

internet**security**suite

Manual del usuario

Versión 8.0



DERECHOS DE PROPIEDAD INTELECTUAL

Copyright © 2005 McAfee, Inc. Reservados todos los derechos. Queda prohibida la reproducción, transmisión, transcripción, almacenamiento en un sistema de recuperación o traducción a cualquier idioma de este documento o parte de él en cualquier forma y por cualquier medio sin el consentimiento previo por escrito de McAfee, Inc., sus proveedores o empresas filiales.

ATRIBUCIONES DE MARCAS COMERCIALES

ACTIVE FIREWALL, ACTIVE SECURITY, ACTIVESECURITY (Y EN KATAKANA), ACTIVESHIELD, ANTI-VIRUS ANYWARE AND DESIGN, CLEAN-UP, DESIGN (E ESTILIZADO), DESIGN (N ESTILIZADO), ENTERCEPT, ENTERPRISE SECURECAST, ENTERPRISE SECURECAST (Y EN KATAKANA), EPOLICY ORCHESTRATOR, FIRST AID, FORCEFIELD, GMT, GROUPSHIELD, GROUPSHIELD (Y EN KATAKANA), GUARD DOG, HOMEGUARD, HUNTER, INTRUSHIELD, INTRUSION PREVENTION THROUGH INNOVATION, M AND DESIGN, MCAFEE, MCAFEE (Y EN KATAKANA), MCAFEE AND DESIGN, MCAFEE.COM, MCAFEE VIRUSSCAN, NA NETWORK ASSOCIATES, NET TOOLS, NET TOOLS (Y EN KATAKANA), NETCRYPTO, NETCTOPUS, NETSCAN, NETSHIELD, NETWORK ASSOCIATES, NETWORK ASSOCIATES COLLISEUM, NETXRAY, NOTESGUARD, NUTS & BOLTS, OIL CHANGE, PC MEDIC, PCNOTARY, PRIMESUPPORT, RINGFENCE, ROUTER PM, SECURECAST, SECURESELECT, SPAMKILLER, STALKER, THREATSCAN, TIS, TMEG, TOTAL VIRUS DEFENSE, TRUSTED MAIL, UNINSTALLER, VIREX, VIRUS FORUM, VIRUSCAN, VIRUSSCAN, VIRUSSCAN (Y EN KATAKANA), WEBSCAN, WEBSHIELD, WEBSHIELD (Y EN KATAKANA), WEBSTALKER, WEBWALL, WHAT'S THE STATE OF YOUR IDS?, WHO'S WATCHING YOUR NETWORK, YOUR E-BUSINESS DEFENDER, YOUR NETWORK. OUR BUSINESS. son marcas registradas o marcas comerciales de McAfee, Inc. o sus empresas filiales en los EE.UU. y otros países. El color rojo en relación con la seguridad es un elemento distintivo de los productos de la marca McAfee. Todas las demás marcas comerciales, registradas y sin registrar, incluidas en el presente documento son propiedad exclusiva de sus respectivos titulares.

INFORMACIÓN SOBRE LA LICENCIA

Acuerdo de licencia

AVISO A TODOS LOS USUARIOS: LEA DETENIDAMENTE EL ACUERDO LEGAL APROPIADO CORRESPONDIENTE A LA LICENCIA ADQUIRIDA, QUE ESTABLECE LOS TÉRMINOS Y CONDICIONES GENERALES DE USO DEL SOFTWARE PARA EL QUE SE CONCEDE LA LICENCIA. SI NO SABE QUÉ TIPO DE LICENCIA HA ADQUIRIDO, CONSULTE LOS DOCUMENTOS DE VENTA Y OTROS DOCUMENTOS RELACIONADOS CON LA CONCESIÓN DE LA LICENCIA O CON LA ORDEN DE COMPRA QUE ACOMPAÑAN AL PAQUETE DE SOFTWARE O QUE HAYA RECIBIDO POR SEPARADO COMO PARTE DE LA COMPRA (POR EJEMPLO, UN MANUAL, UN ARCHIVO DEL CD DEL PRODUCTO O UN ARCHIVO DEL SITIO WEB DESDE EL QUE DESCARGÓ EL PAQUETE DE SOFTWARE). SI NO ESTÁ DE ACUERDO CON TODAS LAS CONDICIONES DESCRITAS EN EL ACUERDO, NO INSTALE EL SOFTWARE. SI PROCEDA, PUEDE DEVOLVER EL PRODUCTO A MCAFEE O AL ESTABLECIMIENTO DE COMPRA PARA QUE SE LE REEMBOLSE EL IMPORTE COMPLETO.

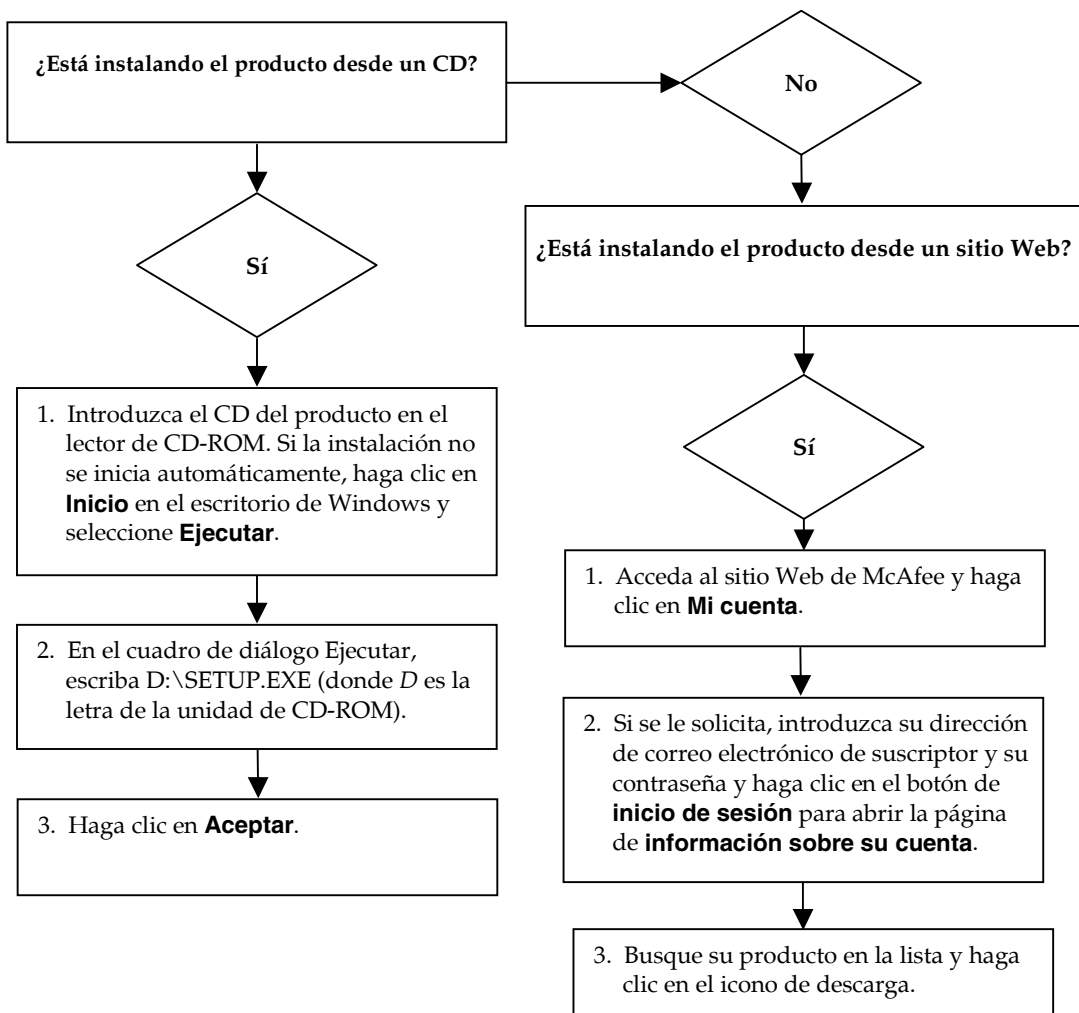
Atribuciones

Este producto incluye o puede incluir lo siguiente:

♦ Software desarrollado por OpenSSL Project para su uso en OpenSSL Toolkit (<http://www.openssl.org/>). ♦ Software criptográfico escrito por Eric A. Young y software escrito por Tim J. Hudson. ♦ Algunos programas de software que se conceden bajo licencia (o sublicencia) al usuario mediante licencia pública general (GPL) u otras licencias similares de software gratuito que, entre otros derechos, permiten al usuario copiar, modificar y redistribuir ciertos programas, o determinadas partes de ellos, así como acceder al código fuente. Esta licencia pública general requiere que cualquier software proporcionado con este tipo de licencia se distribuya en formato binario ejecutable y que el código fuente se ponga a disposición de los usuarios. El código fuente del software con licencia pública general se incluye también en el CD. Si cualquier licencia de software gratuito requiere que McAfee proporcione derechos de utilización, copia o modificación de un programa de software que sean más amplios que los aquí expuestos, tales derechos prevalecerán sobre los derechos y restricciones aquí expresados. ♦ Software escrito originalmente por Henry Spencer, Copyright 1992, 1993, 1994, 1997 Henry Spencer. ♦ Software escrito originalmente por Robert Nordier, Copyright © 1996-7 Robert Nordier. ♦ Software escrito por Douglas W. Sauder. ♦ Software desarrollado por la Apache Software Foundation (<http://www.apache.org/>). Puede encontrar una copia del acuerdo de licencia de este software en www.apache.org/licenses/LICENSE-2.0.txt. ♦ International Components for Unicode ("ICU") Copyright © 1995-2002 International Business Machines Corporation y otros. ♦ Software desarrollado por CrystalClear Software, Inc., Copyright © 2000 CrystalClear Software, Inc. ♦ Tecnología FEAD™ Optimizer®, Copyright Netop Systems AG, Berlín, Alemania. ♦ Outside In® Viewer Technology © 1992-2001 Stellent Chicago, Inc. o Outside In® HTML Export, © 2001 Stellent Chicago, Inc. ♦ Software propiedad de Thai Open Source Software Center Ltd. y Clark Cooper, © 1998, 1999, 2000. ♦ Software propiedad de Xpat maintainers. ♦ Software propiedad de The Regents of the University of California, © 1989. ♦ Software propiedad de Gunnar Ritter. ♦ Software propiedad de Sun Microsystems®, Inc. © 2003. ♦ Software propiedad de Gisle Aas. © 1995-2003. ♦ Software propiedad de Michael A. Chase, © 1999-2000. ♦ Software propiedad de Neil Winton, © 1995-1996. ♦ Software propiedad de RSA Data Security, Inc., © 1990-1992. ♦ Software propiedad de Sean M. Burke, © 1999, 2000. ♦ Software propiedad de Martijn Koster, © 1995. ♦ Software propiedad de Brad Appleton, © 1996-1999. ♦ Software propiedad de Michael G. Schwern, © 2001. ♦ Software propiedad de Graham Barr, © 1998. ♦ Software propiedad de Larry Wall y Clark Cooper, © 1998-2000. ♦ Software propiedad de Frodo Looijgaard, © 1997. ♦ Software propiedad de Python Software Foundation, Copyright © 2001, 2002, 2003. Hay una copia del acuerdo de licencia para este software en www.python.org. ♦ Software propiedad de Beman Dawes, © 1994-1999, 2002. ♦ Software escrito por Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 University of Notre Dame. ♦ Software propiedad de Simone Bordet & Marco Craverio, © 2002. ♦ Software propiedad de Stephen Purcell, © 2001. ♦ Software desarrollado por Indiana University Extreme! Lab (<http://www.extreme.indiana.edu/>). ♦ Software propiedad de International Business Machines Corporation y otros, © 1995-2003. ♦ Software desarrollado por la University of California, Berkeley y sus donantes. ♦ Software desarrollado por Ralf S. Engelschall <rse@engelschall.com> para su uso en el proyecto mod_ssl (<http://www.modssl.org/>). ♦ Software propiedad de Kevlin Henney, © 2000-2002. ♦ Software propiedad de Peter Dimov y Multi Media Ltd. © 2001, 2002. ♦ Software propiedad de David Abrahams, © 2001, 2002. Consulte <http://www.boost.org/libs/bind/bind.html> para obtener la documentación. ♦ Software propiedad de Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock, © 2000. ♦ Software propiedad de Boost.org, © 1999-2002. ♦ Software propiedad de Nicolai M. Josuttis, © 1999. ♦ Software propiedad de Jeremy Siek, © 1999-2001. ♦ Software propiedad de Daryle Walker, © 2001. ♦ Software propiedad de Chuck Allison y Jeremy Siek, © 2001, 2002. ♦ Software propiedad de Samuel Krepp, © 2001. Consulte <http://www.boost.org> para obtener el historial de revisiones, actualizaciones y documentación. ♦ Software propiedad de Doug Gregor (<gregod@cs.rpi.edu>), © 2001, 2002. ♦ Software propiedad de Cadenza New Zealand Ltd., © 2000. ♦ Software propiedad de Jens Maurer, © 2000, 2001. ♦ Software propiedad de Jaakko Järvi (<jaakko.jarvi@cs.utu.fi>), © 1999, 2000. ♦ Software propiedad de Ronald Garcia, © 2002. ♦ Software propiedad de David Abrahams, Jeremy Siek y Daryle Walker, © 1999-2001. ♦ Software propiedad de Stephen Cleary (<shammah@voyager.net>), © 2000. ♦ Software propiedad de Housemarque Oy <<http://www.housemarque.com>>, © 2001. ♦ Software propiedad de Paul Moore, © 1999. ♦ Software propiedad de Dr. John Maddock, © 1998-2002. ♦ Software propiedad de Greg Colvin y Beman Dawes, © 1998, 1999. ♦ Software propiedad de Peter Dimov, © 2001, 2002. ♦ Software propiedad de Jeremy Siek y John R. Bandela, © 2001. ♦ Software propiedad de Joerg Walter y Mathias Koch, © 2000-2002.

Tarjeta de inicio rápido

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



McAfee se reserva el derecho a modificar los planes y las políticas de actualización y asistencia en cualquier momento y sin previo aviso. McAfee y sus nombres de producto son marcas registradas de McAfee, Inc. o de sus empresas filiales en los EE.UU. u otros países.

© 2005 McAfee, Inc. Reservados todos los derechos.

Si desea obtener más información

Para ver los manuales de usuario del CD del producto, asegúrese de que tiene instalado Acrobat Reader; si no es así, instálelo 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 después 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

McAfee recomienda que siga los sencillos pasos dentro del producto que permiten transmitir su registro directamente. Gracias al registro, podrá disfrutar de asistencia técnica especializada y puntual, así como de las ventajas siguientes:

- Asistencia electrónica GRATUITA.
- Actualizaciones de los archivos de definición de virus (.DAT) durante un año a partir de la instalación tras la adquisición del software de VirusScan.

Acceda a <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 CD de software si está defectuoso o dañado.

- Actualizaciones de filtros de SpamKiller durante un año después de instalarlo tras la adquisición del software SpamKiller.

Acceda a <http://es.mcafee.com> para obtener información sobre el precio de un año adicional de actualizaciones de filtros.

- McAfee Internet Security Suite se actualiza durante un año después de la instalación si adquiere el software MIS.

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

Soporte técnico

Para obtener soporte técnico, visite

<http://www.mcafeeayuda.com/>.

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

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

<http://www.mcafeeayuda.com/>.

Contenido

Tarjeta de inicio rápido	iii
1 Presentación	11
Software McAfee Internet Security	12
Requisitos del sistema	12
Utilización de McAfee SecurityCenter	13
Eliminación de programas de Internet Security Suite	14
2 McAfee VirusScan	15
Funciones nuevas	15
Comprobación del funcionamiento de VirusScan	17
Comprobación del funcionamiento de ActiveShield	17
Comprobación del funcionamiento de Analizar	17
Utilización de ActiveShield	19
Activación o desactivación de ActiveShield	19
Configuración de las opciones de ActiveShield	20
Descripción de las alertas de seguridad	30
Análisis manual del equipo	33
Análisis manual para detectar virus y otras amenazas	33
Análisis automático para detectar virus y otras amenazas	37
Descripción de la detección de amenazas	39
Gestión de archivos en cuarentena	40
Creación de un disco de emergencia	42
Protección de un disco de emergencia contra escritura	43
Utilización de un disco de emergencia	44
Actualización de un disco de emergencia	44
Información automática sobre virus	44
Envío de información al World Virus Map	44
Visualización del World Virus Map	45
Actualización de VirusScan	47
Comprobación automática de actualizaciones	47
Comprobación manual de actualizaciones	47

3 McAfee Personal Firewall Plus	49
Funciones nuevas	49
Eliminación de otros cortafuegos	51
Configuración del cortafuegos predeterminado	51
Configuración del nivel de seguridad	52
Comprobación de McAfee Personal Firewall Plus	54
Acerca de la página Resumen	54
Información acerca de la página Aplicaciones de Internet	59
Cambiar reglas de aplicación	60
Permitir y bloquear el acceso a aplicaciones de Internet	60
Información acerca de la página Eventos entrantes	61
Explicación de los eventos	62
Visualización de eventos en el registro de eventos entrantes	64
Respuesta a eventos entrantes	66
Gestión del registro de eventos entrantes	70
Acerca de las alertas	72
Alertas rojas	72
Alertas verdes	78
Alertas azules	79
 4 McAfee Privacy Service	 81
Funciones	81
Administrador	81
Asistente para la configuración	82
Recuperación de la contraseña del administrador	82
Usuario de inicio	82
Apertura de McAfee Privacy Service	83
Apertura e inicio de sesión de Privacy Service	83
Desactivación de Privacy Service	83
Actualización de McAfee Privacy Service	83
Adición de usuarios	84
Definición de la contraseña	84
Definición del grupo de edad	84
Configuración del bloqueador de cookies	84
Definición de límites de tiempo de acceso a Internet	85
Edición de usuarios	85
Cambio de contraseñas	86

Cambio de la información de un usuario	86
Modificación de la configuración del bloqueador de cookies	86
Edición de la lista para aceptar y rechazar cookies	87
Cambio del grupo de edad	87
Modificación de los límites de tiempo de acceso a Internet	87
Cambio del usuario de inicio	88
Eliminación de usuarios	88
Opciones	89
Bloqueo de sitios Web	89
Permiso de acceso a sitios Web	89
Bloqueo de información	89
Adición de información	90
Edición de información	90
Eliminación de información personal	90
Bloqueo de Web bugs	90
Bloqueo de anuncios	90
Admisión de cookies de sitios Web específicos	91
Registro de eventos	91
Fecha y hora	91
Usuario	92
Resumen	92
Detalles del evento	92
Almacenamiento del registro de eventos activo	92
Visualización de registros guardados	92
Utilidades	93
Eliminación de archivos de manera permanente mediante McAfee Shredder	93
Por qué Windows conserva restos de archivos	93
Qué borra McAfee Shredder	93
Eliminación permanente de los archivos del Explorador de Windows	94
Vaciado de la Papelera de reciclaje de Windows	94
Personalización de la configuración de Shredder	94
Copia de seguridad de la base de datos de Privacy Service	94
Restauración de la base de datos desde la copia de seguridad	95
Opciones de usuario	96
Cambio de la contraseña	96
Cambio del nombre de usuario	96
Vaciado de la caché	96

Admisión de cookies	97
Si necesita eliminar un sitio Web de la lista:	97
Rechazo de cookies	97
Si necesita eliminar un sitio Web de la lista:	97

5 McAfee SpamKiller 99

Funciones	99
Opciones de usuario	100
Filtrado	100
Descripción del panel superior	100
Desactivación de SpamKiller	101
Descripción de la página de resumen	101
Integración con Microsoft Outlook y Outlook Express	102
Gestión de cuentas de correo electrónico y de usuarios	103
Adición de cuentas de correo electrónico	103
Orientación del cliente de correo electrónico a SpamKiller	104
Eliminación de cuentas de correo electrónico	104
Eliminación de una cuenta de correo electrónico de SpamKiller	105
Edición de las propiedades de la cuenta de correo electrónico	105
Cuentas POP3	105
Cuentas MSN/Hotmail	107
Cuentas MAPI	109
Adición de usuarios	110
Contraseñas de usuario y protección contra el correo basura para menores	112
Inicio de sesión en SpamKiller en un entorno de múltiples usuarios	113
Utilización de la lista de amigos	114
Apertura de una lista de amigos	115
Importación de libretas de direcciones	116
Importación automática de una libreta de direcciones	116
Importación manual de una libreta de direcciones	117
Edición de información de la libreta de direcciones	117
Eliminación de una libreta de direcciones de la lista de importación automática	118
Adición de amigos	118
Adición de amigos desde las páginas de correos electrónicos bloqueados o aceptados	118
Adición de amigos desde la página Amigos	119
Adición de amigos desde Microsoft Outlook	120

Edición de amigos	120
Eliminación de amigos	120
Trabajo con mensajes bloqueados y aceptados	121
Página de correos electrónicos bloqueados	121
Página de correos electrónicos aceptados	123
Tareas relativas a los correos electrónicos bloqueados y aceptados	124
Recuperación de mensajes	124
Desde la página Correos bloqueados	125
Desde la carpeta SpamKiller de Microsoft Outlook u Outlook Express	125
Bloqueo de mensajes	125
Desde la página Correos aceptados	125
Desde Microsoft Outlook	126
¿Dónde se encuentran los mensajes bloqueados?	126
Eliminación manual de mensajes	126
Modificación del modo en que se procesa el correo no deseado	126
Etiquetado	126
Bloqueo	127
Modificación del modo en que SpamKiller procesa el correo no deseado	127
Configuración del filtro AntiPhishing	127
Adición de amigos a una lista de amigos	128
Adición de filtros	128
Expresiones regulares	130
Notificación de correo basura a McAfee	134
Envío manual de quejas	134
Envío de mensajes de error	134
Envío manual de mensajes de error	135
Índice	137

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 cookies y contraseñas; bloquea el acceso a archivos, carpetas y unidades; filtra los contenidos cuestionables y le concede el control de las conexiones entrantes y salientes de su equipo con Internet.

