McAfee®

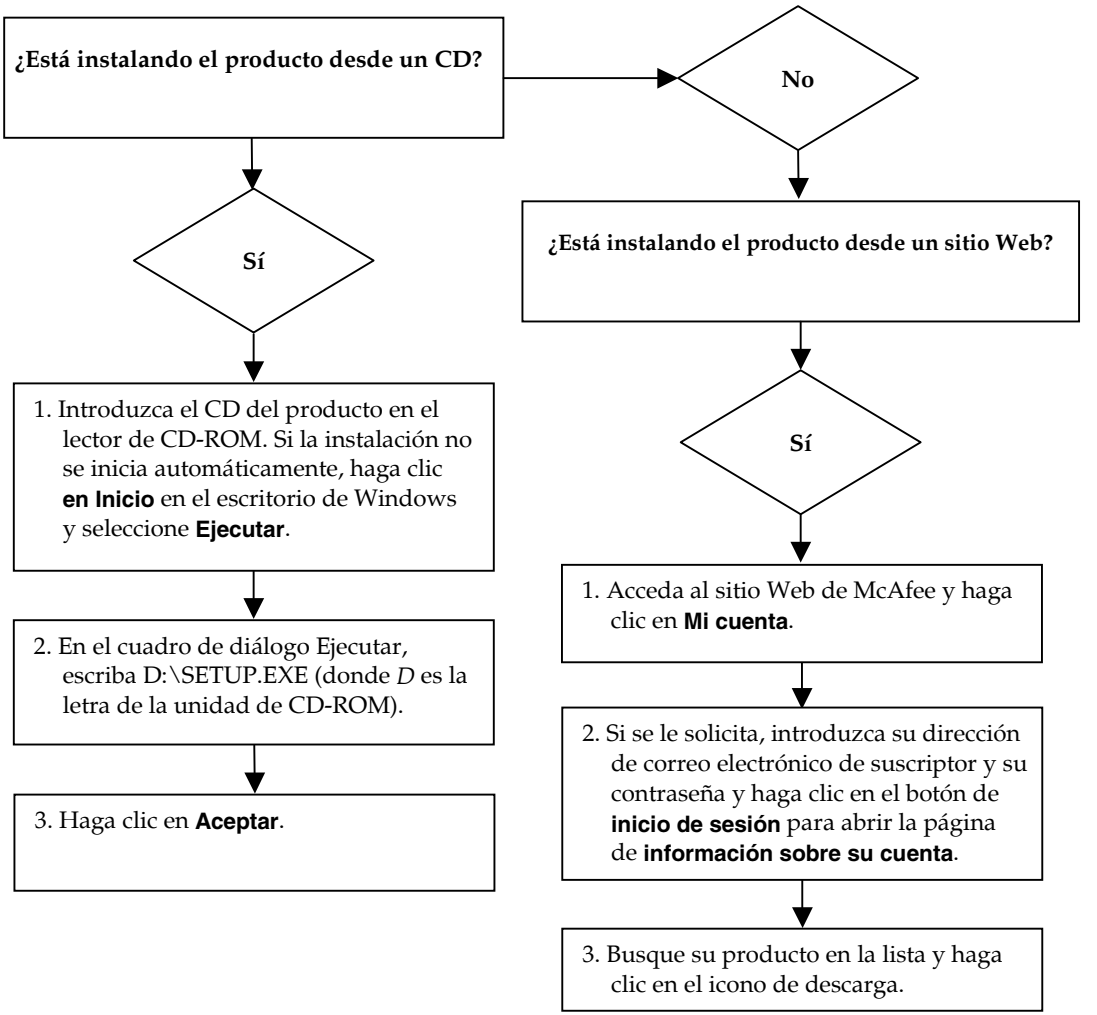
virusscan®

Manual del usuario

McAfee®

Tarjeta de inicio rápido

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



Si desea obtener más información

Para ver los manuales de usuario del CD del producto, asegúrese de que tiene instalado Acrobat Reader; en caso contrario, instálelo ahora desde el CD del producto de McAfee.

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

Ventajas del registro

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

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

  Vaya 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 software o CD si está defectuoso o dañado.
- Actualizaciones de filtros de SpamKiller durante un año después de instalarlo tras la adquisición del software SpamKiller.

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

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

Soporte técnico

Para obtener asistencia técnica, visite

http://www.mcafeeayuda.com/.

