El archivo VSH es un archivo de texto, de formato similar al archivo Windows INI, que define las opciones de configuración de las operaciones de exploración asociadas al acceso a archivos (VSH son las siglas de VShield). Cada una de las variables del archivo tiene un nombre que va seguido del signo igual (=) y de un valor. Los valores definen las opciones de configuración seleccionadas para VShield. Las variables están agrupadas en cinco apartados: DetectionOptions, ActionOptions, ReportOptions, General y ExcludedItems. Para editar el archivo, utilice el **Explorador de Windows** o **Mi PC** para localizar el archivo **default.vsh** en la carpeta de VirusScan, haga clic con el botón derecho en el nombre de archivo y seleccione la opción **Abrir**.

En las variables del tipo Booleano, los valores posibles son 0 y 1. El valor 0 indica a VShield que debe desactivar esa opción, mientras que el 1 indica que debe activarla.

General

Variable	Descripción
bCanBeDisabled	Tipo: Booleano (1/0) Define si VShield puede desactivarse o no Valor predeterminado: 1
bShowTaskbarIcon	Tipo: Booleano (1/0) Define si debe aparecer o no el icono de VShield en la barra de tareas Valor predeterminado: 1

DetectionOptions

Variable	Descripción
bScanOnExecute	Tipo: Booleano (1/0) Indica a VShield que debe explorar los archivos cuando se ejecutan Valor predeterminado: 1
bScanOnOpen	Tipo: Booleano (1/0) Indica a VShield que debe explorar los archivos cuando se abren Valor predeterminado: 1
bScanOnCreate	Tipo: Booleano (1/0) Indica a VShield que debe explorar los archivos cuando se crean Valor predeterminado: 1
bScanOnRename	Tipo: Booleano (1/0) Indica a VShield que debe explorar los archivos cuando se cambian de nombre Valor predeterminado: 1
bScanOnShutdown	Tipo: Booleano (1/0) Indica a VShield que debe explorar el registro de arranque de la unidad A: cuando se cierra el sistema Valor predeterminado: 1
bScanOnBootAccess	Tipo: Booleano (1/0) Indica a VShield que debe explorar el registro de arranque de una unidad de disco la primera vez que se accede a él

	Valor predeterminado: 1
bScanAllFiles	Tipo: Booleano (1/0) Indica al programa que debe explorar el interior de todos los archivos Valor predeterminado: 0
bScanCompressed	Tipo: Booleano (1/0) Indica al programa que debe explorar los archivos comprimidos Valor predeterminado: 0
szProgramExtensions	Tipo: Cadena Define las extensiones de los archivos que deben explorarse Valor predeterminado: EXE COM DO? XL?
SzDefaultProgramExtensions	Tipo: Cadena Define las extensiones que deben utilizarse como extensiones predeterminadas de programa para la configuración de la función de exploración Valor predeterminado: EXE COM DO? XL?

AlertOptions

Variable	**Descripción**
bNetworkAlert	Tipo: Booleano (1/0) Activa el sistema centralizado de alerta Valor predeterminado: 0
szNetworkAlertPath	Tipo: Cadena Define una carpeta centralizada de alertas en el servidor Valor predeterminado: ninguna

ActionOptions

Variable	Descripción
bDisplayMessage	Tipo: Booleano (1/0) Define si debe presentarse o no un mensaje personalizado en el cuadro de diálogo **Consultar antes de actuar** cuando se detecta un virus Valor predeterminado: 0
uVshieldAction	Tipo: Entero (1-5) Indica a VShield que debe emprender la acción especificada cuando se detecte un virus Valores posibles: 1 – Pedir al usuario que seleccione la acción 2 – Mover automáticamente los archivos infectados 3 – Limpiar automáticamente los archivos infectados (Impedir el acceso a los mismos si no pueden limpiarse)

	4 – Borrar automáticamente los archivos infectados 5 – Impedir el acceso a los archivos infectados y continuar Valor predeterminado: 1
bButtonClean	Tipo: Booleano (1/0) Indica a VShield que debe dar al usuario la opción de limpiar un archivo si se ha seleccionado la opción **Consultar antes de actuar** y se detecta un virus Valor predeterminado: 1
bButtonDelete	Tipo: Booleano (1/0) Indica a VShield que debe dar al usuario la opción de borrar un archivo si se ha seleccionado la opción **Consultar antes de actuar** y se detecta un virus Valor predeterminado: 1
bButtonExclude	Tipo: Booleano (1/0) Indica a VShield que debe dar al usuario la opción de excluir un archivo si se ha seleccionado la opción **Consultar antes de actuar** y se detecta un virus Valor predeterminado: 1
bButtonContinue	Tipo: Booleano (1/0) Indica a VShield que debe dar al usuario la opción de continuar la acción interrumpida si se ha seleccionado la opción **Consultar antes de actuar** y se detecta un virus Valor predeterminado: 1
bButtonStop	Tipo: Booleano (1/0) Indica a VShield que debe dar al usuario la opción de impedir el acceso al archivo infectado si se ha seleccionado la opción **Consultar antes de actuar** y se detecta un virus Valor predeterminado: 1
szMoveToFolder	Tipo: Cadena Define la carpeta a la que se deben mover los archivos infectados Valor predeterminado: \Infectado
szCustomMessage	Tipo: Cadena Define el mensaje personalizado que debe presentarse cuando se detecta un virus y la opción de acción seleccionada es **Consultar antes de actuar** Valor predeterminado: Detectado posible virus

ReportOptions

Variable	**Descripción**
bLogToFile	Tipo: Booleano (1/0) Define si los resultados de la exploración de archivos deben o no conservarse en un archivo de

	registro
	Valor predeterminado: 0
bLimitSize	Tipo: Booleano (1/0)
	Define si el tamaño del archivo de registro debe o no tener un límite de tamaño
	Valor predeterminado: 1
uMaxKilobytes	Tipo: Entero (10-999)
	Define el tamaño máximo (en kilobytes) del archivo de registro
	Valor predeterminado: 100
bLogDetection	Tipo: Booleano (1/0)
	Define si los resultados de la exploración de archivos deben quedar registrados o no
	Valor predeterminado: 1
bLogClean	Tipo: Booleano (1/0)
	Define si los resultados de la limpieza de archivos deben quedar registrados o no
	Valor predeterminado: 1
bLogDelete	Tipo: Booleano (1/0)
	Define si los resultados de las operaciones de eliminación de archivos infectados deben quedar registrados o no
	Valor predeterminado: 1
bLogMove	Tipo: Booleano (1/0)
	Defines si las operaciones de mover archivos infectados deben quedar registradas o no
	Valor predeterminado: 1
bLogSettings	Tipo: Booleano (1/0)
	Define si las opciones de configuración empleadas durante la sesión deben quedar o no registradas al cerrar el sistema
	Valor predeterminado: 1
bLogSummary	Tipo: Booleano (1/0)
	Define si debe registrarse o no un resumen de la sesión al cerrar el sistema
	Valor predeterminado: 1
bLogDateTime	Tipo: Booleano (1/0)
	Define si debe registrarse o no la fecha y hora de un evento
	Valor predeterminado: 1
bLogUserName	Tipo: Booleano (1/0)
	Define si debe registrarse o no el nombre de usuario
	Valor predeterminado: 1
szLogFileName	Tipo: Cadena
	Define el nombre del archivo de registro
	Valor predeterminado: C:\Archivos de programa\McAfee\VirusScan\VSHLOG.TXT

SecurityOptions

Variable	Descripción
SzPasswordProtect	Tipo: Booleano (1/0) Define si está activada o no la protección mediante contraseña Valor predeterminado: 0

ExclusionOptions

Variable	Descripción
SzExclusionsFileName	Tipo: Cadena Valor predeterminado: VSHLOG.TXT

AVCONFILE

Variable	Descripción
AVCONFILE	Tipo: Cadena Define la ruta de AVCONSOLE Valor predeterminado: C:\Archivos de programa\McAfee\VirusScan\avconsole.ini
SECTION	Tipo: Cadena Define la ubicación de informes en AVCONSOL.INI Valor predeterminado: Item_0

ExcludedItems

Variable	Descripción
NumExcludedItems	Tipo: Entero (0-n) Define el número de elementos excluidos de la operación de exploración Valor predeterminado: 1
ExcludedItem_x, donde x es un índice que incluye el cero	Tipo: Cadena Indica a VShield que debe excluir el elemento en cuestión de la operación de exploración Valor predeterminado: \Reciclado|*.*|1|1 * * La cadena se compone de varios campos separados por el carácter de barra vertical (|): Campo 1 – Carpeta del elemento a excluir. Debe dejarse en blanco cuando se trata de un archivo que puede encontrarse en cualquier ubicación del sistema. Campo 2 – Nombre de archivo del elemento a excluir. Debe dejarse en blanco si se trata de excluir una carpeta. Campo 3 – Entero (1-3) Valores posibles: 1 – Excluir de la exploración asociada al acceso a archivos 2 – Excluir de la exploración de registro de arranque

3 – Excluir de la exploración de registro de arranque y de acceso a archivos

Campo 4 - Booleano (1/0)

Valores posibles:

1 – Indica a VShield que debe excluir también las subcarpetas del elemento excluido

0 – Indica a VShield que no debe excluir las subcarpetas

Otros temas asociados

El archivo VSC es un archivo de texto, de formato similar al archivo Windows INI, que define las opciones de configuración de las operaciones de exploración realizadas requeridas por el usuario (VSC son las siglas de VirusScan). Cada una de las variables del archivo tiene un nombre que va seguido del signo igual (=) y de un valor. Los valores definen las opciones de configuración seleccionadas para VirusScan. Las variables están agrupadas en tres apartados ScanOptions, AlertOptions y ActivityLogOptions. Para editar el archivo, utilice el **Explorador de Windows** o **Mi PC** para localizar el archivo **default.vsc** en la carpeta de McAfee VirusScan, haga clic con el botón derecho en el nombre de archivo y seleccione la opción **Abrir**.

