de correo asociadas a un usuario específico. Si se agregaron varios usuarios, debe haber iniciado la sesión en SpamKiller como usuario para poder gestionar esta lista.

Puede agregar amigos a una lista de amigos para que no se bloquee su correo. La página de amigos muestra los nombres y direcciones que se han agregado a la lista de amigos. Esta página también muestra la fecha en que se agregó a un amigo y el número total de mensajes recibidos por parte de éste.

Haga clic en la ficha **Direcciones de correo electrónico** para ver las direcciones de correo electrónico de la lista de amigos. Haga clic en la ficha **Dominios** para ver las direcciones de dominio de la lista. Haga clic en la ficha **Listas de correo** para ver las listas de correo de la lista de amigos.

Para pasar de una lista de amigos a otra, haga clic en la flecha abajo situada en las fichas **Dirección de correo electrónico**, **Dominios** o **Listas de correo** y seleccione **Lista personal de amigos**.

Apertura de una lista de amigos

1. Para abrir una lista de amigos, haga clic en la ficha **Amigos**.
2. Haga clic en la ficha **Dirección de correo electrónico**, **Dominio** o **Lista de correo**. Aparece la lista global de amigos. Para ver la lista personal de amigos, haga clic en la flecha abajo de una de las fichas y seleccione **Lista personal de amigos**.

NOTA
Si el sistema operativo de su equipo es Windows 2000 o Windows XP y se han agregado varios usuarios a SpamKiller, los usuarios limitados sólo podrán acceder a la lista personal de amigos.

Importación de libretas de direcciones

La importación de libretas de direcciones a una lista de amigos puede realizarse manual o automáticamente. La importación automática permite que SpamKiller compruebe con regularidad sus libretas de direcciones, para verificar si existen nuevas direcciones e importarlas a una lista de amigos.

Puede importar libretas de direcciones de los siguientes programas de correo electrónico:

- Microsoft Outlook (versión 98 y posterior)
- Microsoft Outlook Express (todas las versiones)
- Netscape Communicator (versión 6 y anteriores, si se exportan como archivo LDIF)
- Qualcomm Eudora (versión 5 y posterior)
- IncrediMail Xe
- MSN/Hotmail
- Cualquier programa que pueda exportar su libreta de direcciones en formato de texto normal.

Para importar una libreta de direcciones automáticamente

Puede actualizar con regularidad la lista personal de amigos, mediante la creación de un calendario de importación de direcciones de las libretas.

1. Haga clic en la ficha **Configuración** y después en **Libreta de direcciones**. Aparece el cuadro de diálogo **Importar libretas de direcciones** donde muestra una lista de libretas de direcciones que SpamKiller comprueba con regularidad y desde las cuales importa nuevas direcciones.
2. Haga clic en **Agregar**. Aparecerá el cuadro de diálogo **Importar calendario**.

3 Seleccione el **Tipo** de libreta de direcciones que desea importar y su **Origen**.

4 En el campo **Calendario** seleccione la frecuencia con la que SpamKiller debe comprobar la libreta de direcciones en busca de nuevas direcciones.

5 Haga clic en **Aceptar**. Después de realizar una actualización, las direcciones nuevas se incluyen en la lista personal de amigos.

Para importar manualmente una libreta de direcciones

Puede importar manualmente libretas de direcciones en las listas personal o global de amigos.

> **NOTA**
> Si utiliza el sistema operativo Windows 2000 o Windows XP y ha agregado a varios usuarios a SpamKiller, debe iniciar una sesión como Administrador para agregar amigos a su lista global.

1 Haga clic en la ficha **Amigos** y después en **Importar libreta de direcciones**.

El cuadro de diálogo **Importar libretas de direcciones** muestra una lista de tipos de libretas de direcciones que se pueden importar.

2 Seleccione el tipo de libreta de direcciones que desee importar o haga clic en **Examinar** para importar direcciones de un archivo.

Para importar una libreta de direcciones sólo a su lista personal de amigos, cerciórese de que la casilla de verificación **Agregar a la lista personal de amigos** está seleccionada. Para importar la libreta de direcciones sólo a la lista global de amigos, cerciórese de que la casilla de verificación *no* está seleccionada.