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

McAfee Internet Security Suite se compone de los productos siguientes:

- [McAfee VirusScan en la página 15](#)
- [McAfee Personal Firewall Plus en la página 49](#)
- [McAfee Privacy Service en la página 81](#)
- [McAfee SpamKiller en la página 99](#)

Software McAfee Internet Security

- **McAfee SecurityCenter:** evalúa, informa y le avisa sobre la vulnerabilidad de la seguridad de su equipo. Cada índice de seguridad evalúa rápidamente su exposición a las amenazas de seguridad y a las existentes en Internet, y propone recomendaciones para proteger su equipo de manera rápida y segura.
- **McAfee VirusScan:** analiza, detecta, soluciona y elimina virus de Internet. Puede personalizar análisis de virus y determinar la respuesta y la acción que tomar cuando se detecta un virus. También puede configurar VirusScan para que registre acciones relacionadas con virus que ocurran en el equipo.
- **McAfee Personal Firewall Plus:** protege el equipo cuando está conectado a Internet y protege las conexiones entrantes y salientes a Internet que realiza.
- **McAfee Privacy Service:** combina protección de la información personal, bloqueo de anuncios en línea y filtrado de contenidos. Protege su información personal a la vez que facilita un mayor control sobre el uso de Internet por parte de su familia. McAfee Privacy Service evita la exposición de información confidencial a amenazas en línea y le protege a usted y a su familia de contenidos inadecuados.
- **McAfee SpamKiller:** el aumento del envío de correo electrónico fraudulento, inapropiado y ofensivo dirigido a adultos, menores y empresas hace de la protección contra el correo basura un componente fundamental de la estrategia de seguridad de su equipo.

Requisitos del sistema

- Microsoft® Windows 98, Me, 2000 o XP
- Ordenador personal con procesador Pentium o compatible
 - ◆ Windows 98, 2000: 133 MHz o superior
 - ◆ Windows Me: 150 MHz o superior
 - ◆ Windows XP (Home y Pro): 300 MHz o superior
- RAM
 - ◆ Windows 98, Me, 2000: 64 MB
 - ◆ Windows XP (Home y Pro): 128 MB
- 100 MB de espacio en el disco duro
- Microsoft® Internet Explorer 5.5 o superior

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


Utilización de McAfee SecurityCenter


McAfee SecurityCenter es una herramienta de seguridad integrada a la que puede acceder desde el icono correspondiente, situado en la bandeja del sistema de Windows, o directamente desde el escritorio de Windows. Con ella puede realizar estas útiles tareas:

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


NOTA

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


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

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

Para abrir McAfee SecurityCenter:

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

Para acceder al producto de McAfee:

- 1 Haga clic con el botón derecho del ratón en el icono de McAfee , en la bandeja del sistema de Windows.
- 2 Elija el producto de McAfee adecuado y seleccione la función que desea utilizar.

Eliminación de programas de Internet Security Suite

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

NOTA

Para poder desinstalar Internet Security Suite, los usuarios deben poseer derechos de Administrador.

- 1 Guarde todo su trabajo y cierre todas las aplicaciones que se encuentren abiertas.
- 2 Abra el **Panel de control**.
 - ♦ En la barra de tareas de Windows, seleccione **Inicio**, elija **Configuración** y después haga clic en **Panel de control** (Windows 98, ME y 2000).
 - ♦ En la barra de tareas de Windows, seleccione **Inicio** y haga clic en **Panel de control** (Windows XP).
- 3 Haga clic en **Agregar o quitar programas**.
- 4 Seleccione el asistente para desinstalación de McAfee, después uno o más programas y finalmente haga clic en **Desinstalar**.
- 5 Para continuar con la eliminación, haga clic en **Sí**.
- 6 Si se le solicita, reinicie el equipo.

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 acceden a ellos.

Analizar: detecta la existencia de virus y programas potencialmente no deseados en las unidades de disco duro, unidades de disquete y en carpetas y archivos individuales.

En 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 actividades semejantes a la de los virus provocada por gusanos o por secuencias de comandos malintencionadas.

Funciones nuevas

Esta versión de VirusScan incluye las siguientes funciones nuevas:

- **Detección y eliminación de software espía y de publicidad**
VirusScan identifica y elimina software espía, de publicidad y otros programas que ponen en peligro su privacidad y reducen el rendimiento del equipo.
- **Actualizaciones automáticas diarias**
Las actualizaciones automáticas diarias de VirusScan protegen frente a las amenazas informáticas más recientes, incluso las aún no identificadas.
- **Análisis rápido en segundo plano**
Los análisis rápidos y discretos identifican y destruyen virus, troyanos, gusanos, software espía, de publicidad y de marcación, y otros programas malintencionados sin interrumpir el trabajo.
- **Alertas de seguridad en tiempo real**
Las alertas de seguridad indican la aparición de emergencias de virus y amenazas contra la seguridad y ofrecen opciones de respuesta para eliminar la amenaza, neutralizarla u obtener más información sobre ella.

- **Detección y limpieza en varios puntos de entrada**
VirusScan supervisa y limpia en los puntos de entrada clave del equipo: correo electrónico, archivos adjuntos de mensajes instantáneos y descargas de Internet.
- **Supervisión en el correo electrónico de actividades parecidas a la de los gusanos**
WormStopper™ supervisa comportamientos susceptibles de ser correo masivo y detiene la propagación de virus y gusanos a otros equipos a través del correo electrónico.
- **Supervisión en las secuencias de comandos de actividades parecidas a la de los gusanos**
ScriptStopper™ supervisa ejecuciones de secuencias de comandos sospechosas y detiene la propagación de virus y gusanos a otros equipos a través del correo electrónico.
- **Soporte técnico gratuito a través de mensajería instantánea y correo electrónico**
El soporte técnico en directo a través de correo electrónico y mensajería instantánea proporcionan ayuda de forma rápida y sencilla.

Comprobación del funcionamiento de VirusScan

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

Comprobación del funcionamiento de ActiveShield

NOTA

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

Para comprobar el funcionamiento de ActiveShield:

- 1 Vaya a la dirección <http://www.eicar.com/> con 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 **Download** (Descargar) verá cuatro vínculos.
- 4 Haga clic en **eicar.com**.

Si ActiveShield funciona correctamente, detectará el archivo eicar.com inmediatamente después de hacer clic en el vínculo. Puede intentar suprimir o poner en cuarentena archivos infectados para comprobar el tratamiento que da ActiveShield a los virus. Consulte la sección *Descripción de las alertas de seguridad en la página 30* para obtener información más detallada.

Comprobación del funcionamiento de Analizar

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

Para descargar los archivos de prueba:

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

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

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

eicar.com.txt (opcional) es el mismo archivo, pero con un nombre diferente, para aquellos usuarios que experimenten algún problema al descargar el primer vínculo. Sólo hay que cambiar su nombre por "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 por **Carpeta de análisis de VSO**.
- f Haga doble clic en **Carpeta de análisis VSO** y después en **Guardar** en cada cuadro de diálogo **Guardar como**.

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

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

Para comprobar el funcionamiento de Analizar:

- 1 Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y haga clic en **Detectar virus**.
- 2 Utilizando el árbol de directorios del panel izquierdo del cuadro de diálogo, vaya a la carpeta **Carpeta de análisis de VSO** en la que guardó los archivos:
 - a Haga clic en el signo + situado junto al icono de la unidad C.
 - b Haga clic en la carpeta **Carpeta de análisis de VSO** para resaltarla (no lo haga en el signo + situado junto a ella).

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

- 3 En el área **Opciones de análisis** del cuadro de diálogo **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 detectados**. Si es así, Analizar funciona correctamente.


Puede intentar eliminar o poner en cuarentena los archivos infectados para comprobar el tratamiento que da Analizar a los virus. Consulte la sección [Descripción de la detección de amenazas en la página 39](#) para obtener información más detallada.

Utilización de ActiveShield

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


Activación o desactivación de ActiveShield

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

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

Activación de ActiveShield

Para activar ActiveShield sólo 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 junto con Windows, se mostrará un mensaje que indica que ya está protegido frente al ataque de virus. De lo contrario, aparecerá un cuadro de diálogo que le permitirá configurar ActiveShield para que se inicie junto con Windows ([figura 2-1 en la página 20](#)).

Desactivación de ActiveShield

Para desactivar ActiveShield sólo durante la sesión de Windows en curso:

- 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 junto con Windows, el equipo estará nuevamente protegido frente al ataque de virus cuando lo reinicie.

Configuración de las opciones de ActiveShield

Puede modificar las opciones de inicio y análisis de ActiveShield en la ficha **ActiveShield** del cuadro de diálogo **VirusScan: Opciones** (Figura 2-1), a la que puede acceder a través del icono de McAfee  situado en la bandeja del sistema de Windows.

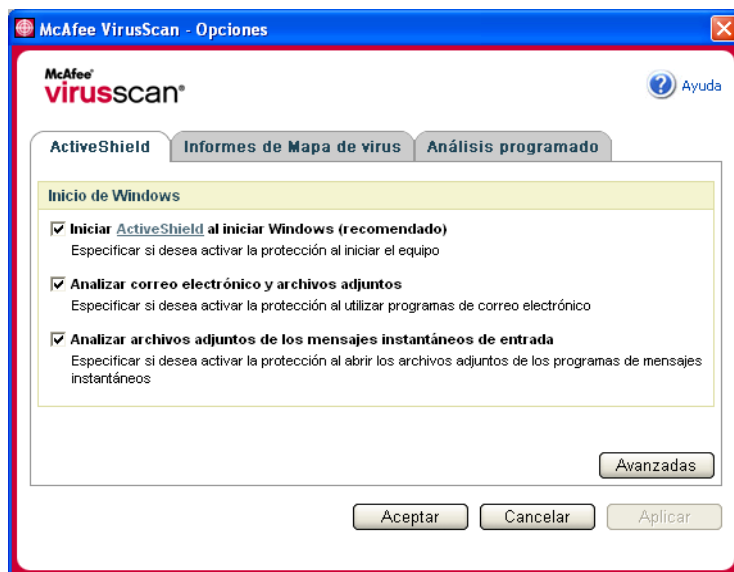



Figura 2-1. Opciones de ActiveShield

Inicio de ActiveShield

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

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

NOTA

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

Para iniciar ActiveShield automáticamente junto con 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 después en **Aceptar**.

Detención de ActiveShield**ADVERTENCIA**

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

Para hacer que ActiveShield no se inicie junto con 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 Desmarque 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 después en **Aceptar**.

Análisis del correo electrónico y los archivos adjuntos

De forma predeterminada, el análisis y la limpieza automática del correo electrónico se activa con la opción **Analizar correo electrónico y archivos adjuntos** (figura 2-1 en la página 20).

Cuando esta opción está activada, ActiveShield analiza y trata de limpiar automáticamente todos los mensajes de correo electrónico entrante (POP3) y saliente (SMTP), así como los archivos adjuntos 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 en los clientes siguientes: correo electrónico basado en Web, IMAP, AOL, POP3 SSL y Lotus Notes. Sin embargo, ActiveShield analiza los archivos adjuntos del correo electrónico cuando se abren.

Si desactiva la opción **Analizar correo electrónico y archivos adjuntos**, las opciones Análisis del correo electrónico y WormStopper ([figura 2-2 en la página 23](#)) se desactivan automáticamente. Si desactiva el análisis de correo electrónico saliente, las opciones de WormStopper se desactivan automáticamente.

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

Correo electrónico entrante

Si un mensaje de correo electrónico o un archivo adjunto entrantes están infectados, ActiveShield realiza los pasos siguientes:

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

Correo electrónico saliente

Si un mensaje de correo electrónico o un archivo adjunto saliente están infectados, ActiveShield realiza los pasos siguientes:

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

NOTA

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

Desactivación del análisis del correo electrónico

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

Para desactivar el análisis del correo entrante o saliente:

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

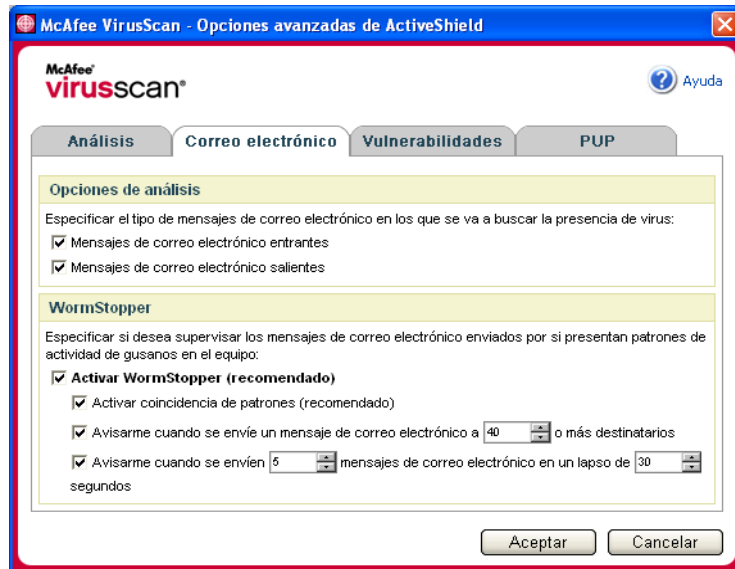


Figura 2-2. Opciones avanzadas de ActiveShield: ficha Correo electrónico

Análisis de gusanos

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

Un “gusano” informático es un virus capaz de replicarse, que reside en la memoria activa y puede enviar copias de sí mismo a través de correo electrónico. Sin WormStopper, los gusanos podrían pasar inadvertidos hasta que su replicación descontrolada consume tantos recursos del sistema que reducen su rendimiento o detienen tareas.

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

- Intento de reenviar correo electrónico a una parte importante de la agenda.
- Intentos de reenviar varios mensajes de correo electrónico en rápida sucesión.

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

Para configurar ActiveShield de modo que analice en los mensajes de correo electrónico actividades parecidas a las de los gusanos:

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

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 o más mensajes de correo electrónico un lapso de 30 segundos.

NOTA

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

Esta opción se puede activar automáticamente después de la primera vez que se detecta un posible gusano (consulte [Gestión de gusanos potenciales en la página 31](#) para obtener información detallada):

- ◆ Bloqueo automático de mensajes sospechosos de correo electrónico saliente

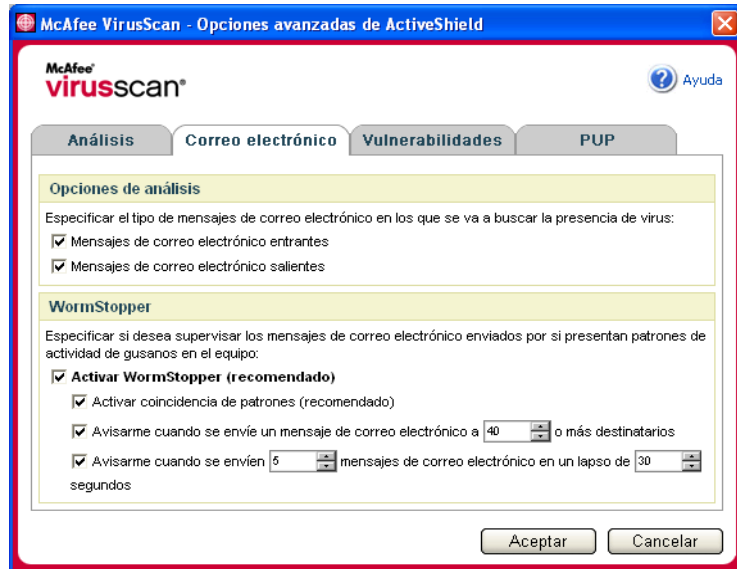


Figura 2-3. Opciones avanzadas de ActiveShield: ficha Correo electrónico

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 entrantes de los programas de mensajería instantánea 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 versión posterior

NOTA

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

Si el archivo adjunto de un mensaje instantáneo entrante está infectado, VirusScan realiza el procedimiento siguiente:

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

Análisis de todos los archivos

Si se ha configurado ActiveShield para utilizar la opción predeterminada **Todos los archivos (recomendado)**, se analizarán todos los tipos de archivos cuando el equipo intente utilizarlos. Utilice esta función para obtener el máximo provecho posible del análisis.

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

- 1 Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y haga clic en **Opciones**.
- 2 Haga clic en **Avanzadas** y después en la ficha **Análisis** (figura 2-4 en la página 26).
- 3 Haga clic en **Todos los archivos (recomendado)** y después en **Aceptar**.

