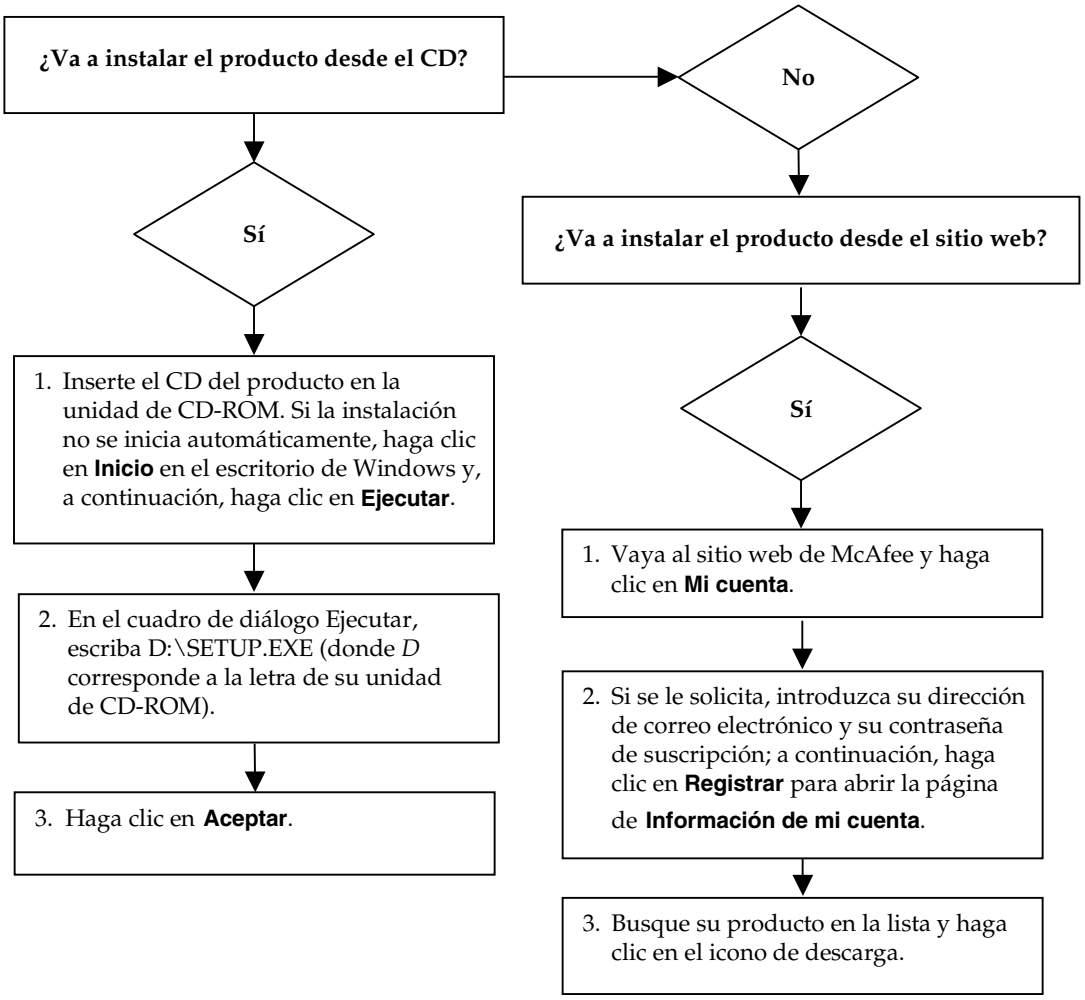
McAfee®

virusscan®

Manual del usuario

Tarjeta de inicio rápido

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



Si desea obtener más información

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

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

Ventajas del registro

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

- Soporte electrónico GRATUITO.
- Actualizaciones de los archivos de definición de virus (.DAT) durante un año a partir de la instalación cuando adquirió el software de VirusScan.

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

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

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

Soporte técnico

Si desea obtener soporte técnico, visite la página http://www.mcafeeayuda.com/. Nuestro sitio de soporte permite acceder durante las 24 horas del día al sencillo Asistente de respuestas para obtener soluciones sobre las preguntas de soporte más comunes.

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

Contenido

Tarjeta de inicio rápido . . . . . **iii**

1 Introducción **7**

Funciones nuevas 7
Requisitos del sistema 9
Comprobación del funcionamiento de VirusScan 9
Comprobación del funcionamiento de ActiveShield 9
Comprobación del funcionamiento de la función de análisis 10
Utilización de McAfee SecurityCenter 12

2 Utilización de McAfee VirusScan **13**

Utilización de ActiveShield 13
Activación o desactivación de ActiveShield 13
Configuración de las opciones de ActiveShield 14
Acciones que ActiveShield lleva a cabo al descubrir un virus 22
Análisis manual del equipo 25
Análisis manual de virus y programas potencialmente no deseados 25
Análisis automático de virus y programas potencialmente no deseados 29
Si el análisis encuentra un virus o un programa potencialmente no deseado 32
Gestión de archivos en cuarentena 33
Creación de un disco de emergencia 34
Protección de un disco de emergencia contra escritura 35
Utilización de un disco de emergencia 36
Actualización de un disco de emergencia 36
Información automática sobre virus 36
Envío de información al World Virus Map 37
Visualización del World Virus Map 38
Actualización de VirusScan 39
Comprobación automática de actualizaciones 39
Comprobación manual de actualizaciones 39

Índice alfabético **41**

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 este cortafuegos, disfrutará de las funciones siguientes:

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

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

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

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

Funciones nuevas

Esta versión de VirusScan incluye las siguientes funciones nuevas:

- **Análisis de programas potencialmente no deseados**
  VirusScan puede analizar programas potencialmente no deseados (incluidos los programas espía, de publicidad y de marcación) durante el análisis manual, el análisis de correo electrónico saliente, los mensajes instantáneos, a través del menú con métodos abreviados del Explorador de Windows y del icono de la barra de herramientas de Microsoft Outlook.

