



**Antivirus**

Manual del usuario

CENTRO DE SEGURIDAD VERSIÓN 1.0



## COPYRIGHT

© 2003 Networks Associates Technology, Inc. Reservados todos los derechos. Queda prohibida la reproducción, transmisión, transcripción, almacenamiento en un sistema de recuperación o traducción a ningún idioma de este documento o parte de él en ningún formato o por ningún medio sin el consentimiento previo por escrito de Networks Associates Technology, Inc., sus proveedores o empresas filiales. Para obtener este permiso, escriba a la atención del departamento jurídico de Network Associates a la dirección: Network Associates International BV, PO Box 58326, 1040 HH Amsterdam, Países Bajos.

## ATRIBUCIONES DE MARCAS COMERCIALES

*Active Firewall, Active Security, Active Security (en Katakana), ActiveHelp, ActiveShield, AntiVirus Anyware y diseño, Bomb Shelter, Certified Network Expert, Clean-Up, CleanUp Wizard, CNX, CNX Certification Certified Network Expert y diseño, Covert, Design (N estilizada), Disk Minder, Distributed Sniffer System, Distributed Sniffer System (en Katakana), Dr Solomon's, la etiqueta de Dr Solomon's, Enterprise SecureCast, Enterprise SecureCast (en Katakana), Event Orchestrator (en Katakana), EZ SetUp, First Aid, ForceField, GMT, GroupShield, GroupShield (en Katakana), Guard Dog, HelpDesk, HomeGuard, Hunter, LANGuru, LANGuru (en Katakana), M y diseño, Magic Solutions, Magic Solutions (en Katakana), Magic University, MagicSpy, MagicTree, McAfee, McAfee (en Katakana), McAfee y diseño, McAfee.com, MultiMedia Cloaking, Net Tools, Net Tools (en Katakana), NetCrypto, NetOctopus, NetScan, NetShield, NetStalker, Network Associates, NetXray, NotesGuard, Nuts & Bolts, Oil Change, PC Medic, PCNotary, PrimeSupport, Recoverkey, Recoverkey - International, Registry Wizard, Remote Desktop, ReportMagic, RingFence, Router PM, Safe & Sound, SalesMagic, SecureCast, Service Level Manager, ServiceMagic, SmartDesk, Sniffer, Sniffer (en Hangul), Stalker, SupportMagic, TIS, TMEG, Total Network Security, Total Network Visibility, Total Network Visibility (en Katakana), Total Service Desk, Total Virus Defense, Trusted Mail, UnInstaller, Virex, Virus Forum, ViruScan, VirusScan, WebScan, WebShield, WebShield (en Katakana), WebSniffer, WebStalker, WebWall, Who's Watching Your Network, WinGauge, Your E-Business Defender, ZAC 2000, Zip Manager* are registered trademarks or trademarks of Network Associates, Inc. and/or its affiliates in the US and/or other countries. Los productos de la marca Sniffer<sup>®</sup> están realizados exclusivamente por Network Associates, Inc. Todas las demás marcas, registradas y sin registrar, mencionadas en este documento son propiedad exclusiva de sus respectivos titulares.

Este producto incluye, o podría incluir, software desarrollado por OpenSSL Project para su utilización en OpenSSL Toolkit (<http://www.openssl.org/>).

Este producto incluye, o podría incluir, software criptográfico elaborado por Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)).

Este producto incluye, o podría incluir, algunos programas de software que se conceden bajo licencia (o sublicencia) al usuario mediante una licencia pública general GNU (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 estos usuarios. El código fuente del software con licencia pública general se incluye también en el CD. Si cualquier licencia de software gratuito requiere que Network Associates 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.

## 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 LICENCIA. SI NO SABE QUÉ TIPO DE LICENCIA HA ADQUIRIDO, CONSULTE LOS DOCUMENTOS DE VENTA U OTROS DOCUMENTOS RELACIONADOS CON LA CONCESIÓN DE LA LICENCIA O CON LA ORDEN DE COMPRA QUE ACOMPAÑAN AL PAQUETE DE SOFTWARE O QUE HAYA RECIBIDO POR SEPARADO COMO PARTE DE LA COMPRA (POR EJEMPLO, UN MANUAL, UN ARCHIVO DEL CD DEL PRODUCTO O UN ARCHIVO DEL SITIO WEB DESDE EL QUE DESCARGÓ EL PAQUETE DE SOFTWARE). SI NO ESTÁ DE ACUERDO CON TODOS LOS TÉRMINOS DESCRITOS EN EL ACUERDO, NO INSTALE EL SOFTWARE. SI PROCEDE, PODRÁ DEVOLVER EL PRODUCTO A NETWORK ASSOCIATES O AL ESTABLECIMIENTO EN QUE LO HAYA ADQUIRIDO PARA QUE SE LE REEMBOLSE EL IMPORTE COMPLETO.

# contenido

<b>1</b>	<b>Introducción</b>	<b>5</b>
	Funciones nuevas	5
	Requisitos del sistema	6
	Descarga e instalación de VirusScan	7
	Comprobación del funcionamiento de VirusScan	10
	Comprobación del funcionamiento de ActiveShield	10
	Comprobación del funcionamiento de la función de análisis	11
	Utilización de McAfee® SecurityCenter™	13
<b>2</b>	<b>Utilización de McAfee VirusScan</b>	<b>15</b>
	Utilización de ActiveShield	15
	Activación o desactivación de ActiveShield	15
	Configuración de las opciones de ActiveShield	16
	Acciones que ActiveShield lleva a cabo al descubrir un virus	25
	Detección de virus en el equipo	27
	Detección manual de virus	28
	Detección de virus en el Explorador de Windows	31
	Detección de virus en Microsoft Outlook	31
	Detección automática de virus	32
	Acciones en caso de detección de virus	34
	Gestión de archivos en cuarentena	35
	Creación de un disco de emergencia	37
	Protección de un disco de emergencia contra escritura	38
	Utilización de un disco de emergencia	38
	Actualización de un disco de emergencia	38



**Antivirus**

Información automática sobre virus	39
Envío de información al Mapa Mundial de Virus (World Virus Map)	39
Visualización del Mapa Mundial de Virus (World Virus Map)	40
Actualización de VirusScan	41
Comprobación automática de actualizaciones	41
Comprobación manual de actualizaciones	42
<b>Índice alfabético</b>	<b>45</b>

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, scripts malintencionados y ataques híbridos.

Gracias a este antivirus, disfrutará de las funciones siguientes:

**ActiveShield:** analiza los archivos en tiempo real cuando el usuario o el equipo tienen acceso a ellos.

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

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

**Detección de actividad hostil:** supervisa el equipo para detectar actividad semejante a la de los virus provocada por scripts malintencionados o gusanos.

## Funciones nuevas

Esta versión de VirusScan incluye las siguientes funciones nuevas:

- **Análisis del correo electrónico**  
VirusScan analiza automáticamente el correo electrónico de entrada (POP3) y salida (SMTP) y sus archivos adjuntos de la mayoría de los clientes de correo electrónico más conocidos, como Microsoft Outlook, Netscape Mail, Eudora y Pegasus.
- **Análisis de mensajes instantáneos**  
VirusScan analiza de modo automático las transferencias de archivos recibidos de los clientes más conocidos de mensajes instantáneos, incluidos Yahoo Instant Messenger, AOL Instant Messenger y Microsoft Windows Messenger.
- **Detección de actividades hostiles**  
VirusScan incluye ScriptStopper™ y WormStopper™ para detectar, notificar y bloquear actividades relacionadas con virus producidas por scripts malintencionados y gusanos.
- **Integración con el Explorador de Windows**  
VirusScan permite utilizar un menú con métodos abreviados para analizar los archivos, carpetas o unidades que se hayan seleccionado dentro del Explorador de Windows.