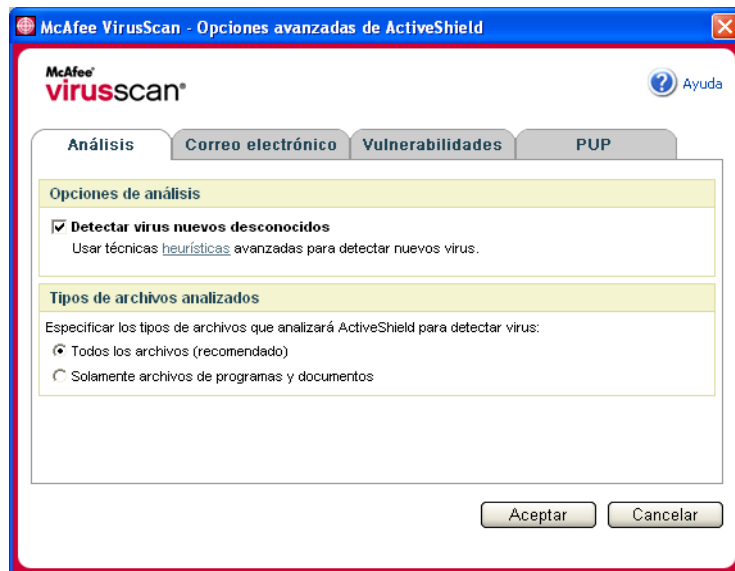


Figura 2-4. Opciones avanzadas de ActiveShield: ficha Análisis

Exploración exclusiva de archivos de programas y documentos

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

- 1 Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y haga clic en **Opciones**.
- 2 Haga clic en **Avanzadas** y después en la ficha **Análisis** (Figura 2-4).
- 3 Haga clic en **Solamente archivos de programas y documentos** y después en **Aceptar**.

Detección de virus nuevos desconocidos

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

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

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

Análisis de secuencias de comandos

VirusScan supervisa el equipo para analizar la actividad sospechosa que pueda indicar la presencia de una amenaza en él. Mientras VirusScan limpia los virus, ScriptStopper™ evita que los archivos troyanos ejecuten secuencias de comandos que puedan hacer proliferar más los virus.

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

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

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

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

Para configurar ActiveShield de modo que analice secuencias de comandos en ejecución buscando actividades parecidas a las de los gusanos:

- 1 Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y haga clic en **Opciones**.
- 2 Haga clic en **Avanzadas** y después en la ficha **Vulnerabilidades** (Figura 2-5).
- 3 Haga clic en **Activar ScriptStopper (recomendado)** y después en **Aceptar**.

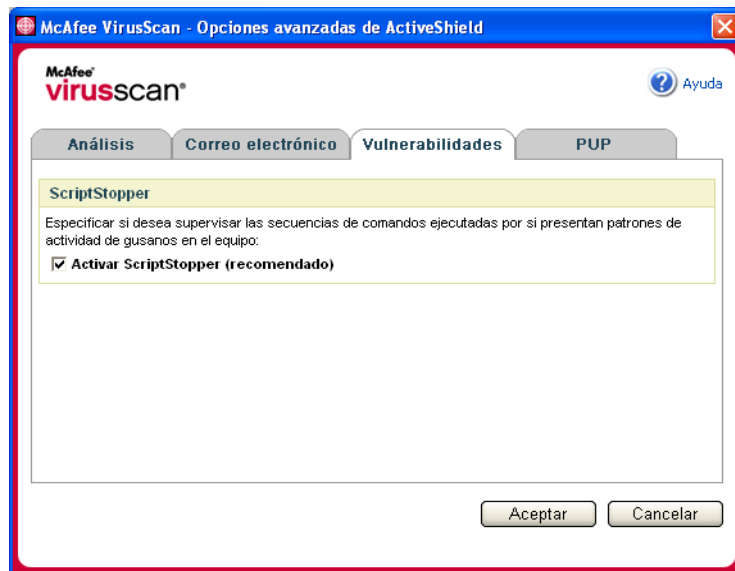


Figura 2-5. Opciones avanzadas de ActiveShield: ficha Vulnerabilidades

Análisis de programas potencialmente no deseados (PUP)

NOTA

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

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

Para configurar ActiveShield de modo que analice PUP:

- 1 Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y haga clic en **Opciones**.
- 2 Haga clic en **Avanzadas** y después en la ficha **PUP** (Figura 2-6).
- 3 Haga clic en **Analizar programas potencialmente no deseados (recomendado)** y a continuación en **Aceptar**.

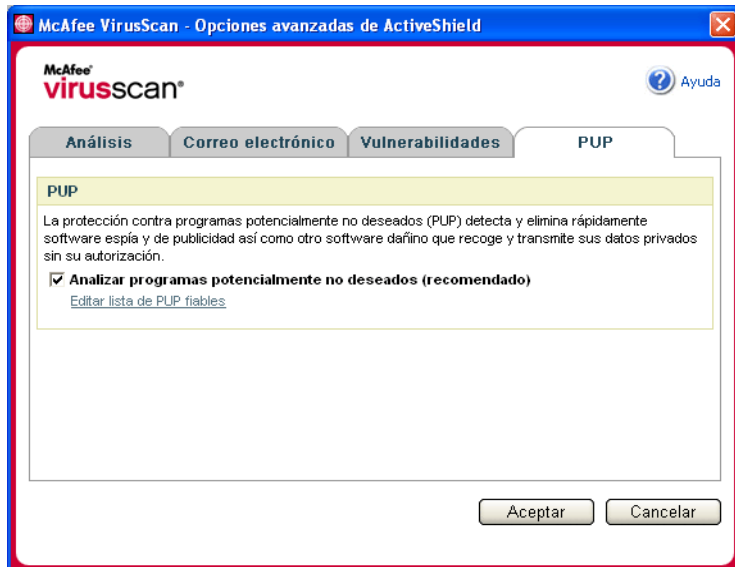


Figura 2-6. Opciones avanzadas de ActiveShield: ficha PUP

Descripción de las alertas de seguridad

Si ActiveShield descubre un virus, aparecerá una alerta similar a esta: [Figura 2-7](#). ActiveShield intenta limpiar automáticamente la mayor parte de los virus, archivos troyanos y gusanos y muestra una alerta. En el caso de programas potencialmente no deseados (PUP), ActiveShield detecta el archivo, lo bloquea automáticamente y le muestra una alerta.

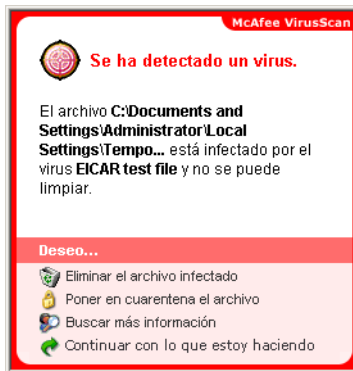


Figura 2-7. Alerta de virus

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

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

Gestión de archivos 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 estaba 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 oportuna.

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

De forma predeterminada, el análisis de correo electrónico intenta limpiar automáticamente los mensajes infectados. Un archivo de alerta, que se incluye en el mensaje entrante, le notifica si el correo electrónico se limpió, se puso en cuarentena o se eliminó.

Administración de secuencias de comandos sospechosas

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

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

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

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

Gestión de gusanos potenciales

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

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

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

Gestionar archivos PUP

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

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

Aparece un mensaje de confirmación.

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

- En caso contrario, haga clic en **Cancelar** para salir del proceso de eliminación automático. Si cambia de opinión más adelante, puede eliminar el programa manualmente utilizando el desinstalador de ese producto.

- ◆ Haga clic en **Continuar con lo que estoy haciendo** para hacer caso omiso de la alerta y bloquear el programa esta vez.

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

- ◆ Haga clic en **Definir como PUP fiable** para agregarlo a la lista blanca y dejar que se ejecute libremente en el futuro.

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

Gestión de PUP fiables

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

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

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

Para eliminar un programa de la lista de PUP fiables:

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

- 2 Haga clic en **Avanzadas** y después en la ficha **PUP**.
- 3 Haga clic en **Editar lista de PUP fiables**, seleccione la casilla de verificación que aparece delante del nombre de archivo y haga clic en **Eliminar**. Cuando haya terminado de eliminar elementos, haga clic en **Aceptar**.

Análisis manual del equipo

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

Análisis manual para detectar virus y otras amenazas

Para analizar su equipo:

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

Se abrirá el cuadro de diálogo **Detectar virus** (Figura 2-8).

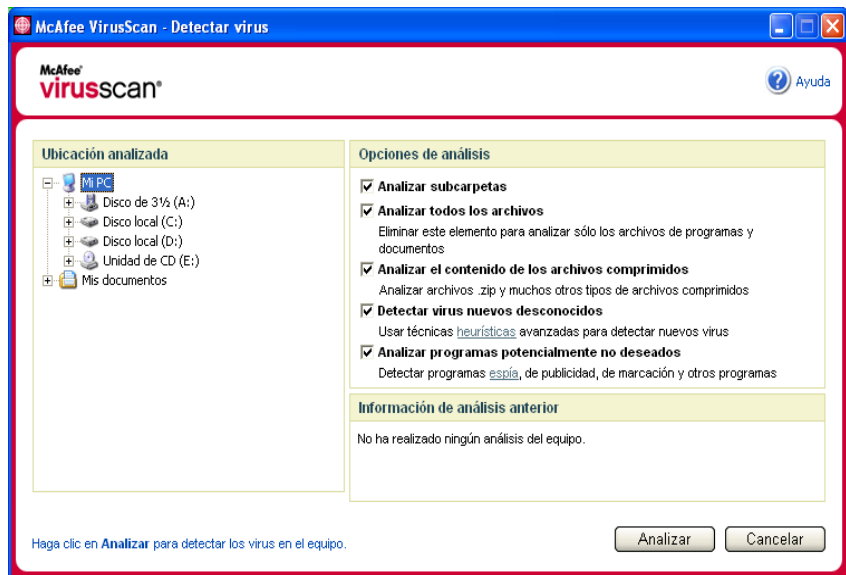


Figura 2-8. Cuadro de diálogo Detectar virus

- 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 2-8):

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

Ejemplo: Los archivos de Figura 2-9 son los únicos que se analizarán si se desmarca la casilla de verificación **Analizar subcarpetas**. Las carpetas y sus contenidos no se analizarán. Para analizar dichas carpetas y sus contenidos, debe dejar marcada la casilla de verificación.

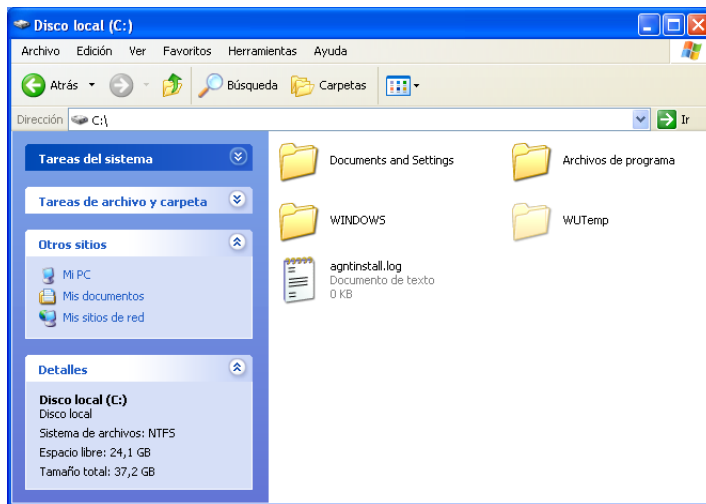


Figura 2-9. Contenido del disco local

- ♦ **Analizar todos los archivos:** utilice esta opción para realizar un análisis completo de todos los tipos de archivos. Desmarque esta casilla de verificación para reducir el tiempo de análisis y examinar únicamente los archivos de programas y documentos.
- ♦ **Analizar el contenido de los archivos comprimidos:** utilice esta opción para encontrar archivos ocultos infectados dentro de .ZIP y otros archivos comprimidos. Desmarque esta casilla de verificación para no analizar ningún archivo (comprimido o no) incluido dentro del archivo comprimido.

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

- ◆ **Detectar virus nuevos desconocidos:** utilice esta opción para encontrar los virus más recientes, para los que puede suceder que no se haya desarrollado aún 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 normalmente puedan descartar la existencia de virus. De esta manera se minimizan las posibilidades de que la función Analizar genere una falsa alarma. Sin embargo, si un análisis heurístico detecta un virus, el archivo se debería tratar con la misma precaución como si se supiera con certeza que contiene un virus.

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

- ◆ **Analizar programas potencialmente no deseados:** utilice esta opción para detectar software espía, de publicidad, de marcación y otros programas que no deseaba instalar en el 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 completarse. Cuanto mayor sea el tamaño del disco duro y más archivos contenga, más tiempo llevará la operación de análisis.

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

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

- Haga clic en **Aceptar** para cerrar el resumen y ver la lista de los archivos detectados en el cuadro de diálogo **Detectar virus** (Figura 2-10).

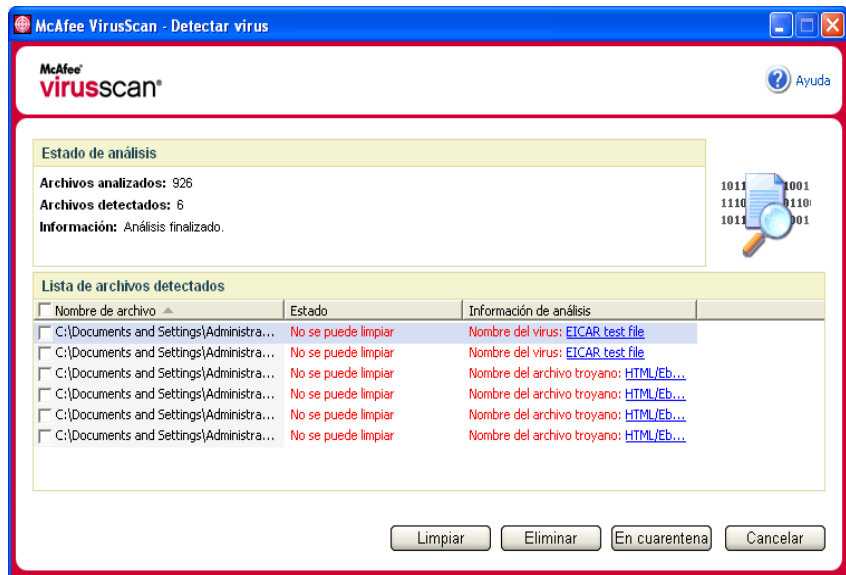


Figura 2-10. Resultados del análisis

NOTA

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

- Si Analizar no detecta ningún virus ni 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 *Descripción de la detección de amenazas 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 el Explorador de Windows.

Para analizar archivos desde 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 después haga clic en **Detectar virus**.

Se abrirá el cuadro de diálogo **Detectar 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 2-8 en la página 33](#)).

Análisis desde Microsoft Outlook

VirusScan proporciona un icono de la barra de herramientas para analizar la presencia de virus y 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 desde el propio Microsoft Outlook 97 o una versión posterior.

Para analizar el correo electrónico en Microsoft Outlook:

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

Se abrirá el analizador de correo electrónico y empezará a analizar los archivos. De manera predeterminada, todas las **Opciones de análisis** están preseleccionadas para aplicar el análisis más completo ([figura 2-8 en la página 33](#)).

Análisis automático para detectar virus y otras amenazas

Aunque VirusScan analiza los archivos cuando el usuario o el equipo acceden a ellos, se puede programar la función de análisis automático para que el Programador de tareas de Windows analice 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 2-11 en la página 38).

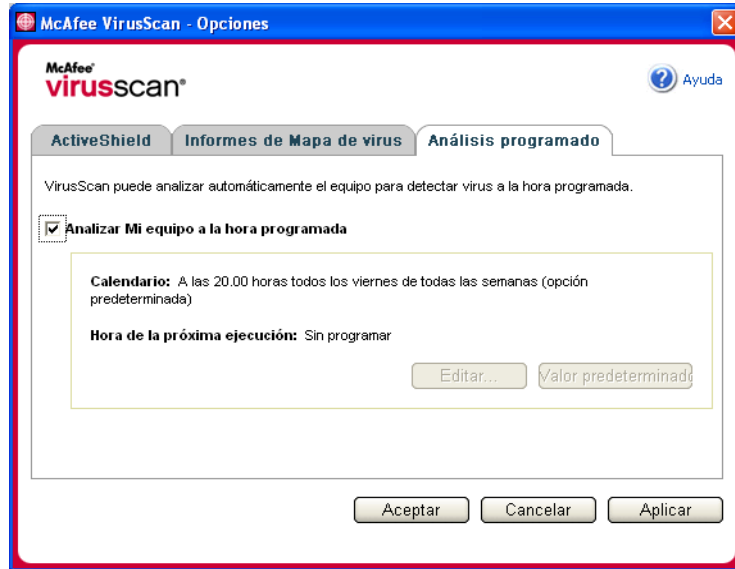


Figura 2-11. Opciones del análisis programado

- 3 Marque la casilla de verificación **Analizar mi equipo a la hora programada** para activar el análisis automático.
- 4 Especifique una programación para el análisis automático:
- ◆ Para aceptar la programación predeterminada (los viernes a las 20:00 horas), haga clic en **Aceptar**.
 - ◆ Para modificar la programación:
 - a. Haga clic en **Editar**.
 - b. Seleccione la frecuencia con la que desea analizar el equipo en la lista **Programar tarea** y seleccione las opciones adicionales en el área dinámica situada debajo:

Diaria: especifique el número de días entre análisis.

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

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

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

- 5 Haga clic en **Aceptar** para guardar los cambios y cerrar el cuadro de diálogo. En caso contrario, haga clic en **Cancelar**.
- 6 Si desea restablecer la programación predeterminada, haga clic en **Valor predeterminado**. De lo contrario, haga clic en **Aceptar**.

Descripción de la detección de amenazas

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

Para gestionar un virus o un programa potencialmente no deseado:

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

NOTA

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

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

- 3 Si Analizar no consigue limpiar el archivo, haga clic en **En cuarentena** para cifrar y aislar temporalmente los archivos infectados y sospechosos en el directorio de cuarentena hasta que se pueda tomar una acción oportuna. (Consulte *Gestión de archivos en cuarentena en la página 40* 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 Analizar no puede limpiar ni eliminar el archivo detectado, consulte la biblioteca de información de virus en <http://us.mcafee.com/virusInfo/default.asp> para obtener instrucciones sobre la eliminación manual de archivos.

Si el archivo detectado no permite utilizar la conexión a Internet o impide usar el equipo, pruebe a utilizar un disco de emergencia para iniciarlo. En muchos casos, el disco de emergencia permite iniciar un equipo inutilizado por un archivo detectado. Consulte la sección *Creación de un disco de emergencia en la página 42* para obtener información más detallada.

Para obtener más ayuda, consulte al servicio de asistencia técnica de McAfee en <http://www.mcafeeayuda.com/>.

Gestión de archivos en cuarentena

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

Para gestionar un archivo que se ha puesto en cuarentena:

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

Aparecerá una lista de archivos en cuarentena (Figura 2-12).