3 Haga clic en **Siguiente**. Aparecerá una página de confirmación que le indicará el número de direcciones que ha agregado SpamKiller.

4 Haga clic en **Finalizar**. Las direcciones aparecen en la lista global de amigos o la lista personal de amigos.

Para editar la información de la libreta de direcciones

Edición de la información de una libreta de direcciones importada de forma automática.

1 Haga clic en la ficha **Configuración** y después en **Libreta de direcciones**.

2 Seleccione una libreta de direcciones y haga clic en **Editar**.

3 Modifique la información de la libreta de direcciones y haga clic en **Aceptar**.

Para suprimir una libreta de direcciones de la lista de importación automática

Cuando no desee que SpamKiller siga importando automáticamente direcciones de una libreta, elimine la entrada correspondiente.

1. Haga clic en la ficha **Configuración** y después en **Libreta de direcciones**.
2. Seleccione una libreta de direcciones y haga clic en **Eliminar**. Aparece un cuadro de diálogo de confirmación.
3. Haga clic en **Sí** para eliminar la libreta de direcciones de la lista.

Agregación de amigos

Para cerciorarse de que recibe los correos electrónicos de todos sus amigos, agregue sus nombres y direcciones a una lista de amigos. Puede agregar amigos de las páginas de amigos, correos electrónicos bloqueados, correos electrónicos aceptados y de Microsoft Outlook o de Outlook Express.

> **NOTA**
> Si utiliza el sistema operativo Windows 2000 o Windows XP y ha agregado a varios usuarios a SpamKiller, debe iniciar una sesión como Administrador para agregar amigos a su lista global.

Para agregar a un amigo desde las páginas Correos bloqueados o Correos aceptados

1. Haga clic en la ficha **Mensajes** y, a continuación, en la ficha **Correos electrónicos bloqueados** o **Correos electrónicos aceptados**.

   O

   En Microsoft Outlook o Outlook Express, haga clic en  para abrir la página Correos bloqueados de esa cuenta.

   Aparece la página de correos electrónicos bloqueados o aceptados.
2. Seleccione un mensaje de un remitente que desee agregar a una lista de amigos y haga clic en **Agregar amigo**.
3. En el campo **Dirección** escriba la dirección que desea agregar a la lista de amigos. Es posible que el campo **Dirección** contenga ya la dirección del mensaje seleccionado.
4. Escriba el nombre del amigo en el campo **Nombre**.

5 Seleccione el tipo de dirección que desea agregar en el campo **Tipo de amigo**:

- **Una dirección de correo electrónico:** La dirección de correo electrónico del remitente se agrega a la sección de Dominios de la lista de amigos.
- **Todos los del dominio:** El nombre del dominio se agrega a la sección **Dominios** de la lista de amigos. SpamKiller acepta todos los correos electrónicos procedentes del dominio.
- **Lista de correo:** La dirección se agrega a la sección de la **Lista de correo** de la lista de amigos.

Para agregar la dirección sólo a su lista personal de amigos, cerciórese de que la casilla de verificación **Agregar a la lista personal de amigos** está seleccionada. Para agregar la dirección sólo a la lista global de amigos, cerciórese de que la casilla de verificación *no está* seleccionada.

6 Haga clic en **Aceptar**. Todos los mensajes de ese amigo se marcan como mensajes procedentes de un amigo y aparecen en la página Correos aceptados.

Para agregar a un amigo de la página de amigos

1 Haga clic en la ficha **Amigos** y después en **Agregar amigo**. Aparecerá el cuadro de diálogo **Propiedades de amigos**.

2 En el campo **Dirección** escriba la dirección que desea agregar a la lista de amigos.

3 Escriba el nombre del amigo en el campo **Nombre**.

4 Seleccione el tipo de dirección que desea agregar en el campo **Tipo de amigo**:

- **Una dirección de correo electrónico:** La dirección de correo electrónico del remitente se agrega a la lista de amigos.
- **Todos los del dominio:** El nombre del dominio se agrega a la sección Dominios de la lista de amigos. SpamKiller acepta todos los correos electrónicos procedentes del dominio.
- **Lista de correo:** La dirección se agrega a la sección Lista de correo de la lista de amigos.