- **Integración con Microsoft Outlook**  
VirusScan permite utilizar un icono de la barra de herramientas para analizar los mensajes, carpetas o mensajes almacenados en Microsoft Outlook.
- **Desinfección automática de archivos**  
VirusScan intenta limpiar de forma automática los archivos infectados al detectar una infección.
- **Análisis programados**  
Ahora puede programar el análisis automático a intervalos específicos para examinar exhaustivamente su equipo en busca de virus.
- **Integración con McAfee SecurityCenter**  
Su perfecta integración con McAfee SecurityCenter proporciona una visión general del estado de seguridad de su equipo y acceso a los últimos virus detectados y alertas de seguridad. Puede ejecutar SecurityCenter con el icono de McAfee que se muestra en la bandeja del sistema de Windows o directamente desde el escritorio de Windows.
- **Cuarentena de archivos**  
Puede utilizar la función de cuarentena para cifrar y aislar temporalmente archivos infectados o sospechosos en la carpeta de cuarentena hasta que se tome alguna medida. Una vez limpio, puede restablecer el archivo en su ubicación original el archivo que estaba en cuarentena.
- **Envío de archivos a AVERT**  
VirusScan incluye ahora la posibilidad de enviar los archivos sospechosos directamente desde la función de cuarentena a AVERT™ (McAfee AntiVirus Emergency Response Team, o Equipo de respuesta de emergencia antivirus de McAfee) para su investigación.
- **Informes del Mapa Mundial de Virus (World Virus Map)**  
Ahora puede enviar información de rastreo de virus de forma anónima para su inclusión en el Mapa Mundial de Virus (World Virus Map). Puede registrarse de forma automática y gratuita para acceder a esta función de seguridad y ver los niveles de infección más recientes en todo el mundo mediante McAfee SecurityCenter.

## Requisitos del sistema

- Microsoft® Windows 98, ME, 2000 o XP.
- PC con procesador a 133 MHz o superior (se recomienda Pentium).
- 16 MB de RAM como mínimo; se recomiendan 32 MB.
- 8 MB de espacio libre en el disco duro (para la instalación).
- Microsoft® Internet Explorer 5.5 o superior.

### NOTA

Para obtener la última versión de Internet Explorer, visite el sitio Web de Microsoft en la dirección <http://www.microsoft.com/worldwide/>.

# Descarga e instalación de VirusScan

Antes de descargar e instalar VirusScan, debe contratar el servicio. Para ello, puede acceder al Centro de Seguridad Terra. Siga los pasos que se le indican para poder contratar el servicio antivirus VirusScan de McAfee a través de Terra.

Antes de instalar VirusScan, guarde el trabajo que esté realizando y cierre las aplicaciones que se encuentren abiertas para continuar con las instrucciones de instalación siguientes. Tras instalar VirusScan, el programa puede pedirle que reinicie el equipo.

## NOTA

Si realiza una actualización de una versión anterior de VirusScan, este programa desinstalará de forma automática la versión anterior antes de instalar la actual. Deberá reiniciar el equipo cuando se lo solicite el **Asistente para la configuración**. Después de reiniciar el equipo, se instalará la versión actual de VirusScan.

Para instalar VirusScan:

- 1 Escriba <http://www.seguridad.terra.es/descarga.asp> y haga clic en el botón **Continuar**.



Figura 1-1. Pantalla de contratación de Terra

- 2 A continuación podrá ver la pantalla **Identifíquese en McAfee Security**, donde se le solicitarán los siguientes datos (correspondientes a la información que Terra le ha facilitado en el correo de bienvenida):
  - ◆ Dirección de correo electrónico.
  - ◆ Número de licencia.

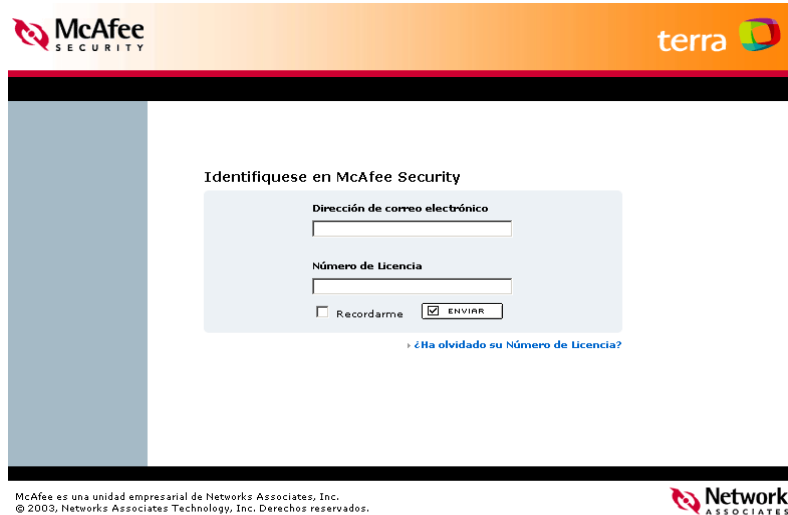


Figura 1-2. Pantalla de identificación en McAfee Security

- 3 Una vez completados los campos, haga clic en el boton **Enviar**.

- Visualizará una pantalla donde aparecerán detallados los productos que ha adquirido. Localice **VirusScan** en la lista **Los servicios Web** y, a continuación, haga clic en el icono Actualizar/Descargar que aparece junto al producto. El proceso de descarga comenzará de forma automática.

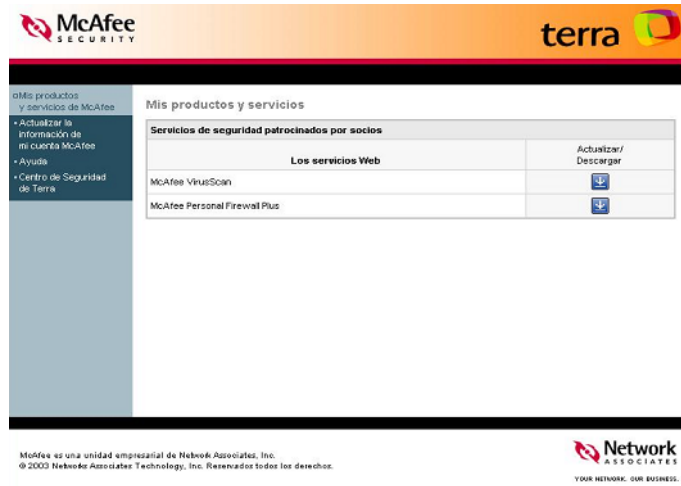


Figura 1-3. Pantalla de productos y servicios

**NOTA**

Si se abre un cuadro de diálogo, haga clic en **Sí** para continuar. En caso de que el **Asistente para la configuración** no aparezca de forma automática, haga clic en **Iniciar**.

- Si el **Asistente para la configuración** detecta la existencia de otros programas antivirus instalados en el equipo, mostrará una lista de los productos detectados. Haga clic en **Sí** (recomendado) para eliminar los productos detectados y, a continuación, reinicie el equipo para continuar la instalación. Al reiniciar el equipo, se mostrará de nuevo el cuadro de diálogo del **Asistente para la configuración**, que le pedirá que continúe con la instalación.

- Haga clic en **Siguiente** para continuar con la instalación de VirusScan.

Aparecerá el cuadro de diálogo **Informes de Virus Map**.

- Acepte la opción predeterminada **Sí, deseo participar** para poder enviar de forma anónima información a McAfee de modo que se incorpore al Mapa Mundial de Virus (World Virus Map) que incluye los niveles de infección a escala mundial. En caso contrario, seleccione **No, no deseo participar** para no enviar ninguna información.

### NOTA

Es posible configurar esta opción más tarde en la ficha **Informes de Virus Map** del cuadro de diálogo **VirusScan: Opciones**.

- Si reside en los Estados Unidos, seleccione el estado y el código postal correspondiente a la ubicación física del equipo. En caso contrario, seleccione el país en el que se encuentre su equipo. Cuando haya finalizado, haga clic en **Siguiente** para continuar.

- Cuando el **Asistente para la configuración** se lo pida, haga clic en **Reiniciar** para reiniciar el equipo.

Aparecerá un cuadro de diálogo de bienvenida cuando se reinicie Windows tras la instalación.

- Se mostrará el cuadro de diálogo **Detectar virus** y comenzará un análisis inicial del equipo con las opciones predeterminadas. Consulte la sección *Detección manual de virus en la página 28* para obtener información más detallada.
- Cuando finalice el análisis, haga clic en **Cerrar** para salir de la función de análisis.

## Comprobación del funcionamiento de VirusScan

Antes de utilizar VirusScan, será conveniente comprobar su instalación. Siga las instrucciones que se indican a continuación para verificar por separado las funciones de análisis y ActiveShield.

## Comprobación del funcionamiento de ActiveShield

Para comprobar el funcionamiento de ActiveShield:

- Diríjase a <http://www.eicar.com/> en el navegador Web.
- Haga clic en el vínculo **The AntiVirus testfile eicar.com** (Archivo de prueba antivirus de eicar.com).
- Desplácese hasta la parte inferior de la página. Bajo **Download Area** (Zona de descarga) verá cuatro vínculos.
- Haga clic en **eicar.com**.