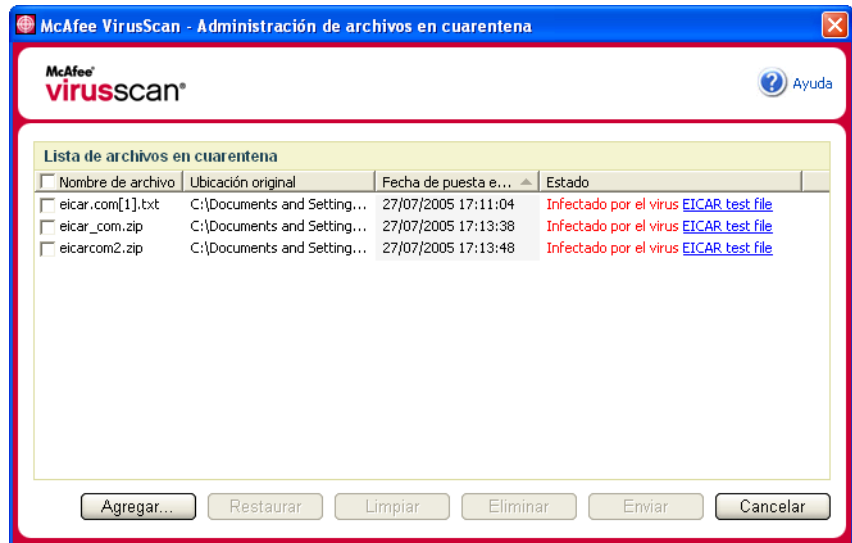


Figura 2-12. Cuadro de diálogo Gestionar archivos en cuarentena

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

NOTA

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

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

- 3 Haga clic en **Limpiar**.
- 4 Si el archivo está limpio, haga clic en **Restaurar** para devolverlo a su ubicación original.
- 5 Si VirusScan no puede limpiar el virus, haga clic en **Eliminar** para eliminar el archivo.

- 6 Si VirusScan no puede limpiar ni eliminar el archivo, y si no se trata de un programa potencialmente no deseado, puede enviarlo para su investigación a AVERT™ (siglas en inglés de McAfee AntiVirus Emergency Response Team o Equipo de respuesta de emergencia antivirus de McAfee):
 - a Actualice los archivos de definición de virus si tienen más de dos semanas de antigüedad.
 - b Compruebe su suscripción.
 - c Seleccione el archivo y haga clic en **Enviar** para enviar el archivo a AVERT.

VirusScan envía el archivo en cuarentena como archivo adjunto de 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 del envío es de un archivo de 1,5 MB por día.
- 7 Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin aplicar ninguna otra medida.

Creación de un disco de emergencia

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

NOTA

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

Para crear un disco de emergencia:

- 1 Inserte un disquete no infectado en la unidad A de un equipo no infectado. Puede utilizar la función Analizar para asegurarse de que el equipo y el disquete están libres de virus. (Consulte [Análisis manual para detectar virus y otras amenazas en la página 33](#) para obtener más información.)

- 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 2-13).



Figura 2-13. Cuadro de diálogo Crear disco de emergencia

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

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

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

- 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.

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

Protección de un disco de emergencia contra escritura

Para proteger un disco de emergencia contra escritura:

- Dé la vuelta al disquete (debería ver el círculo metálico del disquete).
- Busque la pestaña de protección contra escritura. Deslice la pestaña de manera que se vea el orificio.

Utilización de un disco de emergencia

Para usar un disco de emergencia:

- 1 Apague el equipo infectado.
- 2 Inserte el disco de emergencia en la unidad.
- 3 Encienda el equipo.

Aparecerá una ventana de color gris con varias opciones.

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

NOTA

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

Actualización de un disco de emergencia

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

Información automática sobre virus

Puede enviar información de rastreo de virus de manera anónima para su inclusión en el World Virus Map. Participe automáticamente en esta función de protección gratuita durante la instalación de VirusScan (en el cuadro de diálogo **Informes 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 2-14).

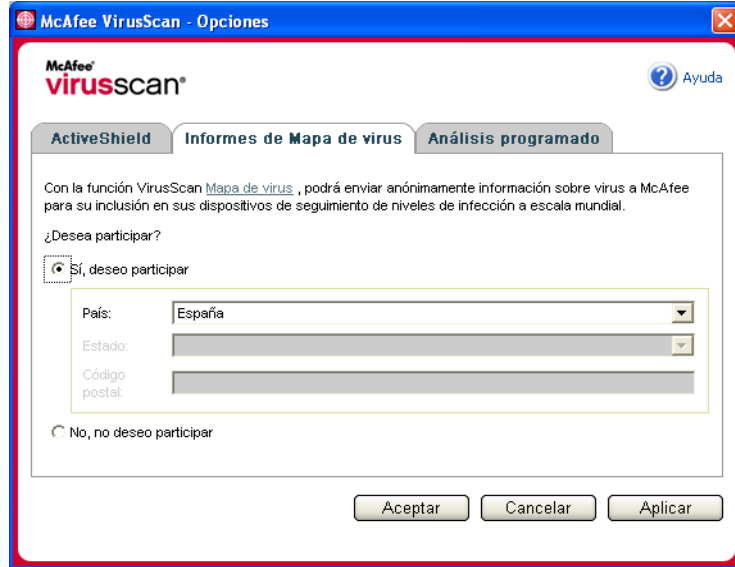


Figura 2-14. Opciones de informes del mapa de virus

- 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 impedir el envío de información.
- 4 Si reside en los Estados Unidos, seleccione el estado y escriba el código postal correspondiente a la ubicación física del equipo. En caso contrario, VirusScan tratará de seleccionar automáticamente el país en el que se encuentra el equipo.
- 5 Haga clic en **Aceptar**.

Visualización del World Virus Map

Aunque no participe 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 2-15).

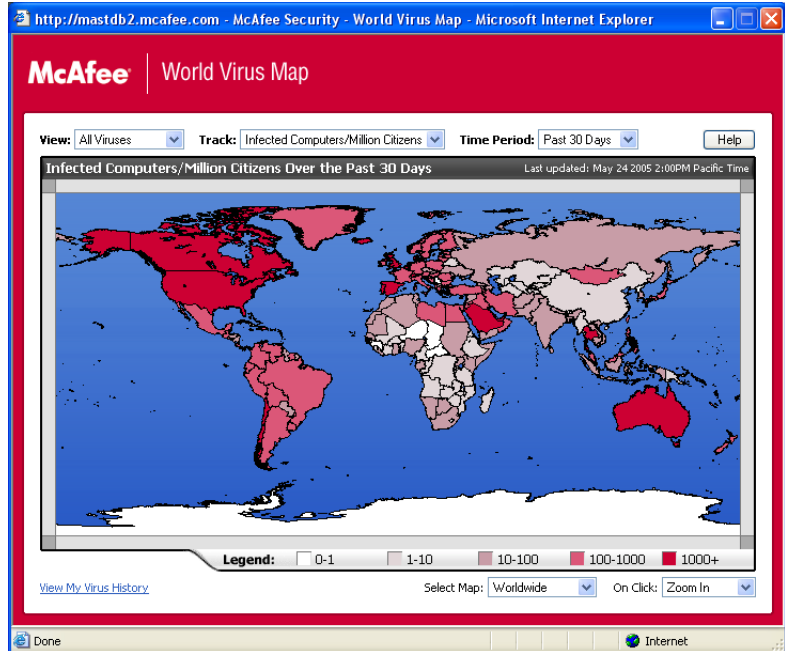


Figura 2-15. World Virus Map

De manera predeterminada, el World Virus Map muestra el número de equipos infectados en todo el mundo en los últimos 30 días y en el momento en el que se actualizó la información por última vez. 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 su descarga apenas afecta al rendimiento del sistema.

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

Comprobación automática de actualizaciones

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

NOTA

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

Comprobación manual de actualizaciones

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

Para comprobar manualmente la existencia de actualizaciones de VirusScan:

- 1 Asegúrese de que 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 de diálogo **Actualizaciones de VirusScan** (figura 2-16 en la página 48). 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.

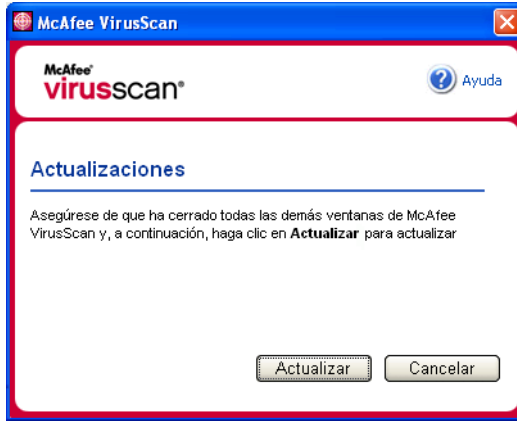


Figura 2-16. Cuadro de diálogo Actualizaciones

- 4 Regístrese en el sitio Web si así se le pide. El **Asistente para actualizaciones** instalará la actualización automáticamente.
- 5 Haga clic en **Finalizar** cuando la actualización haya terminado de instalarse.

NOTA

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

Bienvenido a McAfee Personal Firewall Plus.

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

Gracias a él, disfrutará de las funciones siguientes:

- Protección contra potenciales ataques e intentos de ataque de los piratas informáticos.
- Complemento de defensas antivirus.
- Control 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 sucesos recibidos.
- Funciones de rastreo y búsqueda de eventos.

Funciones nuevas

- **Mejoras en soporte para juegos**
McAfee Personal Firewall Plus protege su equipo de intentos de intrusión y actividades sospechosas en los juegos a toda pantalla, pero puede ocultar alertas si detecta intentos de intrusión o actividades sospechosas. Las alertas rojas aparecen después de salir del juego.
- **Mejoras en la gestión del acceso**
McAfee Personal Firewall Plus permite a los usuarios conceder a las aplicaciones acceso temporal a Internet. El acceso se restringe al lapso de tiempo desde el momento en el que se inicia la aplicación hasta cuando se cierra. Cuando Personal Firewall detecta un programa desconocido, que trata de comunicarse con Internet, una Alerta roja ofrece la opción de conceder a la aplicación acceso temporal a Internet.

- **Mejoras en el control de la seguridad**

Si se utiliza la función Bloqueado en McAfee Personal Firewall Plus podrá bloquear de manera instantánea todo el tráfico de Internet entrante y saliente entre su equipo e Internet. Los usuarios pueden activar o desactivar la función Bloqueado desde tres lugares diferentes de Personal Firewall.
- **Mejoras en las opciones de recuperación**

Puede ejecutar Restablecer opciones para restablecer automáticamente la configuración predeterminada de Personal Firewall. Si Personal Firewall muestra un comportamiento extraño que no puede corregir, puede decidir cambiar la configuración actual y volver a la configuración predeterminada del producto.
- **Protección contra la conexión a Internet**

Para impedir que un usuario desactive de manera accidental su conexión a Internet, la opción de prohibir una dirección de Internet se excluye de una Alerta azul cuando Personal Firewall detecta una conexión que se origina de un servidor DHCP o DNS. Si el tráfico entrante no se origina en un servidor DHCP o DNS, aparece la opción.
- **Integración mejorada con HackerWatch.org**

Ahora resulta más fácil que nunca informar sobre 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.
- **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**

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

McAfee Personal Firewall Plus incluye un Asistente para la configuración y un tutorial para guiar a los usuarios durante la configuración y utilización del cortafuegos. Aunque el producto está diseñado para su uso sin necesidad de intervención del usuario, McAfee ofrece a los usuarios un 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 controla todos los paquetes de datos en busca de transferencias de datos o métodos de transferencia que resulten sospechosos, y los incluye en el registro de eventos.

- **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 sobre las aplicaciones que pudieran mostrarse susceptibles de intrusión.

Eliminación de otros cortafuegos

Antes de instalar McAfee Personal Firewall Plus, es necesario eliminar 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 se detecta que en éste se está ejecutando Windows Firewall.

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 a través del Centro de seguridad de Windows o del Panel de control de Windows, 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 registre dichos eventos. Sin embargo, es posible que McAfee Personal Firewall bloquee tráfico adicional en función de otros factores de seguridad, y quedará un registro de dicho tráfico.

El registro está desactivado en 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**. 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 sobre el icono de McAfee  de la bandeja del sistema de Windows, señale **Personal Firewall** y, a continuación, seleccione **Opciones**.
- 2 Haga clic en el icono **Configuración de seguridad**.
- 3 Configure el nivel de seguridad moviendo el control deslizante hasta el valor deseado.

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

- ◆ **Bloqueado** — Se cierran todas las conexiones a Internet del equipo. Puede utilizar esta opción para bloquear puertos que configuró para estar abiertos en la página Servicios del sistema.
- ◆ **Seguridad estricta** — Cuando una aplicación solicita un tipo de acceso a Internet específico (por ejemplo, Sólo acceso saliente), puede permitir o no que la aplicación se conecte a Internet. Si la aplicación solicita más adelante Acceso pleno, puede concedérselo o restringirlo a Sólo acceso saliente.
- ◆ **Seguridad estándar (recomendado)** — cuando una aplicación solicita y se le concede acceso a Internet, la aplicación disfruta de acceso pleno a Internet para gestionar el tráfico entrante y saliente.
- ◆ **Seguridad fiable** — se confía automáticamente en todas las aplicaciones cuando intentan acceder por primera vez a Internet. Sin embargo, puede configurar Personal Firewall para utilizar alertas que le notifiquen sobre nuevas aplicaciones en su equipo. Utilice este valor si percibe que algunos juegos o medios de transferencia no funcionan.
- ◆ **Abierto** — el cortafuegos está desactivado. Este valor de configuración permite todo el tráfico a través de Personal Firewall sin ningún tipo de filtro.

NOTA

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

- 4 Seleccione configuración de seguridad adicional:

NOTA

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

- ◆ **Eventos de detección de intrusión (IDS) en Registro de eventos entrantes** —si selecciona esta opción, los eventos detectados por IDS aparecerán en el registro 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 no selecciona esta opción, Personal Firewall bloquea todas las solicitudes de ping y las registra en el registro de eventos entrantes.
- ◆ **Permitir a usuarios restringidos cambiar la configuración de Personal Firewall** — si el equipo dispone de Windows XP o Windows 2000 Professional con varios usuarios de XP, seleccione esta opción para permitir que los usuarios de XP restringidos modifiquen la configuración de Personal Firewall.

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

Comprobación de McAfee Personal Firewall Plus

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

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

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

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

Acerca de la página Resumen

El Resumen de Personal Firewall contiene cuatro páginas de resumen:

- ◆ Resumen principal
- ◆ Resumen de la aplicación

- ◆ Resumen de evento
- ◆ Resumen de HackerWatch

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

Para abrir la página Resumen principal en Personal Firewall:





- Haga clic con el botón derecho del ratón sobre el icono de McAfee  de la bandeja del sistema de Windows, señale **Personal Firewall** y, a continuación, seleccione **Ver resumen** (Figura 3-1).



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

La página Resumen principal contiene los datos siguientes:

Elemento	Descripción
Configuración de seguridad	El estado de la configuración de seguridad muestra el nivel de seguridad definido para el cortafuegos. Haga clic en el vínculo para cambiar el nivel de seguridad.
Eventos bloqueados	El estado de los eventos bloqueados muestra el número de eventos que se han bloqueado en el día actual. Haga clic en el vínculo para ver detalles de eventos procedentes de la página Eventos entrantes.
Cambios de reglas de aplicación	El estado de las reglas de aplicación muestra el número de reglas de aplicación que han cambiado recientemente. Haga clic en el vínculo para ver la lista de aplicaciones permitidas y bloqueadas, así como para modificar los permisos de las aplicaciones.
Novedades	Novedades muestra la última aplicación a la que se concedió acceso pleno a Internet.
Último evento	Último evento muestra los eventos entrantes más recientes. Haga clic en un vínculo para rastrear el evento o definir la dirección IP como fiable. Esta última acción permitirá que todo el tráfico procedente de 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:

- 1 Haga clic con el botón secundario del ratón sobre el icono de McAfee  de la bandeja del sistema de Windows, señale **Personal Firewall** y, a continuación, seleccione **Ver resumen**.
- 2 Haga clic en **Cambiar vista** y, a continuación, seleccione **Resumen de aplicaciones**.

La página Resumen de la aplicación contiene los datos siguientes:

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

Para ver la página Resumen de evento:


- 1 Haga clic con el botón secundario del ratón sobre el icono de McAfee  de la bandeja del sistema de Windows, señale **Personal Firewall** y, a continuación, seleccione **Ver resumen**.
- 2 Haga clic en **Cambiar vista** y, a continuación, seleccione **Resumen de eventos**.

La página Resumen de evento contiene 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.

Elemento	Descripción
Infractores principales	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:

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


La página Resumen de HackerWatch incluye 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.
Rastreo de eventos	Rastreo de eventos muestra el número de eventos entrantes enviados a HackerWatch.org.
Actividad mundial de los puertos	Actividad mundial de puertos muestra los puertos que han recibido un mayor número de amenazas en los últimos cinco días. Haga clic en un puerto para ver su número y descripción.
Tareas comunes	Haga clic en un vínculo de Tareas comunes para ir a las páginas de HackerWatch.org, donde podrá obtener información adicional sobre las actividades de piratería a escala mundial.

Información acerca de la página Aplicaciones de Internet

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

Para iniciar la página Aplicaciones de Internet:

- Haga clic con el botón derecho del ratón sobre el icono de McAfee  de la bandeja del sistema de Windows, señale **Personal Firewall** y, a continuación, seleccione **Aplicaciones** (Figura 3-2).

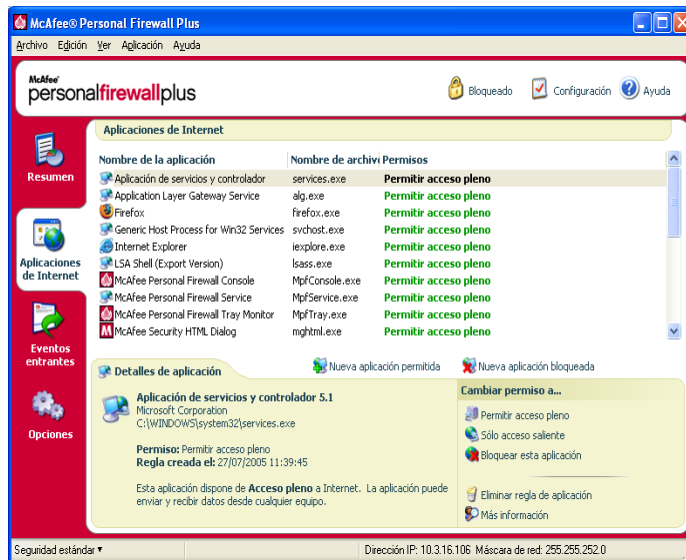


Figura 3-2. Página Aplicaciones de Internet

La página Aplicaciones de Internet contiene los datos siguientes:

- Nombres de aplicaciones
- Nombres de archivo
- Niveles de permiso actuales
- Detalles de la aplicación: nombre y versión de la aplicación, nombre de la compañía, nombre de la ruta, permiso, fechas y horas del evento y explicaciones de los tipos de permisos.

Cambiar reglas de aplicación

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


Para cambiar una regla de aplicación:

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

NOTA

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


Para eliminar una regla de aplicación:

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

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

Permitir y bloquear el acceso a aplicaciones de Internet

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


- 1 Haga clic con el botón secundario del ratón sobre el icono de McAfee  de la bandeja del sistema de Windows, señale **Personal Firewall** y, a continuación, seleccione **Aplicaciones de Internet**.
- 2 En la página Aplicaciones de Internet, haga clic en una de las siguientes opciones:
 - ♦ **Nueva aplicación permitida:** permitir que la aplicación acceda por completo a Internet.

- ◆ **Nueva aplicación bloqueada:** prohibir que una aplicación acceda a Internet.
- ◆ **Eliminar regla de aplicación:** eliminar una 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 las conexiones a Internet no solicitadas.