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

Los usuarios experimentados también pueden utilizar las opciones avanzadas, que incluyen la Búsqueda por claves o el Árbol de la ayuda. Si no logra encontrar una solución a su problema, puede acceder a nuestros servicios GRATUITOS Chat Now! y Email Express!Estas opciones le ayudan 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

Introducción 1

Bienvenido a McAfee VirusScan.

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

Gracias a él, disfrutará de las funciones siguientes:

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

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 diarias automáticas de VirusScan protegen frente a las amenazas informáticas más recientes, incluso las aún no identificadas.
- **Análisis rápido en segundo plano**
  Los análisis rápidos y discretos identifican y destruyen virus, troyanos, gusanos, software espía, de publicidad y de marcación, y otros 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 de 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.

Requisitos del sistema

- Microsoft® Windows 98, Windows Me, Windows 2000 o Windows 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
- 40 MB de espacio en el disco duro
- Microsoft® Internet Explorer 5.5 o posterior

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

Programas de correo electrónico admitidos

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

Programas de mensajería instantánea admitidos

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

Comprobación del funcionamiento de VirusScan

Antes de utilizar VirusScan por primera vez, es recomendable probar su instalación. Siga las instrucciones que se indican a continuación para verificar por separado las funciones de 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. Diríjase a http://www.eicar.com/ en el navegador Web.
2. Haga clic en el vínculo **The AntiVirus testfile eicar.com** (Archivo de prueba antivirus de eicar.com).
3. Desplácese hasta la parte inferior de la página. En **Descargar** verá cuatro vínculos.
4. Haga clic en **eicar.com**.

Si ActiveShield funciona correctamente, detectará el archivo eicar.com inmediatamente después de hacer clic en el vínculo. Puede intentar suprimir o poner en cuarentena archivos infectados para comprobar el tratamiento que da ActiveShield a los virus. Consulte la sección *Descripción de las alertas de seguridad* en la página 24 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 **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 33 para obtener información más detallada.

Utilización de McAfee SecurityCenter

McAfee SecurityCenter es una herramienta de seguridad universal, a la que puede acceder desde su icono 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.
- 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 productos.
- Acceder rápidamente a las preguntas más frecuentes y a la información detallada de la cuenta en el sitio Web de McAfee.

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

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

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

Para abrir McAfee SecurityCenter:

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

2 Haga clic en **Abrir SecurityCenter**.

Para acceder 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 desea utilizar.

Utilización de McAfee VirusScan 2

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 14).

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.

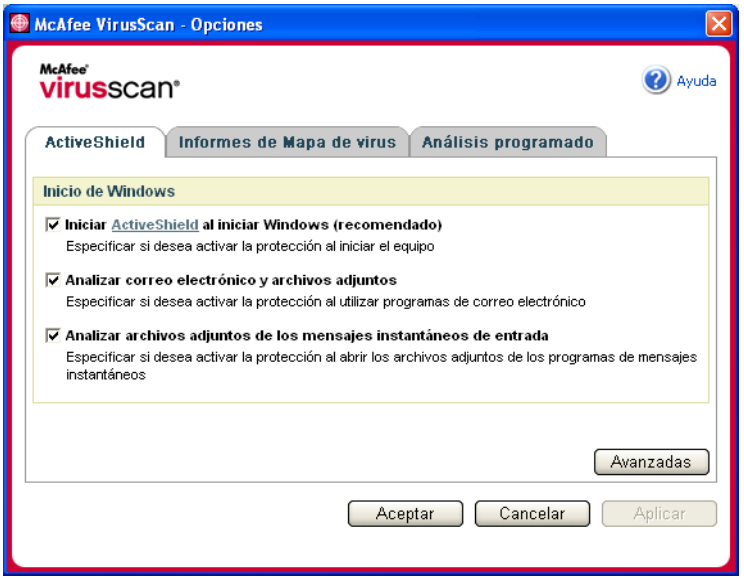


Figura 2-1. Opciones de ActiveShield

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 14).

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 14).

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 14).

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 17) 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**.