- **Análisis de archivos adjuntos salientes de gran tamaño**
  Para afrontar el uso cada vez mayor de las conexiones de Internet y proveedores de servicio de banda ancha aumentando las capacidades de almacenamiento de correo electrónico y los tamaños de las transmisiones, VirusScan se ha optimizado para analizar los archivos adjuntos de correo electrónico de gran tamaño sin interferir en los valores de tiempo de espera de los programas de correo electrónico.

- **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 secuencias de comandos malintencionadas y gusanos.

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

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

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

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

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

Requisitos del sistema

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

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

Comprobación del funcionamiento de VirusScan

Antes del uso inicial de VirusScan, se recomienda probar la instalación. Siga las instrucciones que se indican a continuación para verificar por separado las funciones de análisis y ActiveShield.

Comprobación del funcionamiento de ActiveShield

Para comprobar el funcionamiento de ActiveShield:

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

Si ActiveShield funciona correctamente, detectará el archivo eicar.com inmediatamente después de hacer clic en el vínculo. Puede intentar suprimir o poner en cuarentena los archivos infectados para comprobar el tratamiento que da ActiveShield a los virus. Consulte la sección *Acciones que ActiveShield lleva a cabo al descubrir un virus* en la página 22 para obtener información más detallada.

Comprobación del funcionamiento de la función de análisis

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

Para descargar los archivos de prueba:

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

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

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

   d. Haga clic en cada uno de los vínculos para descargar el archivo correspondiente. Se mostrará el cuadro de diálogo **Descarga de archivos** para efectuar la descarga de cada uno de ellos.
   e. Haga clic en **Guardar**, después en el botón **Crear carpeta nueva** y, a continuación, cambie el nombre de la carpeta a **Carpeta de análisis de VSO**.
   f. Haga doble clic en **Carpeta de análisis VSO** y después otra vez en **Guardar** en cada cuadro de diálogo **Guardar como**.
3. Cuando haya terminado de descargar los archivos, cierre Internet Explorer.
4. Active ActiveShield: haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y haga clic en **Activar**.

Para comprobar el funcionamiento de la función de análisis:

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

      De esta forma, la función de análisis sólo examinará dicha carpeta. También puede colocar los archivos en ubicaciones aleatorias del disco duro para lograr una demostración más convincente de las habilidades de la función de Análisis.
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 **Carpeta de análisis de VSO**. Los archivos de comprobación EICAR guardados en dicha carpeta aparecerán en la **Lista de archivos detectados**. Si es así, la función de análisis funciona correctamente.

Puede intentar eliminar o poner en cuarentena los archivos infectados para comprobar el tratamiento que da la función de análisis a los virus. Consulte la sección *Si el análisis encuentra un virus o un programa potencialmente no deseado* en la página 32 para obtener información más detallada.

Utilización de McAfee SecurityCenter

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

- Obtener un análisis de seguridad del equipo.
- Ejecutar, administrar y configurar todas las suscripciones de McAfee con un solo icono.
- Ver alertas de virus actualizados continuamente y la información más reciente sobre productos.
- Acceder rápidamente a las preguntas más frecuentes e 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 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 McAfee VirusScan 2

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.

Activación o desactivación de ActiveShield

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

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

Activación de ActiveShield

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

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

Si ActiveShield sigue configurado para iniciarse al abrir Windows, se mostrará un mensaje que indica que ya está protegido contra el ataque de virus. De lo contrario, aparecerá un cuadro de diálogo que le permitirá configurar ActiveShield para que se inicie al abrir Windows (figura 2-1 en la página 14).

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 de 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.

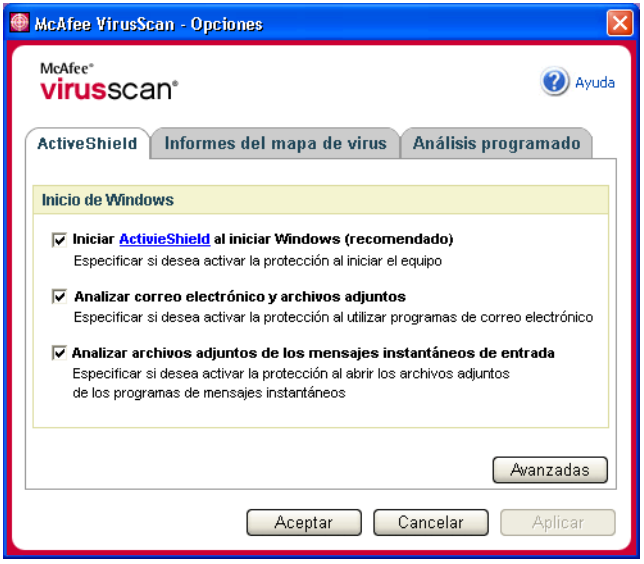


Figura 2-1. Opciones de ActiveShield

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 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, 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 14).

2 Desactive la casilla de verificación **Iniciar ActiveShield al iniciar Windows** (recomendado) y haga clic en **Aplicar** para guardar los cambios.

3 Haga clic en **Aceptar** para confirmar y, a continuación, en **Aceptar**, 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 14) y la opción **Limpiar automáticamente los archivos adjuntos infectados (recomendado)** (figura 2-2 en la página 17).

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

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

- Eudora 5.0 o versión posterior
- Pegasus 4.0 o versión posterior

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

Si desactiva la opción **Analizar correo electrónico y archivos adjuntos**, las opciones de Exploración de correo electrónico (figura 2-2 en la página 17) y la opción de WormStopper (figura 2-5 en la página 22) se desactivan automáticamente. Si desactiva el análisis de correo electrónico saliente, las opciones de WormStopper se desactivan automáticamente.

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

Correo electrónico de entrada

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

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

Correo electrónico de salida

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

- Intenta limpiar el mensaje infectado.
- Intenta poner en cuarentena el mensaje o eliminarlo si no lo puede limpiar.

NOTA
Para obtener detalles sobre los errores de análisis de correos electrónicos salientes, consulte la ayuda en línea.

De forma predeterminada, la ventana **Mostrar estado de análisis de correo electrónico saliente** está desactivada y la ventana de estado sólo aparece si se produce algún error. Puede seleccionar esta opción (en la ficha Análisis de correo del cuadro de diálogo Opciones avanzadas de ActiveShield) para que se muestre siempre la ventana de estado de análisis.