Para abrir la página Eventos entrantes:

- Haga clic con el botón derecho del ratón sobre el icono de McAfee  de la bandeja del sistema de Windows, señale **Personal Firewall** y, a continuación, seleccione **Eventos entrantes** (Figura 3-3).

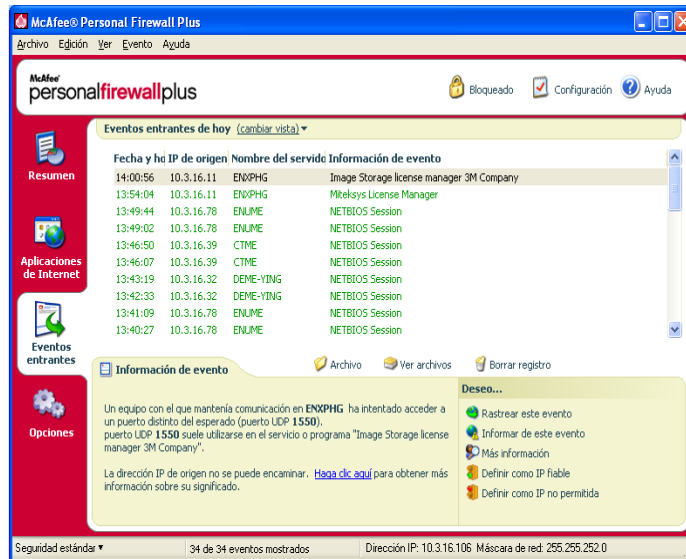


Figura 3-3. Página Eventos entrantes

La página Eventos entrantes incluye los datos siguientes:

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

Explicación de los eventos

Información acerca de las direcciones IP

Las direcciones IP están compuestas por números: 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.

Tipos de direcciones IP

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

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

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

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

Eventos de 127.0.0.1

Los eventos a veces enumerarán su IP de origen como 127.0.0.1. Esto se conoce como una dirección de bucle invertido o host local.

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

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

Algunos programas, principalmente Netscape 6.2 y 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 a determinado tráfico malintencionado.

Eventos procedentes de equipos de la LAN

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

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

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

Eventos procedentes de direcciones IP privadas

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

El bloque 192.168.xxx.xxx se utiliza con 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 se informará acerca de estos eventos, ya que no serviría de nada.

Visualización de eventos en el registro de eventos entrantes

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

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

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

Visualización de los eventos del día actual

Utilice esta opción para consultar los eventos del día.

Para mostrar los eventos del día actual:

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

Visualización de eventos de esta semana

Utilice esta opción para consultar los eventos de la semana.

Para mostrar los eventos de esta semana:

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

Visualización del registro completo de eventos entrantes

Utilice esta opción para consultar todos los eventos.

Para mostrar todos los eventos del registro de eventos entrantes:

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

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

Visualización de los eventos de un día concreto

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

Para mostrar los eventos de un día concreto:

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

Visualización de los eventos de una dirección de Internet específica

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

Para mostrar los eventos de una dirección de Internet:

- 1 Haga clic con el botón derecho del ratón sobre el icono de McAfee de la bandeja del sistema de Windows, señale **Personal Firewall** y haga clic en **Eventos entrantes**.

- 2 En el registro de eventos entrantes, haga clic con el botón derecho en una entrada y, a continuación, haga clic en **Mostrar sólo eventos de una dirección de Internet concreta**.

Visualización de eventos que comparten la misma información de evento

Utilice esta opción para comprobar si existen otros eventos en el registro de eventos entrantes que presenten la misma información 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 eventos que comparten la misma información de evento:

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

Respuesta a eventos entrantes

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

Para rastrear un evento seleccionado:

- 1 Haga clic con el botón derecho del ratón sobre el icono de McAfee de la bandeja del sistema de Windows, señale **Personal Firewall** y seleccione **Eventos entrantes**.
- 2 En el registro de Eventos entrantes, haga clic con el botón derecho del ratón en el evento que desea rastrear y, a continuación, haga clic en **Rastrear evento seleccionado**. También puede hacer doble clic en el evento para rastrear un evento.

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

Obtención de consejos de HackerWatch.org

Para obtener consejos de HackerWatch.org:

- 1 Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall** y seleccione **Eventos entrantes**.
- 2 Seleccione la entrada del evento en la página Eventos entrantes y, a continuación, haga clic en **Obtener más información**. En el panel **Deseo**.

Se abrirá el navegador Web predeterminado y el sitio Web de HackerWatch.org para obtener información sobre el tipo de eventos y consejos sobre si debe informar al respecto.

Informar sobre un evento

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

- 1 Haga clic con el botón derecho del ratón sobre el icono de McAfee de la bandeja del sistema de Windows, señale **Personal Firewall** y seleccione **Eventos entrantes**.
- 2 Haga clic en el evento sobre el que desea informar y, a continuación, seleccione **Informar de este evento** en el panel **Deseo**.

Personal Firewall informa sobre el evento a 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 de eventos a HackerWatch.org sin necesidad de validar su identificación de usuario. Sin embargo, para filtrar eventos y mandarlos por correo electrónico a un amigo, deberá 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 proporcionadas. 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

Puede utilizar la página Eventos entrantes para agregar una dirección IP a la lista de direcciones IP fiables para permitir una conexión permanente.

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

Para agregar una dirección IP a la lista de IP fiables:

- 1 Haga clic con el botón derecho del ratón sobre el icono de McAfee de la bandeja del sistema de Windows, señale **Personal Firewall** y seleccione **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**.

Verifique que la dirección IP que muestra el cuadro de diálogo de confirmación de confianza en esta dirección es correcta y haga clic en **Aceptar**. La dirección IP se agregará a la lista de IP fiables.

Para verificar que la dirección IP se ha agregado:

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

La dirección IP aparecerá señalada en la lista de IP fiables.

Prohibición de una dirección

Una dirección IP que aparece 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 bloquearla.

Si detecta un evento en la página 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.

Puede utilizar la página Eventos entrantes, que enumera las direcciones IP de todo el tráfico entrante de Internet, para prohibir una dirección IP que sospeche es el origen de actividades de Internet no deseadas o sospechosas.

Para agregar una dirección IP a la lista de IP prohibidas:

- 1 Haga clic con el botón derecho del ratón sobre el icono de McAfee de la bandeja del sistema de Windows, señale **Personal Firewall** y, a continuación, seleccione **Eventos entrantes**.
- 2 En la página Eventos entrantes aparecen las direcciones IP de todo el tráfico de Internet entrante. Seleccione una dirección IP y, a continuación, lleve a cabo una de las siguientes acciones:
 - ♦ Haga clic con el botón derecho en la dirección IP y, a continuación, seleccione **Prohibir dirección IP de origen**.
 - ♦ En el menú **Deseo**, haga clic en **Prohibir esta dirección**.
- 3 En el cuadro de diálogo Agregar regla de direcciones IP no permitidas, utilice uno o más de los siguientes parámetros para configurar la dirección de IP prohibida:
 - ♦ **Una sola dirección IP:** la dirección IP que desea prohibir. La entrada predeterminada es la dirección IP que seleccionó en la página Eventos entrantes.
 - ♦ **Una serie de direcciones IP:** las direcciones IP entre la dirección especificada en De dirección IP y la dirección IP especificada en la A dirección IP.
 - ♦ **Caducidad de la regla:** fecha y hora en la que desea que caduque esta regla de dirección IP prohibida. Seleccione los menús desplegables apropiados para seleccionar la fecha y la hora.
 - ♦ **Descripción:** Si lo desea, describa la nueva regla.
 - ♦ Haga clic en **Aceptar**.
- 4 En el cuadro de diálogo, haga clic en **Sí** para confirmar la configuración. Haga clic en **No** para volver al cuadro de diálogo Regla Agregar dirección IP prohibida.

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

Para verificar que la dirección IP se ha agregado:

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

La dirección IP aparecerá señalada en la lista de 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 para guardar todos los eventos entrantes registrados, incluidas fechas y horas, IP de origen, nombres de host, puertos e información de eventos. Archive los registros de eventos entrantes periódicamente para evitar que el registro de eventos entrantes se haga demasiado grande.

Para archivar el registro de eventos entrantes:

- 1 Haga clic con el botón derecho del ratón sobre el icono de McAfee de la bandeja del sistema de Windows, señale **Personal Firewall** y, a continuación, seleccione **Eventos entrantes**.
- 2 En la página Eventos entrantes, haga clic en **Archivar**.
- 3 En el cuadro de diálogo Archivar registro, haga clic en **Sí** para continuar con la operación.
- 4 Haga clic en **Guardar** para guardar el archivo comprimido en la ubicación predeterminada, o bien diríjase a la ubicación en la que desea guardarlo.

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

Visualización del registro de eventos entrantes archivado

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

Para visualizar un registro de eventos entrantes archivado:

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

Borrado del registro de eventos entrantes

Puede borrar toda la información del registro de eventos entrantes.

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

Para borrar 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, seleccione **Eventos entrantes**.
- 2 En la página Eventos entrantes, haga clic en **Borrar registro**.
- 3 Haga clic en **Sí** en el cuadro de diálogo para borrar el registro.

Copia de un evento en el portapapeles

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

Para copiar eventos en el portapapeles:

- 1 Haga clic con el botón derecho en el icono de McAfee, seleccione la opción **Personal Firewall** y, a continuación, seleccione **Eventos entrantes**.
- 2 Haga clic con el botón secundario del ratón en el evento del registro de eventos entrantes.
- 3 Haga clic en **Copiar evento seleccionado en el portapapeles**.
- 4 Abra el Bloc de notas.
 - ♦ Escriba `notepad` en la línea de comando o haga clic en el botón **Inicio** de Windows, señale **Programas** y, a continuación, **Accesorios**. Seleccione **Bloc de notas**.
- 5 Haga clic en **Editar** y, a continuación, haga clic en Pegar. El texto de evento se mostrará en el Bloc de notas. Repita este paso hasta que tenga todos los eventos necesarios.
- 6 Guarde el archivo del Bloc de notas en un lugar seguro.

Eliminación del evento seleccionado

Puede eliminar eventos del registro de eventos entrantes.

Para eliminar eventos del registro de eventos entrantes:

- 1 Haga clic con el botón derecho del ratón sobre el icono de McAfee de la bandeja del sistema de Windows, señale **Personal Firewall** y, a continuación, seleccione **Eventos entrantes**.
- 2 Haga clic en la entrada de evento de la página Eventos entrantes que desee eliminar.
- 3 En el menú Edición, haga clic en **Eliminar elemento seleccionado**. El evento se borra del registro de eventos entrantes.

Acerca de las alertas

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

NOTA

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

Alertas rojas

Las alertas rojas contienen información importante que requiere atención inmediata.

- **Aplicación de Internet bloqueada:** esta alerta aparece cuando Personal Firewall bloquea el acceso a Internet de una aplicación. Por ejemplo, si aparece una alerta sobre un programa troyano, McAfee denegará automáticamente el acceso del programa a Internet y recomendará que se 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.
- **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, debe tener cuidado a la hora de concederle permiso de acceso a Internet.

- **La aplicación desea tener acceso de servidor:** esta alerta aparece cuando Personal Firewall detecta que una aplicación a la que previamente se le concedió permiso para acceder a Internet solicita acceder a Internet como servidor.

NOTA

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

IMPORTANTE

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

Alerta 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. Si McAfee VirusScan no se ha instalado, puede iniciar McAfee SecurityCenter.

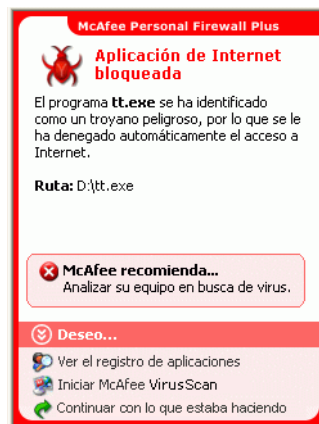


Figura 3-4. Alerta de aplicación de Internet bloqueada

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** 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.
- Haga clic en **Conceder acceso saliente** para permitir una conexión saliente (**Seguridad** estricta).

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

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

Alerta “La aplicación desea tener acceso 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.

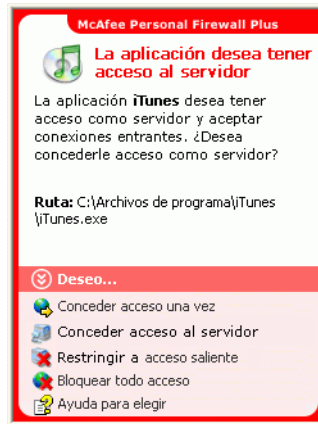


Figura 3-8. Alerta “La aplicación desea tener acceso al servidor”

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

Alertas verdes

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

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

Alerta “Programa con permiso de acceso a Internet”

Si selecciona el nivel de seguridad **Fiable** en las opciones de Configuración de seguridad, Personal Firewall concederá acceso a Internet de forma automática a todas las aplicaciones nuevas y se lo notificará mediante una alerta (Figura 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 estaba haciendo** si no desea aplicar otra medida aparte de la que tome Personal Firewall.
- Haga clic en **Bloquear todo acceso** para prohibir cualquier conexión a Internet.

Alerta de modificación de aplicación

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

- Haga clic en **Ver el registro de aplicaciones** para obtener detalles sobre el evento 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 estaba haciendo** si no desea aplicar otra medida aparte de la que tome Personal Firewall.
- Haga clic en **Bloquear todo acceso** para prohibir cualquier conexión a Internet.

Alertas azules

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

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

Alerta 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.

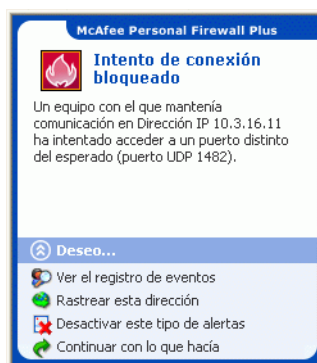


Figura 3-10. Alerta de intento de conexión bloqueado

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 **Confiar en esta dirección IP** para permitir que se acceda al equipo desde esta dirección.
- Haga clic en **Continuar con lo que estaba haciendo** si no desea aplicar otra medida aparte de la que tome Personal Firewall.

Bienvenido a McAfee Privacy Service.

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

Funciones

Esta versión de McAfee Privacy Service incluye las siguientes funciones:

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

Administrador

El administrador especifica qué usuarios pueden acceder a Internet, cuándo pueden hacerlo y qué pueden hacer en Internet.

NOTA

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

Asistente para la configuración

El Asistente para la configuración le permite crear el 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 poder iniciar la sesión en Privacy Service. Si no puede iniciar la sesión, no podrá 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 del administrador, podrá acceder a ella mediante la información de seguridad introducida al crear el perfil del administrador.

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


Usuario de inicio

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

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

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

Apertura de McAfee Privacy Service

Cuando se instala McAfee Privacy Service, el icono de McAfee  aparece 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 de McAfee instalados en el equipo.

Apertura e inicio de sesión de Privacy Service


Para abrir Privacy Service:

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

Desactivación de Privacy Service

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

Para desactivar Privacy Service:


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

NOTA

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


Actualización de McAfee Privacy Service

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

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

Adición de usuarios

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

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

Definición de la contraseña

- 1 Escriba una contraseña en el campo **Contraseña**. La contraseña puede tener un máximo de 50 caracteres e incluir letras en mayúscula y minúscula o 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 adolescente o a un adulto, ésta podrá ser más compleja.

Definición del grupo de edad

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

Configuración del bloqueador de cookies

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

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

- **Aceptar todos los cookies:** permite a los sitios Web leer los cookies que envían al equipo.

NOTA

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

Privacy Service acepta siempre cookies de McAfee.

Definición de límites de tiempo de acceso a Internet

Para permitir el uso de Internet sin restricciones:

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

Para permitir el uso de Internet restringido:

- 1 Seleccione **Restringir el uso de Internet** y haga clic en **Editar**.
- 2 En la página Límites de tiempo para Internet, arrastre el cuadrante temporal para seleccionar las horas y los días en que el usuario puede acceder a Internet. Puede especificar límites temporales en intervalos de treinta minutos. Las partes verdes del cuadrante corresponden a los periodos en que un usuario puede acceder a Internet. Las partes rojas se muestran cuando un usuario no puede acceder a Internet. Si un usuario intenta utilizar Internet cuando no tienen permiso para ello, Privacy Service muestra un mensaje advirtiendo al usuario que no tiene permiso para utilizar Internet en ese momento. Para modificar los periodos en los que un usuario puede acceder a Internet, arrastre las partes verdes del cuadrante.
- 3 Haga clic en **Listo**.
- 4 Haga clic en **Crear**. El usuario nuevo aparecerá en la página Seleccionar a un usuario. Si un usuario intenta utilizar Internet cuando no tienen permiso para ello, Privacy Service muestra un mensaje advirtiendo al usuario que no tiene permiso para utilizar Internet en ese momento.

Para prohibir el acceso a Internet:

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

Edición de usuarios

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

Cambio de contraseñas

- 1 Seleccione el usuario cuya información desee modificar y haga clic en **Editar**.
- 2 Seleccione **Contraseña** e introduzca la nueva contraseña del usuario en el campo **Nueva contraseña**. La contraseña puede tener un máximo de 50 caracteres e incluir letras en mayúscula y minúscula o números.
- 3 Escriba la misma contraseña en el campo **Confirmar contraseña** y haga clic en **Aplicar**.
- 4 Haga clic en **Aceptar** en el cuadro de dialogo de confirmación.

NOTA

Un administrador puede cambiar la contraseña de un usuario sin necesidad de conocer la contraseña en uso de ese usuario.

Cambio de la información de un usuario

- 1 Seleccione el usuario cuya información desee modificar y haga clic en **Editar**.
- 2 Seleccione **Información de usuario**.
- 3 Escriba el nuevo nombre de usuario en el campo **Nuevo nombre de usuario**.
- 4 Haga clic en **Aplicar** y después en **Aceptar**, en el cuadro de diálogo de confirmación.
- 5 Para restringir el acceso de un usuario a los sitios Web de la lista Sitios Web 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 cookies ilegibles a los sitios Web que los han enviado. Para funcionar correctamente, algunos sitios Web necesitan que los cookies estén activados.
 - ♦ **Preguntar al usuario si desea aceptar cookies:** permite al usuario decidir si desea aceptar o rechazar cada cookie de manera individual. Privacy Service notifica al usuario si el sitio Web que está a punto de visitar desea enviar cookies a su equipo. Después de haber realizado la elección, no se le volverá a preguntar acerca de ese cookie.

- ♦ **Aceptar todos los cookies:** permite a los sitios Web leer los cookies que envían al equipo.
- 3 Haga clic en **Aplicar** y después en **Aceptar**, en el cuadro de diálogo de confirmación.