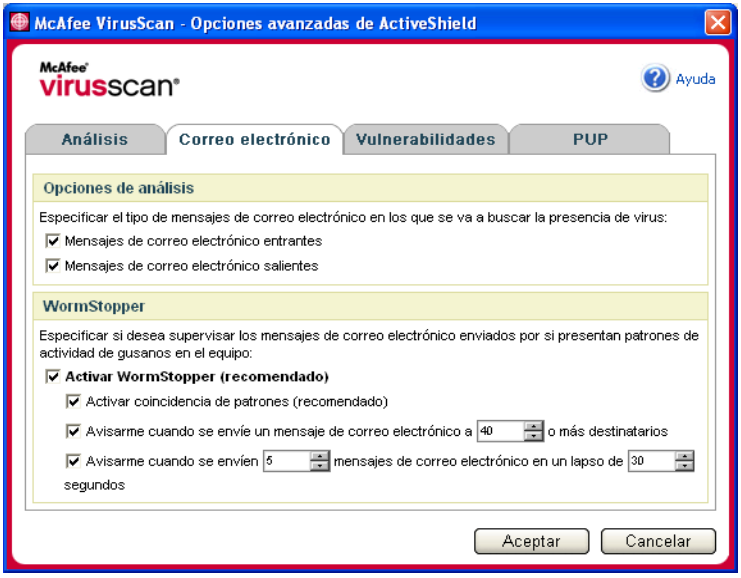


Figura 2-2. Opciones avanzadas de ActiveShield: ficha Correo electrónico

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 25 para obtener información detallada):

- Bloqueo automático de mensajes sospechosos de correo electrónico saliente

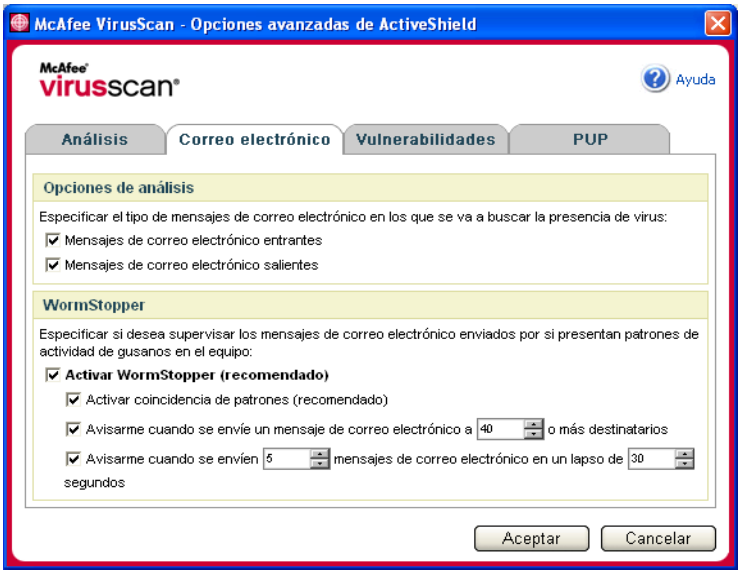


Figura 2-3. Opciones avanzadas de ActiveShield: ficha Correo electrónico

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 14).

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 20).
3. Haga clic en **Todos los archivos (recomendado)** y después en **Aceptar**.

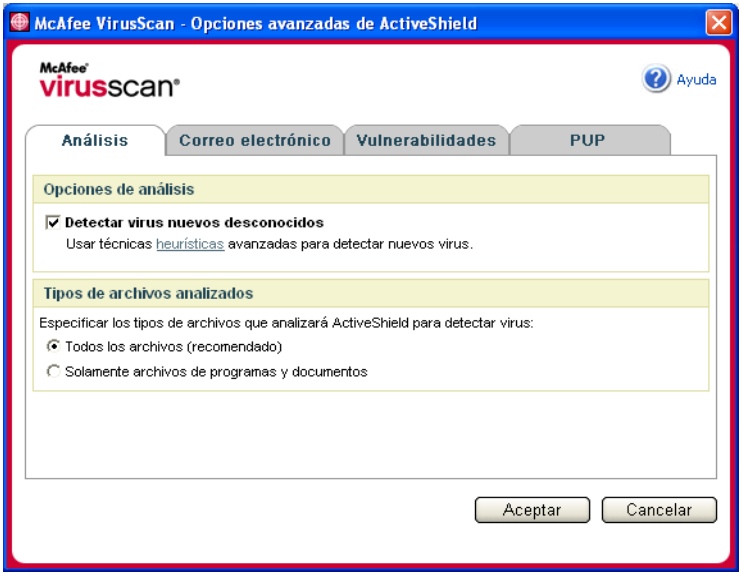


Figura 2-4. Opciones avanzadas de ActiveShield: ficha Análisis

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 (archivo DAT) más reciente determina los tipos de archivo que ActiveShield puede analizar. Para que ActiveShield sólo analice los documentos y los archivos de programas:

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, ScriptStopperTM 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 **Exploits** (Figura 2-5).
3. Haga clic en **Activar ScriptStopper (recomendado)** y después en **Aceptar**.