Si ActiveShield funciona correctamente, detectará el archivo eicar.com inmediatamente después de hacer clic en el vínculo. Puede intentar suprimir o poner en cuarentena los archivos infectados para comprobar el tratamiento que da ActiveShield a los virus. Consulte la sección *Acciones que ActiveShield lleva a cabo al descubrir un virus en la página 25* para obtener información más detallada.

## Comprobación del funcionamiento de la función de análisis

Antes de probar la función de análisis, deberá descargar los archivos de prueba y colocarlos en otra carpeta.

Para descargar los archivos de prueba:

- 1 Desactive ActiveShield: haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y haga clic en **Desactivar**.
- 2 Descargue los archivos de prueba de EICAR del sitio Web de EICAR mencionado anteriormente:
  - a Diríjase a la dirección <http://www.eicar.com/>.
  - b Haga clic en el vínculo **The AntiVirus testfile eicar.com** (Archivo de prueba antivirus de eicar.com).
  - c Desplácese hasta la parte inferior de la página. Bajo **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 primero de ellos. Cambie su nombre a 'eicar.com' después de descargarlo. #\*

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

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

# La función ActiveShield detecta todos estos archivos.

\* La función de análisis detecta todos estos archivos.

- 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. Localice un directorio temporal, haga clic en **Guardar** y, a continuación, en **Guardar** de nuevo en cada uno de los cuadros de diálogo **Guardar como** que vayan apareciendo.
- 3 Cuando haya terminado de descargar los archivos, cierre Internet Explorer.

Para trasladar los archivos de prueba a otra carpeta:

- 1 En el Explorador de Windows, haga doble clic en el icono **Mi PC**.  
Se abrirá la ventana **Mi PC**.
- 2 Haga doble clic en el icono de la unidad de disco duro (normalmente la unidad C).  
Se abrirá una ventana que mostrará el contenido de dicha unidad.
- 3 Haga clic con el botón derecho en una zona del Explorador libre de archivos y carpetas, seleccione **Nuevo** y, a continuación, haga clic en **Carpeta**.  
Aparecerá una carpeta denominada **Nueva carpeta**.
- 4 Llame a la carpeta **Carpeta de análisis VS**.
- 5 Arrastre cada uno de los archivos desde el escritorio a la carpeta **Carpeta de análisis de VS**.
- 6 Active ActiveShield: haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y haga clic en **Activar**.

Para comprobar el funcionamiento de la función de análisis:

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

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

- 3 En el área **Opciones de análisis** del cuadro de diálogo **Análisis de 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 **Carpeta de análisis de VS**. Los archivos guardados en dicha carpeta aparecerán en la **Lista de archivos infectados**. Si es así, la función de análisis funciona correctamente.

Puede intentar suprimir o poner en cuarentena los archivos infectados para comprobar el tratamiento que da la función de análisis a los virus. Consulte la sección [Acciones en caso de detección de virus en la página 34](#) para obtener información más detallada.


# Utilización de McAfee® SecurityCenter™

McAfee SecurityCenter es una herramienta de seguridad integrada, a la que puede tener acceso con el icono situado en la bandeja del sistema de Windows o directamente desde el escritorio de Windows. Gracias a éste, puede realizar estas útiles tareas:

- Obtener un análisis de seguridad del equipo.
- Ver alertas de virus actualizados continuamente y la información más reciente sobre productos.
- Acceder rápidamente a las preguntas más frecuentes e información detallada de su cuenta de usuario en el Centro de Seguridad de Terra.

## NOTA

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


Cuando SecurityCenter se encuentra en ejecución y todas las funciones de McAfee están instaladas en el equipo, se mostrará un icono rojo con una M  en la bandeja del sistema de Windows. Esta área se encuentra normalmente en la esquina inferior derecha del escritorio de Windows e incluye el reloj.

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

## Para abrir McAfee SecurityCenter:

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

## Para tener acceso a una función de VirusScan:

- 1 Haga clic con el botón derecho en el icono de McAfee .
- 2 Seleccione **VirusScan** y haga clic en la función que desee utilizar.



## Utilización de ActiveShield


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

### ADVERTENCIA

- ♦ VirusScan y ActiveShield no son actualizaciones de McAfee VirusScan v4.x–7.x y VShield. Si tiene McAfee VirusScan instalado en su equipo, debe eliminarlo para que ActiveShield se ejecute correctamente.
- ♦ Es posible que paquetes de software como McAfee Internet Security, Guard Dog, Nuts & Bolts, First Aid, McAfee Office y Microsoft Plus! incluyan versiones de McAfee VirusScan. Debe eliminar los componentes antivirus de estas aplicaciones para que ActiveShield pueda funcionar correctamente.


## Activación o desactivación de ActiveShield

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

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

### Activación de ActiveShield

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


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

Si ActiveShield sigue configurado para iniciarse al abrir Windows, se mostrará un mensaje que indica que ya está protegido contra el ataque de virus. De lo contrario, aparecerá un cuadro de diálogo que le permitirá configurar ActiveShield para que se inicie al abrir Windows ([Figura 2-1 en la página 16](#)).

## Desactivación de ActiveShield


Para desactivar ActiveShield sólo durante la sesión actual de Windows:

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

El icono de McAfee pasará a tener color negro .

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

## Configuración de las opciones de ActiveShield

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

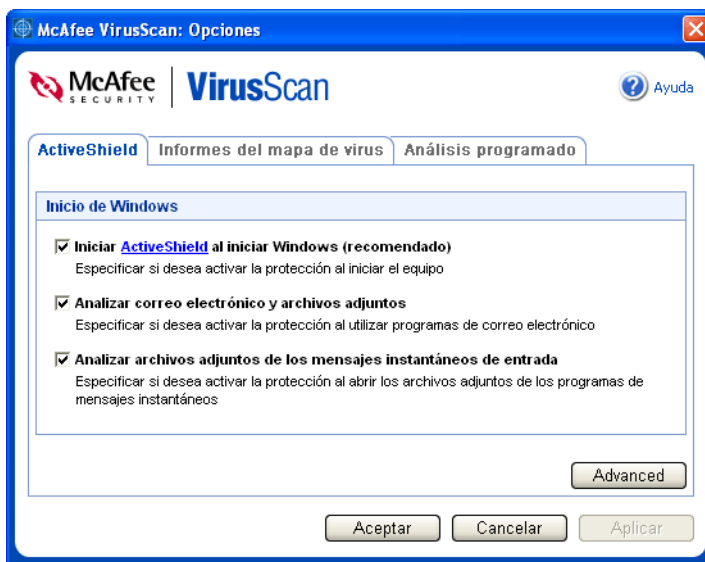




Figura 2-1. Opciones de ActiveShield

## Inicio de ActiveShield

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

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

### NOTA

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

Para iniciar ActiveShield al abrir Windows:

- 1 Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y haga clic en **Opciones**.  
Se abrirá el cuadro de diálogo **VirusScan: Opciones** (Figura 2-1 en la página 16).
- 2 Marque la casilla de activación **Iniciar ActiveShield al iniciar Windows** (recomendado) y haga clic en **Aplicar** para guardar los cambios.
- 3 Haga clic en **Aceptar** para confirmar y, a continuación, en **Aceptar**, de nuevo.

## Detención de ActiveShield

### ADVERTENCIA

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

Para detener ActiveShield al iniciar Windows:

- 1 Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y haga clic en **Opciones**.  
Se abrirá el cuadro de diálogo **VirusScan: Opciones** (Figura 2-1 en la página 16).
- 2 Desactive la casilla de activación **Iniciar ActiveShield al iniciar Windows** (recomendado) y haga clic en **Aplicar** para guardar los cambios.
- 3 Haga clic en **Aceptar** para confirmar y, a continuación, en **Aceptar**, de nuevo.

## **Análisis del correo electrónico y los archivos adjuntos**

De forma predeterminada, el análisis del correo electrónico y la limpieza automática se activan mediante la opción **Analizar correo electrónico y archivos adjuntos** (Figura 2-1 en la página 16) y la opción **Limpiar automáticamente los archivos adjuntos infectados (recomendado)** (Figura 2-2 en la página 19).