Nota

- En las variables del tipo Booleano, los valores posibles son 0 y 1. El valor 0 indica a VirusScan que debe desactivar esa opción, mientras que el 1 indica que debe activarla.

ScanOptions

Variable	Descripción
BAutoStart	Tipo: Booleano (1/0) Indica a VirusScan que debe iniciar inmediatamente la exploración cuando se ejecuta Valor predeterminado: 0
BAutoExit	Tipo: Booleano (1/0) Indica a VirusScan que debe salir automáticamente cuando termine la exploración si no se ha encontrado ningún virus Valor predeterminado: 0
BAlwaysExit	Tipo: Booleano (1/0) Indica a VirusScan que debe salir siempre cuando termine la exploración Valor predeterminado: 0
BSkipMemoryScan	Tipo: Booleano (1/0) Indica a VirusScan que no debe realizar la exploración de la memoria Valor predeterminado: 0
BSkipBootScan	Tipo: Booleano (1/0) Indica a VirusScan que no debe realizar la exploración del sector de arranque sector Valor predeterminado: 0
bSkipSplash	Tipo: Booleano (1/0) Indica a VirusScan que no debe presentar la pantalla de introducción al programa cuando se ejecuta la aplicación Valor predeterminado: 0
nPriority	Tipo: Entero (0-5) Define la prioridad de ejecución de las rutinas de exploración. Valores posibles: 0 – Prioridad normal de ejecución (valor predeterminado) 1 – Mínima prioridad de ejecución 2 – Prioridad de ejecución inferior a la normal 3 – Prioridad de ejecución normal 4 – Prioridad de ejecución superior a la normal 5 – Máxima prioridad de ejecución Valor predeterminado: 0
nChecksum	Reservado

bConfigurableGuiMode	Tipo: Booleano (1/0) Indica a VirusScan que debe utilizar la interfaz Avanzada para usuarios avanzados Valor predeterminado: 0
szTaskName	Reservado

DetectionOptions

Variable	Descripción
bScanAllFiles	Tipo: Booleano (1/0) Indica a VirusScan que debe explorar el interior de todos los archivos Valor predeterminado: 0
bScanCompressed	Tipo: Booleano (1/0) Indica a VirusScan que debe explorar los archivos comprimidos Valor predeterminado: 1
szProgramExtensions	Tipo: Cadena Define las extensiones de los archivos que deben explorarse Valor predeterminado: COM DO? EXE XL?
szDefaultProgramExtensions	Tipo: Cadena Define las extensiones que deben utilizarse como extensiones predeterminadas de programa para la configuración de la función de exploración Valor predeterminado: COM DO? EXE XL?

AlertOptions

Variable	Descripción
bNetworkAlert	Tipo: Booleano (1/0) Activa el sistema centralizado de alerta Valor predeterminado: 0
bSoundAlert	Tipo: Booleano (1/0) Indica a VirusScan que debe hacer sonar una alarma cuando detecte un virus Valor predeterminado: 1
szNetworkAlertPath	Tipo: Cadena Define una carpeta centralizada de alertas en el servidor. Valor predeterminado: ninguno

ActionOptions

Variable	Descripción
bDisplayMessage	Tipo: Booleano (1/0) Define si debe presentarse o no un mensaje personalizado cuando se detecte un virus

	Valor predeterminado: 0
uScanAction	Tipo: Entero (1-5) Indica a VirusScan que debe emprender la acción especificada cuando detecte un virus Valores posibles: 0 – Pedir al usuario que seleccione la acción 1 – Mover automáticamente los archivos infectados 2 – Limpiar automáticamente los archivos infectados 3 – Borrar automáticamente los archivos infectados 4 – Continuar con la exploración Valor predeterminado: 0
bButtonClean	Tipo: Booleano (1/0) Indica a VirusScan que debe dar al usuario la opción de limpiar un archivo si se ha seleccionado la opción **Consultar antes de actuar** y se detecta un virus Valor predeterminado: 1
bButtonDelete	Tipo: Booleano (1/0) Indica a VirusScan que debe dar al usuario la opción de borrar un archivo si se ha seleccionado la opción **Consultar antes de actuar** y se detecta un virus Valor predeterminado: 1
bButtonExclude	Tipo: Booleano (1/0) Indica a VirusScan que debe dar al usuario la opción de excluir un archivo si se ha seleccionado la opción **Consultar antes de actuar** y se detecta un virus Valor predeterminado: 1
bButtonMove	Tipo: Booleano (1/0) Indica a VirusScan que debe dar al usuario la opción de mover el archivo infectado si se ha seleccionado la opción **Consultar antes de actuar** y se detecta un virus Valor predeterminado: 1
bButtonContinue	Tipo: Booleano (1/0) Indica a VirusScan que debe dar al usuario la opción de continuar la acción interrumpida si se ha seleccionado la opción **Consultar antes de actuar** y se detecta un virus Valor predeterminado: 1
bButtonStop	Tipo: Booleano (1/0) Indica a VirusScan que debe dar al usuario la opción de impedir el acceso al archivo infectado si se ha seleccionado la opción **Consultar antes de actuar** y se detecta un virus Valor predeterminado: 1
szMoveToFolder	Tipo: Cadena Define la carpeta a la que se deben mover los archivos infectados Valor predeterminado: \Infectado

szCustomMessage	Tipo: Cadena Define el mensaje personalizado que debe presentarse cuando se detecta un virus y la opción de acción seleccionada es **Consultar antes de actuar** Valor predeterminado: Detectado posible virus

ReportOptions

Variable	**Descripción**
bLogToFile	Tipo: Booleano (1/0) Define si los resultados de la exploración de archivos deben o no conservarse en un archivo de registro Valor predeterminado: 0
bLimitSize	Tipo: Booleano (1/0) Define si el tamaño del archivo de registro debe o no tener un límite de tamaño Valor predeterminado: 1
uMaxKilobytes	Tipo: Entero (10-999) Define el tamaño máximo (en kilobytes) del archivo de registro Valor predeterminado: 100
bLogDetection	Tipo: Booleano (1/0) Define si los resultados de la exploración de archivos deben quedar registrados o no Valor predeterminado: 1
bLogClean	Tipo: Booleano (1/0) Define si los resultados de la limpieza de archivos deben quedar registrados o no Valor predeterminado: 1
bLogDelete	Tipo: Booleano (1/0) Define si los resultados de las operaciones de eliminación de archivos infectados deben quedar registrados o no Valor predeterminado: 1
bLogMove	Tipo: Booleano (1/0) Defines si las operaciones de mover archivos infectados deben quedar registradas o no Valor predeterminado: 1
bLogSettings	Tipo: Booleano (1/0) Define si las opciones de configuración empleadas durante la sesión deben quedar o no registradas al cerrar el sistema Valor predeterminado: 1
bLogSummary	Tipo: Booleano (1/0) Define si debe registrarse o no un resumen de la sesión al cerrar el sistema Valor predeterminado: 1
bLogDateTime	Tipo: Booleano (1/0) Define si debe registrarse o no la

	fecha y hora de un evento
	Valor predeterminado: 1
bLogUserName	Tipo: Booleano (1/0)
	Define si debe registrarse o no el nombre de usuario
	Valor predeterminado: 1
szLogFileName	Tipo: Cadena
	Define el nombre del archivo de registro
	Valor predeterminado: VSCLOG.TXT

ScanItems

Variable	**Descripción**
NumScanItems	Tipo: Entero (0-n)
	Define el número de elementos a explorar
	Valor predeterminado: 1
szScanItem_x	Tipo: Cadena
	Valor predeterminado: C:\
	Indica a VirusScan el elemento que debe explorar
	* La cadena se compone de varios campos separados por el carácter barra vertical (|):
	Campo 1 – Carpeta del elemento a explorar. Debe dejarse en blanco cuando se trata de un archivo que puede encontrarse en cualquier ubicación del sistema.
	Campo 2 – Nombre de archivo del elemento a explorar. Debe dejarse en blanco si se trata de explorar una carpeta.
	Campo 3 – Entero (1-3)
	Valores posibles:
	1 – Explorar archivo
	2 – Explorar registro de arranque
	3 – Explorar archivos y registro de arranque
	Campo 4 – Booleano (1/0)
	Valores posibles:
	1 – Indica a VirusScan que debe explorar también las subcarpetas del elemento
	0 - Indica a VirusScan que no debe explorar las subcarpetas del elemento

SecurityOptions

Variable	**Descripción**
szPasswordProtect	Tipo: Booleano (1/0)
	Define si está activada o no la protección mediante contraseña.
	Valor predeterminado: 0
szPasswordCRC	Reservado. No cambiar este valor.
bInheritSecurity	Tipo: Booleano (1/0)
	Define si está activada o no la función Mantener seguridad. Cuando está

	activada esta función, las copias de una tarea conservan la protección mediante contraseña si la tarea original la tenía. Valor predeterminado: 0

ExcludedItems

Variable	**Descripción**
NumExcludedItems	Tipo: Entero (0-n) Define el número de elementos excluidos de la operación de exploración Valor predeterminado: 1
ExcludedItem_x, donde x es un índice que incluye el cero	Tipo: Cadena Indica a VShield que debe excluir el elemento en cuestión de la operación de exploración Valor predeterminado: \Reciclado|*.*|1|1 * * La cadena se compone de varios campos separados por el carácter (|): Campo 1 – Carpeta del elemento a excluir. Debe dejarse en blanco cuando se trata de un archivo que puede encontrarse en cualquier ubicación del sistema. Campo 2 – Nombre de archivo del elemento a excluir. Debe dejarse en blanco si se trata de excluir una carpeta. Campo 3 – Entero (1-3) Valores posibles: 1 – Excluir de la exploración asociada al acceso a archivos 2 – Excluir de la exploración de registro de arranque 3 – Excluir de la exploración de registro de arranque y de acceso a archivos Campo 4 - Booleano (1/0) Valores posibles: 1 – Indica a VShield que debe excluir también las subcarpetas del elemento excluido 0 – Indica a VShield que no debe excluir las subcarpetas

Otros temas asociados

La siguiente tabla muestra todas las opciones que se pueden utilizar al ejecutar el programa de línea de comandos DOS, SCAN.EXE. Para ejecutar SCAN.EXE, primero debe emplear el comando cd para pasar al directorio (carpeta) en que está instalado VirusScan. A continuación, escriba scan /? para que aparezca en pantalla la lista de opciones, junto con instrucciones para su utilización.