Para agregar la dirección sólo a su lista personal de amigos, cerciórese de que la casilla de verificación **Agregar a la lista personal de amigos** está seleccionada. Para agregar la dirección sólo a la lista global de amigos, cerciórese de que la casilla de verificación *no está* seleccionada.

5 Haga clic en **Aceptar**. Todos los mensajes de ese amigo se marcan como mensajes procedentes de un amigo y aparecen en la página Correos aceptados.

Para agregar a un amigo en Microsoft Outlook.

1. Abra su cuenta de correo electrónico en Microsoft Outlook o Outlook Express.
2. Seleccione un mensaje de un remitente que desee agregar a una lista de amigos.
3. Haga clic en  en la barra de herramientas de Microsoft Outlook. Todos los mensajes de ese amigo se marcan como mensajes procedentes de un amigo y aparecen en la página Correos aceptados.

Edición de amigos

1. Haga clic en la ficha **Amigos** y en las fichas **Direcciones de correo electrónico**, **Dominios** o **Listas de correo**.

   Aparece la lista global de amigos. Para ver la lista personal de amigos, haga clic en la flecha abajo  de una de las fichas y seleccione **Lista personal de amigos**.

   NOTA
   Si el sistema operativo de su equipo es Windows 2000 o Windows XP y se han agregado varios usuarios a SpamKiller, sólo podrá acceder a la lista global de amigos si dispone de derechos de Administrador.

2. Seleccione una dirección de la lista y haga clic en **Editar**.
3. Modifique la información adecuada y haga clic en **Aceptar**.

Eliminación de amigos

Elimine las direcciones que no desee tener en la lista de amigos.

1. Haga clic en la ficha **Amigos** y en las fichas **Direcciones de correo electrónico**, **Dominios** o **Listas de correo**.

   Aparece la lista global de amigos. Para ver la lista personal de amigos, haga clic en la flecha abajo  de una de las fichas y seleccione **Lista personal de amigos**.

   NOTA
   Si el sistema operativo de su equipo es Windows 2000 o Windows XP y se han agregado varios usuarios a SpamKiller, sólo podrá acceder a la lista global de amigos si dispone de derechos de Administrador.

2. Seleccione una dirección de la lista y haga clic en **Eliminar amigo**. Aparece un cuadro de diálogo de confirmación.
3. Haga clic en **Sí** para eliminar el amigo.

Trabajo con mensajes bloqueados y aceptados

Haga clic en la ficha **Mensajes** para acceder a los mensajes bloqueados y aceptados. Las páginas correos electrónicos bloqueados y correos electrónicos aceptados tienen características similares.

Página de correos electrónicos bloqueados

Haga clic en la ficha **Correos electrónicos bloqueados** de la página Mensajes para ver los mensajes bloqueados.

> **NOTA**
> También puede acceder a los mensajes bloqueados desde su cuenta de Microsoft Outlook, abriendo el buzón de entrada de Outlook y haciendo clic en , en la barra de herramientas de Microsoft Outlook o de Outlook Express.

Los mensajes bloqueados son mensajes que SpamKiller ha identificado como correo basura, ha sacado del buzón de entrada y ha puesto en la carpeta de correos electrónicos bloqueados.

La página de correos electrónicos bloqueados muestra todos los mensajes de correo basura eliminados de las cuentas de correo electrónico. Para ver los correos electrónicos bloqueados de una cuenta concreta, haga clic en la flecha abajo de la ficha **Correos electrónicos bloqueados** y seleccione la cuenta que desee ver.

El panel superior de mensajes muestra los mensajes de correo basura, organizados por fechas. El mensaje más reciente aparece en primer lugar. El panel inferior de la vista previa contiene el texto del mensaje seleccionado en ese momento.

> **NOTA**
> Si el equipo funciona con Windows 2000 o Windows XP, se han agregado varios usuarios a SpamKiller y ha iniciado una sesión de usuario restringido en SpamKiller, en el panel de vista previa no se mostrará el contenido del mensaje.

