

**McAfee®**  
**VirusScan USB**  

---

**Guía del usuario**



# Contenido

<b>McAfee VirusScan USB</b>	<b>3</b>
Funciones .....	4
<b>Instalación y actualización de VirusScan USB</b>	<b>5</b>
Instalar VirusScan USB.....	6
Actualizar VirusScan USB.....	8
<b>Configuración de las opciones de análisis</b>	<b>9</b>
Configurar tipos de archivo analizados.....	11
Configurar las ubicaciones que se van a analizar .....	12
Deshabilitar el control en tiempo real.....	13
Iniciar un análisis en el momento de la inserción.....	14
Deshabilitar la detección de software antivirus .....	14
Mostrar mensajes informativos .....	15
<b>Trabajar con alertas</b>	<b>17</b>
Acerca de las alertas.....	17
<b>Análisis del dispositivo USB</b>	<b>19</b>
Analizar un dispositivo USB.....	20
Pausar el análisis .....	21
Reanudar el análisis.....	21
Cancelar el análisis .....	21
<b>Trabajar con los resultados de análisis</b>	<b>23</b>
Ver los resultados de un análisis .....	24
Eliminar un archivo infectado .....	25
Ver el último resumen de análisis.....	25
Ver el resumen del programa VirusScan USB.....	26
<b>Protección del equipo</b>	<b>27</b>
Descargar software antivirus para su equipo .....	27
<b>Renovación de la suscripción de VirusScan USB</b>	<b>29</b>
Renovar la suscripción de VirusScan USB .....	29
<b>Preguntas más frecuentes</b>	<b>31</b>
Se ha detectado una amenaza. ¿Qué debo hacer? .....	31

¿Es preciso estar conectado a Internet para realizar análisis? .....	31
¿VirusScan USB analiza los archivos comprimidos? .....	32
¿Cómo puedo obtener más ayuda de McAfee? .....	32
<b>Glosario</b>	<b>33</b>
<hr/>	
<b>Glosario</b>	<b>34</b>
<hr/>	
<b>Acerca de McAfee</b>	<b>37</b>
<hr/>	
Copyright.....	38
<b>Índice</b>	<b>40</b>
<hr/>	

---

## CAPÍTULO 1

# McAfee VirusScan USB

VirusScan USB ofrece protección total, fiable y actualizada de su dispositivo USB frente a los virus. Desarrollado mediante la galardonada tecnología de análisis de McAfee, VirusScan USB protege el contenido de su unidad USB de todos los virus y troyanos.

### En este capítulo

Funciones .....4

## Funciones

VirusScan USB ofrece las funciones siguientes:

### Control en tiempo real

Cuando está habilitado, el monitor en tiempo real de VirusScan USB controla constantemente el dispositivo USB para localizar cambios en los archivos (por ejemplo, un nuevo archivo agregado al dispositivo o una modificación realizada en un archivo que ya estuviera en el dispositivo). Si el monitor en tiempo real detecta un cambio en un archivo, VirusScan USB analiza el archivo afectado para descubrir la actividad de los virus. Si se detecta un virus o un troyano, VirusScan USB intenta limpiarlo; si no puede limpiarlo, intenta cambiarle el nombre. El control en tiempo real está habilitado de forma predeterminada.

### Análisis bajo demanda

El análisis bajo demanda le permite analizar el dispositivo USB para localizar virus y troyanos en cualquier momento. Por ejemplo, si ha agregado un programa o archivo a su dispositivo USB, puede analizar el dispositivo para garantizar que el programa o archivo no esté infectado. Si se detecta un virus o un troyano, VirusScan USB intenta limpiarlo; si no puede limpiarlo, intenta cambiarle el nombre.

## CAPÍTULO 2

# Instalación y actualización de VirusScan USB

Instale VirusScan USB en su dispositivo USB de la misma forma en la que instala la mayoría de los programas U3 USB; la única diferencia es que debe registrarse con McAfee. Al registrarse, podrá recibir actualizaciones del programa VirusScan USB y de archivos de definición de virus cuando aparezcan. Si se va a registrar con McAfee por primera vez, deberá indicar su nombre, una dirección de correo electrónico válida y una contraseña. Si ya está registrado con McAfee, deberá iniciar sesión con la dirección de correo electrónico y la contraseña que haya indicado en el registro anterior.

Tras instalar y registrar VirusScan USB, puede actualizarlo con los últimos archivos de protección de virus (DAT) en cualquier momento. Las actualizaciones se ejecutan en un segundo plano; puede incluso ejecutar un análisis o cerrar un programa mientras una actualización está en curso. Si está habilitado el control en tiempo real, VirusScan USB ejecuta una actualización automática cada cuatro horas. Para obtener más información acerca del control en tiempo real, consulte Configuración de las opciones de análisis (página 9).

---

**Nota:** si su dispositivo USB se suministra con un programa antivirus ya instalado, McAfee le recomienda que elimine ese programa antes de instalar VirusScan USB.

---

## En este capítulo

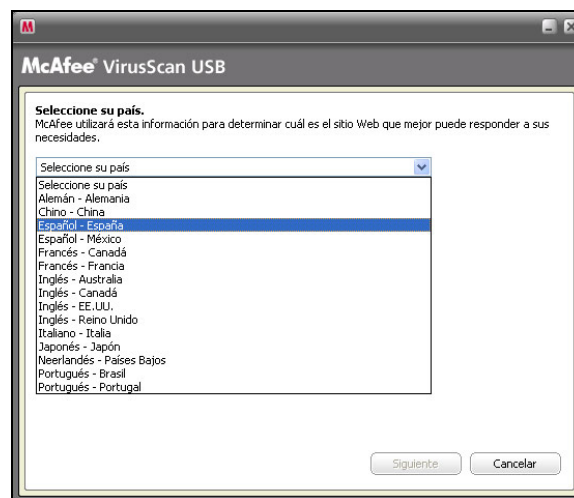
Instalar VirusScan USB .....	6
Actualizar VirusScan USB .....	8

## Instalar VirusScan USB

Instale VirusScan USB en su dispositivo USB de la misma forma en la que instala la mayoría de los programas U3 USB; la única diferencia es que debe registrarse con McAfee. Al registrarse, podrá recibir actualizaciones del programa VirusScan USB y de archivos de definición de virus cuando aparezcan.