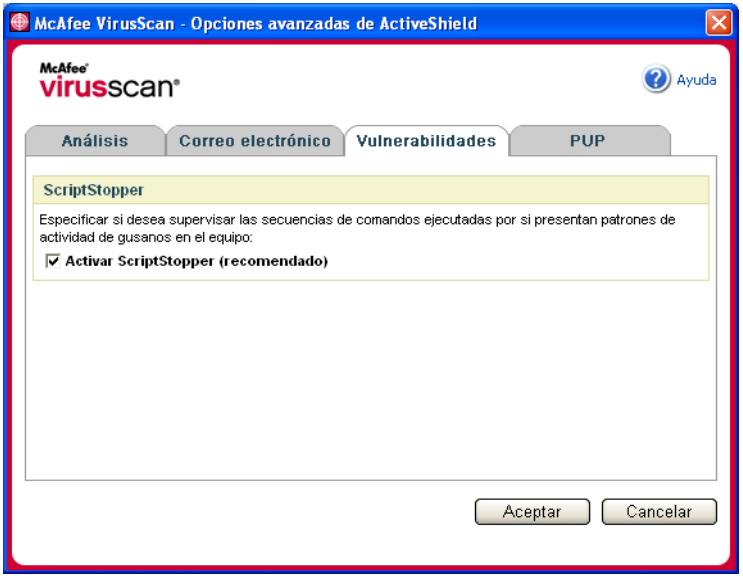


Figura 2-5. Opciones avanzadas de ActiveShield: ficha Exploits

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 **Archivos PUPs** (Figura 2-6).
3. Haga clic en **Analizar programas potencialmente no deseados (recomendado)** y a continuación en **Aceptar**.

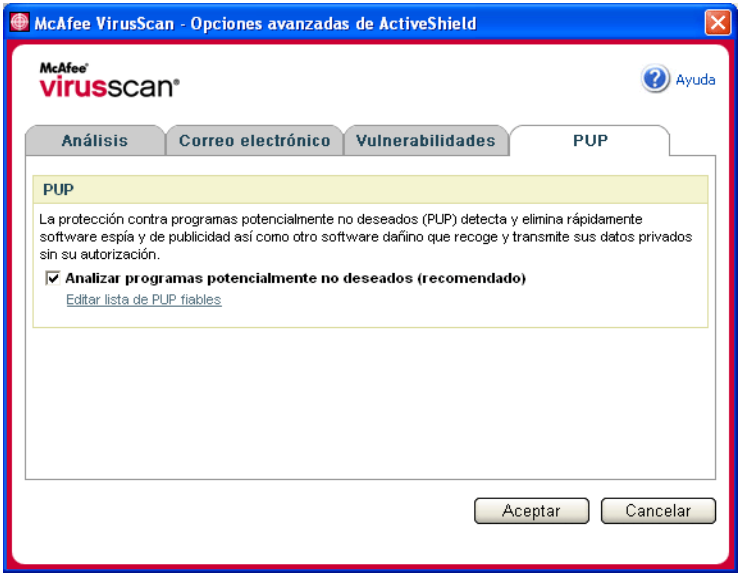


Figura 2-6. Opciones avanzadas de ActiveShield: ficha Archivos PUPs

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.

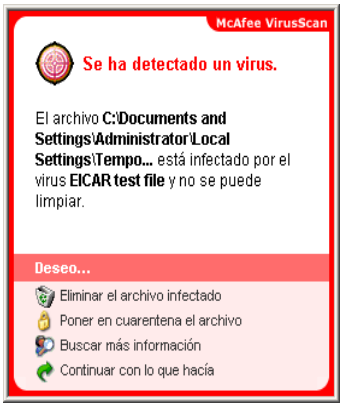


Figura 2-7. Alerta de virus

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 este guión** 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 estaba 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.

Gestión de PUP

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

- Haga clic en **Buscar más información** para ver el nombre, la ubicación y la acción recomendada asociados al 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 estaba 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 **Archivos PUPs**.

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).