El panel central muestra detalles del mensaje. Haga clic en las flechas abajo para ampliar el panel de detalles y ver el texto del mensaje y el encabezado en formato original, incluidas las etiquetas del formato HTML. El panel de detalles del mensaje muestra lo siguiente:

- **Acción:** describe el modo en que SpamKiller ha procesado el mensaje de correo basura. Acción está asociada a la acción del filtro que bloqueó el mensaje.
- **Razón:** explica por qué SpamKiller ha bloqueado el mensaje. Puede hacer clic sobre la razón para abrir el editor de filtros y ver el filtro. El editor de filtros muestra lo que se busca en los mensajes y la acción que SpamKiller debe realizar cuando encuentre mensajes que responden al filtro.
- **De:** muestra el remitente del mensaje.

- **Fecha:** muestra la fecha en que se le envió el mensaje.
- **Para:** muestra el destinatario del mensaje.
- **Asunto:** muestra el tema que aparece en la línea del asunto del mensaje.

En la columna de la izquierda aparecen iconos que se sitúan junto a los mensajes si se han enviado quejas o mensajes manuales de error:

- Queja enviada : Se ha enviado una queja acerca del mensaje.
- Mensaje de error enviado : se ha enviado un mensaje de error a la dirección de respuesta del correo basura.
- Queja y mensaje de error enviados : se han enviado una queja y un mensaje de error.

Página correos electrónicos aceptados

Haga clic en la ficha **Correos electrónicos aceptados** de la página de mensajes para ver los mensajes aceptados.

La página de correos electrónicos aceptados muestra todos los mensajes del buzón de entrada de cada una de sus cuentas de correo electrónico. Sin embargo, para las cuentas MAPI, la página de correos electrónicos aceptados no contiene correos internos. Para ver los correos electrónicos aceptados de una cuenta concreta, haga clic en la flecha abajo de la ficha **Correos electrónicos aceptados** y seleccione la cuenta que desee ver.

> **NOTA**
> SpamKiller está diseñado para aceptar los correos electrónicos legítimos. Sin embargo, si hay correos electrónicos legítimos en la lista de correos electrónicos bloqueados, puede devolverlos al buzón de entrada (y la lista de correos electrónicos aceptados) seleccionando los mensajes y haciendo clic en **Recuperar este mensaje**.

Al igual que en la página Correos bloqueados, el panel superior de mensajes muestra el correo ordenado por fechas. El panel inferior de vista previa contiene el texto del mensaje seleccionado.

El panel central explica si un mensaje ha sido enviado por un remitente incluido en la lista de amigos o si el mensaje cumple los criterios del filtro, pero la acción de filtrado se ha definido como **Aceptar** o **Marcar como posible correo basura**. Haga clic en las flechas abajo para ampliar el panel de detalles y ver el texto del mensaje y el encabezado en formato original, incluidas las etiquetas de formato HTML.

El panel de detalles del mensaje muestra lo siguiente:

- **Acción:** describe el modo en que SpamKiller ha procesado el mensaje.
- **Razón:** si se ha etiquetado un mensaje, este valor explica el motivo de que SpamKiller lo etiquetara.
- **De:** muestra el remitente del mensaje.
- **Fecha:** muestra la fecha en que se le envió el mensaje.
- **Para:** muestra el destinatario del mensaje.
- **Asunto:** muestra el tema que aparece en la línea del asunto del mensaje.

Al lado del mensaje puede aparecer uno de los iconos siguientes:

- Correo electrónico de un amigo : SpamKiller ha detectado que el remitente está en una lista de amigos. Éste es un mensaje que usted desea conservar.
- Posible correo basura : este mensaje coincide con un filtro cuya acción consiste en Marcar como posible correo basura.
- Queja enviada : se ha enviado una queja acerca del mensaje.
- Mensaje de error enviado : se ha enviado un mensaje de error a la dirección de respuesta del correo basura.
- Queja y mensaje de error enviados : se han enviado una queja y un mensaje de error.

Tareas relativas a los correos electrónicos bloqueados y aceptados

El panel de la derecha de las páginas de correos bloqueados y correos aceptados enumera las tareas que se pueden realizar.