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

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

### **NOTA**

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

## **Correo electrónico de entrada**

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

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

## Correo electrónico de salida

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

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

Si el servidor de correo electrónico está configurado de modo que sólo se reciba y envíe correo electrónico mientras el usuario está utilizando su equipo, puede desactivar la limpieza automática para que aparezcan alertas que le pidan que limpie los mensajes infectados. Siga el procedimiento siguiente para desactivar la limpieza automática y, a continuación, consulte [Gestión del correo electrónico infectado en la página 26](#) para obtener más información sobre la forma de responder a las alertas.

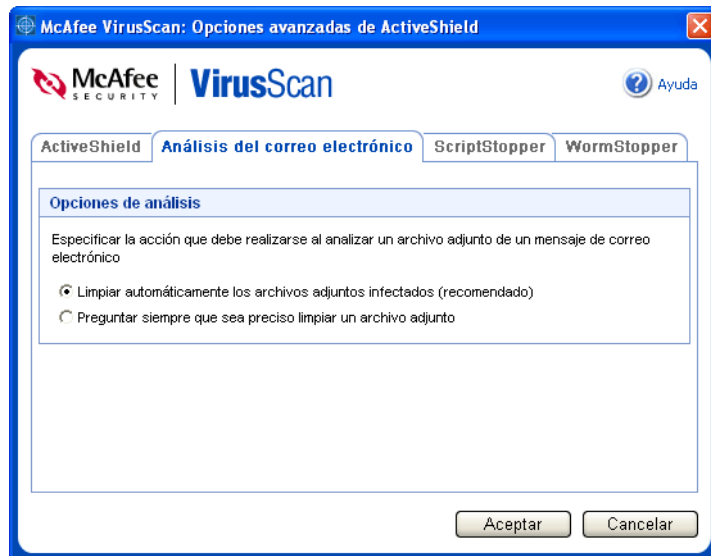


Figura 2-2. Opciones de análisis del correo electrónico

Para desactivar la limpieza automática del correo electrónico infectado:

- 1 Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y haga clic en **Opciones**.
- 2 Haga clic en **Avanzadas** y, a continuación, en la ficha **Análisis del correo electrónico** (Figura 2-2).
- 3 Haga clic en **Preguntar siempre que sea preciso limpiar un archivo adjunto** y, a continuación, en **Aceptar**.

## Análisis de archivos adjuntos de los mensajes instantáneos de entrada

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 16).

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

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

### NOTA

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

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

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

## 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 que utilice su equipo al intentar utilizarlos. Utilice esta función para obtener del análisis el máximo provecho posible.

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

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

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

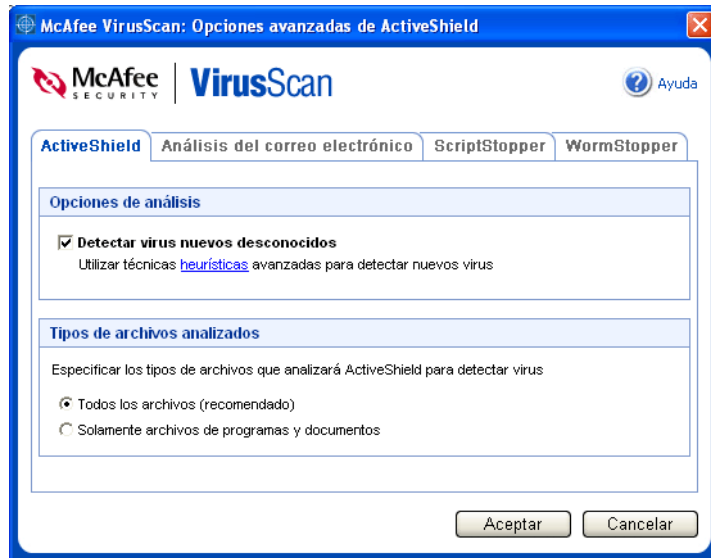


Figura 2-3. Opciones avanzadas de ActiveShield

## Análisis exclusivo de los archivos de programas y documentos

Si configura ActiveShield para que utilice la opción **Solamente archivos de programas y documentos (recomendado)**, se analizarán únicamente los archivos de programas y documentos pero no se analizará ningún otro archivo utilizado por el equipo. El archivo de definición de virus (archivo DAT) más reciente determina qué tipos de archivo puede analizar ActiveShield.

Para que ActiveShield analice sólo los documentos y los archivos de programas:

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

## Detección de virus nuevos desconocidos

Si configura ActiveShield de modo que utilice la opción predeterminada **Analizar virus nuevos y desconocidos**, se emplearán técnicas heurísticas que comparan los archivos con las definiciones de nuevos virus y, al mismo tiempo, buscan signos delatores de virus no identificados en los archivos.

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

- 1 Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y haga clic en **Opciones**.
- 2 Haga clic en **Avanzadas** y, a continuación, en la ficha **ActiveShield** (Figura 2-3 en la página 21).
- 3 Haga clic en **Analizar virus nuevos y desconocidos (recomendado)** y, a continuación, en **Aceptar**.

## Detección de scripts y gusanos

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

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

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

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

Para configurar ActiveShield de modo que detecte actividades parecidas a las de los scripts y los gusanos:

- 1 Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y haga clic en **Opciones**.
- 2 Haga clic en **Avanzadas**, luego en la ficha **ScriptStopper** y, a continuación, en **Activar ScriptStopper (recomendado)** (Figura 2-4 en la página 23).

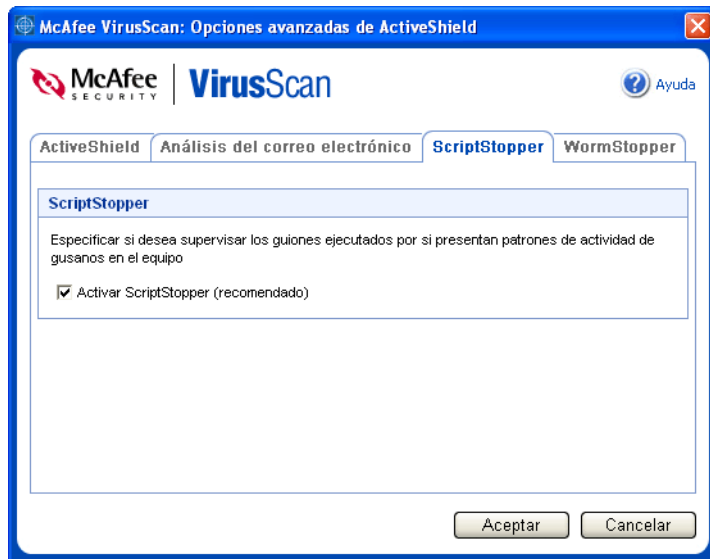


Figura 2-4. Opciones de ScriptStopper

- 3 Haga clic en la ficha **WormStopper**, luego en **Activar WormStopper (recomendado)** y, a continuación, en **Aceptar** (Figura 2-5 en la página 24).

De forma predeterminada están activadas las siguientes opciones detalladas:

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

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 27](#) para obtener información detallada):

- ◆ Bloqueo automático de mensajes sospechosos de correo electrónico de salida

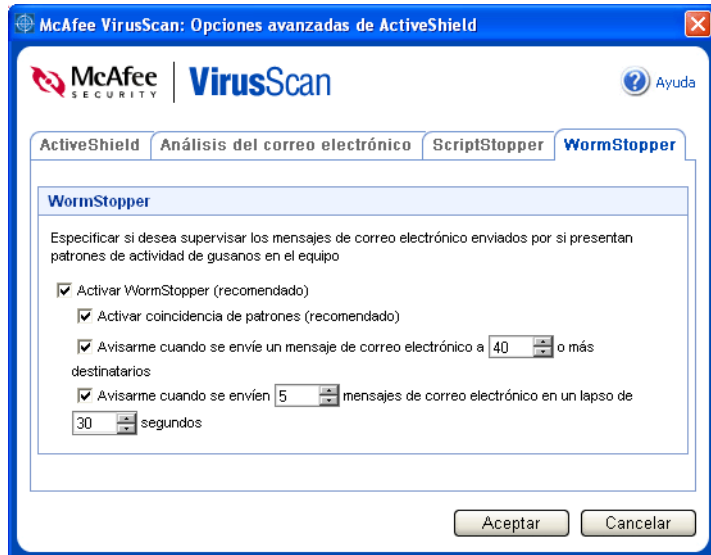


Figura 2-5. Opciones de WormStopper

## Acciones que ActiveShield lleva a cabo al descubrir un virus

Si ActiveShield descubre un virus, aparecerá una alerta similar a la que se muestra en la [Figura 2-6](#). ActiveShield intenta limpiar automáticamente la mayor parte de los virus, archivos troyanos y gusanos. A continuación, puede elegir cómo desea tratar los archivos infectados, el correo electrónico infectado, los scripts sospechosos y los posibles gusanos; si lo desea, también puede enviar los archivos infectados a los laboratorios de McAfee AVERT para su investigación.