### Para instalar VirusScan USB:

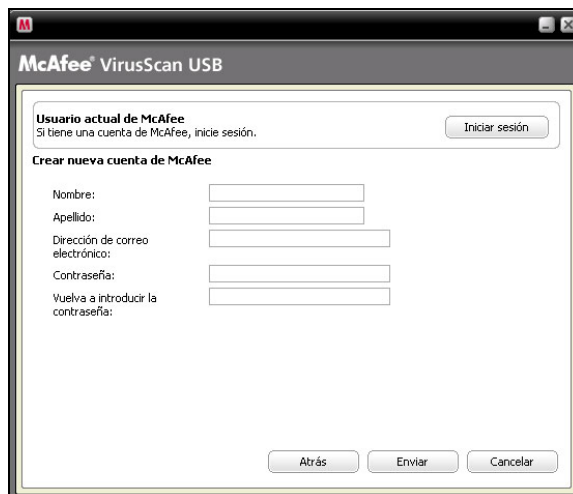
- 1 Introduzca el dispositivo USB en el equipo.
- 2 En la plataforma U3 Launchpad, haga clic en **Agregar programas** y, a continuación, en **Instalar desde mi equipo**.
- 3 En el cuadro de diálogo Abrir, acceda a la carpeta donde esté almacenado el archivo de instalación, seleccione el archivo y, a continuación, haga clic en **Abrir**.
- 4 En el Asistente para agregar programas, haga clic en **Siguiente**.
- 5 En el cuadro de diálogo Seleccione su país, haga clic en la combinación de país e idioma que mejor represente su ubicación actual y, a continuación, haga clic en **Siguiente**.



- 6 En el cuadro de diálogo Configuración del programa, revise la política de privacidad y después haga clic en **Siguiente**.
- 7 En el cuadro de diálogo de Acuerdo de licencia del usuario de McAfee, seleccione un país, revise el acuerdo de licencia de usuario y, a continuación, haga clic en **Aceptar**.
- 8 Siga uno de estos procedimientos:
  - Si se va a registrar por primera vez, escriba su nombre, primer apellido, dirección de correo electrónico, contraseña y confirmación de contraseña en las casillas correspondientes y, a continuación, haga clic en **Enviar**.



- Si ya ha registrado previamente un programa con McAfee, haga clic en **Iniciar sesión**, escriba la dirección de correo electrónico y la contraseña asociadas a su cuenta de McAfee y, a continuación, haga clic en **Iniciar sesión**.



- 9 En el cuadro de diálogo Instalación del programa finalizada, grabe su información de registro y después haga clic en **Finalizar**.

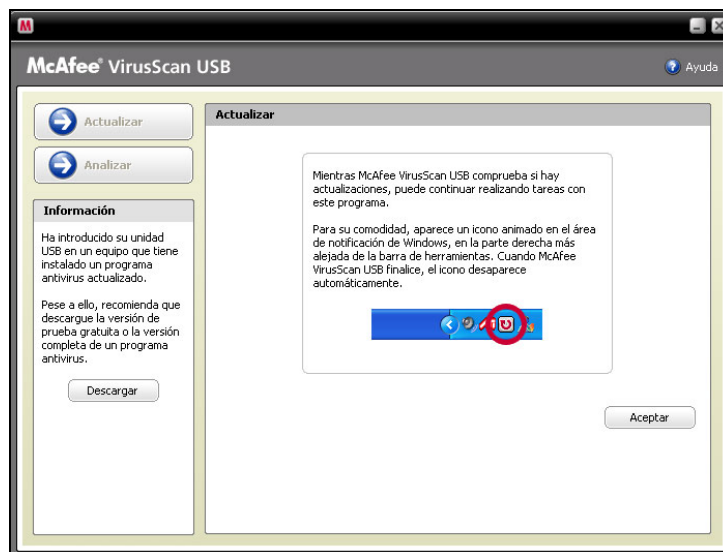
**Nota:** también puede ejecutar el archivo de instalación de VirusScan USB directamente desde un sitio Web. En el sitio Web, inicie la descarga y haga clic en **Sí** ante cualquier advertencia de seguridad que aparezca y que le pregunte si quiere descargar el archivo. A continuación, ejecute el archivo de instalación y siga las instrucciones indicadas en el asistente de instalación.

## Actualizar VirusScan USB

Una vez instalado VirusScan USB en su dispositivo USB, se ejecutará automáticamente una actualización cada vez que conecte el dispositivo a su equipo. Asimismo, puede actualizar VirusScan USB manualmente con las últimas actualizaciones del programa o de archivos de definición de virus en cualquier momento. Las actualizaciones se ejecutan en un segundo plano; puede incluso ejecutar un análisis o cerrar un programa mientras una actualización está en curso.

### Para actualizar VirusScan USB:

- 1 En el panel principal de VirusScan USB, haga clic en **Actualizar**.