- Bloquear este mensaje: elimina un mensaje del buzón de entrada y lo pone en la carpeta de correos electrónicos bloqueados de SpamKiller. Esta opción sólo aparece en la página de correos electrónicos aceptados.
- Recuperar este mensaje: vuelve a poner este mensaje en el buzón de entrada (esta opción aparece únicamente en la página de correos electrónicos bloqueados) y abre el cuadro de diálogo **Opciones de recuperación**. Puede agregar automáticamente al remitente a la lista de amigos y recuperar todos los mensajes de este remitente.
- Eliminar este mensaje: elimina un mensaje seleccionado.
- Agregar amigo: agrega el nombre del remitente, la dirección de correo electrónico, el dominio o una lista de correo a una lista de amigos.

- Agregar un filtro: crea un filtro.
- Notificar a McAfee: informa a McAfee sobre mensajes de correo basura específicos que ha recibido.
- Enviar una queja: envía una queja sobre correo basura al administrador del dominio del remitente o a otra dirección de correo electrónico que introduzca.
- Enviar un error: envía un mensaje de error a la dirección de respuesta de un mensaje de correo basura.

Recuperación de mensajes

Si la página de correos electrónicos bloqueados contiene mensajes legítimos, puede devolverlos al buzón de entrada.

Para recuperar un mensaje:

1. Haga clic en la ficha **Mensajes** y después en la ficha **Correos electrónicos bloqueados**.

   O

   En el buzón de entrada de Microsoft Outlook o de Outlook Express, haga clic en  para abrir la página de correos electrónicos bloqueados de esa cuenta.

   Aparece la página de correos electrónicos bloqueados.

2. Seleccione un mensaje y haga clic en **Recuperar este mensaje**. Aparece el cuadro de diálogo **Opciones de recuperación**.

   - **Agregar amigo:** agrega al remitente a la lista de amigos.
   - **Recuperar todo del mismo remitente:** recupera todos los mensajes bloqueados del remitente que envió el mensaje seleccionado.

3. Haga clic en **Aceptar**. El mensaje se vuelve a colocar en el buzón de entrada y en la carpeta de correos electrónicos aceptados.

Bloqueo de mensajes

Bloquea los mensajes de correo basura que están actualmente en el buzón de entrada. Cuando se bloquea un mensaje, SpamKiller crea automáticamente un filtro para eliminar ese mensaje del buzón de entrada. Puede bloquear mensajes del buzón de entrada en la página de correos electrónicos, en Microsoft Outlook o Outlook Express.

Para bloquear un mensaje en la página de correos electrónicos aceptados

1. Haga clic en la ficha **Mensajes** y, a continuación, en la ficha **Correos electrónicos aceptados**. Aparece la página de correos electrónicos aceptados con los mensajes que se encuentran actualmente en el buzón de entrada.
2. Seleccione un mensaje y haga clic en **Bloquear este mensaje**. El mensaje se elimina del buzón de entrada y de la página de correos electrónicos aceptados y aparece una copia en la carpeta de correos bloqueados.

Para bloquear un mensaje en Microsoft Outlook

Sólo se pueden bloquear mensajes externos (mensajes procedentes de un servidor de Internet).

1. Abra el buzón de entrada de Microsoft Outlook o de Outlook Express.
2. Seleccione un mensaje y haga clic en  . En la carpeta de correos electrónicos bloqueados se introduce una copia del mensaje.

Eliminación de mensajes

SpamKiller elimina automáticamente los mensajes de la carpeta de correos electrónicos bloqueados 15 días después de haberlos retirado del buzón de entrada. Puede cambiar el número de días al cabo de los cuales se eliminarán los mensajes o eliminarlos manualmente.

SpamKiller no elimina automáticamente los mensajes de la carpeta de correos electrónicos aceptados, porque ésta refleja los mensajes que están actualmente en el buzón de entrada.

Para cambiar la configuración de la eliminación automática de los mensajes bloqueados

De forma predeterminada, cuando SpamKiller localiza correo basura, lo elimina del buzón de entrada y lo pone en la carpeta de correos electrónicos bloqueados. SpamKiller elimina automáticamente los mensajes bloqueados de esta carpeta transcurridos 15 días. Es posible configurar la frecuencia con la que SpamKiller elimina los mensajes bloqueados automáticamente.