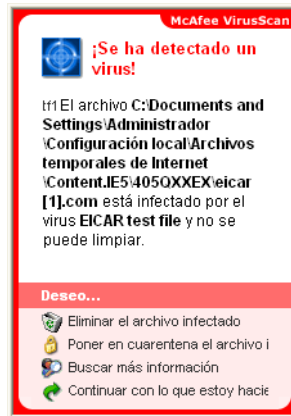


Figura 2-6. Alerta de virus

### Gestión de archivos infectados

- 1 Si ActiveShield es capaz de limpiar el archivo, puede obtener más información al respecto o hacer caso omiso de la alerta:
  - ♦ Haga clic en **Buscar más información** para ver el nombre del archivo, la ubicación y el nombre del virus asociado al archivo infectado.
  - ♦ Haga clic en **Continuar con lo que estoy haciendo** para hacer caso omiso de la alerta y cerrarla.
- 2 Si ActiveShield no puede limpiar el archivo, haga clic en **Poner en cuarentena el archivo infectado** para cifrar y aislar temporalmente los archivos infectados y sospechosos en el directorio de cuarentena hasta que se pueda tomar una medida conveniente.

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

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

## Gestión del correo electrónico infectado

- 1 Si ha desactivado la limpieza automática del correo electrónico, puede obtener más información y limpiar el mensaje:
  - a Haga clic en **Buscar más información** para ver el nombre del archivo, el nombre del virus, el estado de la infección, el remitente y el asunto asociados al mensaje infectado.
  - b Haga clic en **Limpiar los archivos adjuntos infectados**.
- 2 Si ActiveShield no puede limpiar el mensaje de correo electrónico, haga clic en **Poner en cuarentena los archivos adjuntos infectados** para cifrar y aislar temporalmente los archivos infectados y sospechosos en el directorio de cuarentena hasta que pueda tomar una medida conveniente.

Aparecerá un mensaje de confirmación y se le pedirá que examine su equipo en busca de virus. Haga clic en **Analizar** para completar el proceso de cuarentena.
- 3 Si ActiveShield no puede poner el mensaje de correo electrónico en cuarentena, haga clic en **Eliminar los archivos adjuntos infectados** para intentar eliminar el archivo.

## Administración de los scripts sospechosos

- 1 Si ActiveShield detecta un script sospechoso, puede obtener más información y, a continuación, detener el script si no tenía intención de iniciarlo:
  - a Haga clic en **Buscar más información** para ver el nombre, la ubicación y la descripción de la actividad asociada al script sospechoso.
  - b Haga clic en **Detener este guión** para evitar la ejecución del script sospechoso.
- 2 Si está seguro de que el script es fiable, puede permitir que se ejecute:
  - a Haga clic en **Permitir el guión completo esta vez** para dejar que todos los scripts contenidos en un archivo concreto se ejecuten una vez.
  - b Haga clic en **Continuar con lo que estoy haciendo** para hacer caso omiso de la alerta y dejar que se ejecute el script.

## Gestión de gusanos potenciales

- 1 Si ActiveShield detecta un gusano potencial, puede obtener más información y, a continuación, detener la actividad de correo electrónico si no tenía intención de iniciarla:
  - a Haga clic en **Buscar más información** para ver la lista de destinatarios, el asunto, el cuerpo del mensaje y la descripción de la actividad sospechosa asociados al mensaje de correo electrónico infectado.
  - b Haga clic en **Detener este mensaje de correo electrónico** para evitar que el mensaje sospechoso se envíe y para suprimirlo de la cola de mensajes.

### NOTA

La primera vez que se detecta un gusano potencial aparece un cuadro de diálogo después de detener o de enviar el mensaje de correo electrónico sospechoso. Marque la casilla de activación **Bloquear automáticamente todos los mensajes sospechosos** y, a continuación, haga clic en **Aceptar** para configurar WormStopper de modo que bloquee sin avisar el envío de los mensajes sospechosos de correo electrónico en el futuro.

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

## Detección de virus en el equipo

La función de análisis permite seleccionar discos duros, disquetes, y archivos y carpetas individuales para detectar virus en ellos. Cuando la función de análisis detecta un archivo infectado, intenta su limpieza automáticamente. Si ActiveShield no puede limpiar el virus, puede eliminar el archivo o ponerlo en cuarentena.

## Detección manual de virus

Para analizar su equipo:

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

Se abrirá el cuadro de diálogo **Análisis de virus** (Figura 2-7 en la página 28).

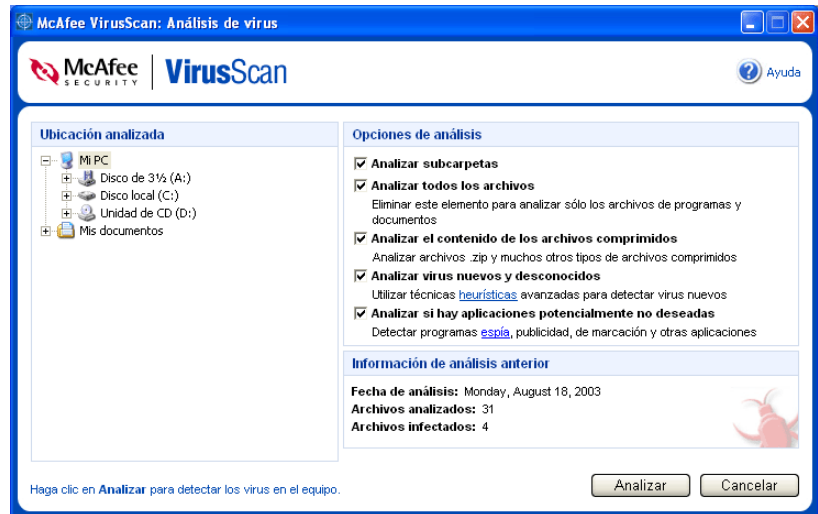


Figura 2-7. Detección de virus

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

3 Seleccione las **Opciones de análisis** deseadas. De manera predeterminada, todas las **Opciones de análisis** están preseleccionadas para aplicar el análisis más completo (Figura 2-7):

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

**Ejemplo:** Los archivos de la Figura 2-8 en la página 29 son los únicos que se analizarán si se desactiva la casilla de activación **Analizar subcarpetas**. Las carpetas y sus contenidos no se analizarán. Para analizar dichas carpetas y sus contenidos, debe dejar la casilla activada.

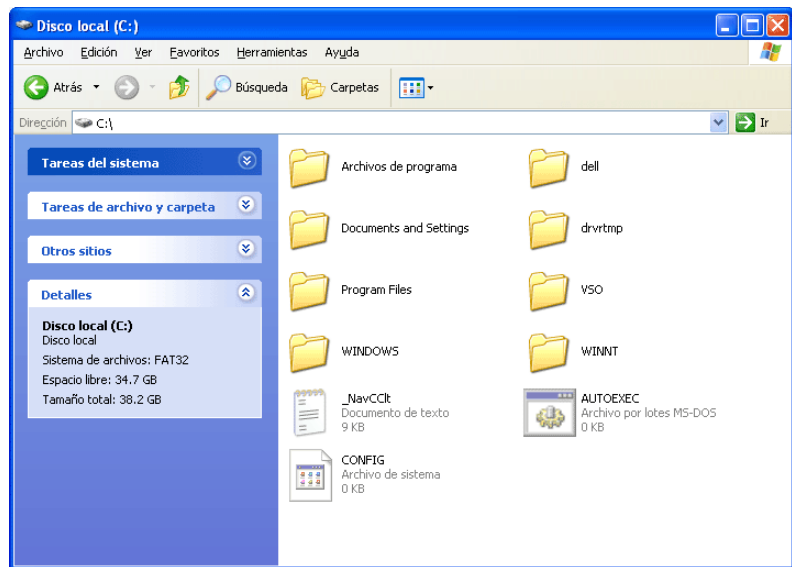


Figura 2-8. Contenidos del disco local

- ◆ **Analizar todos los archivos:** utilice esta opción para realizar un análisis completo de todos los tipos de archivos. Desactive esta casilla de activación para reducir el tiempo de análisis y examinar únicamente los archivos de programas y documentos.
- ◆ **Analizar el contenido de los archivos comprimidos:** utilice esta opción para encontrar los archivos infectados ocultos en los archivos .ZIP y otros archivos comprimidos. Desactive esta casilla de activación para no analizar ningún archivo, ya esté comprimido o no, incluido dentro del archivo comprimido.