Desactivación del análisis de correo electrónico

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

Para desactivar la exploración de correo entrante o saliente:

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

Si el servidor de correo electrónico está configurado de modo que sólo se reciba y envíe correo electrónico mientras el usuario está utilizando su equipo, puede desactivar la limpieza automática para que aparezcan alertas que le pidan que limpie los mensajes infectados. Siga el procedimiento siguiente para desactivar la limpieza automática y, a continuación, consulte *Gestión del correo electrónico infectado* en la página 23 para obtener más información sobre la forma de responder a las alertas.

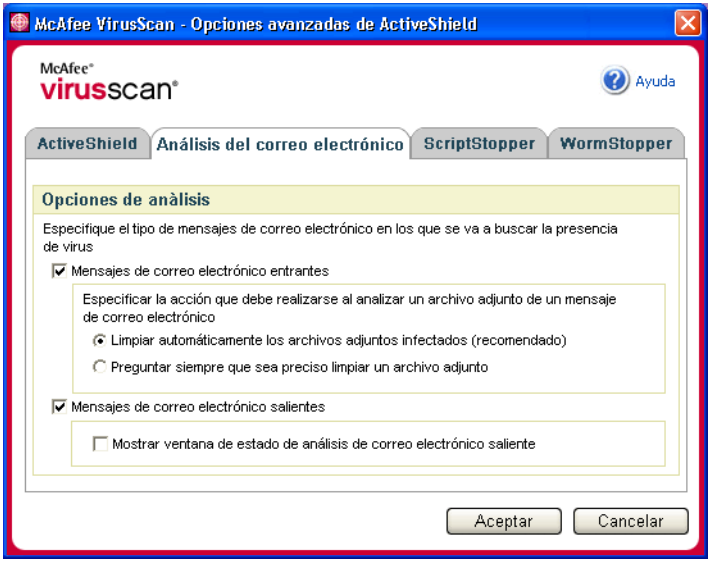


Figura 2-2. Opciones de análisis del correo electrónico

Desactivación de la limpieza automática de 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 en la página 17).
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 14).

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** (recomendada), 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).

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

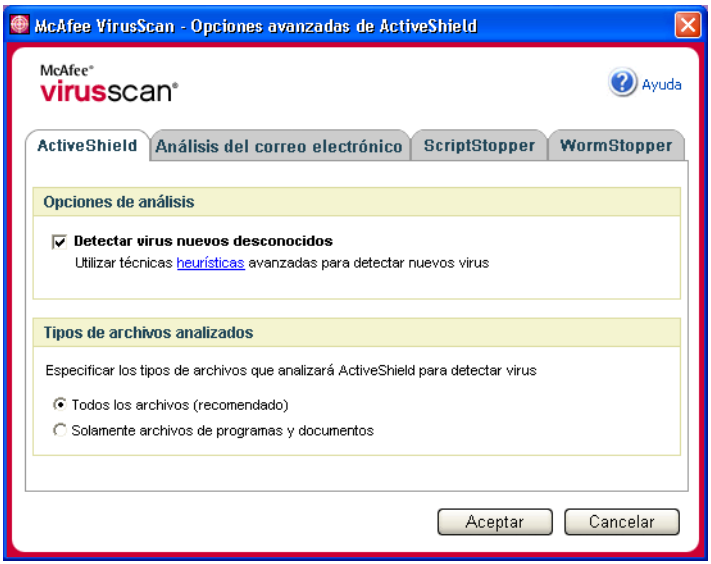


Figura 2-3. Opciones avanzadas de ActiveShield

Análisis exclusivo de los archivos de programas y documentos

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

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

2 Haga clic en **Avanzadas** y, a continuación, en la ficha **ActiveShield** (figura 2-3).

3 Haga clic en **Solamente archivos de programas y documentos** y, a continuación, en **Aceptar**.

Detección de virus nuevos desconocidos

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

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

1. Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y haga clic en **Opciones**.
2. Haga clic en **Avanzadas** y, a continuación, en la ficha **ActiveShield** (figura 2-3 en la página 19).
3. Haga clic en **Detectar virus nuevos desconocidos** y, a continuación, en **Aceptar**.

Análisis de secuencias de comandos y gusanos

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

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

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

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

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

1. Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y haga clic en **Opciones**.
2. Haga clic en **Avanzadas** y, a continuación, en la ficha **ScriptStopper**.
3. Haga clic en **Activar ScriptStopper (recomendado)** (figura 2-4 en la página 21).

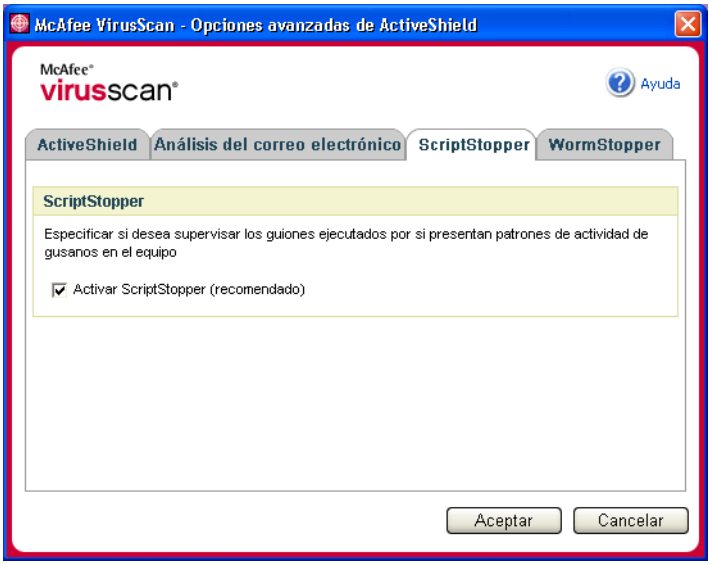


Figura 2-4. Opciones de ScriptStopper

4 Haga clic en la ficha **WormStopper**, luego en **Activar WormStopper (recomendado)** y, a continuación, en **Aceptar** (figura 2-5 en la página 22).