Notas

- Al especificar un nombre de archivo como parte de una opción de línea de comandos, debe incluir la ruta completa si el archivo no está almacenado en la carpeta en que está instalado VirusScan.
- Estas opciones sólo están disponibles en el programa SCAN.EXE y se pueden utilizar únicamente en la línea de comandos de DOS.

Sugerencia

- Para explorar todas las unidades de disco del sistema (incluyendo las unidades comprimidas y las unidades de CD-ROM y PCMCIA asignadas localmente, pero excluyendo las unidades de disquete) en busca de virus conocidos, escriba el siguiente comando:

  scan /adl

Opción de línea de comandos	Descripción
`/?` o `/HELP`	No realiza una exploración, sino que presenta una lista con las opciones de línea de comandos de VirusScan, acompañando a cada una de ellas una breve descripción. Cada una de esas opciones puede utilizarse independientemente en la línea de comandos (sin ninguna otra opción).
/ADL	Explora las unidades locales (incluyendo las unidades comprimidas, unidades de CD-ROM y PCMCIA, pero sin incluir a las unidades de disquete), además de las unidades que se indiquen específicamente en la línea de comandos. Para explorar conjuntamente unidades locales y unidades de red, combine en la misma línea de comandos las opciones /ADL y /ADN.
/ADN	Explora las unidades de red en busca de virus, además de las unidades que se indiquen específicamente en la línea de comandos. Para explorar conjuntamente unidades locales y unidades de red, combine en la misma línea de comandos las opciones /ADL y /ADN.
/AF nombre_de_archivo	Guarda los códigos de validación y recuperación en el archivo *nombre_de_archivo.* Ayuda a detectar virus nuevos o desconocidos. La opción /AF registra, en el archivo que especifique, datos de validación y recuperación correspondientes a archivos ejecutables, sector de arranque o al Registro Principal de Arranque de un disco duro o disquete. El archivo de registro contiene unos 89 bytes de información para cada archivo validado. Debe especificar un *nombre_de_archivo*, que puede incluir la ruta completa de acceso. Si la ruta de acceso tiene como destino una unidad de red, debe tener los

	derechos necesarios para crear y borrar archivos en esa unidad. Si el archivo *nombre_de_archivo* existe, VirusScan lo actualizará. /AF casi triplica el tiempo necesario para realizar una exploración. *La opción /AF realiza casi la misma función que la opción /AV, aunque guarda sus datos en un archivo independiente en lugar de cambiar los propios archivos ejecutables.* La opción /AF no guarda ninguna información acerca del Registro Principal de Arranque o sector de arranque de la unidad explorada.
/ALERTPATH carpeta	Especifica la carpeta de red de centralización de alertas que controla NetShield. Vea NetShield de Network Associates.
/ALL	Ignora las opciones de configuración predeterminadas y explora todos los archivos. Esta opción aumenta considerablemente el tiempo necesario para realizar una exploración. Utilícela cuando haya encontrado un virus o sospeche que existe uno. *La lista de extensiones estándar de nombre de archivo para ejecutables ha cambiado respecto de versiones anteriores de VirusScan.*
/APPEND	Se utiliza junto con la opción /REPOT y agrega el texto del mensaje de informe al archivo de informe especificado. Si no se utiliza esta opción, la opción /REPOT sobrescribe el archivo de informe especificado, caso de existir.
/AV	Esta opción ayuda a detectar y eliminar virus nuevos o desconocidos, /AV agrega datos de validación y recuperación a cada archivo ejecutable estándar (.EXE, .COM, .SYS, .BIN, .OVL, and .DLL), aumentando el tamaño de cada uno de esos archivos en 98 bytes. Para actualizar archivos guardados en una unidad de red compartida, debe disponer de derechos de acceso y actualización en esa unidad. Para excluir de esta función archivos que se modifican o exploran a si mismos, o archivos dañados que puedan dar lugar a falsas alarmas, se utiliza la opción /EXCLUDE. Si se usan conjuntamente en la misma línea de comandos las opciones /AV, /CV o /RV, se produce un error. *La opción /AV no guarda ninguna información acerca del Registro Principal de Arranque ni el sector de arranque de la unidad explorada.*
/BOOT	Explora sólo el sector de arranque y el Registro Principal de Arranque de la unidad especificada.
/CF nombre_de_archivo	Esta opción ayuda a detectar virus nuevos o desconocidos. Comprueba los datos de validación que guarda la opción /AF en el archivo

	nombre_de_archivo. Si un archivo o área del sistema ha cambiado, VirusScan informa que se ha podido producir una infección con virus. La opción /CF aumentan en un 250% el tiempo necesario para realizar la exploración. El uso combinado de las opciones /AF, /CF o /RF en una línea de comandos da lugar a un error. *Algunos equipos antiguos de Hewlett-Packard y Zenith modifican el sector de arranque cada vez que se inicia el sistema. Si utiliza la opción /CF, VirusScan informará continuamente que el sector de arranque ha sido modificado, aunque no exista ningún virus presente. Examine el manual de referencia de su equipo para determinar si su PC utiliza un programa de arranque que se automodifica.*
/CLEANDOC	Limpia de virus sólo los archivos de Microsoft Word que estén infectados.
/CLEANDOCALL	Quita todas las macros de los archivos de Microsoft Word infectados.
/CONTACTFILE nombre_de_archivo	Identifica un archivo que contiene un mensaje (cadena) que debe aparecer en pantalla cuando se detecta un virus. Esta opción es muy útil en entornos de red, ya que se puede mantener con facilidad el texto del mensaje en un archivo central, en lugar de en cada estación de trabajo. El mensaje puede contener cualquier carácter excepto la barra inversa (\). Los mensajes que comienzan por una barra (oblicua) (/) o un guión (-) deben ponerse entre comillas.
/CV	Esta opción ayuda a detectar virus nuevos o desconocidos. Comprueba los datos de validación que agrega a los archivos la opción /AV. Si un archivo se modifica, VirusScan informa que se puede haber producido una infección con virus. La opción /CV aumenta en un 50% el tiempo necesario para la exploración. El uso combinado de las opciones /AV, /CV o /RV en la misma línea de comandos da lugar a un error. *La opción /CV no comprueba si se han producido o no cambios en el sector de arranque.*
/DEL	Elimina los archivos infectados. Una vez eliminados, los archivos infectados se recuperan a partir de la copia de seguridad.
/EXCLUDE nombre_de_archivo	Excluye de la exploración los archivos indicados en el archivo *nombre_de_archivo*. Esta opción permite excluir determinados archivos de la validación que realizan las opciones /AF y /AV y de las comprobaciones de las opciones /CF y /CV. Los archivos que se automodifican o se autoexploran, pueden dar lugar a falsas alarmas durante su exploración.
/FAST	Acelera la exploración. Reduce el tiempo necesario para una exploración en un 15%. Al usar la

	opción /FAST, VirusScan explora una porción más pequeña de cada archivo en busca de virus. El uso de la opción /FAST puede hacer que no se detecten infecciones que si se detectan con una exploración más completo (y lento). No utilice esta opción si ha encontrado algún virus o sospecha que puede haber uno.
/FORCE	Utiliza el registro principal de arranque genérico durante la limpieza de virus de la tabla de partición.
/FREQUENCY horas	Número de horas que deben transcurrir entre dos exploraciones consecutivas que concluyan con éxito (Ejemplo: `/FREQUENCY 1`). En entornos en los que el riesgo de infección con virus es muy bajo, esta opción sirve para evitar exploraciones innecesarias o demasiado frecuentes. Cuanto menor sea el número de horas especificado, mayor será la frecuencia de las exploraciones y, por tanto, la protección frente a infecciones.
/LOAD nombre_de_archivo	Realiza una exploración utilizando la información guardada en el archivo *nombre_de_archivo*. Se pueden guardar todas las opciones de configuración personalizadas en un archivo de configuración (un archivo de texto ASCII) y utilizar posteriormente la opción /LOAD para cargar las opciones de configuración desde ese archivo.
/LOCK	Al detectar VirusScan un virus, detiene el sistema para impedir que la infección progrese. La opción /LOCK es adecuada para entornos de red muy vulnerables, como pueden ser los laboratorios de prácticas de informática. Si utiliza la opción /LOCK, es aconsejable que use también la opción /CONTACTFILE para informar a los usuarios qué deben hacer o con quién deben ponerse en contacto cuando se detecte un virus y el sistema quede bloqueado.
/LOG	Crea o actualiza el archivo SCAN.LOG, en el directorio raíz de la unidad de disco seleccionada. En este archivo se registra la fecha y hora en que se ejecuta el programa VirusScan.
/MANY	Explora consecutivamente múltiples disquetes en la misma unidad. VirusScan pide que se introduzca cada disquete. Una vez que haya logrado limpiar totalmente de virus un sistema, esta opción permite explorar múltiples disquetes de forma muy rápida. El programa VirusScan debe estar guardado en un disco que no se extraiga durante la exploración. Por ejemplo, si está explorando la unidad A: y ejecuta el programa también desde la unidad A:, el programa se interrumpirá cuando cambie de disquete. El siguiente comando da lugar a un error de