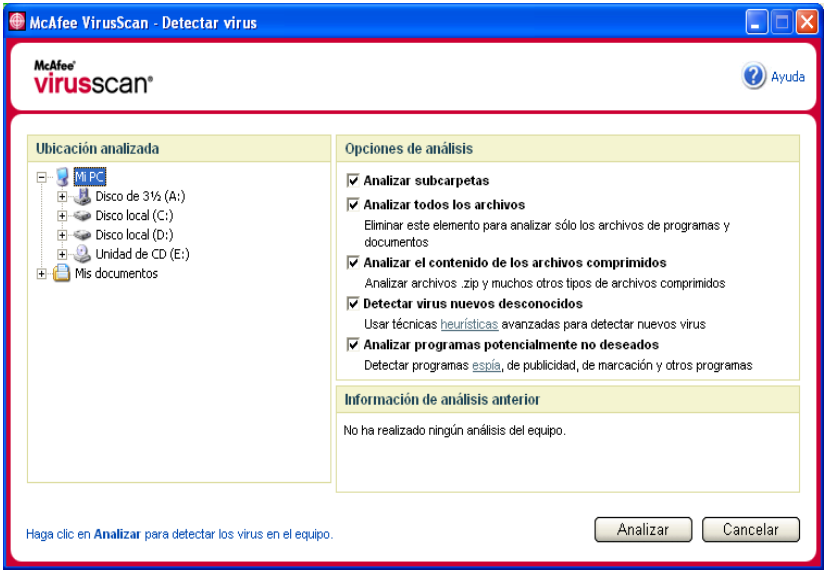


Figura 2-8. Cuadro de diálogo Detectar virus

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 la 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.

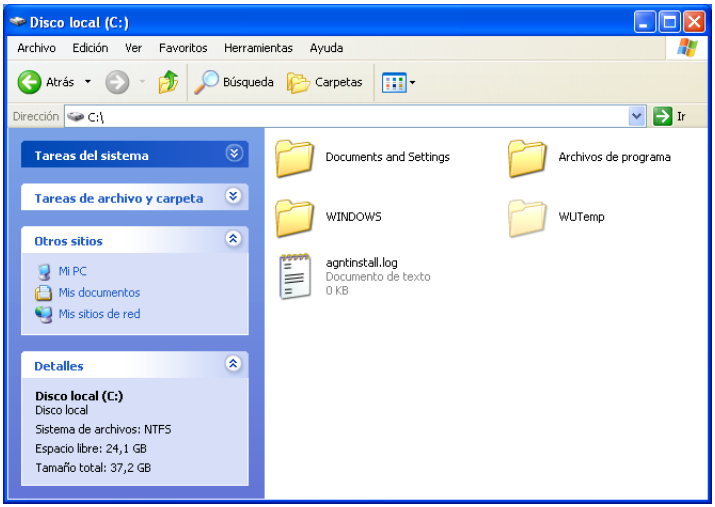


Figura 2-9. Contenido del disco local

- **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 detectar 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 colocan virus en un archivo .ZIP y, a su vez, insertan este archivo .ZIP dentro de otro archivo .ZIP con el objeto de intentar eludir la acción de los analizadores antivirus. La función Analizar los puede detectar si esta opción está seleccionada.
- **Detectar virus nuevos desconocidos**: utilice esta opción para encontrar los virus más recientes, para los que puede suceder que no se haya desarrollado aún 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.

5 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).

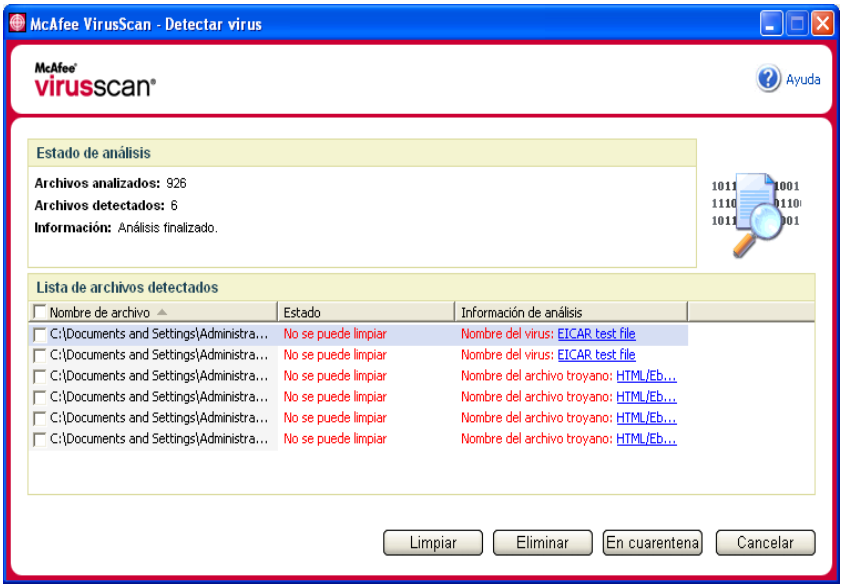


Figura 2-10. Resultados de exploración

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

6 Si 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 33.

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 27).