De forma predeterminada están activadas las siguientes opciones detalladas:

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

> **NOTA**
> Si modifica el número de destinatarios o segundos para controlar los mensajes de correo enviados, es posible que se realicen detecciones no válidas. McAfee recomienda que haga clic en **No** para conservar el valor predeterminado. De lo contrario, haga clic en **Sí** para cambiar el ajuste predeterminado 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 24 para obtener información detallada):

- Bloqueo automático de mensajes sospechosos de correo electrónico de salida

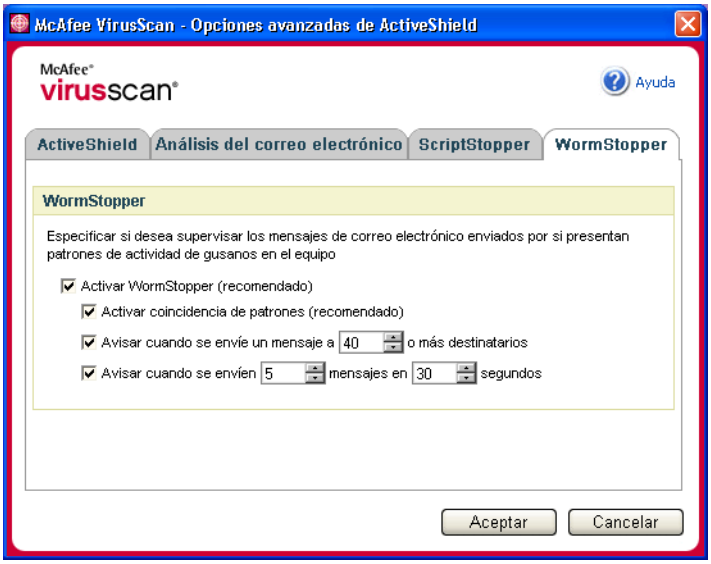


Figura 2-5. Opciones de WormStopper

Acciones que ActiveShield lleva a cabo al descubrir un virus

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

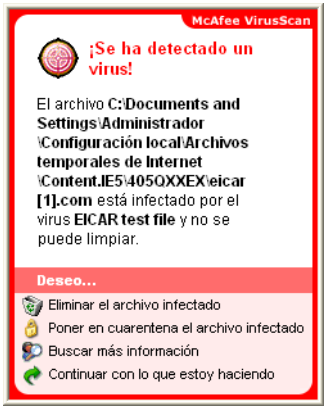


Figura 2-6. Alerta de virus

Gestión de archivos infectados

1 Si ActiveShield es capaz de limpiar el archivo, puede obtener más información al respecto o hacer caso omiso de la alerta:

- Haga clic en **Buscar más información** para ver el nombre del archivo, la ubicación y el nombre del virus asociado al archivo infectado.
- Haga clic en **Continuar con lo que estoy haciendo** para hacer caso omiso de la alerta y cerrarla.

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

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

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

Gestión del correo electrónico infectado

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

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

b Haga clic en **Limpiar arch. adjuntos infectados**.

2 Si ActiveShield no puede limpiar el mensaje de correo electrónico, haga clic en **Poner en cuarentena adjuntos infec.** 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 arch. adjuntos infectados** para intentar eliminar el archivo.

Administración de secuencias de comandos sospechosas

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

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

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

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

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

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

Gestión de gusanos potenciales

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

   a Haga clic en **Buscar más información** para ver la lista de destinatarios, el asunto, el cuerpo del mensaje y la descripción de la actividad sospechosa asociados al mensaje de correo electrónico infectado.

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

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

Análisis manual del equipo

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

Análisis manual de virus y programas potencialmente no deseados

Para analizar su equipo:

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

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

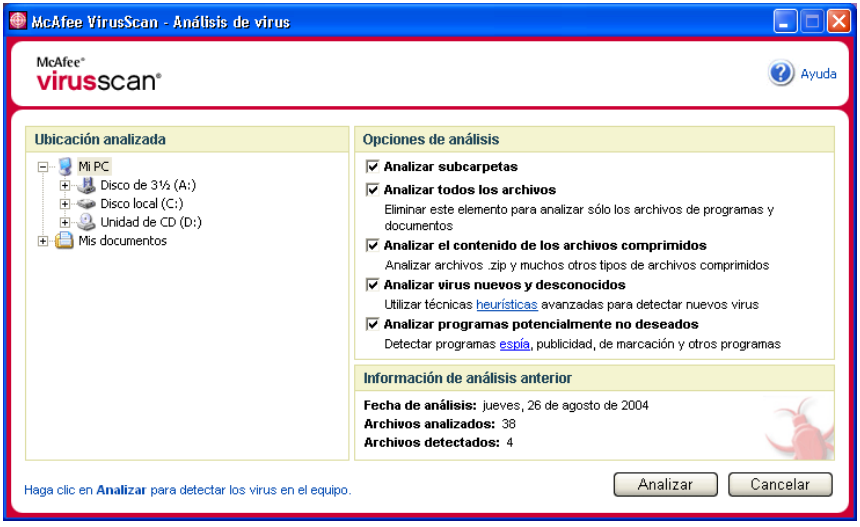


Figura 2-7. Análisis de virus

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

3 Seleccione las **Opciones de análisis** deseadas. De manera predeterminada, todas las **Opciones de análisis** están preseleccionadas para aplicar el análisis más completo (figura 2-7 en la página 25):

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

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

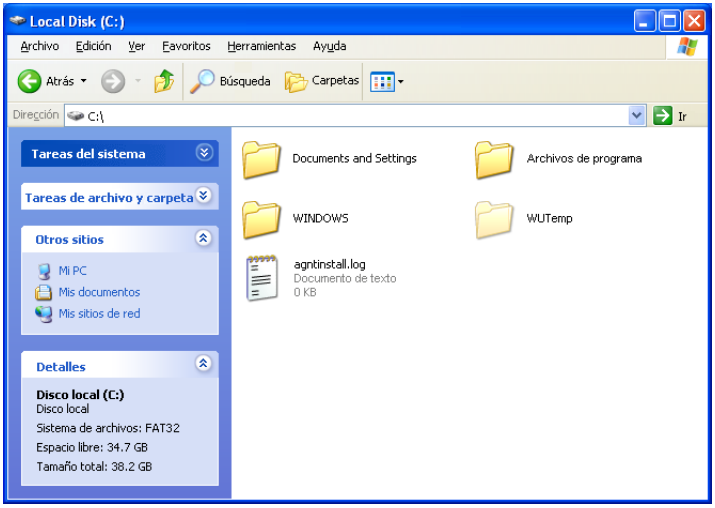


Figura 2-8. Contenido del disco local

- **Analizar todos los archivos**: utilice esta opción para realizar un análisis completo de todos los tipos de archivos. Desactive esta casilla de verificación para reducir el tiempo de análisis y examinar únicamente los archivos de programas y documentos.