	ejecución:
	a:\scan a: /many
/MAXFILESIZE xxx.x	Especifica el tamaño máximo de los archivos que se exploran en busca de virus.
/MEMEXCL	Excluye una determinada área de memoria de la exploración (el valor predeterminado es A000-FFFF, 0000=Scan all).
	Esta opción de la línea de comandos impide que VirusScan explore áreas de la memoria superior, que pueden contener referencias asociadas al hardware y pueden dar lugar a falsas alarmas.
/MOVE directorio	Mueve todos los archivos infectados que se han encontrado durante la exploración al directorio que se especifica. Para mantener la estructura de unidades y directorios, esta opción no tiene efecto cuando es el Registro Principal de Arranque o el sector de arranque los infectados, dado que en realidad no se trata de archivos.
/NOBEEP	Desactiva el tono de aviso que se escucha cuando VirusScan encuentra un virus.
/NOBREAK	Desactiva las combinaciones de teclas CTRL-C y CTRL-INTERRUMPIR (INT) durante las exploraciones. Los usuarios no pueden así detener una exploración en curso empleando esas combinaciones de teclas.
	Utilice esta opción junto con la opción /LOG para poder disponer de un registro que permita auditar exploraciones programadas y realizadas de forma regular.
/NOCOMP	Evita la exploración de ejecutables comprimidos mediante los programas de compresión de archivos LZEXE o PKLITE.
	Así se reduce el tiempo necesario para la exploración cuando no es necesario hacer una exploración total. Si no se utiliza esta opción, y como opción predeterminada, VirusScan explora el interior de los archivos ejecutables, o descomprimibles automáticamente, que se hayan creado con los programas de compresión de archivos LZEXE o PKLITE. VirusScan descomprime en memoria cada uno de los archivos y comprueba si contienen "firmas" de virus, esta operación consume tiempo pero da como resultado una exploración más concienzuda. Si utiliza la opción /NOCOMP, VirusScan no explora en busca de virus el interior de los archivos comprimidos, aunque puede comprobar si se han producido modificaciones en esos archivos si previamente se han validado usando códigos de validación y recuperación.
/NODDA	Sin acceso directo al disco.
	Impide que VirusScan tenga acceso al registro de arranque. Esta opción se ha agregado para permitir el uso de

	VirusScan con Windows NT. Puede tener que usar esta opción en algunas unidades controladas como dispositivos.
/NODOC	Evita la exploración de archivos de Microsoft Word.
/NOEMS	Impide que VirusScan utilice memoria expandida (LIM EMS 3.2), garantizando así que ésta queda disponible para otros programas.
/NOEXPIRE	Desactiva el mensaje de ‘‘fecha de expiración’’ que aparece cuando los archivos de datos de VirusScan caducan.
/NOMEM	Reduce el tiempo necesario para la exploración omitiendo todas las exploraciones en busca de virus en memoria. La opción /NOMEM sólo se debe utilizar cuando existe la certeza de que el equipo no tiene virus. VirusScan puede explorar la memoria del sistema en busca de todos los virus informáticos conocidos que pueden residir en ella. Además de la memoria principal, desde 0 Kb a 640 Kb, VirusScan comprueba la memoria del sistema desde 640 Kb a 1.088 Kb en la que puede haber virus en sistemas 286 y posteriores. A las direcciones de memoria por encima de 1.088 Kb no tiene acceso directamente el procesador y actualmente no pueden contener virus.
/PAUSE	Permite detener (pausa) la pantalla. Si utiliza la opción /PAUSE, aparecerá el mensaje ‘‘Presione cualquier tecla para continuar’’ cuando VirusScan llena una pantalla con mensajes (por ejemplo, si utiliza las opciones /SHOWLOG o /VIRLIST). En caso contrario, y como opción predeterminada, VirusScan llena la pantalla y continúa presentando nuevos mensajes sin detenerse, esto permite usar VirusScan en equipos que cuentan con muchas unidades o que padecen infecciones graves sin necesidad de que el usuario tenga que intervenir constantemente. Es aconsejable no utilizar la opción /PAUSE cuando se guarda un registro de los mensajes de VirusScan por medio de las opciones de generación de informes (/REPOT, /RPTCOR, /RPTMOD y /RPTERR).
/PLAD	Conserva las últimas fechas de acceso (en unidades de las que se es propietario). Impide cambiar el atributo de fecha de último acceso en los archivos almacenados en una unidad de red. Normalmente, las unidades de red actualizan la fecha de último acceso cuando VirusScan abre y examina un archivo. Sin embargo, algunos sistemas de copia de seguridad en cinta utilizan esta fecha de último acceso para determinar si deben o no hacer una copia de seguridad del archivo. Utilice la opción /PLAD para asegurarse que la fecha de

	último acceso no cambia como resultado de la exploración.
/REPOT nombre_de_archivo	Crea un informe con las unidades infectadas y los errores de sistema. Esta opción guarda la salida del programa VirusScan en el archivo *nombre_de_archivo*, en formato de archivo de texto ASCII. Si el archivo *nombre_de_archivo* existe, /REPOT lo elimina y reemplaza por uno nuevo (o si se usa también la opción /APPEND, agrega el nuevo informe al final del archivo ya existente). Puede incluir la unidad y directorio de destino (como por ejemplo, D:\VSREPRT\ALL.TXT), pero si la unidad de destino es una unidad de red, deberá disponer de los permisos necesarios para crear y borrar archivos en esa unidad. También puede utilizar las opciones /RPTALL, /RPTCOR, /RPTMOD y /RPTERR para agregar al informe datos de los archivos explorados, archivos dañados, archivos modificados y errores de sistema.
/RF nombre_de_archivo	Elimina los datos de validación y recuperación del archivo *nombre_de_archivo* creado con la opción /AF. Si el archivo *nombre_de_archivo* reside en una unidad compartida de red, debe disponer de los permisos necesarios para borrar archivos en esa unidad. El uso combinado de las opciones /AF, /CF o /RF en la misma línea de comandos da lugar a un error.
/RPTALL	Agrega al archivo del informe una lista con los archivos explorados (esta opción se utiliza junto con la opción /REPOT).
/RPTCOR	Cuando se usa en combinación con la opción /REPOT, agrega al archivo del informe los nombres de los archivos dañados. Un archivo puede haber sido dañado por un virus. Puede utilizar la opción /RPTCOR junto con las opciones /RPTMOD y /RPTERR en la misma línea de comandos. *Pueden producirse lecturas erróneas en algunos archivos que necesitan de otro ejecutable para ejecutarse adecuadamente (es decir, en archivos que no son ralamente ejecutables en si mismos).*
/RPTERR	Agrega al archivo del informe una lista con los errores de sistema. Esta opción se usa en combinación con la opción /REPOT. Entre los errores de sistema se incluyen problemas de lectura o escritura en unidades de disco o disquetes, problemas de red o del sistema de archivos, problemas asociados a la generación del informe y otros problemas relacionados con el sistema. Puede utilizar la opción /RPTERR junto con las

	opciones /RPTCOR y /RPTMOD en la misma línea de comandos.
/RPTMOD	Agrega al archivo del informe la lista de los archivos modificados. Esta opción se usa en combinación con la opción /REPOT. VirusScan identifica los archivos modificados cuando sus códigos de validación y recuperación no coinciden (para ello se usan las opciones /CF o /CV). La opción /RPTMOD se puede utilizar con las opciones /RPTCOR y /RPTERR en la misma línea de comandos.
/RV	Elimina los datos de validación y recuperación de los archivos validados mediante la opción /AV. Para actualizar archivos en una unidad compartida de red, debe disponer de los derechos de acceso necesarios para actualizarlos. El uso combinado de las opciones /AV, /CV o /RV en la misma línea de comandos da lugar a un error.
/SHOWLOG	Presenta el contenido del archivo SCAN.LOG. SCAN.LOG guarda las fechas y horas en que se ejecuta el programa VirusScan. El archivo se crea en el directorio actual y se actualiza con la fecha y hora de todas las exploraciones en que se utiliza la opción /LOG. El archivo SCAN.LOG contiene texto y algún formato especial. Para detener la pantalla cuando se llena de mensajes, puede combinar con esta opción la opción /PAUSE.
/SUB	Explora los subdirectorios que forman parte del directorio. Como opción predeterminada, cuando se especifica un directorio a explorar en lugar de una unidad de disco, VirusScan explora únicamente los archivos que contiene y no sus subdirectorios. Utilice la opción /SUB para explorar todos los subdirectorios que pertenecen a los directorios especificados. No utilice la opción /SUB cuando trate de explorar una unidad completa.
/VIRLIST	Muestra el nombre y una breve descripción de cada uno de los virus que detecta VirusScan. Para detener la pantalla cuando se llena de mensajes, puede combinar esta opción con la opción /PAUSE. La opción /VIRLIST, sola o combinada con la opción /PAUSE, se utilizan desde la línea de comandos. Puede guardar la lista con los nombres y descripciones de los virus en un archivo, redireccionando previamente la salida del comando. Por ejemplo, en DOS, debe escribir: scan /virlist > filename.txt *Dado que VirusScan puede detectar muchos virus, el archivo tiene más de 250 páginas.*