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

- ♦ **Analizar virus nuevos y 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 delatores de virus no identificados en los archivos.

Este método de análisis también busca atributos de archivos que, por regla general, puedan descartar la existencia de virus. De esta manera, se minimizan las posibilidades de que la función de análisis devuelva una falsa alarma. No obstante, si un análisis heurístico detecta un virus, el archivo se debería tratar con la misma precaución que cualquier otro archivo que contenga un virus con certeza.

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

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

**NOTA**

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

- 4 Haga clic en **Analizar** para comenzar a analizar los archivos. Cuando termine el análisis, aparecerá una lista con todos los archivos infectados en el cuadro de diálogo **Análisis de virus** (Figura 2-9).

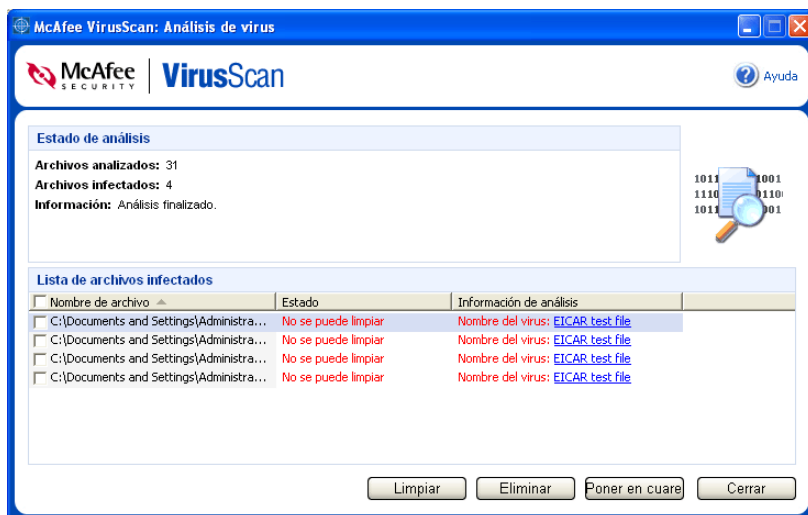


Figura 2-9. Resultados del análisis

**NOTA**

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

- 5 Si no se detecta ningún virus, haga clic en **Atrás** para seleccionar otra unidad o carpeta que analizar, o bien en **Cerrar** para cerrar el cuadro de diálogo.

## Detección de virus en el Explorador de Windows

VirusScan permite utilizar un menú con métodos abreviados para analizar los archivos, las carpetas o las unidades que se hayan seleccionado en el Explorador de Windows.

Análisis de archivos en el Explorador de Windows:


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

Se abrirá el cuadro de diálogo **Análisis de virus** y se iniciará el análisis de los archivos. De manera predeterminada, todas las **Opciones de análisis** están preseleccionadas para aplicar el análisis más completo ([Figura 2-7 en la página 28](#)).

## Detección de virus en Microsoft Outlook

VirusScan permite utilizar un icono de la barra de herramientas para analizar los almacenes de mensajes y sus subcarpetas, las carpetas de correo o los mensajes de correo electrónico que contengan archivos adjuntos en el seno de Microsoft Outlook 97 o una versión posterior.

Para analizar el correo electrónico en Microsoft Outlook:

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

Aparecerá el analizador de correo electrónico, que empezará a analizar los archivos. De manera predeterminada, todas las **Opciones de análisis** están preseleccionadas para aplicar el análisis más completo ([Figura 2-7 en la página 28](#)).

## Detección automática de virus

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

Para programar un análisis:

- 1 Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y haga clic en **Opciones**.  
Se abrirá el cuadro de diálogo **VirusScan: Opciones**.
- 2 Haga clic en la ficha **Análisis programado** (Figura 2-10 en la página 32).

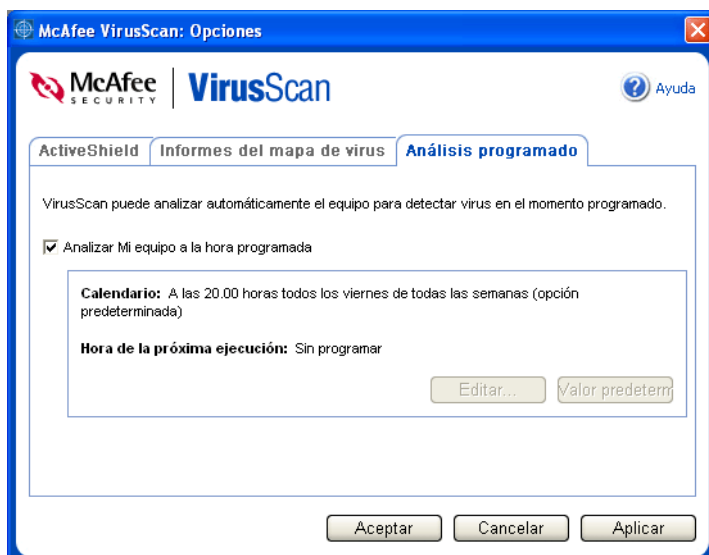


Figura 2-10. Opciones del análisis programado

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

4 Defina un programa para el análisis automático mediante uno de los métodos siguientes:

- ◆ Para aceptar la programación predeterminada (**los viernes a las 20:00 horas**), haga clic en **Aceptar**.
- ◆ Para modificar una programación:
  - a Haga clic en **Editar**.
  - b Seleccione la programación en la lista.
  - c Seleccione la frecuencia con la que desee analizar el equipo en la lista **Frecuencia** y seleccione las opciones adicionales en el área dinámica situada debajo:

**Diariamente:** especifique el número de días entre análisis.

**Semanalmente** (opción predeterminada): especifique el número de semanas entre análisis, así como el nombre del día o días de la semana.

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

**Una vez:** especifique en qué fecha desea realizar el análisis.

**Al iniciar la sesión del usuario:** esta opción analiza automáticamente el equipo cada vez que un usuario inicia una sesión.

**NOTA**

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

- d Seleccione la hora del día en la que desea analizar su equipo en el cuadro **Hora de inicio**.
- e Para seleccionar opciones avanzadas, haga clic en **Avanzadas**. Se abrirá el cuadro de diálogo **Opciones de programación avanzadas**. 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 hora dada en caso de que el análisis esté todavía en ejecución.

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

## Acciones en caso de detección de virus

ActiveShield intenta limpiar automáticamente la mayor parte de los virus, archivos troyanos y gusanos. A continuación, puede elegir la forma de administrar los archivos infectados, incluso si desea enviarlos a los laboratorios de McAfee AVERT para su investigación.

Si ActiveShield no puede limpiar el virus, puede eliminar el archivo o ponerlo en cuarentena:

- 1 Si aparece un archivo en la lista de archivos infectados, haga clic en la casilla de activación situada delante del archivo para seleccionarlo.

### NOTA

Si la lista contiene más de un archivo, puede marcar la casilla de activación 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 **Virus** para ver los detalles de la biblioteca de información de virus.

- 2 Si la función de análisis no consigue limpiar el virus, haga clic en **Poner en cuarentena** para cifrar y aislar temporalmente los archivos infectados y sospechosos en el directorio de cuarentena hasta que se pueda tomar una medida conveniente. (Consulte *Gestión de archivos en cuarentena* para obtener más información.)
- 3 Si la función de análisis no puede limpiar el archivo o ponerlo en cuarentena, puede realizar una de las acciones siguientes:
  - ♦ Haga clic en **Eliminar** para eliminar el archivo.
  - ♦ Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin aplicar ninguna otra medida.

Si el análisis no puede limpiar ni eliminar el archivo, consulte la biblioteca de información de virus en <http://es.mcafee.com/virusInfo/default.asp?affid=152&langid=86> para obtener instrucciones sobre la eliminación manual de virus.

Si el virus no permite utilizar su conexión a Internet o impide el acceso al equipo, pruebe a utilizar el disco de emergencia para iniciarlo. En muchos casos, el disco de emergencia permite iniciar un equipo inutilizado por un virus. Consulte la sección *Creación de un disco de emergencia en la página 37* para obtener información más detallada.