- **Analizar el contenido de los archivos comprimidos**: utilice esta opción para encontrar los archivos infectados ocultos en los archivos .ZIP y otros archivos comprimidos. Desactive esta casilla de verificación para no analizar ningún archivo, ya esté comprimido o no, incluido dentro del archivo comprimido.

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

- **Analizar virus nuevos desconocidos**: utilice esta opción para encontrar los virus más recientes, para los que puede suceder que no se haya desarrollado aún la "vacuna". Esta opción utiliza técnicas heurísticas que comparan los archivos con las definiciones de virus conocidos y a la vez buscan signos que denoten la presencia de virus no identificados en los archivos.

  Este método de análisis también busca atributos de archivos que, por regla general, puedan descartar la existencia de virus. De esta manera, se minimizan las posibilidades de que la función de análisis 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 programas potencialmente no deseados**: esta opción se utiliza para detectar programas espía, publicidad, de marcación y otros programas que no tenga intención de instalar en su equipo.

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

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

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

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

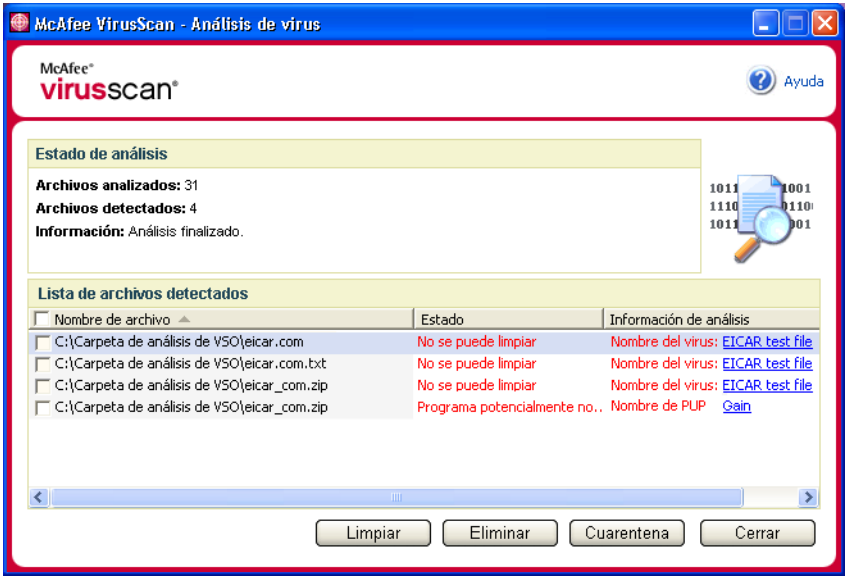


Figura 2-9. Resultados del análisis

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

6 Si no se detecta ningún virus ni ningún programa potencialmente no deseado, haga clic en **Atrás** para seleccionar otra unidad o carpeta que analizar, o bien en **Cerrar** para cerrar el cuadro de diálogo. En cualquier otro caso, consulte *Si el análisis encuentra un virus o un programa potencialmente no deseado* en la página 32.

Análisis desde el Explorador de Windows

VirusScan proporciona un menú de métodos abreviados para analizar los archivos, las carpetas o las unidades seleccionados en busca de virus y de programas potencialmente no deseados desde dentro del Explorador de Windows.

Análisis de archivos en el Explorador de Windows:

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

   Se abrirá el cuadro de diálogo **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 2-7 en la página 25).

Análisis desde Microsoft Outlook

VirusScan proporciona un icono de la barra de herramientas para analizar la presencia de virus o de programas potencialmente no deseados en los almacenes de mensajes seleccionados y sus subcarpetas, las carpetas de correo o los mensajes de correo electrónico que contengan archivos adjuntos en el seno de Microsoft Outlook 97 o una versión posterior.

Para analizar el correo electrónico en Microsoft Outlook:

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

   Aparecerá el analizador de correo electrónico, 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 25).

Análisis automático de virus y programas potencialmente no deseados

Aunque VirusScan analiza los archivos cuando el usuario o el equipo tienen acceso a ellos, puede programar la función de análisis automático en la ventana Programador de tareas de Windows para analizar el equipo exhaustivamente en busca de virus y programas potencialmente no deseados a intervalos especificados.

Para programar un análisis:

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

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

2 Haga clic en la ficha **Análisis programado** (figura 2-10).

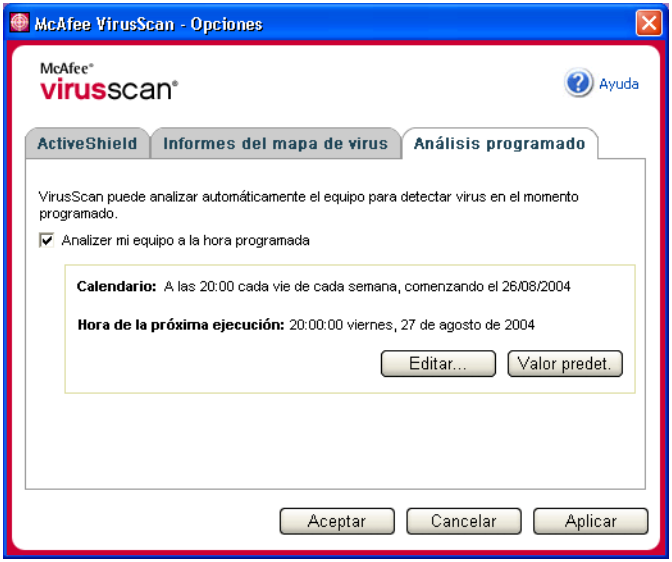


Figura 2-10. Opciones del análisis programado

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

4 Especifique un programa para el análisis automático:

- Para aceptar la programación predeterminada (los viernes a las 20:00 horas), haga clic en **Aceptar**.
- Para modificar la programación:

  a. Haga clic en **Editar**.

  b. Seleccione la frecuencia con la que desee analizar el equipo en la lista **Programar tarea** y seleccione las opciones adicionales en el área dinámica situada debajo:

  Diariamente: especifique el número de días entre análisis.