Otros temas asociados

El archivo ALR es el texto de centralización de alertas que contiene las variables de eventos relacionados con virus. Cada variable del archivo tiene un nombre que va seguido del signo igual (=) y de un valor. La siguiente tabla describe línea a línea el formato del archivo ALR de centralización de alertas:

[CentralAlert]	Identificador de centralización de alertas
uFileVersion	Tipo: Entero
	Número de versión de centralización de alertas
uStatus	Reservado
szVirusName	Tipo: Cadena
	Nombre del virus.
szItemName	Tipo: Cadena
	Nombre y ruta de acceso del archivo infectado.
szUserName	Tipo: Cadena
	Nombre del usuario.
szSoftware	Tipo: Cadena
	Nombre de la aplicación anti-virus de Network Associates instalada en la máquina que informa de la infección.
szSoftwareVersion	Tipo: Cadena
	Versión de la aplicación anti-virus.
szComputerName	Tipo: Cadena
	Nombre de la máquina que informa acerca del evento.
uYear	Tipo: Entero (0000-9999)
	Año en que tiene lugar el evento.
uMonth	Tipo: Entero (1-12)
	Mes del evento.
uDay	Tipo: Entero (1-31)
	Día del evento.
uHour	Tipo: Entero (0-23)
	Hora del evento.
uMinute	Tipo: Entero (0-59)
	Minuto del evento.
uSecond	Tipo: Entero (0-59)
	Segundo del evento.

Otros temas asociados

Las siguientes opciones se utilizan con VirusScan para Windows 95 y Windows 98, no con VirusScan para DOS. Estas opciones pueden utilizarse como parámetros de la línea de comandos, en los accesos directos e iconos, para controlar el estado de VirusScan cuando inicia su ejecución:

- **NoSplash:** Elimina la pantalla de presentación de VirusScan
- **/AutoScan:** Comienza automáticamente la exploración

 Otros temas asociados

Un virus de ordenador es un programa que se reproduce, se combina con otros programas y realiza operaciones no solicitadas o deseadas, cuando no dañinas, al ejecutarlo. Los virus pertenecen a dos categorías principales , virus de "arranque" y virus de "archivo".

Los virus de arranque se alojan en el sector de arranque del disco o disquete infectado. Estos virus se ejecutan al arrancar el equipo. Una vez que se copian en la memoria del equipo, pueden extenderse a otros discos o equipos de la red, dejando cada vez una copia del virus que a su vez pueden repetir el ciclo.

Los virus de archivo sólo se activan cuando se ejecuta el programa que los contiene. Normalmente, estos virus infectan los archivos con extensiones .EXE, .COM o .DLL y otros archivos ejecutables como los archivos de datos de Microsoft Word o Excel y los archivos de plantillas. Una vez que se ejecuta, el virus de archivo se carga también en la memoria del equipo y se copia e infecta otros programas ejecutables.

La siguiente lista describe algunas de las características de los virus comunes. Haga clic en cualquiera de estos elementos para conocer más detalles.

{button ,PI(`vscan4.hlp',`Boot_Virus')} Virus de arranque
{button ,PI(`vscan4.hlp',`File_virus')} Virus de archivo
{button ,PI(`vscan4.hlp',`Stealth_virus')} Virus de "ocultación"
{button ,PI(`vscan4.hlp',`Multi_partite_virus')} Virus "multipartito"
{button ,PI(`vscan4.hlp',`Mutating_virus')} Virus mutante
{button ,PI(`vscan4.hlp',`Encrypted_virus')} Virus encriptado
{button ,PI(`vscan4.hlp',`Polymorphic_virus')} Virus polimórfico
{button ,PI(`vscan4.hlp',`Macro_Virus')} Virus de macro

 Otros temas asociados

Conforme ha ido creciendo la popularidad de Internet en los últimos años, el diseño de los sitios web se ha ido haciendo cada vez más sofisticado. Muchos sitios incluyen en la actualidad elementos interactivos, como pueden ser formularios, sistemas de búsqueda, animaciones y otras muchas características multimedia que facilitan y hacen más interesante la exploración del web. Gran parte de la tecnología que posibilita esas nuevas características reside en pequeños programas, fácilmente descargables, que en combinación con el software del explorador permiten el intercambio de información, la presentación de archivos multimedia, las consultas en bases de datos y la realización de otras muchas tareas. Java y ActiveX son las herramientas que los programadores utilizan para escribir este tipo de programas.

Los programadores utilizan el lenguaje de programación Java de Sun Microsystems para escribir pequeñas aplicaciones de uso especializado o subprogramas (applets) que se ejecutan en una máquina virtual Java que está incluida en el software del explorador, ya sea directamente o como un módulo complementario. Una clase de Java es un módulo de software ya escrito (de uso genérico) que los programadores pueden modificar para adaptarlo a su uso específico.

Los programadores también usan la tecnología ActiveX de Microsoft con fines similares. ActiveX se diferencia de Java principalmente en que Java se ejecuta en una máquina virtual creada específicamente para interpretar los subprogramas Java, mientras que ActiveX sirve como un sofisticado puente software entre programas existentes o entre otros programas y el propio Windows. Un control ActiveX es un módulo software que enlaza programas y les permite compartir datos sin que ninguno de los dos tenga que saber nada acerca de la forma en que el otro opera.

Las clases de Java y los controles de ActiveX se conocen colectivamente con el nombre de ‘‘objetos’’.

» Otros temas asociados

No hace mucho tiempo aún era posible mantener un equipo libre de infecciones víricas sin dedicar mucho esfuerzo ni planificación, ya que en la práctica eran pocas las ocasiones en que entraban en contacto con posible fuentes de contagio. Sin embargo, en la actualidad la mayor parte de los usuarios de ordenadores intercambian mensajes entre sí, comparten datos y se transfieren archivos constantemente, ya sea a través de un módem, por medio de disquetes o a través de redes y de Internet. En este mismo período de tiempo, se han llegado a identificar millares de virus que ahora pueden propagarse con mayor rapidez y facilidad que nunca.

En este entorno, ya no es un lujo adoptar las medidas necesarias para protegerse de una infección, sino que ha llegado a ser una necesidad. Piense en el valor que tienen los datos que guarda su equipo. Probablemente fueran necesarias considerables inversiones en tiempo y dinero para reemplazar esos datos si llegaran a ser dañados o quedaran inutilizados como consecuencia de una infección con virus, puede que incluso algunos de ellos sean irremplazables. Pero,. tanto si sus datos son importantes como si no, la falta de cuidado en la protección anti-virus puede hacer que su equipo se convierta involuntariamente en la guarida de un virus que puede propagarse y afectar a datos de los equipos que utilizan sus compañeros de trabajo y amigos.

La realización periódica de exploraciones anti-virus con VirusScan para Windows 95 y Windows 98, junto con otras soluciones anti-virus de Network Associates, reducen notablemente la vulnerabilidad de su equipo frente a las infecciones y evitan pérdidas innecesarias de tiempo, dinero y datos.

Otros temas asociados

Tanto ActiveX como Java incluyen medidas de protección diseñadas para impedir que su equipo pueda resultar dañado. Sin embargo, algunos programadores mal intencionados han desarrollado objetos que utilizan a Java o ActiveX para leer datos del disco duro y transferirlos a los sitios web que visita; con estos datos es posible crear y enviar mensajes de correo electrónico groseros en su nombre, dañar o destruir sus datos o causar otros daños al sistema.

Objetos peligrosos como los descritos pueden permanecer ocultos en sitios web hasta que los visite y descargue en su sistema, normalmente sin llegar nunca a sospechar que existen. La mayor parte de los exploradores incluyen una opción que impide bloquear conjuntamente los controles de ActiveX o los subprogramas de Java o activar características de seguridad que permiten autentificar los objetos antes de descargarlos en el sistema. Sin embargo, estas medidas de seguridad pueden privarle de las ventajas interactivas que ofrecen los sitios web que visite, ya que se bloquearán indiscriminadamente todos los objetos, sean o no peligrosos.

VirusScan para Windows 95 y Windows 98 permite emplear un método más razonable. Utiliza una base de datos actualizada de objetos que se sabe que causan daños para filtrar los controles de ActiveX y las clases de Java que va encontrando al explorar el web. Los objetos posiblemente peligrosos se quedan donde están, sin poder acceder a su sistema, mientras que los restantes objetos pueden funcionar normalmente.

Otros temas asociados

VirusScan para Windows 95 y Windows 98 cuenta con una pantalla de presentación que proporciona acceso a los tres componentes principales del programa: VirusScan, VShield y Planificador, así como a sus tres herramientas: Enviar a McAfee, Disco de emergencia e Info acerca de virus. A continuación se describen las funciones de cada uno de estos elementos, de forma general, incluyendo vínculos con temas donde se describen algunos aspectos en mayor detalle. Los usuarios normales no tienen necesidad de utilizar directamente los archivos ejecutables (.exe) que ejecutan o controlan la configuración de cada uno de los componentes. La siguiente información se proporciona para aclarar conceptos y como fuente de consulta.