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 27).

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 32).

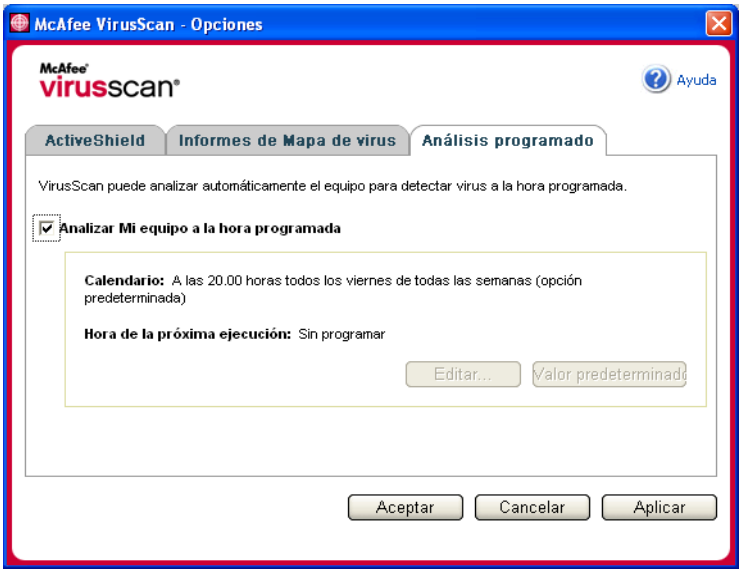


Figura 2-11. Opciones del análisis programado

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 **Planificar tarea** y seleccione las opciones adicionales en el área dinámica situada debajo:

  Diaria: especifique el número de días entre análisis.

  Semanal (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

La función Analizar 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 34 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 36 para obtener información más detallada.

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

Gestión de archivos en cuarentena

La función 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).

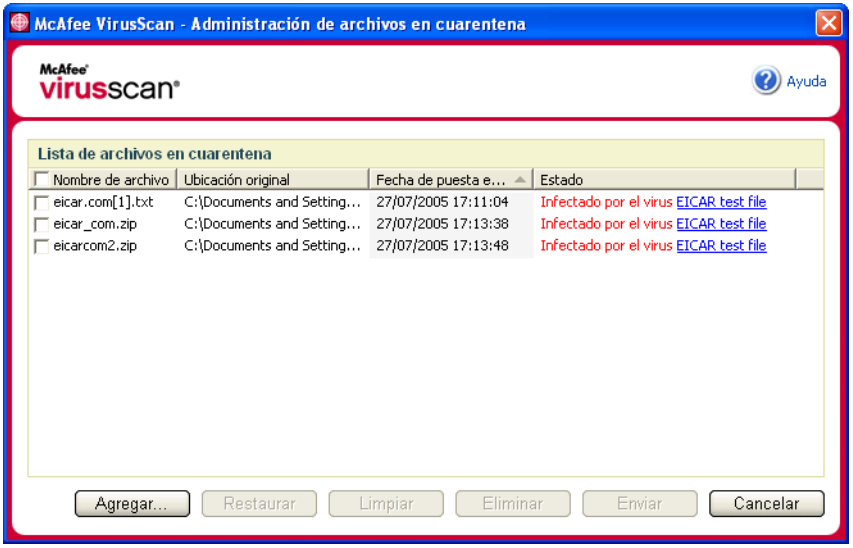


Figura 2-12. Cuadro de diálogo Gestionar archivos en cuarentena

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 27 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 2-13).

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

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

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

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

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

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

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

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

Protección de un disco de emergencia contra escritura

Para proteger un disco de emergencia contra escritura:

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

Utilización de un disco de emergencia

Para usar un disco de emergencia:

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

   Aparecerá una ventana de color gris con varias opciones.
4. Elija la opción que mejor se adapte a sus necesidades pulsando las teclas de función (por ejemplo, F2, F3).