Edición de la lista para aceptar y rechazar cookies

- 1 Seleccione **Preguntar al usuario si desea aceptar cookies** y haga clic en **Editar** para especificar los sitios Web que pueden leer cookies.
- 2 Especifique la lista que quiera modificar seleccionando **Sitios Web que pueden establecer cookies** o **Sitios Web que no pueden establecer cookies**.
- 3 En el campo **http://**, introduzca la dirección del sitio Web del que vaya a aceptar o rechazar cookies.
- 4 Haga clic en **Agregar**. El sitio 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 la página de Límites de tiempo para Internet, seleccione un cuadrado verde o rojo y arrástrelo en el cuadrante para cambiar las horas y los días definidos para que un usuario pueda acceder a Internet.
Puede especificar límites temporales en intervalos de treinta minutos. Las partes verdes del cuadrante corresponden a los periodos en que un usuario puede acceder a Internet. Las partes rojas se muestran cuando un usuario no puede acceder a Internet. Si un usuario intenta utilizar Internet cuando no tienen permiso para ello, Privacy Service muestra un mensaje advirtiendo al usuario que no tiene permiso para utilizar Internet en ese momento.
- 3 Haga clic en **Aplicar**.
- 4 En la página Límites de tiempo, haga clic en **Aceptar**.
- 5 En el cuadro de diálogo de configuración de McAfee Privacy Service, haga clic en **Aceptar**.

Cambio 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 después 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 de Privacy Service cuando haya terminado de realizar cambios.

Opciones

Para configurar las opciones de Privacy Service, deberá iniciar la 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://**, escriba la URL del sitio Web que quiera bloquear y después haga clic en **Agregar**. El sitio aparecerá en la lista **Sitios Web bloqueados**.

NOTA

Los usuarios (incluidos los administradores) 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. Para probar los sitios bloqueados, los administradores deberán iniciar la sesión como usuarios no adultos.

Permiso de acceso a sitios Web

El administrador puede permitir a todos los usuarios que visiten sitios Web específicos. De esta forma se anula la configuración predeterminada de Privacy Service y los sitios Web agregados a la lista de sitios bloqueados.

- 1 Haga clic en **Opciones** y seleccione **Lista para permitir**.
- 2 En el campo **http://**, escriba la URL del sitio Web que quiera permitir y después haga clic en **Agregar**. El sitio 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 seguir enviando esa información).

Cuando Privacy Service detecte información personal identificable (PII, del inglés Personal Identifiable Information) en algún elemento que vaya a ser enviado, sucederá lo siguiente:

- Si el usuario es un administrador, se le preguntará y podrá decidir si desea enviar o no la información.
- Si el usuario que tiene la sesión iniciada no es el administrador, la información bloqueada será sustituida con *MFEMFEMFE*. Por ejemplo, si se envía el correo electrónico *Lance Armstrong gana el tour* y Armstrong está definido como información personal que se debe bloquear, el correo que se envía en realidad es *Lance MFEMFEMFE gana el tour*.

Adición de información

- 1 Haga clic en **Opciones** y seleccione **Información para bloquear**.
- 2 Haga clic en **Agregar**. Se mostrará el menú desplegable **Seleccionar tipo**.
- 3 Seleccione el tipo de información que desee bloquear.
- 4 Escriba la información en los campos adecuados y haga clic en **Aceptar**. La información introducida se mostrará 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 necesarios y después haga clic en **Aceptar**. Si no es preciso 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 **Eliminar**.
- 3 Haga clic en **Sí** en el cuadro de diálogo de confirmación.

Bloqueo de Web bugs

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

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

Bloqueo de anuncios

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

Las ventanas emergentes son ventanas secundarias del navegador que contienen anuncios no deseados que se muestran automáticamente al visitar un 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 y actualice la página Web.

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

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

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

Admisión de cookies de sitios Web específicos

Si bloquea los cookies o si se le pregunta antes de aceptarlos y detecta que determinados sitios Web no funcionan correctamente, deberá configurar Privacy Service para que permita que el sitio Web lea los cookies correspondientes.

- 1 Haga clic en **Opciones** y seleccione **Cookies**.
- 2 En el campo **http://**, escriba la dirección del sitio Web que tenga que leer los cookies correspondientes y después haga clic en **Agregar**. El sitio aparecerá en la lista **Aceptar cookies de sitios Web**.

Registro de eventos

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

Fecha y hora

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

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

Usuario

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

Resumen

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

Detalles del evento

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

Almacenamiento del registro de eventos activo

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

Para guardar el registro de eventos activo

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

Visualización de registros guardados

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

Para ver un registro guardado


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

Utilidades

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

Para eliminar archivos, carpetas o todo el contenido de los discos, haga clic en **McAfee Shredder**. Para guardar la configuración de la base de datos de Privacy Service, haga clic en **Copia de seguridad**. Para restaurar la configuración, haga clic en **Restaurar**.

Eliminación de archivos de manera permanente mediante McAfee Shredder

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

Puede recuperar los archivos eliminados incluso después de vaciar la Papelera de reciclaje. Cuando se elimina un archivo, Windows sólo marca ese espacio en la unidad de disco como espacio que ya no está en uso, pero el archivo sigue ahí.

Por qué Windows conserva restos de archivos

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

NOTA

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

Qué borra McAfee Shredder

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

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

Eliminación permanente de los archivos del Explorador de Windows

Para purgar archivos mediante el Explorador de Windows:

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

Vaciado de la Papelera de reciclaje de Windows

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

Para purgar el contenido de la Papelera de reciclaje:

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

Personalización de la configuración de Shredder

Puede realizar lo siguiente:

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

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

Copia de seguridad de la base de datos de Privacy Service

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

- 1 Haga clic en **Utilidades** y seleccione **Copia de seguridad**.
- 2 Haga clic en **Examinar** para seleccionar la ubicación del archivo de la base de datos y haga clic en **Aceptar**.

- 3 Escriba una contraseña en el campo **Contraseña**.
- 4 Introduzca de nuevo la contraseña en el campo **Confirmar contraseña** y haga clic en **Copia de seguridad**.
- 5 Haga clic en **Aceptar** en el cuadro de dialogo de confirmación.
- 6 Cierre la ventana de Privacy Service cuando haya terminado.

NOTA

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

Restauración de la base de datos desde la copia de seguridad

- 1 Puede restaurar la configuración original de Privacy Service de dos formas.
 - ♦ Cargando el archivo de copia de seguridad de la base de datos cuando Privacy Service le solicite que restaure la configuración porque la base de datos se ha dañado o eliminado.
 - ♦ Cargando el archivo de copia de seguridad de la base de datos mientras se esté ejecutando Privacy Service.

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

- 1 Haga clic en **Examinar** para localizar el archivo.
- 2 Escriba la contraseña en el campo **Contraseña**.
- 3 Haga clic en **Restaurar**.
Si no ha realizado una copia de seguridad de la base de datos de Privacy Service, si ha olvidado la contraseña de la copia de seguridad o si la restauración de la base de datos no funciona, deberá desinstalar y volver a instalar Privacy Service.

Para restaurar la configuración de Privacy Service mientras se esté ejecutando:

- 1 Haga clic en la ficha **Utilidades**.
- 2 Haga clic en **Restaurar**.
- 3 Haga clic en **Examinar** y escriba la ruta y el nombre del archivo de copia de seguridad.
- 4 Haga clic en **Abrir**.
- 5 Escriba la contraseña en el campo **Contraseña**.
- 6 Haga clic en **Restaurar** y después en **Aceptar** en el cuadro de diálogo de confirmación de McAfee Privacy Service.

Opciones de usuario

Estas instrucciones no se aplican al administrador.

Puede cambiar su nombre de usuario y su contraseña. Recomendamos que cambie la contraseña cuando el administrador se la proporcione. También 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 contraseña en el campo **Contraseña antigua**.
- 3 Escriba la contraseña nueva en el campo **Nueva contraseña**.
- 4 Vuelva a escribir la nueva contraseña en el campo **Confirmar contraseña** y haga clic en **Aplicar**.
- 5 Haga clic en **Aceptar** en el cuadro de dialogo de confirmación. Dispondrá así 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 Escriba un nombre de usuario nuevo en el campo **Nombre nuevo de usuario** y haga clic en **Aplicar**.
- 4 Haga clic en **Aceptar** en el cuadro de dialogo de confirmación. Dispondrá así de un nuevo nombre de usuario.

Vaciado de la caché

Recomendamos que vacíe la memoria caché para evitar que los niños puedan acceder a las páginas Web que haya visitado recientemente. Para vaciar la caché, haga lo siguiente.

- 1 Abra Internet Explorer.
- 2 En el menú **Herramientas**, haga clic en **Opciones de Internet** para acceder al cuadro de diálogo Opciones de Internet.

- 3 En la sección **Archivos temporales de Internet**, haga clic en **Eliminar archivos**. Se abrirá el cuadro de diálogo Eliminar archivos.
- 4 Seleccione **Eliminar todo el contenido sin conexión** y haga clic en **Aceptar**.
- 5 Haga clic en **Aceptar** para cerrar el cuadro de diálogo Opciones de Internet.

Admisión de cookies

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

Si accede a sitios Web que requieran cookies, puede permitir que esos 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 Escriba la URL del sitio Web en el campo **http://** y haga clic en **Agregar**. El sitio aparecerá en la lista de sitios Web.

Si necesita eliminar un sitio Web de la lista:

- 1 Seleccione la URL del sitio en la lista de sitios Web.
- 2 Haga clic en **Eliminar** y después en **Sí**, en el cuadro de diálogo de confirmación.

Rechazo de cookies

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

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

- 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 Escriba la URL del sitio Web en el campo **http://** y haga clic en **Agregar**. El sitio aparecerá en la lista de sitios Web.

Si necesita eliminar un sitio Web de la lista:

- 1 Seleccione la URL del sitio en la lista de sitios Web.
- 2 Haga clic en **Eliminar** y después en **Sí**, en el cuadro de diálogo de confirmación.

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:

Funciones

Esta versión de SpamKiller ofrece las siguientes funciones:

- **Filtrado:** las opciones avanzadas de filtrado proporcionan nuevas técnicas de filtrado, incluido soporte para filtrado por metacaracteres e identificación de texto basura.
- **Phishing:** el complemento del navegador de AntiPhishing a través de la barra de herramientas de Internet Explorer identifica con facilidad los sitios Web potenciales de phishing y los bloquea.
- **Integración con Microsoft Outlook y Outlook Express:** la barra de herramientas proporciona una carpeta en el cliente de correo para bloquear directamente el correo no deseado.
- **Instalación:** configuración e instalación mejorada. La detección automática de cuentas asegura una instalación, configuración e integración sin problemas con las cuentas de correo electrónico existentes.
- **Actualizaciones:** las actualizaciones automáticas se ejecutan en segundo plano sin que el usuario lo perciba y siempre están activas para minimizar la exposición a las posibles amenazas de correo basura emergentes.
- **Interfaz:** una interfaz de usuario intuitiva para mantener al equipo libre de correo basura.
- **Soporte técnico:** gratuito y en directo por correo electrónico y mensajería instantánea, para ofrecer una atención al cliente directa, fácil y rápida.

Procesamiento de mensajes basura: de forma predeterminada, los mensajes basura son etiquetados como [CORREO BASURA] y se colocan en la carpeta SpamKiller en Outlook y Outlook Express, o en la bandeja de entrada. Los mensajes etiquetados también aparecen en la página de correos aceptados.

Opciones de usuario


- Bloquear el correo basura con filtros y ponerlo en cuarentena fuera de su buzón de entrada.
- Ver 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.
- Compatibilidad con juegos de caracteres de doble byte.
- Admitir a 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.


Descripción del panel superior


Los iconos siguientes aparecen en el panel superior de cada página de SpamKiller:

- Haga clic en **Cambiar usuario**  para iniciar una sesión como otro 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.

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


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

Cuando se instala SpamKiller, el icono de McAfee  aparece en la bandeja del sistema, cerca del reloj del sistema. Mediante este icono se puede acceder a SpamKiller, McAfee SecurityCenter y otros productos de McAfee instalados en el equipo.

Desactivación de SpamKiller

Puede desactivar SpamKiller para evitar que se filtren los mensajes de correo electrónico.

Para desactivar el filtrado:

Haga clic con el botón derecho sobre el icono de McAfee , seleccione **SpamKiller** y haga clic en **Desactivar**. O haga clic en la ficha **Resumen** y luego en **Haga clic aquí para desactivar**.

Para activar el filtrado:

Haga clic con el botón derecho sobre el icono de McAfee, seleccione **SpamKiller** y haga clic en **Activar**. O haga clic en la ficha **Resumen** y luego en **Haga clic aquí para activar**.

Descripción de la página de resumen

Haga clic en la ficha **Resumen** para abrir la página de resumen (Figura 5-11).

- **Información general sobre el estado de SpamKiller:** indica si está activado el filtrado, cuando se activó por última vez una lista de amigos y el número de 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.
- **Correos más recientes identificados como correos basura y bloqueados:** los mensajes de correo basura que SpamKiller ha bloqueado más recientemente (mensajes retirados del buzón de entrada).
- **Info. gen. correo elect.:** número total de correos electrónicos, mensajes de correo basura (mensajes bloqueados) y el porcentaje del correo basura total recibido.

- **Correo basura reciente:** desglose del tipo de correo basura que ha recibido en los últimos 30 días.



Figura 5-11. Página Resumen

Integración con Microsoft Outlook y Outlook Express

Puede acceder a las funciones principales de SpamKiller desde Outlook Express 6.0, Outlook 98, Outlook 2000 y Outlook XP, seleccionando el menú SpamKiller o la barra de herramientas de SpamKiller.

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

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

Gestión de cuentas de correo electrónico y de usuarios

Esta sección describe cómo gestionar cuentas y usuarios.

Adición de cuentas de correo electrónico

Puede agregar los siguientes tipos de cuentas de correo electrónico:

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

NOTA

Si su equipo utiliza Windows 2000 o Windows XP y desea agregar 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 [Adición de usuarios en la página 110](#). 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** para abrir la página Configuración ([Figura 5-12](#)) y luego haga clic en **Cuentas de correo electrónico**. Aparecerá el cuadro de diálogo **Cuentas de correo electrónico**, que muestra todas las cuentas de correo agregadas 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. Siga las instrucciones de los cuadros de diálogo que aparezcan.

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



Figura 5-12. Página de configuración

Orientación del cliente de correo electrónico a SpamKiller

Si agrega una cuenta y SpamKiller no la detecta (la cuenta no aparece en el cuadro de diálogo **Seleccionar cuenta**) o si desea leer su correo MSN/Hotmail como una cuenta POP3 en SpamKiller, oriente su cliente de correo electrónico a SpamKiller modificando el servidor de correo entrante.

Por ejemplo, si el servidor de mensajes entrantes es "mail.mcafee.com", cámbielo a "localhost".

Eliminación de cuentas de correo electrónico

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

Eliminación de una cuenta de correo electrónico de SpamKiller

- 1 Haga clic en la ficha **Configuración** y seleccione **Cuentas de correo electrónico**. Aparecerá el cuadro de diálogo **Cuentas de correo electrónico**, que muestra todas las cuentas de correo agregadas 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

Edición de cuentas POP3

- 1 Haga clic en la ficha **Configuración** y seleccione **Cuentas de correo electrónico**. Aparecerá el cuadro de diálogo **Cuentas de correo electrónico**, que muestra todas las cuentas de correo agregadas a SpamKiller.

NOTA

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

- 2 Seleccione una cuenta POP3 y haga clic en **Editar**.
- 3 Haga clic en la ficha **General** para editar la descripción de la cuenta y la dirección de correo electrónico.
 - ♦ **Descripción:** descripción de la cuenta. Puede escribir todo tipo de información en este cuadro.
 - ♦ **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 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 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**; después, seleccione o indique una hora en el cuadro correspondiente. Si introduce el número cero, SpamKiller sólo comprobará la cuenta al conectarse.
 - 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 conecte a Internet.
- 6 Haga clic en la ficha **Conexión** para especificar el modo en que SpamKiller debe establecer la conexión a Internet para que pueda comprobar su 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 a Internet disponible, SpamKiller intenta conectarse automáticamente con la conexión predeterminada a 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. Podrá ver el correo desde el cliente de correo electrónico y la página de correos bloqueados de SpamKiller. Si la casilla no está seleccionada, sólo podrá ver los mensajes bloqueados en la página de correos electrónicos bloqueados.
 - ♦ **Puerto POP3:** (número de puerto POP3) el servidor POP3 gestiona los mensajes entrantes.
 - ♦ **Puerto SMTP:** (número de puerto SMTP) el servidor SMTP gestiona los mensajes salientes.
 - ♦ **Tiempo de espera del servidor:** el tiempo que esperará SpamKiller para recibir mensajes de correo antes de agotar el tiempo de espera y detenerse.

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

Cuentas MSN/Hotmail

Edición de 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**, que muestra todas las cuentas de correo electrónico que se han agregado a SpamKiller.

NOTA
Si se han agregado varios usuarios a SpamKiller, la lista mostrará las cuentas de correo electrónico del usuario que tiene una sesión iniciada en SpamKiller.
- 2 Seleccione una cuenta MSN/Hotmail y haga clic en **Editar**.
- 3 Haga clic en la ficha **General** para editar la descripción de la cuenta y la dirección de correo electrónico.
 - ♦ **Descripción:** descripción de la cuenta. Puede escribir todo tipo de información en este cuadro.
 - ♦ **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 entrante:** nombre del servidor que recibe el correo electrónico entrante.
 - ◆ **Contraseña:** contraseña que utiliza para acceder a la cuenta.
 - ◆ **Correo 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**; después, seleccione o indique una hora en el cuadro correspondiente. Si introduce el número cero, SpamKiller sólo comprobará la cuenta al conectarse.
 - 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 conecte a Internet.
- 6 Haga clic en la ficha **Conexión** para especificar el modo en que SpamKiller debe establecer la conexión a Internet para que pueda comprobar su 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 a Internet disponible, SpamKiller intenta conectarse automáticamente con la conexión predeterminada a 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 **Sí**.

Configuración de una cuenta de Hotmail de modo que bloquee el correo basura en Outlook u 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 ni 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 u Outlook Express, debe eliminarla antes.
- 3 Agregue la cuenta de Hotmail a Outlook u 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 y agregar amigos.

Cuentas MAPI

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

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

Edición de cuentas MAPI

- 1 Haga clic en la ficha **Configuración** y seleccione **Cuentas de correo electrónico**. Aparecerá el cuadro de diálogo **Cuentas de correo electrónico**, que muestra todas las cuentas de correo agregadas 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. Puede escribir todo tipo de información en este cuadro.
 - ◆ **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 a Internet disponible, SpamKiller intenta conectarse automáticamente con la conexión predeterminada a 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 **Sí**.

Adición de usuarios

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

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

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

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

Tareas	Administrador	Usuario restringido
Gestionar cuentas personales de correo electrónico, filtros personales, lista personal de amigos y configuración personal de sonido.	X	X
Gestionar las páginas personales de correos electrónicos bloqueados y 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 inicie la sesión en su equipo una vez agregado, se le pedirá que agregue una cuenta de correo a su perfil de usuario.

Para agregar y 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 también resulta útil para evitar que los niños accedan a SpamKiller y vean el contenido de los correos basura.

Creación de una contraseña para 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 cuadro **Contraseña**. Cuando un usuario accede a SpamKiller, debe usar la contraseña de inicio de sesión.

IMPORTANTE

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

Adición de un usuario a SpamKiller

- 1 Haga clic en la ficha **Configuración** y 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 el usuario que desee agregar y haga clic en **Aceptar**. El usuario se agregará a SpamKiller y su nombre aparecerá en la lista de usuarios de SpamKiller.
- 4 Haga clic en **Cerrar** cuando termine de agregar usuarios.

Para crear una contraseña para un usuario, consulte [Creación de una contraseña para un usuario existente de SpamKiller](#) en la página 112.