Componente	Función	Acción
Programa de inicio de la Consola VirusScan (VScan40.exe)	Iniciar componentes (programas y herramientas).	Proporciona el acceso a los otros componentes (programas): § Abre VirusScan, VShield, Planificador y Caja de herramientas. § Presenta información útil acerca del estado y configuración de los elementos de los programas.
VirusScan (scan32.exe)	Exploraciones requeridas de archivos y discos. Para más información sobre exploración de correo electrónico requerida, vea Realizar una exploración de correo electrónico requerida .	Realiza una exploración cuando desee: § de cualquier conjunto de archivos en una unidad de disco local o de red. § de los registros de arranque, sectores de arranque y en busca de virus en los archivos del sistema (automáticamente cada vez que se enciende o reinicia el equipo. {button ,JI(`vscan4.HLP>First',`The_Virus_Scan_User_Interface')} Haga clic para ver la interfaz de **Virus Scan**
VShield (vsconfig.exe)	Exploraciones automáticas de acceso	Automáticamente explora cuando: § se ejecuta, crea o cambia de nombre un archivo en una unidad de disco local o de red. § se entra en disquetes o se apaga el sistema con un disquete insertado en la unidad de disquete. § se recibe un mensaje de correo electrónico con un archivo adjunto (vea Realizar una exploración de correo electrónico requerida para tener más información acerca de las exploraciones de correo electrónico requeridas). § se descarga un archivo de Internet § se visitan páginas web que incluyen objetos de Java o ActiveX. {button ,JI(`vscan4.HLP>First',`The_Vshield_User_Interface')} Haga clic para ver la interfaz de **VShield**
VirusScan Planificador (avconsol.exe)	Exploraciones planificadas	Explora automáticamente las unidades de disco locales o de red, siguiendo la planificación que se haya definido. {button ,JI(`vscan4.HLP>First',`The_Scheduler_User_Interface')} Haga clic para ver la interfaz del **Planificador**

Enviar a McAfee (SendVir.exe)	Enviar virus nuevos o no identificados para su estudio.	Si ha encontrado algo que sospecha puede tratarse de un virus nuevo o no identificado, debe enviar el archivo infectado al equipo de emergencias de McAfee Labs (McAfee Labs Anti-Virus Emergency Response Team) para su estudio
Disco de emergencia (edisk.exe)	Crear un disco de emergencia	Crea un disco que permite explorar el sistema e identificar los virus que se encuentren en memoria.
Info acerca de virus (Virlist32.exe**)**	Ver la lista de virus definida en los archivos .DAT instalados actualmente en el equipo.	Presenta una lista con todos los virus definidos en los archivos .DAT instalados actualmente en el equipo.

Otras funciones importantes permiten:

- utilizar la tecnología SecureCast para facilitar la actualización de los archivos de definición de virus cuando se identifiquen virus nuevos, así como la mejora del sistema de identificación de virus cuando se realicen cambios en el software de VirusScan.
- proteger mediante contraseña los parámetros de configuración de los programas.
- detectar todos los tipos de virus conocidos, incluyendo los virus de arranque , archivo , mutantes , de macros , de ocultación y encriptados.
- realizar una Exploración con el Analizador de macros para evaluar la posibilidad de que alguna macro de Microsoft Office sea en realidad un virus.
- responder automáticamente ante la detección de un virus. Esta respuesta puede consistir en alertar al usuario, limpiar el virus y borrar o aislar el archivo infectado.
- explorar archivos comprimidos.
- informar acerca de las actividades de detección y respuesta frente a virus.
- notificar a otras personas acerca de la detección de virus, incluyendo los compañeros de trabajo, el administrador de la red y los destinatarios de correo electrónico.
- impedir el acceso a determinados sitios web.
- VirusScan para Windows 95 y Windows 98 es el resultado de combinar dos programas de detección de virus de McAfee certificados por ICSA (antes NCSA). Así es posible asegurar la detección del 100% de los virus que se encuentren. Visite el sitio web de ICSA, www.ncsa.com, para conocer el estado de certificación o haga clic aquí .
- VirusScan para Windows 95 y Windows 98 emplea las tecnologías Code Trace™, Code Poly™ y Code Matrix™ de Network Associates para alcanzar la máxima precisión en la identificación de los virus.

Exploración: asociada a accesos, requerida o planificada

Fundada en 1986, Network Associates, Inc. es el principal proveedor de herramientas informáticas para entornos DOS, OS/2, UNIX y Windows. Más de 16.000 empresas utilizan nuestros productos anti-virus en todo el mundo. Nuestros otros productos permiten proporcionar seguridad a sus datos, actualizar automáticamente las versiones e inspeccionar y editar los sistemas. Network Associates es además una empresa pionera y uno de los principales proveedores de software distribuido electrónicamente. Todos los productos de Network Associates pueden adquirirse en nuestros distribuidores o descargarse a través de BBS y servicios en línea de todo el mundo.

Network Associates no cesa en su esfuerzo para desarrollar los mejores productos de utilidad y anti-virus a nivel mundial. Nuestros productos tienen además el respaldo del mejor servicio de soporte técnico. El soporte al producto esta garantizado por un equipo de investigadores, programadores y personal de soporte que se dedican exclusivamente a la tarea. Este servicio de soporte los proporciona directamente Network Associates o alguno de sus agentes autorizados en más de 50 países.

 Otros temas asociados

Para hacer un pedido de productos de Network Associates o solicitar información, puede ponerse en contacto con nuestro departamento de Asistencia al cliente en el teléfono (408) 988-3832 o en la siguiente dirección postal:

Network Associates, Inc.
3695 Freedom Circle
Santa Clara, CA 95054
U.S.A.

 Otros temas asociados

Si desea conocer más detalles acerca de las posibilidades de formación en las instalaciones del usuario que ofrece Network Associates para cualquiera de sus productos, llame al teléfono (800) 338-8754.

 Otros temas asociados

Para elegir un explorador de web a utilizar cuando se conecte al sitio web de Network Associates desde el sistema de ayuda de VirusScan, haga clic aquí 

- **Vea la nota**

  Si tiene acceso a Internet, pero no dispone de ninguno de los exploradores compatibles, puede descargarlos de uno de estos sitios:

  Sitio web de Netscape: http://www.netscape.com

  Sitio web de Microsoft: http://www.microsoft.com

- **Vea la nota**

Network Associates tiene fama por su interés en la atención al cliente y ha seguido esa tradición haciendo del sitio de Network Associates en el WWW un sistema muy útil para contestar a los problemas de sus clientes relacionados con el soporte técnico. Network Associates le anima a visitar ese sitio donde encontrará respuestas a las preguntas más frecuentes, podrá actualizar su software de Network Associates y tendrá acceso a las últimas noticias e informaciones. Haga clic en la dirección del sitio web que aparece debajo para conectarse directamente al sitio web de Network Associates. Si desea especificar el explorador que desea utilizar o quiere saber cómo puede obtener software para la exploración del web, haga clic aquí.

World Wide Web	**http://www.nai.com** Haga clic aquí para conectarse con el sitio web de Network Associates.

Si no encuentra la respuesta que necesita o no tiene acceso al web, utilice uno de los servicios automatizados de Network Associates:

Sistema de respuesta automatizada de voz y fax	(408) 988-3034
Correo electrónico	support@nai.com
Conexión al BBS de Network Associates	(408) 988-4004 de 1.200 bps a 28.800 bps 8 bits, sin paridad, 1 bit de parada 24 horas, 365 días al año
CompuServe	GO NAI
America Online	Password NAI

Si no encuentra en nuestros servicios automatizados la respuesta que necesita, póngase en contacto con Network Associates llamando a uno de los siguientes números, de lunes a viernes entre 6:00 a.m. y 6:00 p.m. (hora del Pacífico).

Para clientes con licencias de empresa:

Teléfono	(408) 988-3832
Fax	(408) 970-9727

Para clientes con licencias comerciales:

Teléfono	(972) 278-6100
Fax	(408) 970-9727

Para poderle responder rápida y eficientemente, el personal de soporte técnico de Network Associates necesita conocer algunos datos acerca de su equipo y del software en él instalado. Por favor, tenga a mano la siguiente información cuando realice la llamada:

- Nombre del producto y número de versión
- Marca y modelo del ordenador
- Otro hardware y periféricos conectados a su equipo
- Tipo del sistema operativo y número de versión
- Tipo de red y número de versión del software
- Contenido de los archivos AUTOEXEC.BAT y CONFIG.SYS y de la secuencia de comandos LOGIN de su sistema
- Pasos concretos que permiten reproducir el problema (si se conocen)
- Contenido de los archivos AUTOEXEC.BAT y CONFIG.SYS y de la secuencia de comandos LOGIN de su sistema

Otros temas asociados

Cada mes se descubren 200 virus nuevos, entre los que se incluyen peligrosos controles de ActiveX y clases de Java. A menudo, estos nuevos virus y objetos peligrosos no se pueden detectar con los archivos de datos antiguos. Los investigadores en virus de Network Associates trabajan constantemente para actualizar esos archivos de datos, incluyendo en ellos las definiciones más actualizadas de los virus. Cada cuatro o seis semanas se generan nuevos archivos de datos, archivos .DAT. Periódicamente el programa le avisará que ha llegado el momento de actualizar sus archivos de datos. Para asegurar la máxima protección, debería actualizar sus archivos .DAT de VirusScan de forma regular.