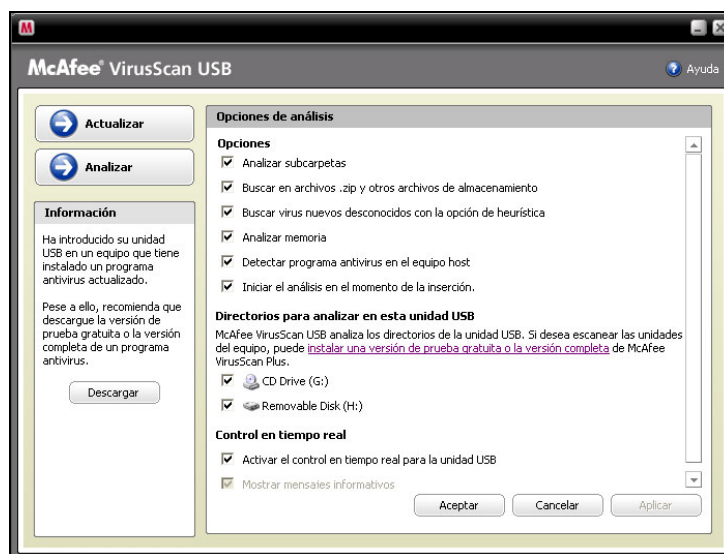
- 2 Haga clic en **Aceptar**.

**Nota:** para actualizar satisfactoriamente VirusScan USB, deberá estar conectado a Internet.

## CAPÍTULO 3

# Configuración de las opciones de análisis

Puede personalizar el comportamiento de VirusScan USB mediante la configuración de las opciones de análisis. Por ejemplo, puede especificar los tipos de archivos objeto de análisis (archivos, subcarpetas y memoria del equipo) y las ubicaciones que se vayan a analizar. También puede habilitar o deshabilitar el control en tiempo real. Cuando está habilitado, el monitor en tiempo real de VirusScan USB controla constantemente el dispositivo USB para localizar cambios en los archivos (por ejemplo, un nuevo archivo agregado al dispositivo o una modificación realizada en un archivo que ya estuviera en el dispositivo). Si el monitor en tiempo real detecta un cambio en un archivo, VirusScan USB analiza el archivo afectado para descubrir la actividad de los virus. Si se detecta un virus o un troyano, VirusScan USB intenta limpiarlo; si no puede limpiarlo, intenta cambiarle el nombre. El control en tiempo real está habilitado de forma predeterminada y McAfee recomienda que no se deshabilite. Cuando está habilitado el control en tiempo real, se controlan todos los tipos de archivo; cuando se ejecuta un análisis bajo demanda, VirusScan USB analiza los tipos y ubicaciones de archivos especificados en las opciones de análisis. Para obtener más información acerca de la ejecución de análisis bajo demanda, consulte Análisis de un dispositivo USB (página 19).



Cuando se instala VirusScan USB, se agrega automáticamente a la lista de programas de la plataforma U3 Launchpad y se configura para que se inicie en el momento de la inserción. Esto significa que se inicia un análisis bajo demanda de VirusScan USB cada vez que se introduce un dispositivo USB en el equipo. Si deshabilita la opción de inicio en el momento de la inserción en la plataforma U3 Launchpad, sólo se iniciará un análisis bajo demanda de VirusScan USB la primera vez que introduzca un dispositivo USB en su equipo. A continuación, puede configurar VirusScan USB para iniciar o no el análisis en el momento de la inserción. Si configura VirusScan USB para que no inicie un análisis en el momento de la inserción, VirusScan USB no se inicia hasta que el control en tiempo real detecta una infección o se inicia manualmente. McAfee recomienda no deshabilitar la opción de iniciar análisis en el momento de la inserción en VirusScan USB.

VirusScan USB detecta virus y troyanos en el dispositivo USB y la memoria del equipo, y también detecta si tiene instalado software antivirus actualizado en su equipo. Si no tiene instalado en su equipo software antivirus actualizado, se le pedirá que descargue una versión completa o de prueba de McAfee VirusScan para garantizar que su equipo está protegido. Al configurar las opciones de análisis, puede deshabilitar la detección de software antivirus, lo que impide a VirusScan USB detectar si hay un software antivirus actualizado instalado en su equipo. Asimismo, si ha ocultado algunos cuadros de diálogo de alertas u otra información, puede volver a mostrarlos.

## En este capítulo

Configurar tipos de archivo analizados.....	11
Configurar las ubicaciones que se van a analizar .....	12
Deshabilitar el control en tiempo real.....	13
Iniciar un análisis en el momento de la inserción ....	14
Deshabilitar la detección de software antivirus.....	14
Mostrar mensajes informativos .....	15

---

## Configurar tipos de archivo analizados

Puede especificar los tipos de archivo que se han analizado en su dispositivo USB para localizar virus o troyanos durante un análisis bajo demanda. Por ejemplo, puede determinar si se han analizado subcarpetas y archivos. Asimismo, puede determinar si quiere que VirusScan USB analice la memoria de su equipo.

### Para configurar tipos de archivo analizados:

- 1 En el panel de inicio de VirusScan USB, en **Opciones de análisis actuales**, haga clic en **Configurar**.
- 2 En el panel Opciones de análisis, en **Opciones**, seleccione o elimine las siguientes casillas:
  - **Analizar subcarpetas:** se analizan subcarpetas (carpetas incluidas en otras carpetas).
  - **Buscar en archivos .zip y otros archivos de almacenamiento:** se analizan archivos de almacenamiento, incluidos los archivos .zip.
  - **Buscar virus nuevos desconocidos con la opción de heurística:** los archivos se comparan con las firmas de virus conocidos para detectar indicios de virus no identificados. Esta opción proporciona el análisis más completo, pero suele resultar más lenta que un análisis normal.
  - **Analizar memoria:** se analiza la memoria de su equipo.
- 3 Haga clic en **Aceptar**.