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

Actualización de un disco de emergencia

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

Información automática sobre virus

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

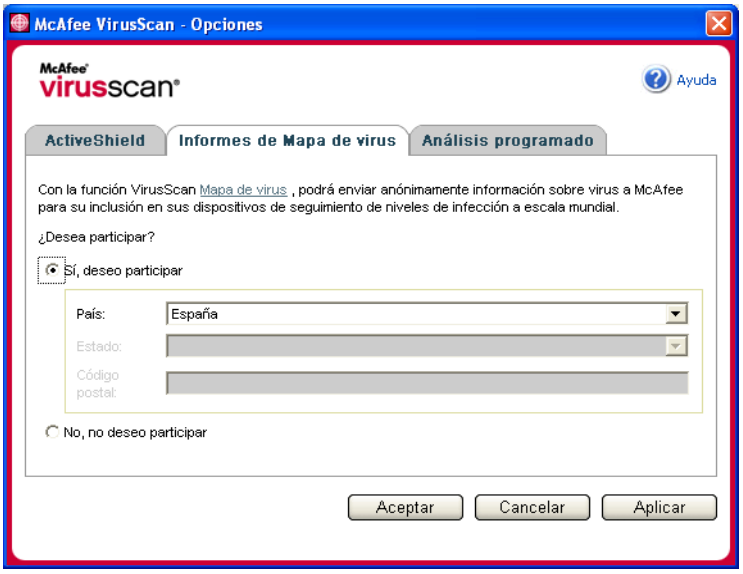


Figura 2-14. Opciones de informes del mapa de virus

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).

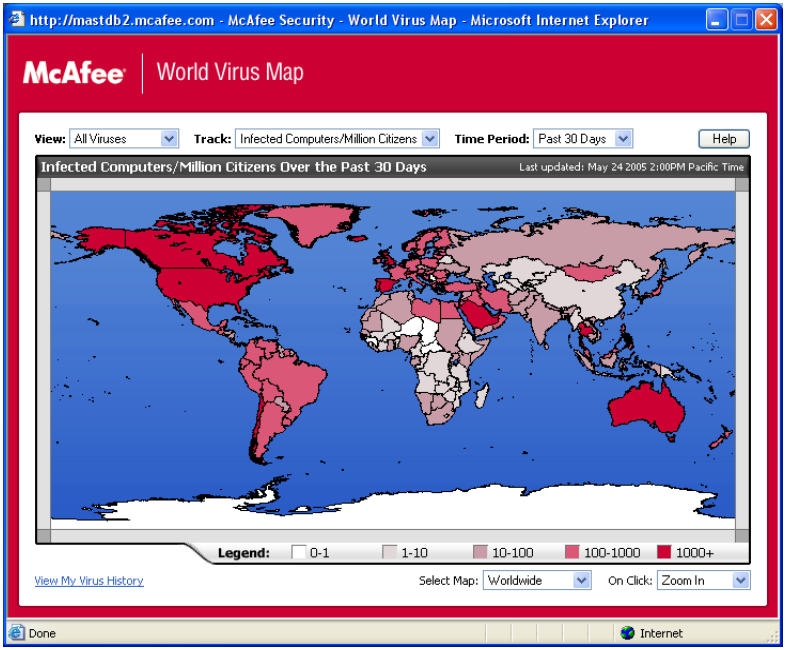


Figura 2-15. World Virus Map

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 42). 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.

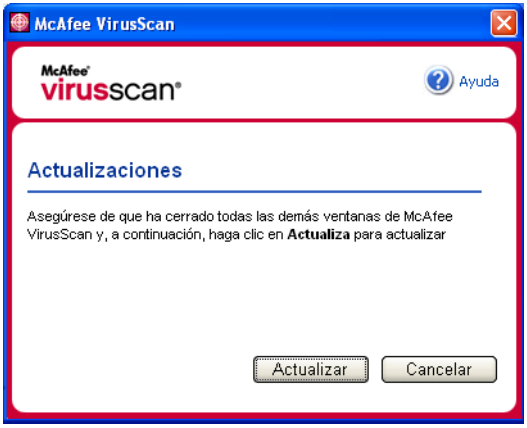


Figura 2-16. Cuadro de diálogo Actualizaciones

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.

Índice

A

C

D

E

F

G

I

L

M

O

P

R

S

T

U

V

W