Vea la nota

Al adquirir VirusScan para Windows 95 y Windows 98 tiene derecho a actualizar gratuitamente sus archivos de datos mientras utilice esta versión de VirusScan. Sin embargo, no es posible actualizar las copias de evaluación del programa VirusScan. Tenga en cuenta además que Network Associates no puede garantizar que las futuras versiones de los archivos de datos sigan siendo compatibles con las versiones antiguas de sus productos.

Vea la nota

Para actualizar regularmente y con comodidad sus archivos, utilice uno de los siguientes métodos:

- **SecureCast.** Instale y utilice el servicio de actualización automático de Network Associates para aprovechar la más moderna tecnología de "descarga" que actualizará sus archivos de datos de forma automática e invisible. Si desea conocer más detalles acerca de esta opción, haga clic aquí.
- **Actualización electrónica (pulsando un botón) de VirusScan.** Haga clic en **Actualizar**, cuando aparezca el cuadro de definiciones antiguas de virus de VirusScan, para conectarse directamente a uno de los sitios FTP de Network Associates. Si desea conocer más detalles acerca de esta opción, haga clic aquí.
- **Servicios electrónicos de Network Associates.** Conéctese a alguno de los servicios electrónicos de Network Associates para actualizar los archivos de definición de virus. Si desea conocer más detalles acerca de esta opción, haga clic aquí.
- **Principales servicios electrónicos.** Conéctese a America Online o CompuServe, para actualizar sus archivos de definición de virus. Si desea conocer más detalles acerca de esta opción, haga clic aquí.

Otros temas asociados

La tecnología SecureCast de Network Associates ofrece varias opciones para mantener actualizado su programa VirusScan, cada una de esas opciones requiere un distinto grado de intervención del usuario. Una opción utiliza la tecnología BackWeb para actualizar automática y regularmente los archivos de datos cuando existe conexión con Internet. Si la conexión no dura el tiempo suficiente como para realizar la descarga completa, el software dividirá la tarea en porciones más pequeñas y le informará cuando haya logrado descargar un paquete de actualización completo .

Para utilizar SecureCast, debe instalar el software del cliente mediante el CD-ROM que contiene VirusScan o descargarlo del sitio web de Network Associates **http://www.nai.com**.

El sitio web de Network Associates incluye instrucciones para la descarga e instalación del software SecureCast. Por favor, viste el sitio si desea conocer más detalles.

VirusScan le recuerda periódicamente, al arrancar el equipo, que debe actualizar sus archivos de definición de virus. Puede descargar automáticamente nuevos archivos de definición de virus mediante el siguiente procedimiento:

 **Vea la nota**

1. Haga clic en **Actualizar**, en el cuadro de diálogo **Definiciones antiguas de virus**, para conectarse automáticamente al directorio que contiene los archivos de datos actualizados.
2. Aparecerá entonces el diálogo **Actualizar archivos**, elija en él el sitio del que desea descargar los nuevos archivos de definición. Seleccione el sitio más próximo a su localidad para reducir el tiempo necesario para la descarga.
3. Haga clic en **Aceptar**. VirusScan descargará entonces los nuevos archivos.

Para preparar los nuevos archivos de forma que los pueda utilizar VirusScan, realice las siguientes operaciones:

1. Descargue el fichero guardándolo en un directorio nuevo de su equipo.
2. El archivo está comprimido. Descomprímalo con cualquier software de descompresión compatible con PKUNZIP. Si no tienen ningún programa de descompresión, puede descargar PKUNZIP (un programa de uso compartido) desde cualquiera de los servicios electrónicos de Network Associates.
3. Localice las carpetas de su disco duro que contienen los archivos de VirusScan. Si ha seguido las recomendaciones del procedimiento de instalación, VirusScan se instala en: C:\Archivos de programa\Network Associates\McAfee VirusScan.
4. Copie los nuevos archivos en el directorio o directorios que contienen actualmente los archivos de VirusScan. Cuando Windows pregunte si se desean reemplazar los archivos antiguos por los nuevos archivos de datos, haga clic en **Si**.
5. Reinicie su equipo para que los cambios tengan efecto inmediatamente.

 **Vea la nota**

Para actualizar los archivos de datos de VirusScan descargando nuevos archivos del sitio web de Network Associates o de su BBS, realice las siguientes operaciones:

1 Descargue el archivo de datos correcto (por ejemplo, DAT-3102.ZIP) de uno de los servicios electrónicos de Network Associates.

   En la mayoría de esos servicios, encontrará los archivos de actualización en una sección especial dedicada a anti-virus. El sitio web de Network Associates incluye además las instrucciones necesarias para elegir los archivos de datos correctos. Haga clic aquí **http://www.nai.com** para conectarse a él.

» **Vea la nota**

2 Descargue el archivo en un nuevo directorio.

   El archivo está comprimido. Descomprímalo con cualquier software de descompresión compatible con PKUNZIP. Si no tienen ningún programa de descompresión, puede descargar PKUNZIP (un programa de uso compartido) desde cualquiera de los servicios electrónicos de Network Associates.

3 Localice las carpetas de su disco duro que contienen los archivos de VirusScan. Si ha seguido las recomendaciones del procedimiento de instalación, VirusScan se instala en: C:\Archivos de programa\Network Associates\McAfee VirusScan.

4 Copie los nuevos archivos en el directorio o directorios que contienen actualmente los archivos de VirusScan. Cuando Windows pregunte si se desean reemplazar los archivos antiguos por los nuevos archivos de datos, haga clic en **Si**.

5 Reinicie su equipo para que los cambios tengan efecto inmediatamente.

» **Vea la nota**

» Otros temas asociados

Network Associates está presente en los servicios America Online y CompuServe. Cada uno de estos servicios incluye un área de descarga de software en la que se encuentran los archivos .DAT actualizados, así como otros programas de Network Associates. Las contraseñas necesarias para acceder a Network Associates en estos servicios aparecen en la siguiente tabla:

CompuServe	GO NAI
America Online	Password NAI

Una vez que haya encontrado el área de descarga de software de Network Associates, realice las siguientes operaciones para actualizar los archivos de datos de VirusScan:

1 Descargue el archivo de datos correcto (por ejemplo, DAT-3007.ZIP).

En la mayoría de los servicios, los archivos de actualización se encuentran en una sección especial dedicada a anti-virus. En el mismo área se incluyen además las instrucciones necesarias para elegir los archivos de datos correctos.

Vea la nota

2 Descargue el archivo en un nuevo directorio.

El archivo está comprimido. Descomprímalo con cualquier software de descompresión compatible con PKUNZIP. Si no tienen ningún programa de descompresión, puede descargar PKUNZIP (un programa de uso compartido) desde cualquiera de los servicios electrónicos de Network Associates.

3 Localice las carpetas de su disco duro que contienen los archivos de VirusScan. Si ha seguido las recomendaciones del procedimiento de instalación, VirusScan se instala en: C:\Archivos de programa\Network Associates\McAfee VirusScan.

4 Copie los nuevos archivos en el directorio o directorios que contienen actualmente los archivos de VirusScan. Cuando Windows pregunte si se desean reemplazar los archivos antiguos por los nuevos archivos de datos, haga clic en **Sí**.

5 Reinicie su equipo para que los cambios tengan efecto inmediatamente.

Vea la nota

Otros temas asociados

Network Associates se ha comprometido a proporcionar herramientas eficaces y actualizadas que permitan proteger su sistema. Para facilitar nuestra tarea le invitamos a que nos informe de cualquier nuevo virus, clase de Java, control de ActiveX o sitio web peligroso que VirusScan no detecte actualmente. Tenga en cuenta que Network Associates se reserva el derecho a utilizar la información que nos proporcione de la forma que estime adecuada, sin que al hacerlo incurra en ninguna obligación.

Si encuentra algo que sospecha puede tratarse de un virus nuevo o no identificado, envíe el archivo infectado al equipo de investigadores de McAfee Labs (Anti-Virus Emergency Response Team) para su estudio, utilice para ello el asistente **Enviar a McAfee**. Tiene la opción de eliminar sus datos personales del archivo antes de enviarlo. Vea el apartado dedicado a Envío de información acerca de los virus al equipo de respuesta de emergencia anti-virus.

Para informar acerca de nuevos virus, controles de ActiveX y clases de Java dañinas, o sitios web peligrosos, utilice las siguientes direcciones de correo electrónico:

U.S.A	virus_research@nai.com
Europa	virus_research_europe@nai.com
Japón	avert-jp@nai.com
Asia-Pacífico	avert-apac@nai.com

La Biblioteca de documentación técnica de Network Associates contiene toda la información disponible actualmente acerca del virus. Está ubicada en el sitio web http://www.nai.com/vinfo/ y se tiene acceso directo a ella desde la caja de herramientas de **Consola VirusScan**. Incluye los siguientes temas:

Información acerca de virus

- Nuevos virus
- 10 virus más comunes
- Lista de virus ordenada por nombre
- Lista de virus ordenada por tipo
- Lista de virus ordenada por fecha de activación

Información acerca de virus inocuos

- Virus inocuos

Investigación acerca de virus

- Departamento de investigación acerca de virus de McAfee'

Documentación técnica

- Terminología anti-virus

 Documentos técnicos

NetShield es una de las soluciones anti-virus para servidor que ofrece Network Associates. Permite a un administrador de red establecer un sistema de centralización de alertas, un procedimiento de cliente-servidor para la detección y solución de infecciones víricas de forma regular, coherente y a través de toda la red. NetShield recoge los mensajes de alerta de los programas cliente, como puede ser VirusScan, en un archivo de texto (CENTALRT.TXT) y los pone a disposición del administrador de la red. Para indicar a VirusScan a dónde debe dirigir sus mensajes de alerta de red, es preciso especificar correctamente la ruta de la carpeta que contiene el archivo CENTALRT.TXT. Si desea más información, consulte la Guía de usuario de NetShield.