La próxima vez que el usuario inicie una sesión en el equipo, se le pedirá que agregue una cuenta de correo electrónico a su perfil de usuario de SpamKiller. Puede agregar cuentas de correo electrónico al perfil de usuario si ha iniciado una sesión en SpamKiller como ese usuario y dispone de la información necesaria sobre la cuenta de correo electrónico. Para obtener más información, consulte [Adición de cuentas de correo electrónico](#) en la página 103.

Edición de perfiles de usuario de SpamKiller

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

Eliminación de un perfil de usuario de SpamKiller

ADVERTENCIA

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

- 1 Haga clic en la ficha **Configuración** y luego 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.

Cambio de usuario

Debe haber iniciado la sesión en SpamKiller como administrador.

- 1 Haga clic en **Cambiar usuario**, en la parte superior de la página. Aparecerá el cuadro de diálogo **Cambiar usuario**.
- 2 Seleccione un usuario y haga clic en **Aceptar**. Si el usuario tiene una 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:** afecta a todas las cuentas de correo electrónico asociadas a un usuario específico. Si se agregaron varios usuarios, debe haber iniciado la sesión en SpamKiller como usuario para poder gestionar esta lista.

Puede agregar amigos a una lista de amigos para que no se bloquee su correo. La página de amigos muestra los nombres y direcciones que se han agregado a la lista de amigos. Esta página también muestra la fecha en que se agregó 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**. Aparecerá la página de amigos (Figura 5-13).
- 2 Haga clic en la ficha **Dirección de correo electrónico, Dominios** o **Lista de correo**. Aparecerá la lista global de amigos. Para ver la lista personal de amigos, haga clic en la flecha abajo  de una de las fichas y seleccione **Lista personal de amigos**.

NOTA

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

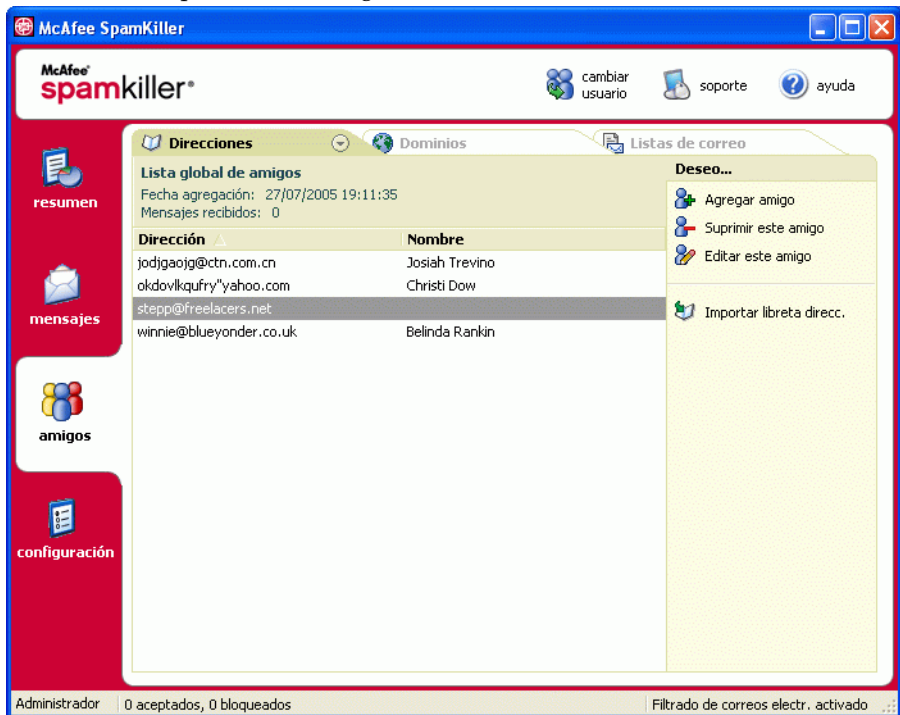


Figura 5-13. Página de amigos

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.

Importación automática de una libreta de direcciones

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

- 1 Haga clic en la ficha **Configuración** y luego en **Libretas de direcciones**. Aparecerá el cuadro de diálogo **Importar libretas de direcciones**, que muestra una lista de libretas de direcciones que SpamKiller comprueba regularmente y de las que importa las nuevas direcciones.
- 2 Haga clic en **Agregar**. Aparecerá el cuadro de diálogo **Importar calendario**.
- 3 Seleccione el **Tipo** de libreta de direcciones que desea importar y su **Origen**.
- 4 En el cuadro de diálogo **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 se incluyen en la lista personal de amigos.

Importación manual de una libreta de direcciones

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

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 libreta de direcciones** muestra una lista de tipos de libretas de direcciones que se pueden importar.

- 2 Seleccione el tipo de libreta de direcciones que desee importar o haga clic en **Examinar** para importar direcciones 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 aparecerán en la lista global o en la lista personal de amigos, según corresponda.

Edición de 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**.

Eliminación de 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**. Aparecerá un cuadro de diálogo de confirmación.
- 3 Haga clic en **Sí** para eliminar la libreta de direcciones de la lista.

Adición 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.

Adición de amigos desde las páginas de correos electrónicos bloqueados o aceptados

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

O

Desde el menú SpamKiller de Microsoft Outlook u Outlook Express, seleccione **Ver correos bloqueados** para abrir la página Correos bloqueados correspondiente a esa cuenta.

Aparecerá 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 cuadro **Dirección** escriba la dirección que desee agregar a la lista de amigos. Es posible que el cuadro **Dirección** contenga ya la dirección del mensaje seleccionado.
- 4 Escriba el nombre de su amigo en el cuadro **Nombre**.

- 5 Seleccione el tipo de dirección que desea agregar en el cuadro **Tipo de amigo**:
 - ♦ **Una dirección de correo electrónico**: la dirección de correo electrónico del remitente se agrega a la sección **Dominios** de la lista de amigos.
 - ♦ **Todos los del dominio**: el nombre de dominio se agrega a la sección **Dominios** de la lista de amigos. SpamKiller acepta todos los 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.
- 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.

Adición de amigos desde la página Amigos

- 1 Haga clic en la ficha **Amigos** y, a continuación, en **Agregar amigo**. Aparecerá el cuadro de diálogo **Propiedades de amigos**.
- 2 En el cuadro **Dirección** escriba la dirección que desee agregar a la lista de amigos.
- 3 Escriba el nombre de su amigo en el cuadro **Nombre**.
- 4 Seleccione el tipo de dirección que desea agregar en el cuadro **Tipo de amigo**:
 - ♦ **Una dirección de correo electrónico**: la dirección de correo electrónico del remitente se agrega a la sección **Dominios** de la lista de amigos.
 - ♦ **Todos los del dominio**: el nombre de dominio se agrega a la sección **Dominios** de la lista de amigos. SpamKiller acepta todos los 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.

Adición de amigos desde Microsoft Outlook

- 1 Abra su cuenta de correo electrónico en Microsoft Outlook u 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**.

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

Aparecerá la lista global de amigos. Para ver la lista personal de amigos, haga clic en la flecha abajo  de una de las fichas y 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 **Suprimir amigo**. Aparecerá un cuadro de diálogo de confirmación.
- 3 Haga clic en **Sí** para eliminar la dirección del amigo.

Trabajo con mensajes bloqueados y aceptados

Haga clic en la ficha **Mensajes** para abrir la página Mensajes (Figura 5-14) y acceder a los mensajes de correo electrónico bloqueados y aceptados. Las páginas de correos electrónicos bloqueados y correos electrónicos aceptados tienen características similares.

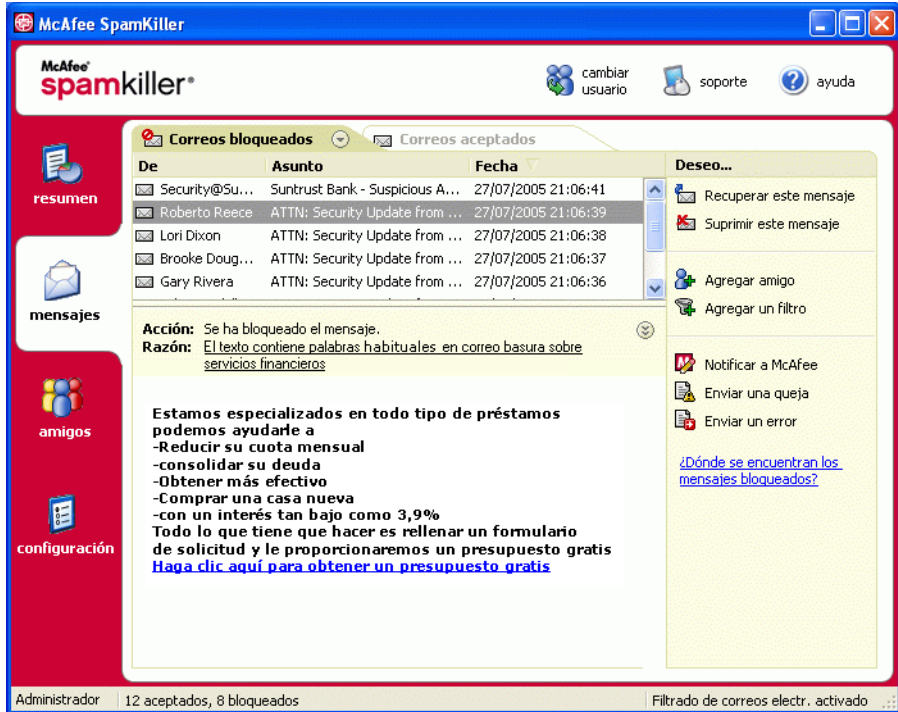


Figura 5-14. Página de mensajes


Página de correos electrónicos bloqueados

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

NOTA

También puede acceder a los mensajes bloqueados desde su cuenta de Microsoft Outlook, seleccionando el menú de SpamKiller y haciendo clic en **Ver mensajes bloqueados**.


Los mensajes bloqueados son mensajes que SpamKiller ha identificado como correo basura, ha sacado del buzón de entrada y ha puesto en la página 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 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 respondan al filtro.
- **De:** muestra el remitente del mensaje.
- **Fecha:** muestra la fecha en que se envió el mensaje.
- **Para:** muestra el destinatario del mensaje.
- **Asunto:** muestra el tema que aparece en la línea del asunto del mensaje.


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

Para obtener más información acerca de dónde se encuentran los mensajes bloqueados, consulte [¿Dónde se encuentran los mensajes bloqueados? en la página 126.](#)

Página de correos electrónicos aceptados


Haga clic en la ficha **Correos aceptados** de la página 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 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 intermedio explica si el correo ha sido enviado por un miembro de la lista de amigos, o bien si cumple los criterios de un filtro, pero la acción de dicho filtro era **Aceptar** o **Marcar como posible correo basura**. Haga clic en las flechas abajo  para ampliar el panel de detalles y ver el texto del mensaje y el encabezado en formato original, incluidas las etiquetas de formato HTML.

El panel de detalles del mensaje muestra lo siguiente:

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

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

- Correo electrónico de un amigo : SpamKiller ha detectado que el remitente está en una lista de amigos. 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 muestra las tareas que se pueden realizar.

- **Bloquear este mensaje:** elimina un mensaje del buzón de entrada y lo pone en la página 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 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 Correos bloqueados o la carpeta SpamKiller de Microsoft Outlook y Outlook Express contienen mensajes de correo electrónico legítimos, puede hacer que vuelvan a colocarse en la carpeta de entrada.

Desde la página Correos bloqueados

- 1 Haga clic en la ficha **Mensajes** y después en la ficha **Correos bloqueados**.
 O
 Desde el menú SpamKiller de Microsoft Outlook u Outlook Express, seleccione **Ver correos bloqueados** para abrir la página Correos bloqueados correspondiente a esa cuenta.
- 2 Seleccione un mensaje y haga clic en **Recuperar este mensaje** . Aparecerá el cuadro de diálogo **Opciones de recuperación**.
 - ◆ **Agregar amigo:** agrega al remitente a la lista de amigos.
 - ◆ **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 página de correos electrónicos aceptados.

Desde la carpeta SpamKiller de Microsoft Outlook u Outlook Express

Seleccione los mensajes y haga clic en **Recuperar selección** en el menú o barra de herramientas de SpamKiller. La selección se vuelve a colocar en el buzón de entrada y se elimina la etiqueta de mensaje ([CORREO BASURA] de forma predeterminada).

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 en Outlook Express.

Desde la página Correos aceptados

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

Desde Microsoft Outlook

En Microsoft Outlook, los mensajes de miembros de un servidor de Exchange se consideran seguros y SpamKiller no los filtra. Sólo se filtran los mensajes de origen externo.

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

¿Dónde se encuentran los mensajes bloqueados?

De modo predeterminado, los mensajes no deseados se etiquetan como [CORREO BASURA] y se colocan en la carpeta SpamKiller de Outlook y Outlook Express, o en el buzón de entrada. Los mensajes etiquetados también aparecen en la página de correos aceptados.

Eliminación manual de mensajes

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

○

Desde el menú SpamKiller de Microsoft Outlook u Outlook Express, seleccione **Ver correos bloqueados** para abrir la página Correos bloqueados correspondiente a esa cuenta.

- 2 Seleccione el mensaje que desea eliminar.
- 3 Haga clic en **Suprimir este mensaje**. Aparecerá un cuadro de diálogo de confirmación.
- 4 Haga clic en **Sí** para eliminar el mensaje.

Modificación del modo en que se procesa el correo no deseado

Cuando se detectan mensajes de correo electrónico no deseados, dichos mensajes se marcan o se bloquean. Los mensajes no deseados se eliminan del servidor cada vez que SpamKiller se conecta a él.

Etiquetado

La línea del asunto del mensaje de correo se etiqueta como [CORREO BASURA] y el mensaje pasa al buzón de entrada o a la carpeta SpamKiller, si dispone de Microsoft Outlook u Outlook Express.

Bloqueo

El mensaje se elimina y se coloca en la página de correos electrónicos bloqueados de SpamKiller. Si por error se bloquean mensajes de correo electrónico legítimos, es posible recuperar estos mensajes (consulte Recuperación de mensajes).

SpamKiller elimina automáticamente los mensajes bloqueados de esta página cuando transcurren 15 días. Es posible configurar la frecuencia con la que se eliminan los mensajes bloqueados.

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

Modificación del modo en que SpamKiller procesa el correo no deseado

- 1 Haga clic en la ficha **Configuración** y, a continuación, en el icono **Opciones de filtrado**.
- 2 Haga clic en la ficha **Procesamiento**.
 - ◆ **Poner el correo basura en una bandeja de mensajes bloqueados:** el correo basura se eliminará del buzón de entrada y se enviará a la página de correos bloqueados de SpamKiller.
 - ◆ **Etiquetar el correo basura y conservar en el buzón de entrada:** éste es el valor predeterminado. El correo basura se conserva en el buzón de entrada, pero en la línea del asunto se añade la indicación [CORREO BASURA].

Conservar los mensajes bloqueados durante ____ días: los mensajes bloqueados permanecen en la página de correos electrónicos bloqueados durante el tiempo que se especifique.

Conservar los mensajes aceptados durante ____ días: los mensajes aceptados permanecen en la página de correos electrónicos aceptados durante el tiempo que se especifique.
- 3 Haga clic en **Sí**.

Configuración del filtro AntiPhishing

Los mensajes de correo basura se dividen en dos categorías: correos no deseados (mensajes de correo electrónico que solicitan que el usuario compre productos) o phishing (mensajes que solicitan que el usuario proporcione información personal en un sitio Web falsificado).

El filtro McAfee AntiPhishing proporciona protección contra sitios Web incluidos en una lista negra (con actividades de phishing confirmadas o sospechosos de falsificar sitios Web), o bien una lista gris (incluyen contenidos parciales peligrosos o enlaces a sitios Web incluidos en la lista negra).

Si accede a un sitio Web cuyas actividades de phishing son conocidas o del que se sospecha que es una página Web falsificada, será redirigido a la página del filtro McAfee AntiPhishing.

Para modificar la configuración del filtro AntiPhishing, lleve a cabo los siguientes pasos.

- 1 Abra Internet Explorer.
- 2 En el menú **Herramientas**, seleccione el **filtro McAfee AntiPhishing**.
 - **Activar filtrado de sitio Web:** activado de forma predeterminada. Para desactivar el filtro AntiPhishing, desactive esta casilla de verificación.
 - **Permitir acceso a los sitios Web de la lista negra:** coloca un enlace en la página de redireccionamiento que permite acceder a los sitios de la lista negra. Al hacer clic en dicho enlace, accederá al sitio Web.
 - **Permitir acceso a los sitios Web de la lista gris:** coloca un enlace en la página de redireccionamiento que permite acceder a los sitios de la lista gris. Al hacer clic en dicho enlace, accederá al sitio Web.
- 3 Cuando haya terminado, haga clic en **Aceptar**.

Adición de amigos a una lista de amigos

Consulte [Adición de amigos desde las páginas de correos electrónicos bloqueados o aceptados](#) en la página 118.

Adición de filtros

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

- 1 Para crear un filtro global, haga clic en la ficha **Configuración**, seleccione **Filtros globales** y haga clic en **Agregar**.

Para crear un filtro personal, haga clic en la ficha **Configuración**, seleccione **Filtros personales** y haga clic en **Agregar**.

Haga clic en la ficha **Mensajes**, en **Correos bloqueados** o **Correos aceptados** y haga clic en **Agregar un filtro**.

- 2 Haga clic en **Agregar** para empezar a crear una condición de filtrado. Aparecerá el cuadro de diálogo **Condición de filtrado**.
- 3 Cree una condición de filtrado a través de los pasos siguientes.

Una condición de filtrado es una declaración que indica a SpamKiller lo que debe buscar en un mensaje. En el ejemplo “El texto de mensaje contiene hipoteca”, el filtro busca los mensajes que contengan la palabra “hipoteca”. Para obtener más información, consulte *Condiciones de filtrado* en la ayuda en línea.

- a Seleccione un tipo de condición del primer cuadro.
- b Seleccione o introduzca valores en los cuadros siguientes.
- c Si aparecen las siguientes opciones, selecciónelas para definir mejor la condición de filtrado.

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

Variaciones de coincidencia: permite a SpamKiller detectar errores de escritura utilizados habitualmente por los remitentes de correo basura. Por ejemplo, la palabra “común” se puede escribir de forma incorrecta como “c0mVn” para eludir los filtros.

Expresiones regulares (RegEx): permite especificar patrones de caracteres empleados en las condiciones de filtrado. Para comprobar un patrón de caracteres, haga clic en **Probar RegEx**.

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

- d Haga clic en **Sí**.
- 4 Cree otra condición de filtrado como se indica a continuación o vaya al [Paso 5](#) para seleccionar una acción de filtrado:
 - a Haga clic en **Agregar** y cree la condición de filtrado. Haga clic en **Aceptar** cuando haya terminado de crear la condición de filtrado.

Ambas condiciones de filtrado aparecerán en la lista de condiciones de filtrado y estarán unidas por el operador **Y**. El operador **Y** indica que SpamKiller busca mensajes que coincidan con *ambas* condiciones de filtrado. Si desea que SpamKiller busque mensajes que coincidan al menos con una de las dos condiciones, cambie **y** por **o** haciendo clic en **y** seleccionando **o** en el cuadro que aparece.

- b Haga clic en **Agregar** para crear otra condición, o vaya al **Paso 5** para seleccionar una acción de filtrado.