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

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

Sólo una vez: especifique en qué fecha desea realizar el análisis.

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

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

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

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

i. Especifique una fecha de inicio, una fecha de finalización, la duración y una hora de finalización. También puede especificar si se detiene la tarea a una hora dada en caso de que el análisis esté todavía en ejecución.

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

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

6 Si desea restablecer la programación predeterminada, haga clic en **Valor predet**. De lo contrario, haga clic en **Aceptar**.

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

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 el análisis detecta un programa potencialmente no deseado, puede intentar limpiarlo manualmente, ponerlo en cuarentena o eliminarlo (envío a AVERT no disponible).

Para tratar 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 virus en la lista **Información de análisis** para ver los detalles de la biblioteca de información de virus.

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

3 Si la función de análisis no consigue limpiar el archivo, haga clic en **Cuarentena** para cifrar y aislar temporalmente los archivos infectados y sospechosos en el directorio de cuarentena hasta que se pueda tomar una medida conveniente. (Consulte *Gestión de archivos en cuarentena* para obtener más información.)

4 Si la función de análisis no puede limpiar el archivo o ponerlo en cuarentena, puede realizar una de las acciones siguientes:

- Haga clic en **Eliminar** para eliminar el archivo.
- Haga clic en **Cerrar** para cerrar el cuadro de diálogo sin aplicar ninguna otra medida.

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

Si el archivo infectado no permite utilizar su conexión a Internet o impide el acceso al equipo, pruebe a utilizar el disco de emergencia para iniciarlo. En muchos casos, el disco de emergencia permite iniciar un equipo inutilizado por un archivo infectado. Consulte la sección *Creación de un disco de emergencia* en la página 34 para obtener información más detallada.

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

Gestión de archivos en cuarentena

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

Para gestionar un archivo que se ha puesto en cuarentena:

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

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

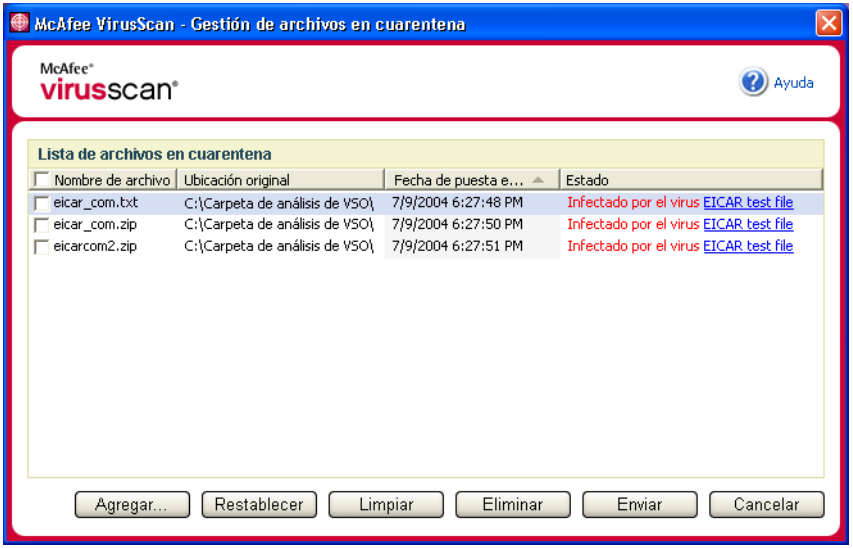


Figura 2-11. Gestión de archivos en cuarentena

2 Marque la casilla de verificación situada junto al archivo o los archivos que desee limpiar.

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

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

3 Haga clic en **Limpiar**.

4 Si el archivo está limpio, haga clic en **Restablecer** para devolverlo a su ubicación original.

5 Si VirusScan no puede limpiar el virus, haga clic en **Eliminar** para eliminar el archivo.

6 Si VirusScan no puede limpiar ni eliminar el archivo, y si no se trata de un programa potencialmente no deseado, puede enviarlo a AVERT™ (siglas del inglés de McAfee AntiVirus Emergency Response Team, o Equipo de respuesta de emergencia antivirus de McAfee) para su investigación:

   a Actualice los archivos de definición de virus si tienen más de dos semanas de antigüedad.

   b Compruebe su suscripción.

   c Seleccione el archivo y haga clic en **Enviar** para enviar el archivo a AVERT.

   VirusScan envía el archivo en cuarentena como archivo adjunto con un mensaje de correo electrónico que incluya su dirección de correo electrónico, país, versión de software, sistema operativo y el nombre original y el nombre del archivo. El volumen máximo que puede enviar es un archivo de 1,5 MB por día.

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

Creación de un disco de emergencia

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

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

Para crear un disco de emergencia:

1 Inserte un disquete no infectado en la unidad A de un equipo no infectado. Puede utilizar la función de análisis para asegurarse de que el equipo y el disquete están libres de virus. (Consulte *Análisis manual de virus y programas potencialmente no deseados* en la página 25 para obtener más información.)

2 Haga clic con el botón derecho del ratón en el icono de McAfee, seleccione **VirusScan** y haga clic en **Crear disco de emergencia**.