---

## Configurar las ubicaciones que se van a analizar

Puede especificar las ubicaciones (unidades USB) que quiera analizar en un análisis bajo demanda. Dado que VirusScan USB sólo analiza unidades asociadas con dispositivos USB, las unidades de disco que no estén asociadas con dispositivos no aparecerán en la lista **Unidades para analizar en este dispositivo USB**; éstas incluyen unidades extraíbles del equipo y unidades asociadas con otros dispositivos USB.

### Para configurar las ubicaciones que se van a analizar:

- 1 En el panel de inicio de VirusScan USB, en **Opciones de análisis actuales**, haga clic en **Configurar**.
- 2 En el panel Opciones de análisis, en **Unidades para analizar en este dispositivo USB**, marque o desactive las siguientes casillas:
  - **Sistema U3:** se analiza la partición del CD-ROM en el dispositivo. Esta es la ubicación en la que se almacenan los archivos del sistema U3.
  - **Mi unidad U3:** se analiza la partición de datos en el dispositivo. Esta es la letra de la unidad asignada a la unidad USB.
- 3 Haga clic en **Aceptar**.

---

## Deshabilitar el control en tiempo real

Cuando está habilitado, el monitor en tiempo real de VirusScan USB controla constantemente el dispositivo USB para localizar cambios en los archivos (por ejemplo, un nuevo archivo agregado al dispositivo o una modificación realizada en un archivo que ya estuviera en el dispositivo). Si el monitor en tiempo real detecta un cambio en un archivo, VirusScan USB analiza el archivo para descubrir la actividad de los virus. Si se detecta un virus o un troyano, VirusScan USB intenta limpiarlo; si no puede limpiarlo, intenta cambiarle el nombre. El control en tiempo real controla todos los tipos de archivo (independientemente de la configuración del análisis bajo demanda). McAfee recomienda que no se deshabilite el control en tiempo real.

### Para deshabilitar el control en tiempo real:

- 1 En el panel de inicio de VirusScan USB, en **Opciones de análisis actuales**, haga clic en **Configurar**.
- 2 En el panel Opciones de análisis, en **Control en tiempo real**, desactive la casilla **Habilitar control en tiempo real de dispositivo USB**.
- 3 Haga clic en **Aceptar**.

---

**Nota:** si se habilita el control en tiempo real, podría detectarse un archivo infectado mientras el análisis bajo demanda está en curso. Como siempre, para garantizar que se informe de la infección al menos una vez, el control en tiempo real muestra una alerta.

---

---

## Iniciar un análisis en el momento de la inserción

Cuando se instala VirusScan USB, se agrega automáticamente a la lista de programas de la plataforma U3 Launchpad y se configura para que se inicie en el momento de la inserción. Esto significa que se inicia un análisis bajo demanda de VirusScan USB cada vez que se introduce un dispositivo USB en el equipo. Si deshabilita la opción de inicio en el momento de la inserción en la plataforma U3 Launchpad, se iniciará un análisis bajo demanda de VirusScan USB la primera vez que introduzca un dispositivo USB en su equipo. A continuación, puede configurar VirusScan USB para iniciar o no el análisis en el momento de la inserción. Si configura VirusScan para que no inicie un análisis tras la inserción, VirusScan USB no se inicia hasta que el control en tiempo real detecta una infección o se inicia manualmente. McAfee recomienda no deshabilitar la opción de iniciar análisis en el momento de la inserción en VirusScan USB.

### Para iniciar un análisis en el momento de la inserción:

- 1 En el panel de inicio de VirusScan USB, en **Opciones de análisis actuales**, haga clic en **Configurar**.
- 2 En el panel Opciones de análisis, en **Opciones**, asegúrese de que esté marcada la casilla **Iniciar análisis en el momento de la inserción**.
- 3 Haga clic en **Aceptar**.

---

**Sugerencia:** también puede marcar la casilla **Iniciar análisis en el momento de la inserción** en el panel Progreso del análisis cuando finalice, pause o cancele un análisis.

---

---

## Deshabilitar la detección de software antivirus

De forma predeterminada, VirusScan USB detecta si dispone de software antivirus actualizado en el equipo; sin embargo, puede deshabilitar esta detección.

### Para deshabilitar la detección de software antivirus:

- 1 En el panel de inicio de VirusScan USB, en **Opciones de análisis actuales**, haga clic en **Configurar**.
- 2 En el panel Opciones de análisis, en **Opciones**, desactive la casilla **Detectar software antivirus en el equipo host**.
- 3 Haga clic en **Aceptar**.



---

## Mostrar mensajes informativos

Si decide que quiere mostrar algunas alertas y cuadros de diálogo de VirusScan USB que había decidido ocultar, puede hacerlo.

**Para mostrar mensajes informativos:**

- 1 En el panel de inicio de VirusScan USB, en **Opciones de análisis actuales**, haga clic en **Configurar**.
- 2 En el panel Opciones de análisis, en **Opciones**, marque la casilla **Mostrar mensajes informativos**.
- 3 Haga clic en **Aceptar**.



---

## CAPÍTULO 4

# Trabajar con alertas

McAfee utiliza alertas para ayudarle a gestionar la seguridad. Las alertas se agrupan en tres tipos básicos:

- Alerta roja
- Alerta amarilla
- Alerta verde

A continuación, puede elegir la forma de gestionar los archivos detectados, conforme a las recomendaciones de las alertas.

## En este capítulo

Acerca de las alertas ..... 17

---

## Acerca de las alertas

El control en tiempo real de VirusScan USB tiene tres tipos de alerta básicas: roja, amarilla y verde.

### Alerta roja

Las alertas rojas indican que se ha detectado un archivo infectado, pero no se ha podido limpiar ni cambiar el nombre. Estas alertas le permiten eliminar el archivo infectado del dispositivo USB u omitir la infección.