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

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

- 5 Seleccione una acción de filtrado en el cuadro **Acción**. La acción de filtrado le indica a SpamKiller cómo debe procesar los mensajes que encuentre ese filtro. Para obtener más información, consulte *Acciones de filtrado* en la ayuda en línea.
- 6 Haga clic en **Avanzadas** para seleccionar opciones avanzadas de filtrado (la selección de opciones avanzadas no es obligatoria). Para obtener más información, consulte *Opciones de filtros avanzadas* en la ayuda en línea.
- 7 Haga clic en **Aceptar** cuando haya terminado de crear el filtro.

NOTA

Para editar una condición, selecciónela y haga clic en **Editar**.
Para eliminar una condición, selecciónela y haga clic en **Eliminar**.

Expresiones regulares

Las expresiones regulares sólo están disponibles para las siguientes condiciones de filtrado: **El asunto**, **El texto del mensaje**, **Al menos una de las frases siguientes**.

Las secuencias y los caracteres especiales descritos a continuación se pueden emplear como expresiones regulares al definir condiciones de filtrado.
Por ejemplo:

- La expresión regular `[0-9]*\,[0-9]+` coincide con los números con coma flotante siempre que no se utilice una notación de ingeniería. La expresión regular coincide con: "12,12", ",1212" y "12,0", pero no con "12" y "12".
- La expresión regular `\D*[0-9]+\D*` coincide con todas las palabras que incluyan números: "SpamKiller" y "VIAGRA", pero no "SpamKiller" ni "VIAGRA".

\

Marca el siguiente carácter como especial o literal. Por ejemplo, "n" coincide con el carácter "n". "\n" coincide con un carácter de nueva línea. La secuencia "\\\" coincide con "\" y "\" con "\".

^

Coincide con el comienzo de la introducción de datos.

\$

Coincide con el fin de la introducción de datos.

Coincide con el carácter anterior cero o más veces. Por ejemplo, "zo*" coincide con el carácter "z" o con "zoo".

+

Coincide con el carácter anterior una o más veces. Por ejemplo, "zo+" coincide con "zoo", pero no con "z".

?

Coincide con el carácter anterior cero veces o una vez. Por ejemplo, "e?ca?" coincide con "ca" en "nunca".

.

Coincide con cualquier carácter individual excepto un carácter de nueva línea.

(patrón)

Coincide con un patrón y recuerda la coincidencia. La cadena secundaria que coincide se puede recuperar del conjunto de resultados, empleando la expresión [0]...[n]. Para hacer coincidir los caracteres de paréntesis (), utilice "\(" o "\)".

x|y

Coincide con x o y. Por ejemplo, "z|madera" coincide con "z" o con "madera". "(z|m)adera" coincide con "zoológico" o con "madera".

{n}

La n es un número entero no negativo. Coincide exactamente n veces. Por ejemplo, "o{2}" no coincide con la "o" de "Bob", pero sí con las primeras dos de "coooooomida".

{n,}

La n es un número entero no negativo. Coincide al menos n veces. Por ejemplo, "o{2,}" no coincide con la "o" de "Bob", pero sí con todas las de "coooooomida". "o{1,}" equivale a "o+". "o{0,}" equivale a "o*".

{n,m}

Las letras m y n son números enteros no negativos. Coincide al menos n veces y como mucho m veces. Por ejemplo, "o{1,3}" coincide con las tres primeras letras o de "coooooomida". "o{0,1}" equivale a "o?".

[xyz]

Un conjunto de caracteres. Coincide con cualquiera de los caracteres incluidos. Por ejemplo, "[abc]" coincide con la "a" de "plano".

[^xyz]

Un conjunto negativo de caracteres. Coincide con cualquiera de los caracteres no incluidos. Por ejemplo, "[^abc]" coincide con la "p" de "plano".

[a-z]

Un intervalo de caracteres. Coincide con cualquiera de los caracteres incluidos en el intervalo especificado. Por ejemplo, "[a-z]" coincide con cualquier carácter alfabético en el intervalo de la "a" a la "z".

[^m-z]

Un conjunto negativo de caracteres. Coincide con cualquiera de los caracteres no incluidos en el intervalo especificado. Por ejemplo, "[^m-z]" coincide con cualquier carácter que no se encuentre en el intervalo de la "m" a la "z".

\b

Coincide con un límite de palabra, es decir, con la posición entre una palabra y un espacio. Por ejemplo, "ca\b" coincide con "ca" en "nunca", pero no con "ca" en "casa".

\B

Coincide con un límite que no sea el espacio entre palabras. "ta*r\B" coincide con "tar" en "nunca tarde".

\d

Coincide con un carácter de dígito. Equivale a [0-9].

\D

Coincide con un carácter que no sea un dígito. Equivale a [^0-9].

\f

Coincide con un carácter de salto de página.

\n

Coincide con un carácter de nueva línea.

\r

Coincide con un carácter de retorno de carro.

\s

Coincide con cualquier espacio en blanco, incluidos espacios, tabulaciones, saltos de página, etc. Equivale a “[\f\n\r\t\v]”.

\S

Coincide con cualquier carácter que no sea un espacio en blanco. Equivale a “[^\f\n\r\t\v]”.

\t

Coincide con un carácter de tabulación.

\v

Coincide con un carácter de tabulación vertical.

\w

Coincide con cualquier carácter de palabra, incluido el subrayado. Equivale a “[A-Za-z0-9_]”.

\W

Coincide con cualquier carácter que no forme parte de una palabra. Equivale a “[^A-Za-z0-9_]”.

\num

Coincide con num, donde num es un entero positivo. Referencia a las coincidencias recordadas. Por ejemplo, “(.)\1” coincide con dos caracteres idénticos consecutivos.

\n

Coincide con n, donde n es un valor de escape octal. Los valores de escape octales deben tener una longitud de 1, 2 o 3 dígitos. Por ejemplo, tanto “\11” como “\011” coinciden con un carácter de tabulación. “\0011” equivale a “\001” y “1”. Los valores de escape octales no deben ser superiores a 256. Si lo son, sólo se tienen en cuenta los dos primeros dígitos para la expresión. Permite emplear los códigos ASCII en las expresiones regulares.

\xn

Coincide con n, donde n es un valor de escape hexadecimal. Los valores de escape hexadecimales deben tener una longitud de dos dígitos. Por ejemplo, “\x41” coincide con “A”. “\x041” equivale a “\x04” y “1”. Permite emplear los códigos ASCII en las expresiones regulares.

Notificación de correo basura a McAfee

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

- 1 Haga clic en la ficha **Mensajes** y, a continuación, haga clic en la ficha **Correos bloqueados** o **Correos aceptados**. Aparecerá la página de correos electrónicos bloqueados o aceptados.
- 2 Seleccione un mensaje y haga clic en **Notificar a McAfee**. Aparecerá un cuadro de diálogo de confirmación.
- 3 Haga clic en **Sí**. El mensaje se enviará automáticamente a McAfee.

Envío manual de quejas

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

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

ADVERTENCIA

En la mayoría de los casos no es recomendable seleccionar el **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.

Envío manual de mensajes de error

- 1 Haga clic en la ficha **Mensajes** y, a continuación, en la ficha **Correos bloqueados** o **Correos aceptados**. Aparecerá una lista de mensajes.
- 2 Para enviar un mensaje de error sobre un mensaje de correo basura específico, seleccione el mensaje y haga clic en **Enviar error**. Se enviará un mensaje de error a la dirección de respuesta incluida en el mensaje no deseado.

Índice

A

- ActiveShield
 - activar, 19
 - análisis de secuencias de comandos, 27
 - analizar archivos adjuntos de mensajes instantáneos entrantes, 25
 - analizar correo electrónico y archivos adjuntos, 21
 - analizar gusanos, 23
 - analizar programas potencialmente no deseados (PUP), 29
 - analizar sólo archivos de programas y documentos, 27
 - analizar todos los archivos, 26
 - analizar todos los tipos de archivo, 26
 - comprobar, 17
 - configuración de análisis predeterminada, 21, 24 to 29
 - desactivar, 20
 - detectar virus nuevos desconocidos, 27
 - detener, 21
 - iniciar, 21
 - limpiar un virus, 30
 - opciones de análisis, 20
- Actualizaciones automáticas de Windows, 73
- actualizar
 - un disco de emergencia, 44
 - VirusScan
 - automáticamente, 47
 - manualmente, 47
- administrador, 81, 110, 112
 - recuperar contraseña, 82
- agregar a lista blanca
 - PUP, 32
- agregar cuentas de correo electrónico, 103
- agregar filtros, 128
- agregar una dirección de correo electrónico a una lista de amigos, 118
- agregar usuarios, 84
 - bloquear contenido, 84
 - bloquear cookies, 84
 - límites de tiempo de acceso a Internet, 85
- alertas
 - Aplicación de Internet bloqueada, 72
 - de archivos infectados, 30
 - de correo electrónico infectado, 31
 - de gusanos potenciales, 31
 - de PUP, 32
 - de secuencias de comandos sospechosas, 31
 - de virus, 30
 - Intento de conexión bloqueado, 79
 - La aplicación desea tener acceso a Internet, 72
 - La aplicación desea tener acceso de servidor, 73
 - Nueva aplicación permitida, 78
 - Se ha modificado la aplicación, 72
- Analizar
 - análisis automático, 37
 - análisis manual, 33
 - análisis manual desde el Explorador de Windows, 37
 - analizar manualmente desde la barra de herramientas de Microsoft Outlook, 37
 - comprobar, 17 to 18
 - eliminar un virus o un programa potencialmente no deseado, 40
 - limpiar un virus o un programa potencialmente no deseado, 39
 - opción Analizar el contenido de los archivos comprimidos, 34
 - opción Analizar programas potencialmente no deseados, 35
 - opción Analizar subcarpetas, 34
 - opción Analizar todos los archivos, 34
 - opción Detectar virus nuevos desconocidos, 35
 - poner en cuarentena un virus o un programa potencialmente no deseado, 40

- analizar
 - archivos comprimidos, 34
 - desde el Explorador de Windows, 37
 - desde la barra de herramientas de Microsoft Outlook, 37
 - gusanos, 23
 - programar análisis automáticos, 37
 - programas potencialmente no deseados (PUP), 29
 - secuencias de comandos, 27
 - sólo archivos de programas y documentos, 27
 - subcarpetas, 34
 - todos los archivos, 26, 34
 - virus nuevos desconocidos, 35
 - aplicaciones de Internet
 - acerca de, 59
 - cambiar las reglas de aplicación, 60
 - permitir y bloquear, 60
 - archivos adjuntos de mensajes instantáneos entrantes
 - analizar, 25
 - limpiar automáticamente, 25
 - archivos troyanos
 - alertas, 30
 - detectar, 39
 - Asistente para la actualización, 21
 - asistente para la configuración, 82
 - AVERT, enviar archivos sospechosos, 42
- B**
- bloquear mensajes, 125
- C**
- cambiar usuarios, 114
 - comprobar funcionamiento de VirusScan, 17
 - comprobar Personal Firewall, 54
 - configurar
 - VirusScan
 - ActiveShield, 19
 - Analizar, 33
 - contraseñas, 112
 - correo electrónico y archivos adjuntos
 - analizar
 - activar, 21
 - desactivar, 23
 - errores, 22
 - limpiar automáticamente
 - activar, 21
 - correos aceptados
 - agregar a una lista de amigos, 128
 - enviar mensajes de error, 134
 - iconos de la lista de mensajes aceptados, 123
 - tareas, 124
 - trabajar con mensajes aceptados, 121
 - correos bloqueados
 - agregar a una lista de amigos, 128
 - dónde se encuentran los mensajes bloqueados, 126
 - enviar mensajes de error, 134
 - iconos de la lista de mensajes bloqueados, 122
 - modificar el modo en que se procesa el correo no deseado, 126
 - recuperar mensajes, 124
 - tareas, 124
 - trabajar con mensajes bloqueados, 121
 - cortafuegos predeterminado, configurar, 51
 - crear disco de emergencia, 42
 - cuentas de correo electrónico, 103
 - agregar, 103
 - editar, 105
 - editar cuentas MAPI, 109
 - editar cuentas MSN/Hotmail, 107
 - editar cuentas POP3, 105
 - eliminar, 104
 - orientar su cliente de correo electrónico a SpamKiller, 104
- D**
- desinstalar
 - otros cortafuegos, 51
 - direcciones IP
 - acerca de, 62
 - confiar, 68
 - prohibir, 68

- Disco de emergencia
- actualizar, [44](#)
 - crear, [42](#)
 - proteger contra escritura, [43](#)
 - usar, [40,44](#)
- E**
- editar listas blancas, [33](#)
- editar usuarios, [85](#)
- bloquear cookies, [86](#)
 - contraseña, [86](#)
 - eliminar usuarios, [88](#)
 - grupo de edad, [87](#)
 - información de usuario, [86](#)
 - límites de tiempo de acceso a Internet, [87](#)
 - usuario de inicio, [88](#)
- En cuarentena
- agregar archivos sospechosos, [40](#)
 - eliminar archivos, [40](#)
 - eliminar archivos sospechosos, [41](#)
 - enviar archivos sospechosos, [42](#)
 - gestionar archivos sospechosos, [40](#)
 - limpiar archivos, [40 to 41](#)
 - restablecer archivos limpiados, [40 to 41](#)
- enviar archivos sospechosos a AVERT, [42](#)
- eventos
- acerca de, [61](#)
 - archivar el registro de eventos, [70](#)
 - borrar el registro de eventos, [71](#)
 - bucle invertido, [63](#)
 - consejos de HackerWatch.org, [67](#)
 - copiar, [71](#)
 - de 0.0.0.0, [62](#)
 - de 127.0.0.1, [63](#)
 - de direcciones IP privadas, [64](#)
 - desde equipos de la LAN, [63](#)
 - eliminar, [72](#)
 - exportar, [71](#)
 - información adicional, [67](#)
 - informar, [67](#)
- mostrar
- con la misma información de evento, [66](#)
 - de una dirección concreta, [65](#)
 - día actual, [64](#)
 - semana actual, [65](#)
 - todos, [65](#)
 - un día concreto, [65](#)
- rastrear
- explicación, [61](#)
 - ver registros de eventos archivados, [70](#)
- responder a, [66](#)
- Explorador de Windows, [37](#)
- expresiones regulares, [130](#)
- F**
- filtrado
- activar, [101](#)
 - desactivar, [101](#)
- filtro AntiPhishing, utilizar, [127](#)
- filtros, agregar, [128](#)
- funciones, [81,99](#)
- funciones nuevas, [15,49](#)
- G**
- gusanos
- alertas, [30 to 31](#)
 - detectar, [30,39](#)
 - detener, [31](#)
- H**
- HackerWatch.org
- consejos, [67](#)
 - informar de un evento a, [67](#)
 - registrarse, [67](#)
- I**
- icono de ayuda, [101](#)
- icono de cambio de usuario, [100](#)
- icono de soporte, [100](#)
- importar una libreta de direcciones a una lista de amigos, [116](#)
- informar de un evento, [67](#)
- iniciar sesión en SpamKiller en un entorno de múltiples usuarios, [113](#)

L

- lista de amigos, [114](#)
 - agregar amigos desde las páginas de correos electrónicos bloqueados o aceptados, [118](#)
 - agregar una dirección de correo electrónico, [118](#)
 - importar una libreta de direcciones, [116](#)
- lista de archivos detectados (Analizar), [36,39](#)
- lista de PUP fiables, [33](#)

M

- McAfee Privacy Service, [83](#)
 - abrir, [83](#)
 - actualizar, [83](#)
 - desactivar, [83](#)
 - iniciar sesión, [83](#)
- McAfee SecurityCenter, [13](#)
- Microsoft Outlook, [37](#)
- mostrar eventos en el registro de eventos, [64](#)

N

- notificar correo basura a McAfee, [134](#)

O

- opción Analizar el contenido de los archivos comprimidos (Analizar), [34](#)
- opción Analizar programas potencialmente no deseado (Analizar), [35](#)
- opción Analizar subcarpetas (Analizar), [34](#)
- opción Analizar todos los archivos (Analizar), [34](#)
- opción Detectar virus nuevos desconocidos (Analizar), [35](#)
- opciones, [89](#)
 - bloquear anuncios, [90](#)
 - bloquear información, [89](#)
 - bloquear sitios Web, [89](#)
 - copia de seguridad, [94](#)
 - permitir cookies, [91](#)
 - permitir sitios Web, [89](#)
 - Web bugs, [90](#)
- opciones de análisis
 - ActiveShield, [20,26 to 27](#)
 - Analizar, [33](#)

- opciones de usuario, [96](#)
 - aceptar cookies, [97](#)
 - cambiar contraseña, [96](#)
 - cambiar nombre de usuario, [96](#)
 - rechazar cookies, [97](#)
 - vaciar la caché, [96](#)
- orientar su cliente de correo electrónico a SpamKiller, [104](#)

P

- página de amigos, [115](#)
- página de configuración, [103](#)
- página de correos aceptados, [123](#)
- página de correos bloqueados, [121](#)
- página de mensajes, [121](#)
- Página Resumen, [54](#)
- página Resumen, [101](#)
- Personal Firewall
 - comprobar, [54](#)
- programar análisis, [37](#)
- programas agregados a lista blanca, [33](#)
- programas potencialmente no deseado (PUP), [29](#)
 - alertas, [32](#)
 - confianza, [32](#)
 - detectar, [39](#)
 - eliminar, [32,40](#)
 - limpiar, [39](#)
 - poner en cuarentena, [40](#)
- proteger a menores, [112](#)
- proteger un disco de emergencia contra escritura, [43](#)

R

- rastrear un evento, [66](#)
- recuperar mensajes, [124](#)
- Registro de eventos
 - acerca de, [61](#)
 - gestionar, [70](#)
 - ver, [70](#)
- registro de eventos, [91](#)

S

- ScriptStopper, 27
- secuencias de comandos
 - alertas, 31
 - detener, 31
 - permitir, 31
- Shredder, 93
- soporte técnico, 40
- SpamKiller
 - activar filtrado, 101
 - desactivar filtrado, 101
 - página de correos aceptados, 123
 - página de correos bloqueados, 121

T

- tareas relativas a los mensajes bloqueados y aceptados, 124
- Tarjeta de inicio rápido, iii

U

- usar un disco de emergencia, 44
- usuario de inicio, 82, 84
- usuarios, 103
 - agregar usuarios, 110
 - cambiar usuarios, 114
 - crear contraseñas, 112
 - editar perfiles de usuario, 113
 - eliminar perfiles de usuario, 113
 - iniciar sesión en SpamKiller, 113
 - tipos de usuario, 111
- utilidades, 93

V

- virus
 - alertas, 30
 - detectar, 39
 - detectar con ActiveShield, 30
 - detener gusanos potenciales, 31
 - detener secuencias de comandos sospechosas, 31
 - eliminar, 30, 39
 - eliminar archivos infectados, 31
 - eliminar PUP, 32

- informar automáticamente, 44 to 45
 - limpiar, 30, 39
 - permitir secuencias de comandos sospechosas, 31
 - poner en cuarentena, 30, 39
 - poner en cuarentena archivos infectados, 30
- VirusScan
- actualizar automáticamente, 47
 - actualizar manualmente, 47
 - analizar desde el Explorador de Windows, 37
 - analizar desde la barra de herramientas de Microsoft Outlook, 37
 - comprobar, 17
 - informar automáticamente sobre virus, 44 to 45
 - programar análisis, 37

W

- Windows Firewall, 51
- World Virus Map
 - informar, 44
 - visualizar, 45
- WormStopper, 23