En lugar de trasladar los correos basura a la carpeta de correos electrónicos bloqueados, SpamKiller puede etiquetar la línea del asunto con la mención "[correo basura]" o con una etiqueta que usted elija, y conserva el mensaje en el buzón de entrada. El etiquetado de los mensajes puede resultar práctico si usted desea trasladar los mensajes a otra carpeta de su cliente de correo electrónico, como una carpeta de mensajes basura. Puede mover los mensajes etiquetados mediante la creación de una regla en el cliente de correo electrónico para que busque los mensajes que tengan una etiqueta "[correo basura]" y los ponga en la carpeta indicada.

1 Haga clic en la ficha **Configuración** y, a continuación, en el icono **Opciones de filtrado**.

2 Seleccione cómo gestiona SpamKiller el correo basura:

- **Poner el correo basura en una bandeja de mensajes bloqueados:** el correo basura se elimina del buzón de entrada y se envía a la carpeta de correos bloqueados de SpamKiller.
- **Conservar los mensajes bloqueados durante ____ días:** los mensajes bloqueados permanecen en la carpeta de correos electrónicos bloqueados durante el tiempo que se especifique.
- **Etiquetar el correo basura y conservar en el buzón de entrada:** el correo basura se conserva en el buzón de entrada, pero en la línea del asunto se pone la indicación "[correo basura]" o cualquier otra etiqueta que desee.

3 Haga clic en **Aceptar**.

Para eliminar manualmente un mensaje

1 Haga clic en la ficha **Mensajes** y después en la ficha **Correos electrónicos bloqueados**.

O

En el buzón de entrada de Microsoft Outlook o de Outlook Express, haga clic en  para abrir la página de correos electrónicos bloqueados de esa cuenta.

2 Seleccione el mensaje que desea eliminar.

3 Haga clic en **Eliminar este mensaje**. Aparece un cuadro de diálogo de confirmación.

4 Haga clic en **Sí** para eliminar el mensaje.

Agregación de amigos a una lista de amigos

Consulte *Para agregar a un amigo desde las páginas Correos bloqueados o Correos aceptados* en la página 115.

Agregación de filtros

Si desea información sobre los filtros, consulte *Trabajo con filtros*, en la ayuda en línea.

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

2 Haga clic en las fichas **Correos electrónicos bloqueados** o **Correos electrónicos aceptados** y, a continuación, en **Agregar un filtro**. Aparecerá el cuadro de diálogo **Editor de filtros**.

3 Haga clic en **Agregar** para empezar a crear una condición de filtrado. Aparecerá el cuadro de diálogo **Condición de filtrado**.

4 Cree una condición de filtrado a través de los pasos siguientes:

Una condición de filtrado es una instrucción que le indica a SpamKiller lo que debe buscar en un mensaje, por ejemplo: "El texto de mensaje contiene hipoteca". En este ejemplo, el filtro busca los correos electrónicos cuyo texto contenga la palabra "hipoteca". Para obtener más información, consulte *Condiciones de filtrado* en la ayuda en línea.

a Seleccione un tipo de condición del primer campo.

b Seleccione o introduzca valores en los cuadros siguientes.

c Si aparecen las siguientes opciones, selecciónelas para definir mejor la condición de filtrado.

Buscar también en los códigos de formato: esta opción aparece sólo si la condición de filtrado está configurada para buscar en el texto del mensaje. Si selecciona esta casilla de verificación, SpamKiller busca en el texto y en los códigos de formato del mensaje correspondientes al texto que se haya indicado.

Diferencia entre mayúsculas y minúsculas: esta opción aparece sólo para las condiciones en las que se introduce un valor de condición. Si selecciona esta casilla de verificación, SpamKiller diferenciará entre las letras mayúsculas y minúsculas del valor que haya introducido.

Variaciones de coincidencia: permite a SpamKiller detectar habituales errores de escritura utilizados por los remitentes de correo basura. Por ejemplo, la palabra "hipoteca" se puede escribir de forma incorrecta como "hipot@c3" para eludir los filtros.

d Haga clic en **Aceptar**.