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

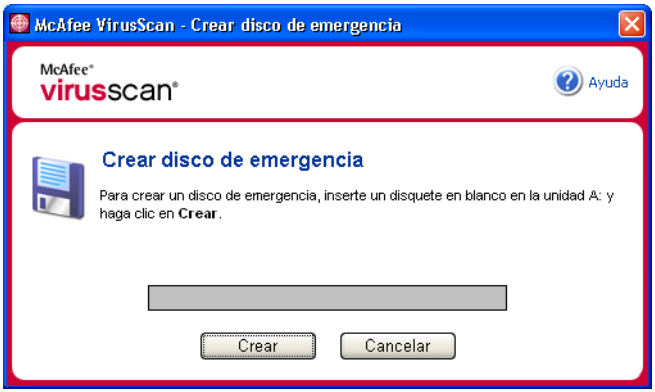


Figura 2-12. Creación de un disco de emergencia

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

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

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

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

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

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

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

Protección de un disco de emergencia contra escritura

Para proteger un disco de emergencia contra escritura:

1 Dé la vuelta al disquete (debería ver el círculo metálico del disquete).

2 Busque la pestaña de protección contra escritura. Deslice la pestaña de manera que se vea el agujero.

Utilización de un disco de emergencia

Para usar un disco de emergencia:

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

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

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

Actualización de un disco de emergencia

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

Información automática sobre virus

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

Envío de información al World Virus Map

Para enviar automáticamente información sobre virus al World Virus Map:

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

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

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

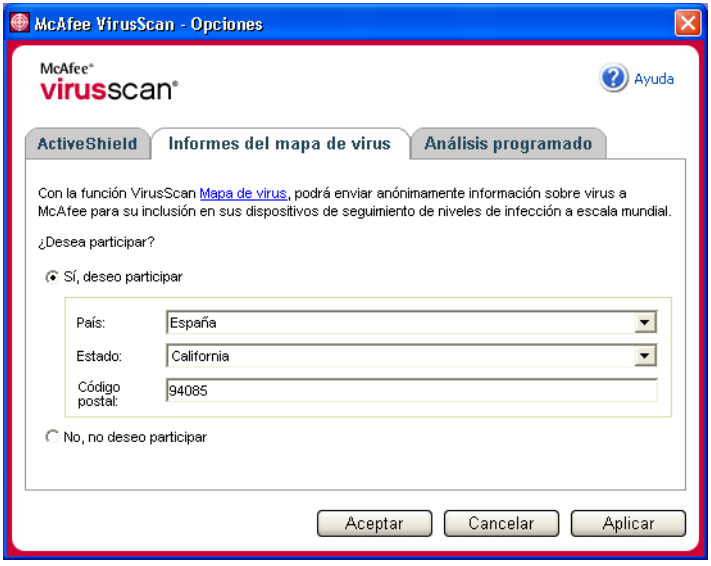


Figura 2-13. Opciones de Informes del mapa de virus

3 Acepte la opción predeterminada **Sí, deseo participar** para enviar información sobre virus de manera anónima a McAfee para incorporarla al World Virus Map, que incluye los niveles de infección a escala mundial. De lo contrario, seleccione **No, no deseo participar** para evitar enviar su información.

4 Si reside en los Estados Unidos, seleccione el estado y el código postal correspondiente a la ubicación física del equipo. En caso contrario, VirusScan tratará de seleccionar automáticamente el país en el que se encuentre su equipo.

5 Haga clic en **Aceptar**.

Visualización del World Virus Map

Participe o no en el World Virus Map, puede consultar los últimos índices de infecciones a escala mundial por medio del icono de McAfee situado en la bandeja del sistema de Windows.

Para ver el World Virus Map:

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

  Aparecerá la página Web **World Virus Map** (figura 2-14).

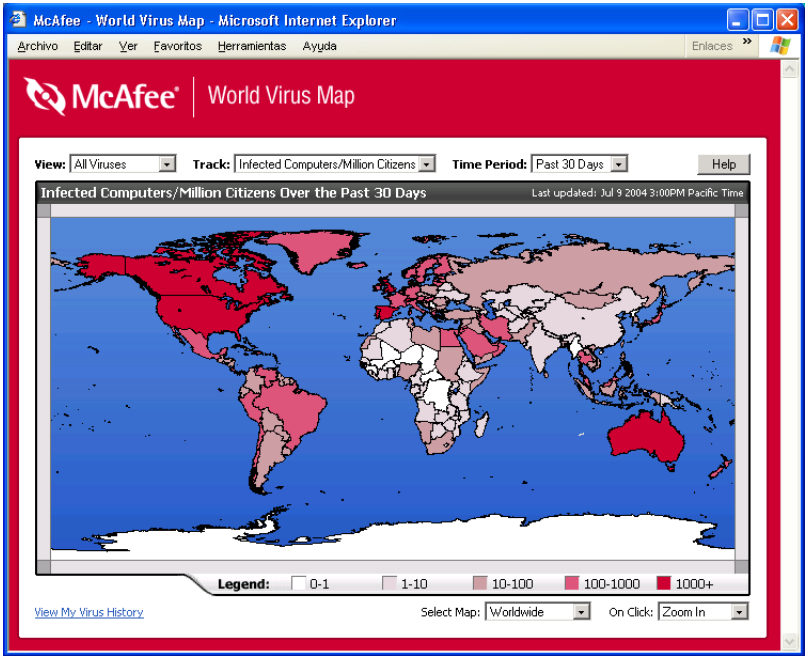


Figura 2-14. World Virus Map

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

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

Actualización de VirusScan

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

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

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

Comprobación automática de actualizaciones

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

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

Comprobación manual de actualizaciones

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

Para comprobar manualmente la existencia de actualizaciones de VirusScan:

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

   Se abrirá el cuadro de diálogo **Actualizaciones de SecurityCenter**.
3. Haga clic en **Comprobar ahora**.

   Si existiese una actualización, se abriría el cuadro **Actualizaciones de VirusScan** (figura 2-15 en la página 40). Haga clic en **Actualizar** para continuar.

   Si no hay actualizaciones disponibles, aparecerá un cuadro de diálogo que le indicará que VirusScan está actualizado. Haga clic en **Aceptar** para cerrar el cuadro de diálogo.