### Alerta amarilla

Las alertas amarillas indican que se ha detectado un archivo infectado y que no ha podido limpiarse, pero al que se le ha cambiado el nombre por la extensión .vir. Estas alertas le permiten eliminar el archivo infectado del dispositivo USB u omitir la infección.

### Alerta verde

Las alertas verdes indican que se ha detectado y limpiado un archivo infectado. Dado que estas alertas son principalmente informativas, puede decidir no mostrarlas de nuevo.



## CAPÍTULO 5

# Análisis del dispositivo USB

Cuando se instala VirusScan USB, se agrega automáticamente a la lista de programas de la plataforma U3 Launchpad y se configura para que se inicie en el momento de la inserción. Esto significa que se inicia un análisis bajo demanda de VirusScan USB cada vez que se introduce un dispositivo USB en el equipo. Si deshabilita la opción de inicio en el momento de la inserción en la plataforma U3 Launchpad, sólo se iniciará un análisis bajo demanda de VirusScan USB la primera vez que introduzca un dispositivo USB en su equipo. A continuación, puede configurar VirusScan USB para iniciar o no el análisis en el momento de la inserción. Si configura VirusScan para que no inicie el análisis en el momento de la inserción, VirusScan USB no se inicia hasta que el control en tiempo real detecta una infección o puede ejecutar un análisis bajo demanda. Cuando se ejecuta un análisis bajo demanda, VirusScan USB analiza los tipos de archivo y las ubicaciones en sus opciones de análisis. Para obtener más información sobre la configuración de las opciones de análisis bajo demanda, consulte Configuración de las opciones de análisis (página 9).

---

**Nota:** McAfee recomienda no deshabilitar la opción de iniciar análisis en el momento la inserción en VirusScan USB.

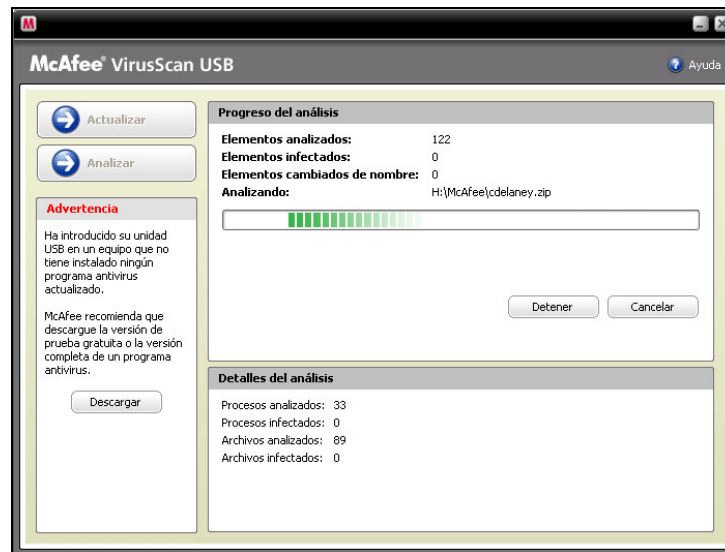
---

Cuando VirusScan USB detecta un virus o troyano en uno de los archivos de un dispositivo USB, realiza una de las siguientes operaciones:

- Limpiar: el virus o troyano se quita del archivo.
- Cambiar el nombre: se cambia de nombre el archivo por la extensión .vir (si la operación de limpieza ha fallado).

Si fallan tanto las operaciones de limpieza como de cambio de nombre, puede eliminar el archivo infectado. Para obtener más información, consulte Eliminar un archivo infectado (página 25).

Tras iniciar el análisis del archivo USB, puede pausar el análisis y reanudarlo después desde ese punto en un momento más apropiado. Por ejemplo, si está realizando una tarea que consume muchos recursos cuando VirusScan USB esté analizando, puede pausar el análisis y reanudarlo después cuando finalice la otra tarea. Asimismo, puede cancelar un análisis en cualquier momento.



## En este capítulo

Analizar un dispositivo USB .....	20
Pausar el análisis .....	21
Reanudar el análisis .....	21
Cancelar el análisis.....	21

## Analizar un dispositivo USB

Puede analizar un dispositivo USB en cualquier momento. Por ejemplo, si acaba de instalar VirusScan USB, puede realizar un análisis para comprobar que su dispositivo USB no tiene virus ni otras amenazas.

### Para analizar manualmente un dispositivo USB:

- En el panel izquierdo de VirusScan USB, haga clic en **Analizar**.

---

## Pausar el análisis

Puede pausar un análisis en curso. De este modo, se detiene el análisis en un punto específico y puede reanudar el análisis desde ese punto cuando lo crea conveniente.

**Para pausar un análisis:**

- En el panel Progreso del análisis, en **Progreso del análisis**, haga clic en **Pausar**.

---

**Sugerencia:** para reanudar el análisis desde el punto en el que lo pausó, haga clic en el botón **Reanudar** .

---

---

## Reanudar el análisis

Cuando se pausa un análisis, se detiene temporalmente. Puede reanudar el análisis desde el punto en el que lo pausó. Para obtener más información acerca de cómo pausar un análisis, consulte Pausar el análisis (página 21).

**Para reanudar un análisis:**

- En el panel Progreso del análisis, en **Progreso del análisis**, haga clic en **Reanudar**.

---

## Cancelar el análisis

Puede cancelar (terminar) un análisis en todo momento. A diferencia de pausar, no se puede reanudar un análisis cancelado.

**Para detener definitivamente un análisis:**

- En el panel Progreso del análisis, en **Progreso del análisis**, haga clic en **Cancelar** y luego en **Finalizar**.