5 Cree otra condición de filtrado como se indica a continuación o vaya al Paso 6 para seleccionar una acción de filtrado:

a Haga clic en **Agregar** y cree la condición de filtrado. Haga clic en **Aceptar** cuando haya terminado de crear la condición de filtrado.

Las dos condiciones aparecerán en la lista de condiciones de filtrado unidas por **y**. Esta **y** indica que SpamKiller buscará mensajes que coincidan con *las dos* condiciones de filtrado. Si desea que SpamKiller busque mensajes que coincidan al menos con una de las dos condiciones, cambie **y** por **o** haciendo clic en **y** seleccionando **o** en el campo correspondiente.

b Haga clic en **Agregar** para crear otra condición, o vaya al Paso 6 para seleccionar una acción de filtrado.

Si crea tres o más condiciones de filtrado, puede agruparlas para formar cláusulas. Si desea ver ejemplos de agrupaciones, consulte *Agrupación de filtros* en la ayuda en línea.

Para agrupar condiciones de filtrado, seleccione una condición y haga clic en **Agrupar**.

Las condiciones agrupadas se marcan en azul.

NOTA
Para desagrupar condiciones de filtrado, seleccione una condición agrupada y haga clic en **Desagrupar**.

6 Seleccione una acción de filtrado en el cuadro **Acción**. La acción de filtrado le indica a SpamKiller cómo debe procesar los mensajes que encuentre ese filtro. Para obtener más información, consulte *Acciones de filtrado* en la ayuda en línea.

7 Haga clic en **Avanzadas** para seleccionar opciones avanzadas de filtrado. No es necesario seleccionar las opciones avanzadas. Para obtener más información, consulte *Opciones de filtros avanzadas* en la ayuda en línea.

8 Haga clic en **Aceptar** cuando haya terminado de crear el filtro.

NOTA
Si desea editar una condición, selecciónela primero. Si desea suprimir una condición, selecciónela y, luego, haga clic en **Eliminar**.

Notificación de correo basura a McAfee

Puede notificar acerca de correo basura a McAfee para que lo analice y actualice los filtros.

Para informar del correo basura a McAfee

1 Haga clic en la ficha **Mensajes** y, a continuación, haga clic en la ficha **Correos electrónicos bloqueados** o **Correos electrónicos aceptados**. Aparece la página de correos electrónicos bloqueados o aceptados.

2 Seleccione un mensaje y haga clic en **Notificar a McAfee**. Aparece un cuadro de diálogo de confirmación.

3 Haga clic en **Sí**. El mensaje se envía automáticamente a McAfee.

Envío manual de quejas

Envíe una queja para que el remitente no le vuelva a enviar correo basura. Para obtener más información sobre el envío de quejas, consulte *Envío de quejas y mensajes de error* en la ayuda en línea.

Para enviar una queja manualmente

1. Haga clic en la ficha **Mensajes** y, a continuación, en la ficha **Correos electrónicos bloqueados** o **Correos electrónicos aceptados**. Aparecerá una lista de mensajes.
2. Seleccione un mensaje sobre el que desea quejarse y haga clic en **Enviar queja**. Aparecerá el cuadro de diálogo **Enviar queja**.
3. Seleccione a quién desea enviarle la queja.

   ADVERTENCIA
   En la mayoría de los casos, no se debe seleccionar **Remitente**. Si se envía una queja al remitente del correo basura, éste puede confirmar su dirección de correo electrónico y enviarle aún más mensajes.
4. Haga clic en **Siguiente** y siga las instrucciones de los cuadros de diálogo que irán apareciendo.

Envío de mensajes de error

Para obtener más información sobre el envío de mensajes de error, consulte *Envío de quejas y mensajes de error* en la ayuda en línea.

Envíe un mensaje de error para que el remitente no le vuelva a enviar correo basura.

Para enviar manualmente un mensaje de error

1. Haga clic en la ficha **Mensajes** y, a continuación, en la ficha **Correos electrónicos bloqueados** o **Correos electrónicos aceptados**. Aparecerá una lista de mensajes.
2. Para enviar un mensaje de error sobre un mensaje de correo basura específico, seleccione el mensaje y haga clic en **Enviar error**. Se envía un mensaje de error a la dirección de respuesta del correo basura.

Índice alfabético

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W