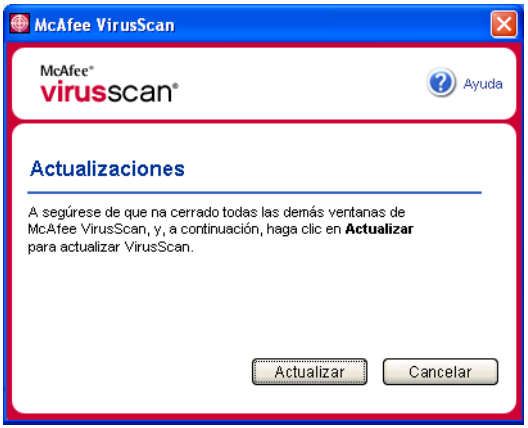


Figura 2-15. Cuadro de diálogo Actualizaciones

4 Regístrese en el sitio Web si se le pide que lo haga. El **Asistente para actualizaciones** instalará la actualización automáticamente.

5 Haga clic en **Finalizar** cuando la actualización haya terminado de instalarse.

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

Índice alfabético

A

ActiveShield
- activación, 13
- análisis de mensajes de correo electrónico y archivos adjuntos, 15
- análisis de secuencias de comandos y gusanos, 20
- análisis de todos los archivos, 18
- analizar archivos adjuntos de mensajes instantáneos de entrada, 18
- analizar sólo archivos de programas y documentos, 19
- analizar todos los tipos de archivo, 19
- comprobación, 9
- desactivación, 13
- detección de virus nuevos desconocidos, 20
- detención, 15
- inicio, 15
- limpieza de un virus, 22
- opción de análisis predeterminada, 15, 18, 20 a 21
- opciones de análisis, 14

actualización
- un disco de emergencia, 36
- VirusScan
  - automáticamente, 39
  - manual, 39

alertas
- de archivos infectados, 23
- de correo electrónico infectado, 23
- de gusanos potenciales, 24
- de secuencias de comandos sospechosas, 24
- de virus, 22

análisis
- análisis automático, 30
- análisis manual, 25
- análisis manual desde el Explorador de Windows, 29
- análisis manual desde la barra de herramientas de Microsoft Outlook, 29
- analizar nuevos virus desconocidos, 27
- archivos comprimidos, 26
- comprobación, 10 a 11
- desde el Explorador de Windows, 29
- desde la barra de herramientas de Microsoft Outlook, 29
- eliminación de un virus o un programa potencialmente no deseado, 32
- limpieza de un virus o un programa potencialmente no deseado, 32
- nuevos virus desconocidos, 27
- opción Analizar el contenido de los archivos comprimidos, 26
- opción Analizar programas potencialmente no deseados, 27
- opción Analizar subcarpetas, 26
- opción Analizar todos los archivos, 26
- programación de análisis automáticos, 30
- puesta en cuarentena de un virus o un programa potencialmente no deseado, 32
- secuencias de comandos y gusanos, 20
- sólo archivos de programas y documentos, 19
- subcarpetas, 26
- todos los archivos, 18, 26

análisis programados, 30

archivos adjuntos de mensajes instantáneos de entrada
- análisis, 18
- limpiar automáticamente, 18

archivos troyanos
- alertas, 22
- detección, 32

Asistente para la actualización, 14

AVERT, envío de archivos infectados, 34

C

comprobación del funcionamiento de VirusScan, 9
configuración
  VirusScan
    ActiveShield, 13
    análisis, 25
creación de un disco de emergencia, 34
cuarentena
  agregación de archivos sospechosos, 33
  eliminación de archivos, 33
  eliminación de archivos sospechosos, 34
  envío de archivos sospechosos, 34
  gestión de archivos sospechosos, 33
  limpieza de archivos, 33 a 34
  restablecimiento de archivos limpios, 33 a 34

D

disco de emergencia
  actualización, 36
  creación, 34
  protección contra escritura, 35
  uso, 32, 36

E

envío de archivos infectados a AVERT, 34
Explorador de Windows, 29

F

funciones nuevas, 7

G

gusanos
  alertas, 22, 24
  detección, 22, 32
  detención, 24

I

introducción a VirusScan, 7

L

lista de archivos detectados (Analizar), 32

M

McAfee SecurityCenter, 12
mensajes de correo electrónico y archivos adjuntos
  análisis
    activación, 15
    desactivación, 17
    errores, 16
    ventana de estado, 16
  eliminación, 23
  limpieza, 23
  limpieza automática
    activación, 15
    desactivación, 18
  puesta en cuarentena, 23
Microsoft Outlook, 29

O

opción Analizar el contenido de los archivos comprimidos (Analizar), 26
opción Analizar programas potencialmente no deseados, 27
opción Analizar subcarpetas (Analizar), 26
opción Analizar todos los archivos (Analizar), 26
opción Analizar virus nuevos desconocidos (Analizar), 27
opciones de análisis
  ActiveShield, 14, 18 a 19
  análisis, 25

P

programas potencialmente no deseados
  detección, 32
  eliminación, 32
  limpieza, 32
  puesta en cuarentena, 32
protección de un disco de emergencia contra escritura, 35

R

requisitos del sistema, 9

S

ScriptStopper, 20
secuencias de comandos
- alertas, 24
- detención, 24
- permiso, 24

soporte técnico, 32

T

Tarjeta de inicio rápido, iii

U

uso de un disco de emergencia, 36

V

virus
- alertas, 22
- detección, 32
- detección con ActiveShield, 22
- detención de gusanos potenciales, 24
- detención de secuencias de comandos sospechosas, 24
- eliminación, 22, 32
- eliminación de archivos infectados, 23
- eliminación de los archivos adjuntos infectados del correo electrónico, 23
- información automática, 36, 38
- limpieza, 22, 32
- limpieza de archivos adjuntos infectados del correo electrónico, 23
- permiso de secuencias de comandos sospechosas, 24
- puesta en cuarentena, 22, 32
- puesta en cuarentena de archivos adjuntos infectados del correo electrónico, 23
- puesta en cuarentena de archivos infectados, 23

VirusScan
- actualización manual, 39
- actualizar automáticamente, 39
- análisis desde el Explorador de Windows, 29
- análisis desde la barra de herramientas de Microsoft Outlook, 29
- análisis programados, 30
- comprobación, 9
- información automática sobre virus, 36, 38
- introducción, 7

W

World Virus Map
- información, 36
- visualización, 38

WormStopper, 20