Si desea obtener más ayuda, consulte la sección de ayuda en la siguiente dirección: <http://seguridad.terra.es/ayuda.asp>.

## Gestión de archivos en cuarentena

Haga clic en **En cuarentena** para cifrar y aislar temporalmente los archivos infectados y sospechosos en el directorio de cuarentena hasta adoptar una medida conveniente. Una vez limpio, puede restablecer el archivo en su ubicación original el archivo que estaba en cuarentena.

Para gestionar un archivo que se ha puesto en cuarentena:

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

Aparecerá una lista de archivos en cuarentena (Figura 2-11 en la página 35).

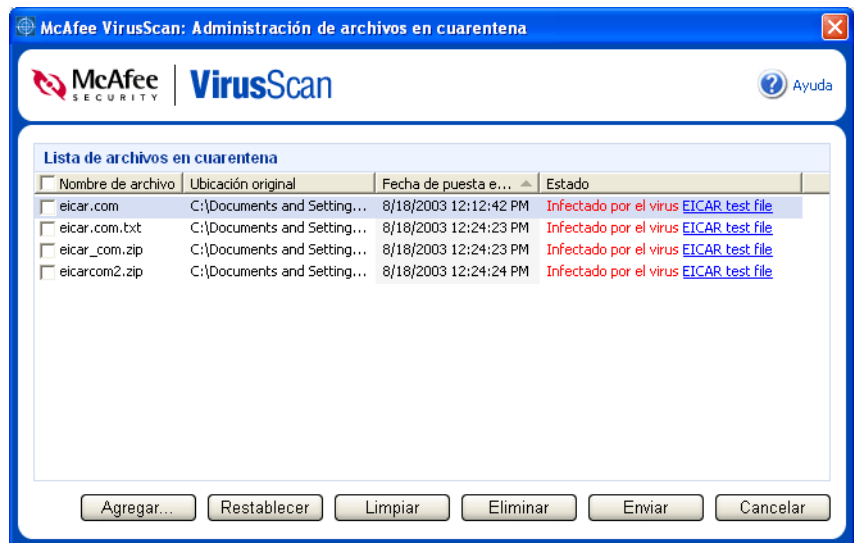


Figura 2-11. Gestión de archivos en cuarentena

- 2 Marque la casilla de activación situada junto al archivo o archivos que desee limpiar.

**NOTA**

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

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

- 3 Haga clic en **Limpiar**.
- 4 Si el archivo está limpio, haga clic en **Restablecer** para devolverlo a su ubicación original.
- 5 Si VirusScan no puede limpiar el virus, haga clic en **Eliminar** para eliminar el archivo.
- 6 Si VirusScan no puede limpiar ni eliminar el archivo, puede enviarlo a AVERT™ (siglas del inglés McAfee AntiVirus Emergency Response Team, o Equipo de respuesta de emergencia antivirus de McAfee) para su investigación:
  - a Actualice los archivos de definición de virus si tienen más de dos semanas de antigüedad.
  - b Compruebe su suscripción.
  - c Seleccione el archivo y haga clic en **Enviar** para enviar el archivo a AVERT.

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

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

## Creación de un disco de emergencia

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

### NOTA

Debe estar conectado a Internet para descargar la imagen del disco de emergencia. El disco de emergencia sólo está disponible para equipos con particiones FAT (FAT 16 y FAT 32) de disco duro. No se puede utilizar para particiones NTFS.

Para crear un disco de emergencia:

- 1 Inserte un disquete no infectado en la unidad A de un equipo no infectado. Puede utilizar la función de análisis para asegurarse de que el equipo y el disquete están libres de virus. (Consulte [Detección manual de virus en la página 28](#) para obtener más información.)
- 2 Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y haga clic en **Crear disco de emergencia**.

Se abrirá el cuadro de diálogo **Crear disco de emergencia** (Figura 2-12).



Figura 2-12. Creación de un disco de emergencia

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

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

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

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

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

- 5 Cuando aparezca un mensaje que indica que se ha creado el disco de emergencia, haga clic en **Aceptar** y cierre el cuadro de diálogo **Crear disco de emergencia**.
- 6 Extraiga el disco de emergencia de su unidad, protéjalo contra escritura y guárdelo en un lugar seguro.

## Protección de un disco de emergencia contra escritura

Para proteger un disco de emergencia contra escritura:

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

## Utilización de un disco de emergencia

Para usar un disco de emergencia:

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

Aparecerá una ventana de color gris con varias opciones.

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

### **NOTA**

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

## Actualización de un disco de emergencia

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

## Información automática sobre virus

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

### Envío de información al Mapa Mundial de Virus (World Virus Map)

Para enviar automáticamente información sobre virus al Mapa Mundial de Virus (World Virus Map):

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

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

- 2 Haga clic en la ficha **Informes del mapa de virus** (Figura 2-13).

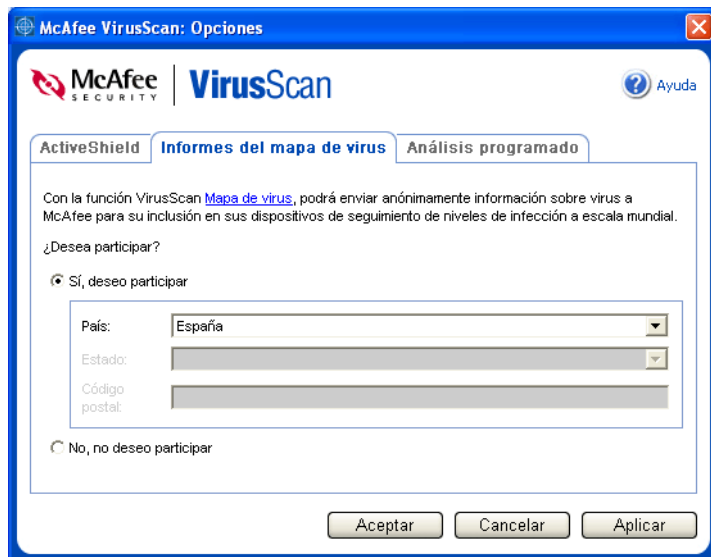


Figura 2-13. Opciones de informes del Virus Map

- 3 Acepte la opción predeterminada **Sí, deseo participar** para enviar información sobre virus de manera anónima a McAfee para incorporarla al Mapa Mundial de Virus (World Virus Map) que incluye los niveles de infección a escala mundial. En caso contrario, seleccione **No, no deseo participar** para no enviar ninguna información.
- 4 Si reside en los Estados Unidos, seleccione el estado y el código postal correspondiente a la ubicación física del equipo. En caso contrario, VirusScan tratará de seleccionar automáticamente el país en el que se encuentre su equipo.
- 5 Haga clic en **Aceptar**.

## Visualización del Mapa Mundial de Virus (World Virus Map)

Participe o no en el Mapa Mundial de Virus (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 Mapa Mundial de Virus (World Virus Map):

- Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y haga clic en **Mapa Mundial de Virus (World Virus Map)**.

Aparecerá la página Web **Mapa Mundial de Virus (World Virus Map)** (Figura 2-14).

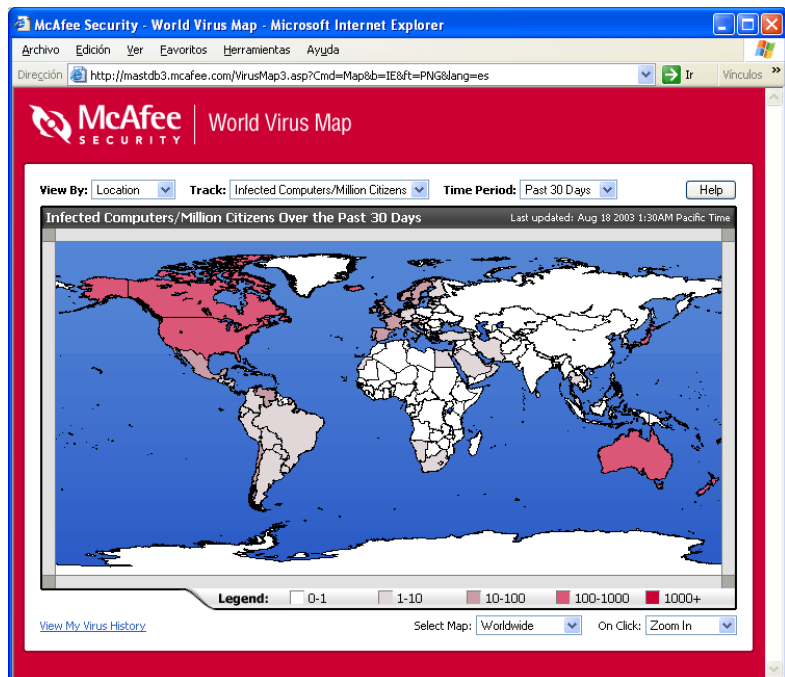


Figura 2-14. Mapa Mundial de Virus (World Virus Map)

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

La sección **Virus Tracking** enumera los totales acumulados correspondientes a los archivos examinados y a los archivos y equipos infectados sobre los que se ha recibido información desde la fecha indicada.