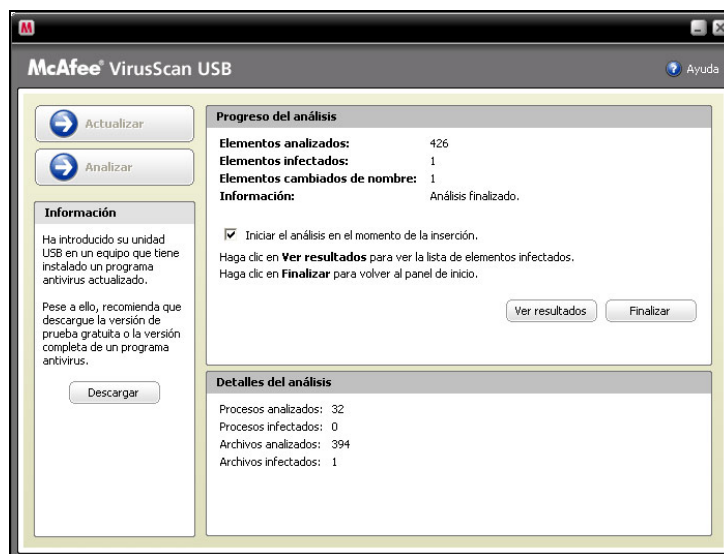


## CAPÍTULO 6

# Trabajar con los resultados de análisis

Mientras se ejecuta un análisis, VirusScan USB muestra el número de elementos analizados, infectados o a los que se ha cambiado el nombre por encima de la barra de progreso del análisis. Cuando se detecta una infección y finaliza un análisis, puede ver un resumen de los resultados, lo que incluye la ruta y el nombre de cada archivo infectado, así como la operación realizada en ese archivo (por ejemplo, limpiado o cambiado el nombre). También puede ver información detallada acerca de cada archivo infectado, incluido el tipo de objeto, el nombre, el estado y el nombre del archivo.

Si VirusScan USB detecta un virus o troyano en uno de los archivos de su dispositivo USB, intenta limpiar el archivo infectado: si la operación de limpieza falla, VirusScan USB intenta cambiar el nombre del archivo. Si fallan tanto la operación de limpieza como la de cambio de nombre, puede eliminar el archivo del dispositivo USB.



VirusScan USB también muestra un resumen del último análisis en el panel de inicio para que pueda revisar los procesos analizados, los procesos infectados, los archivos analizados, los archivos infectados y la fecha del último análisis.

## En este capítulo

Ver los resultados de un análisis .....	24
Eliminar un archivo infectado.....	25
Ver el último resumen de análisis .....	25
Ver el resumen del programa VirusScan USB .....	26

---

## Ver los resultados de un análisis

Cuando finaliza un análisis, puede consultar los resultados para ver una lista de elementos infectados.

### **Para ver los resultados de un análisis:**

- 1 En el panel Progreso del análisis, en **Progreso del análisis**, haga clic en **Ver resultados**.
- 2 En el panel Resultados del análisis, haga clic en el nombre del archivo infectado.
- 3 En **Detalles**, consulte la información más específica sobre el archivo infectado.
- 4 Haga clic en **Finalizar**.

---

**Nota:** el botón **Ver resultados** sólo aparece cuando se detectan archivos infectados.

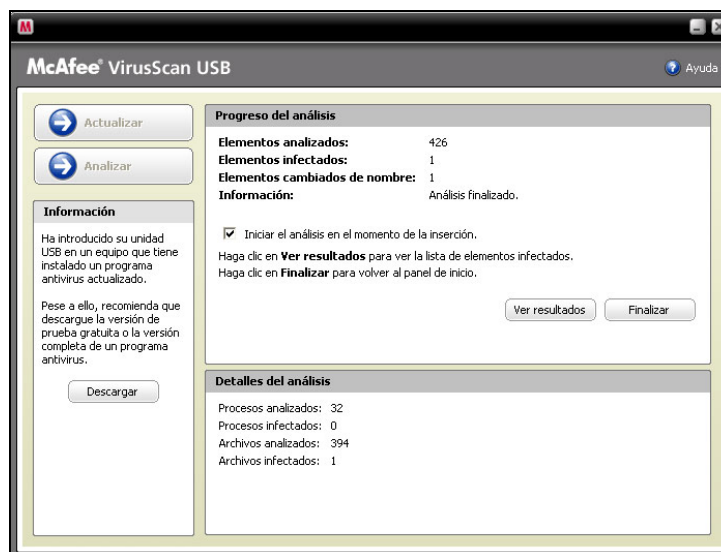
---

## Eliminar un archivo infectado

Si VirusScan USB detecta un virus o troyano en uno de los archivos de su dispositivo USB, intenta limpiar el archivo infectado: si la operación de limpieza falla, VirusScan USB intenta cambiar el nombre del archivo. Si fallan tanto la operación de limpieza como la de cambio de nombre, puede eliminar el archivo del dispositivo USB.

### Para eliminar un archivo infectado:

- 1 En el panel Progreso del análisis, en **Progreso del análisis**, haga clic en **Ver resultados**.
- 2 En el panel Resultados del análisis, haga clic en el nombre del archivo infectado.



- 3 En **Deseo**, haga clic en **Eliminar**.
- 4 Haga clic en **Finalizar**.

## Ver el último resumen de análisis

Para su comodidad, VirusScan USB muestra un resumen del último análisis en el panel de inicio.

### Para ver el último resumen de análisis:

- En el panel de inicio de VirusScan USB, consulte los detalles en **Resumen del último análisis**.

---

## Ver el resumen del programa VirusScan USB

VirusScan USB muestra la fecha en la que se produjo la comprobación de la última actualización y la versión actual de los archivos de definición de virus (DAT) en el panel de inicio.

**Para ver el resumen del programa VirusScan USB:**

- En el panel de inicio de VirusScan USB, consulte los detalles en **Resumen de programa**.