## Actualización de VirusScan

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

Los archivos de definición de virus suelen tener unos 100 KB y, por consiguiente, su descarga no afecta prácticamente al rendimiento del sistema.

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

## Comprobación automática de actualizaciones

Debe estar conectado a Internet para que VirusScan compruebe las actualizaciones disponibles. Si hay una actualización, se mostrará una alerta (parecida a la [Figura 2-15](#)).



Figura 2-15. Alerta de actualización

Para actualizar VirusScan:

- 1 Haga clic en **Actualizar ahora** en la alerta **Actualización disponible** (Figura 2-15).
- 2 Regístrese en el sitio Web de McAfee si VirusScan así se lo pide. La actualización se descargará automáticamente.
- 3 Haga clic en **Finalizar** en el cuadro de diálogo **Finalización del Asistente de VirusScan** cuando la actualización haya terminado de instalarse.

**NOTA**

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

Si está demasiado ocupado para actualizar VirusScan cuando aparezca la alerta, puede posponer la operación de actualización como se indica a continuación:

- Haga clic en **Recibir un recordatorio más tarde** en la alerta **Actualización disponible** (Figura 2-15 en la página 41), seleccione el plazo en que desee que se le recuerde la actualización y haga clic en **Aceptar**. Puede escoger entre 10 minutos, 20 minutos, 30 minutos, 1 hora, 2 horas o 4 horas (opción predeterminada).
- Haga clic en **Continuar con lo que estoy haciendo** para cerrar la alerta sin tomar ninguna medida.

## Comprobación manual de actualizaciones

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

Para comprobar manualmente la existencia de actualizaciones de VirusScan:

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

Se abrirá el cuadro de diálogo **Actualizaciones de SecurityCenter**.

- 3 Haga clic en **Comprobar ahora**.

Si existiese una actualización, se abriría el cuadro **Actualizaciones de VirusScan** (consulte la [Figura 2-16](#)). 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 se le pide que lo haga. El **Asistente para actualizaciones** instalará la actualización automáticamente.
- 5 Haga clic en **Finalizar** cuando la actualización haya terminado de instalarse.

**NOTA**

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



# Índice alfabético

## A

- ActiveShield
  - activar, 15
  - analizar archivos adjuntos de mensajes instantáneos de entrada, 20
  - analizar correo electrónico y archivos adjuntos, 18
  - analizar sólo archivos de programas y documentos, 21
  - analizar todos los archivos, 20
  - analizar todos los tipos de archivo, 20
  - comprobar, 10
  - desactivar, 16
  - detectar scripts y gusanos, 22
  - detectar virus nuevos desconocidos, 22
  - detener, 17
  - iniciar, 17
  - limpiar un virus, 25
  - opción de análisis predeterminada, 17 a 18, 20, 22 a 23
  - opciones de análisis, 16
- actualizar
  - disco de emergencia, 38
  - VirusScan
    - automáticamente, 41
    - manualmente, 42
- alertas
  - de archivos infectados, 25
  - de correo electrónico infectado, 26
  - de gusanos potenciales, 27
  - de scripts sospechosos, 26
  - de virus, 25
- análisis programados, 32
- analizar
  - análisis automático, 32
  - analizar manualmente desde el Explorador de Windows, 31
  - analizar manualmente desde la barra de herramientas de Microsoft Outlook, 31
  - archivos comprimidos, 29
  - comprobar, 11 a 12
  - desde el Explorador de Windows, 31
  - desde la barra de herramientas de Microsoft Outlook, 31
  - detectar manualmente, 28
  - detectar nuevos virus desconocidos, 30
  - eliminar un virus, 34
  - nuevos virus desconocidos, 30
  - opción Analizar el contenido de los archivos comprimidos, 29
  - opción Analizar si hay aplicaciones potencialmente no deseadas, 30
  - opción Analizar subcarpetas, 29
  - opción Analizar todos los archivos, 29
  - programar análisis automáticos, 32
  - scripts y gusanos, 22
  - sólo archivos de programas y documentos, 21
  - subcarpetas, 29
  - todos los archivos, 20, 29
- archivos adjuntos de mensajes instantáneos de entrada
  - analizar, 20
  - limpiar automáticamente, 20
- archivos troyanos
  - alertas, 25
  - detectar, 34
- Asistente para la actualización, 17
- AVERT, enviar archivos infectados, 36

## C

- comprobar funcionamiento de VirusScan, 10
- configurar
  - VirusScan
    - ActiveShield, 15
    - analizar, 27
- correo electrónico y archivos adjuntos
  - analizar, 18
  - desactivar limpieza automática, 19
  - eliminar, 26
  - limpiar, 26
  - limpiar automáticamente, 18
  - poner en cuarentena, 26
- crear un disco de emergencia, 37
- cuarentena
  - agregar archivos sospechosos, 35
  - eliminar archivos, 35
  - eliminar archivos infectados, 36
  - enviar archivos infectados, 36
  - gestionar archivos infectados, 35
  - limpiar archivos, 35 a 36
  - restablecer archivos limpios, 35 a 36

## D

- descargar VirusScan, 7
- disco de emergencia
  - actualizar, 38
  - crear, 37
  - proteger contra escritura, 38
  - usar, 34, 38

## E

- enviar archivos infectados a AVERT, 36
- Explorador de Windows, 31

## F

- funciones nuevas, 5

## G

- gusanos
  - alertas, 25, 27
  - detectar, 25, 34
  - detener, 27

## I

- instalar VirusScan, 7
- introducción a VirusScan, 5

## L

- lista de archivos infectados (Analizar), 30, 34

## M

- Mapa Mundial de Virus (World Virus Map)
  - informar, 39
  - ver, 40
- Microsoft Outlook, 31

## O

- opción Analizar el contenido de los archivos comprimidos (Analizar), 29
- opción Analizar si hay aplicaciones potencialmente no deseadas (Analizar), 30
- opción Analizar subcarpetas (Analizar), 29
- opción Analizar todos los archivos (Analizar), 29
- opción Analizar virus nuevos y desconocidos (Analizar), 30
- opciones de análisis
  - ActiveShield, 16, 20 a 21
  - analizar, 27

## P

- proteger un disco de emergencia contra escritura, 38

## R

- requisitos del sistema, 6

## S

- scripts
  - alertas, 26
  - detener, 26
  - permitir, 26
- ScriptStopper, 22
- suscribirse a VirusScan, 7

## U

- usar un disco de emergencia, 38

**V**

## virus

- alertas, [25](#)
- detectar, [34](#)
- detectar con ActiveShield, [25](#)
- detener gusanos potenciales, [27](#)
- detener scripts sospechosos, [26](#)
- eliminar, [25, 34](#)
- eliminar archivos infectados, [25](#)
- eliminar los archivos adjuntos infectados del correo electrónico, [26](#)
- informar automáticamente, [39 a 40](#)
- limpiar, [25, 34](#)
- limpiar archivos adjuntos infectados del correo electrónico, [26](#)
- permitir scripts sospechosos, [26](#)
- poner en cuarentena, [25, 34](#)
- poner en cuarentena archivos adjuntos infectados del correo electrónico, [26](#)
- poner en cuarentena archivos infectados, [25](#)

## VirusScan

- actualizar automáticamente, [41](#)
- actualizar manualmente, [42](#)
- análisis programados, [32](#)
- analizar desde el Explorador de Windows, [31](#)
- analizar desde la barra de herramientas de Microsoft Outlook, [31](#)
- comprobar, [10](#)
- descargar, [7](#)
- informar sobre virus automáticamente, [39 a 40](#)
- instalar, [7](#)
- introducción, [5](#)
- suscribirse a, [7](#)

**W**

- WormStopper, [22](#)