---

## CAPÍTULO 7

# Protección del equipo

VirusScan USB no controla ni analiza los archivos almacenados en el equipo. Esta protección la proporciona McAfee VirusScan. Puede descargar una versión completa o de prueba de McAfee VirusScan desde el sitio de descarga de McAfee.

### En este capítulo

Descargar software antivirus para su equipo.....27

---

## Descargar software antivirus para su equipo

Si se configura VirusScan USB para detectar si tiene un software antivirus instalado en su equipo, y detecta que no hay nada, se le pedirá que descargue una versión completa o de prueba de McAfee VirusScan.

### Para descargar software antivirus para su equipo:

- 1 En **Advertencia** o **Información** en el panel de la izquierda, haga clic en **Descargar**.
- 2 Siga las instrucciones que aparecen en pantalla para descargar McAfee VirusScan.

---

**Sugerencia:** puede descargar VirusScan haciendo clic en el vínculo **Unidades para analizar en este dispositivo USB** del panel Opciones de análisis.

---



---

## CAPÍTULO 8

# Renovación de la suscripción de VirusScan USB

Cuando caduque su suscripción de VirusScan USB, VirusScan USB ya no funcionará y no podrá recibir actualizaciones del programa ni archivos de definición de virus (DAT). Sin embargo, podrá seguir accediendo al panel de inicio principal de VirusScan USB, que le pedirá que renueve su suscripción.

**Sugerencia:** si renueva una suscripción antes de que caduque, el tiempo restante se agregará a la nueva suscripción.

### En este capítulo

Renovar la suscripción de VirusScan USB.....29

---

## Renovar la suscripción de VirusScan USB

Cuando caduque su suscripción de VirusScan USB, se le pedirá que renueve la suscripción cada vez que conecte el dispositivo USB o cada vez que intente ejecutar el programa. Aunque VirusScan USB no analice su dispositivo USB ni reciba actualizaciones una vez caducada la suscripción, sí le permite renovar su suscripción.

### **Para renovar la suscripción de VirusScan USB:**

- En el panel de inicio de VirusScan USB, en **Resumen de programa**, haga clic en **Renovar**.





---

## CAPÍTULO 9

# Preguntas más frecuentes

En este capítulo se da respuesta a las preguntas más frecuentes.

### En este capítulo

Se ha detectado una amenaza. ¿Qué debo hacer? ....	31
¿Es preciso estar conectado a Internet para realizar análisis? .....	31
¿VirusScan USB analiza los archivos comprimidos? .....	32
¿Cómo puedo obtener más ayuda de McAfee? .....	32

---

## Se ha detectado una amenaza. ¿Qué debo hacer?

McAfee utiliza alertas para ayudarle a gestionar la seguridad. Las alertas se agrupan en tres tipos básicos:

- Alerta roja
- Alerta amarilla
- Alerta verde

A continuación, puede elegir la forma de gestionar los archivos detectados, conforme a las recomendaciones de las alertas.

---

## ¿Es preciso estar conectado a Internet para realizar análisis?

No es necesario tener conexión a Internet para ejecutar un análisis, aunque debe conectarse al menos una vez a la semana para recibir las actualizaciones de McAfee.

---

## ¿VirusScan USB analiza los archivos comprimidos?

VirusScan USB analiza los archivos .zip y otros archivos comprimidos.

---

## ¿Cómo puedo obtener más ayuda de McAfee?

Para obtener más ayuda y respuestas a las preguntas más habituales, visite la página de inicio del Servicio de atención al cliente y soporte técnico de McAfee en:  
<http://www.mcafeeayuda.com> (<http://www.mcafeehelp.com>)

## CAPÍTULO 10

# Glosario

El glosario de términos enumera y define la terminología que se utiliza con más frecuencia en los productos de McAfee.

# Glosario

## A

### análisis bajo demanda

Un análisis que se inicia bajo demanda, es decir, cuando se hace clic en el botón **Análisis**. A diferencia del análisis en tiempo real o del control en tiempo real, los análisis bajo demanda no se inician automáticamente.

### archivos DAT

Archivos de definición de virus. Estos archivos contienen las definiciones de virus que se utilizan cuando se detectan virus y troyanos en un equipo o dispositivo USB.

## C

### control en tiempo real

Los archivos y carpetas se controlan constantemente por si se producen cambios (por ejemplo, se agrega un nuevo archivo a una carpeta o se modifica un archivo). Si el monitor en tiempo real detecta un cambio en un archivo, se analiza el archivo afectado para supervisar la actividad de los virus. Si se detecta un virus o un troyano, se limpia; si no puede limpiarse, se cambia el nombre.

## D

### dispositivo USB

Una unidad de poca memoria que se conecta al puerto USB del equipo. Un dispositivo USB actúa como un pequeño disco duro que facilita la transferencia de archivos de un equipo a otro.

## L

### launchpad

Un componente de interfaz U3 que actúa como punto de inicio para abrir y gestionar programas U3 USB.

## T

### troyano

Los troyanos son programas que muestran la apariencia de aplicaciones inofensivas. Los troyanos no son virus porque no se replican, pero pueden ser igual de destructivos.

## U

### U3

Una plataforma para ejecutar programas de Windows 2000 o XP directamente desde un dispositivo USB. La iniciativa U3 fue fundada en 2004 por M-Systems y SanDisk y permite a los usuarios ejecutar programas U3 en un equipo Windows sin instalar ni almacenar datos u opciones en el equipo. Gráficamente, U3 procede de “U”, calco fonético de la palabra inglesa “you” (usted, usuario), sumado al 3 que corresponde a las tres principales cualidades de la citada plataforma: simplificada, inteligente y móvil.

### unidad inteligente

Consulte dispositivo USB.

### USB

(Bus Serie Universal) Una interfaz informática serie estandarizada que le permite conectar dispositivos periféricos.

## V

### virus

Los virus informáticos son programas que se reproducen automáticamente y que pueden modificar archivos o datos. A menudo parecen proceder de un remitente de confianza o incluir un contenido inofensivo.



## Acerca de McAfee

McAfee, Inc., con sede central en Santa Clara, California, y líder mundial en prevención de intrusiones y gestión de riesgos de seguridad, proporciona servicios y soluciones proactivas y probadas que protegen sistemas y redes en todo el mundo. Su experiencia y su compromiso inigualable con la innovación permiten a McAfee dotar a usuarios particulares, empresas, sector público y proveedores de servicios de la capacidad de bloquear ataques, evitar problemas y controlar y mejorar de manera continua su seguridad.

## Copyright

Copyright © 2006 McAfee, Inc. Reservados todos los derechos. Queda prohibida la reproducción, transmisión, transcripción, almacenamiento en un sistema de recuperación o traducción a ningún idioma de este documento o parte de él en ninguna forma ni por ningún medio sin el consentimiento previo por escrito de McAfee, Inc. McAfee y cualquier otra marca comercial contenida en el presente documento son marcas comerciales registradas o marcas de McAfee, Inc. y/o sus empresas filiales en Estados Unidos u otros países. El color rojo asociado a la seguridad es el distintivo de los productos de la marca McAfee. Todas las demás marcas comerciales, tanto registradas como no registradas, y el material protegido contenidos en este documento son propiedad exclusiva de sus propietarios respectivos.

### ATRIBUCIONES DE MARCAS COMERCIALES

ACTIVE FIREWALL, ACTIVE SECURITY, ACTIVESECURITY (Y EN KATAKANA), ACTIVESHIELD, ANTIVIRUS ANYWARE AND DESIGN, CLEAN-UP, DESIGN (E ESTILIZADO), DESIGN (N ESTILIZADO), ENTERCEPT, ENTERPRISE SECURECAST, ENTERPRISE SECURECAST (Y EN KATAKANA), EPOLICY ORCHESTRATOR, FIRST AID, FORCEFIELD, GMT, GROUPSHIELD, GROUPSHIELD (Y EN KATAKANA), GUARD DOG, HOMEGUARD, HUNTER, INTRUSHIELD, INTRUSION PREVENTION THROUGH INNOVATION, M AND DESIGN, MCAFEE, MCAFEE (Y EN KATAKANA), MCAFEE AND DESIGN, MCAFEE.COM, MCAFEE VIRUSSCAN, NA NETWORK ASSOCIATES, NET TOOLS, NET TOOLS (Y EN KATAKANA), NETCRYPTO, NETOCTOPUS, NETSCAN, NETSHIELD, NETWORK ASSOCIATES, NETWORK ASSOCIATES COLLISEUM, NETXRAY, NOTESGUARD, NUTS & BOLTS, OIL CHANGE, PC MEDIC, PCNOTARY, PRIMESUPPORT, RINGFENCE, ROUTER PM, SECURECAST, SECURESELECT, SITEADVISOR, SITEADVISOR, SPAMKILLER, STALKER, THREATSCAN, TIS, TMEG, TOTAL VIRUS DEFENSE, TRUSTED MAIL, UNINSTALLER, VIREX, VIRUS FORUM, VIRUSCAN, VIRUSSCAN, VIRUSSCAN (Y EN KATAKANA), WEBSCAN, WEBSHIELD, WEBSHIELD (Y EN KATAKANA), WEBSTALKER, WEBWALL, WHAT'S THE STATE OF YOUR IDS?, WHO'S WATCHING YOUR NETWORK, YOUR E-BUSINESS DEFENDER, YOUR NETWORK. OUR BUSINESS.



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

# Índice

## ¿

- ¿Cómo puedo obtener más ayuda de McAfee?.....32
- ¿Es preciso estar conectado a Internet para realizar análisis?.....31
- ¿VirusScan USB analiza los archivos comprimidos?.....32

## A

- Acerca de las alertas .....17
- Acerca de McAfee .....37
- Actualizar VirusScan USB .....8
- análisis bajo demanda.....34
- Análisis del dispositivo USB.....9, 19
- Analizar un dispositivo USB .....20
- archivos DAT.....34

## C

- Cancelar el análisis .....21
- Configuración de las opciones de análisis ..... 5, 9, 19
- Configurar las ubicaciones que se van a analizar .....12
- Configurar tipos de archivo analizados .11
- control en tiempo real.....34
- Copyright .....38

## D

- Descargar software antivirus para su equipo .....27
- Deshabilitar el control en tiempo real ...13
- Deshabilitar la detección de software antivirus .....14
- dispositivo USB.....34

## E

- Eliminar un archivo infectado ..... 19, 25

## F

- Funciones.....4

## G

- Glosario .....33

## I

- Iniciar un análisis en el momento de la inserción ..... 14
- Instalación y actualización de VirusScan USB .....5
- Instalar VirusScan USB .....6

## L

- launchpad ..... 34

## M

- McAfee VirusScan USB .....3
- Mostrar mensajes informativos ..... 15

## P

- Pausar el análisis .....21
- Preguntas más frecuentes.....31
- Protección del equipo .....27

## R

- Reanudar el análisis .....21
- Renovación de la suscripción de VirusScan USB.....29
- Renovar la suscripción de VirusScan USB ..... 29

## S

- Se ha detectado una amenaza. ¿Qué debo hacer?.....31

## T

- Trabajar con alertas ..... 17
- Trabajar con los resultados de análisis ..23
- troyano ..... 34

## U

- U3 ..... 35
- unidad inteligente ..... 35
- USB.....35

## V

- Ver el resumen del programa VirusScan USB .....26
- Ver el último resumen de análisis .....25
- Ver los resultados de un análisis .....24