 Otros temas asociados

El sistema de centralización de alertas es una solución de Network Associates para la notificación de eventos asociados con virus en toda una empresa. Una vez configurado, las estaciones de trabajo que utilizan VirusScan envían información acerca de los virus detectados en los servidores que ejecutan NetShield. Esto ayuda a los administradores de la red a localizar el origen de las infecciones por virus, evitando así su propagación.

1 Pregunte al administrador del sistema cuál es el nombre del servidor que ejecuta NetShield y cuál es la carpeta de centralización de alertas.

2 Asegúrese de que dispone de los privilegios necesarios para poder escribir en esa carpeta.

3 Busque la página de propiedades **Alerta** de VirusScan o de cualquier otro módulo de VShield que desee que genere mensajes de alerta de red.

4 Seleccione la opción **Enviar alerta de red** en cada página de propiedades.

5 Haga clic en **Examinar** para buscar la carpeta de centralización de alertas del servidor que le ha indicado el administrador del sistema.

6 Designe un archivo de nombre **CENTALRT.TXT** como destino para los mensajes de aviso de alerta.

 Haga clic para ver más información acerca de las páginas configurables de propiedades Alerta .

La exploración con el **Analizador de macros** evalúa la posibilidad de que una macro de una aplicación de Microsoft Office sea en realidad un virus. VirusScan para Windows 95 y Windows 98 trata las macros como si fueran virus cuando superan el nivel de detección que se fije.

Para configurar el **Analizador de macros:**

1 Haga clic en **Analizador de macros.** Aparecerá entonces el cuadro de diálogo **Opciones de exploración con Analizador de macros**.

2 Haga clic para seleccionar la casilla **Activar exploración con Analizador de macros**.

3 Utilice la pestaña deslizante para ajustar el nivel de sensibilidad que definirá una macro como virus.

Nota: Al seleccionar el nivel más bajo, se desactiva el **Analizador de macros**.

4 Seleccione la casilla **Eliminar todas las macros al limpiar documentos infectados** para eliminar todas las macros del documento, tanto si pueden tratarse de un virus como si no.

Nota: Al seleccionar esta casilla conjuntamente con el máximo nivel de sensibilidad, todas las macros de Microsoft Office se considerarán virus y se eliminarán durante la limpieza.

5 Haga clic en **Aceptar**.

Nota: Esta característica puede activarse en tres momentos:

{button ,JI(`vscan4.HLP',`Configuring_System_Scan_Detection_Properties')} cuando se configuran las propiedades de detección del Explorador de sistema para exploración asociada a accesos.

{button ,JI(`vscan4.HLP',`Perform_an_Advanced_On_Demand_Scan')} cuando se configuran las propiedades de detección para una exploración avanzada requerida.

{button ,JI(`vscan4.HLP',`Configuring_VirusScan_Detection_Properties')} cuando se configura la página de propiedades Programa para una tarea de exploración planificada.

Los usuarios de Lotus cc:Mail pueden buscar los nombres de las personas que desean incluir en la lista de distribución de correo electrónico para notificaciones de VShield.

Para agregar una persona destinataria a la lista:

1. Escriba el nombre del **destinatario** en el cuadro **Nombre**.
2. Haga clic en **Agregar**. El nombre se agregará entonces a la lista.
3. Haga clic en **Cerrar**.

Para borrar un destinatario de la lista:

1. Seleccione el nombre del destinatario en el cuadro de lista.
2. Haga clic en **Borrar**. El nombre desaparecerá entonces de la lista.
3. Haga clic en **Cerrar**.

Para seleccionar un directorio o una lista de distribución en particular:

1. Haga clic en  del cuadro **Buscar en**.
2. Seleccione un directorio o lista de distribución en la lista desplegable.

Proporcionar a VirusScan la ruta de cc:Mail.

1 Escriba su nombre.
2 Escriba su contraseña de cc:Mail.
3 Escriba la ruta del archivo ejecutable de cc:Mail.

Agregar una extensión de nombre o tipo de archivo a explorar.

1 Escriba los tres caracteres de la extensión de nombre de archivo que desea incluir en la exploración. No incluya el punto que normalmente precede a la extensión.
2 Haga clic en **Aceptar**.

Especificar una dirección IP prohibida de Internet. Si desea ver más detalles acerca de este tema, vea el apartado de Bloqueo de acceso de Internet a una dirección IP concreta

1 Escriba la dirección en el cuadro **Dirección IP**.
2 Escriba la subred en el cuadro **Máscara de subred**.
3 Haga clic en **Aceptar**.

Especificar un URL prohibido. Si desea ver más detalles acerca de este tema, vea el apartado de Bloqueo de acceso de Internet a un URL concreto.

1 Escriba la dirección URL en el cuadro **Nombre de URL**.
2 Haga clic en **Aceptar**.

Elija los elementos que desea incluir en una exploración del sistema.

1. Si desea explorar varias unidades conectadas a su equipo, haga clic en **Seleccionar elemento para explorar.**
   Si desea explorar una ubicación determinada, haga clic en **Seleccionar unidad o carpeta para explorar**.
2. Si elige la opción **Seleccionar elemento a explorar**, haga clic en  y seleccione el ámbito de la exploración. Puede incluir todas las unidades conectadas a su equipo, todas las unidades desmontables, todas las unidades fijas o todas las unidades de red.
   O
3. Si elige la opción **Seleccionar unidad o carpeta a explorar**, haga clic en **Examinar** y seleccione la unidad o carpeta que desea incluir en la exploración. A continuación, seleccione la casilla **Incluir subcarpetas** si desea incluir las subcarpetas en la exploración.
4. Cuando haya terminado, haga clic en **Aceptar** para guardar los cambios efectuados y cerrar el cuadro de diálogo.

- Comienza inmediatamente la exploración usando las selecciones efectuadas en las pestañas **Dónde y qué**, **Acciones** e **Informes**.

- Detiene inmediatamente la exploración.

- Recupera los valores predeterminados de todas las opciones de las pestañas **Dónde y qué**, **Acciones** e **Informes**.

Selecciona la unidad de disco, carpeta o tipos de archivo para explorar.

- Selecciona la respuesta de VirusScan cuando detecta un virus.

- Selecciona el método de notificación al usuario de que VirusScan ha detectado un virus y selecciona un archivo para guardar los resultados de las exploraciones.

La función de **exploración asociada a accesos** se activa automáticamente cuando se produce un evento determinado, como puede ser la apertura o ejecución de un archivo. Las exploraciones asociadas a accesos se controlan mediante el componente **VShield**. Se pueden configurar para que se ejecuten automáticamente cuando:

- ejecute, cree o cambio de nombre un archivo en una unidad de disco local o de red.
- entre en un disquete o cierre el sistema con un disquete insertado en la unidad de disquetes.
- reciba un mensaje de correo electrónico que tenga un archivo adjunto.
- descargue un archivo de Internet
- visite páginas web que incluyan objetos de Java o ActiveX.

{button ,JI(`vscan4.HLP>First',`The_VShield_User_Interface')} Haga clic para ver la interfaz de **VShield**

La función de **exploración requerida** se activa cuando el usuario utiliza el comando de inicio de exploración. Puede ejecutar **exploraciones requeridas** en cualquier momento que desee.

- Las exploraciones de carpetas o archivos de una unidad de disco local o de red se controlan mediante el componente **VirusScan** y se basan en sus parámetros de configuración Clásica o Avanzada. Si desea tener más información, vea el apartado Exploraciones clásicas requeridas respecto a exploraciones avanzadas requeridas
- Las exploraciones de correo electrónico se controlan mediante el componente **Exploración de correo electrónico**.

{button ,JI(`vscan4.HLP>First',`The_Virus_Scan_User_Interface')} Haga clic para ver la interfaz de **Virus Scan**

{button ,JI(`vscan4.HLP>First',`The_On_Demand_E_mail_Scan_Configuration_Screen')} Haga clic para ver la interfaz de la página de propiedades **Exploración de correo electrónico requerida**.

Las **exploraciones planificadas** tienen lugar en el momento que el usuario define previamente y se controlan mediante el componente **Planificador de VirusScan**. Las tareas planificadas sólo se ejecutan si el Planificador está abierto a la hora definida para la exploración.

- Se puede planificar la exploración automática de carpetas o archivos en cualquier unidad de disco local o de red.
- Las tareas de exploración definidas por el usuario pueden especificar la inclusión de determinadas unidades de disco, carpetas y archivos.

{button ,JI(`vscan4.HLP>First',`The_Scheduler_User_Interface')} Haga clic para ver la interfaz del **Planificador**

Visión general de las funciones

Si desea explorar unidades de disco locales o de red durante los momentos en que aparece el protector de pantalla, es necesario realizar una instalación Personalizada de VirusScan para Windows 95 y Windows 98 e incluir el componente **ScreenScan** en la instalación.

1 Haga clic con el botón derecho en su escritorio y seleccione la opción Propiedades. Si está instalado ScreenScan, seleccione la página de propiedades denominada **McAfee ScreenScan**. Si no aparece esta página de propiedades, ScreenScan no está instalado.

2 Seleccione la casilla denominada **Activar exploración en modo de protector de pantalla**.

3 Como opción predeterminada, ScreenScan está configurado para explorar todas las unidades fijas de disco. Puede modificar la lista de elementos a explorar, así:

 Para agregar elementos a la lista, haga clic en **Agregar** (aparece en la parte inferior de la pantalla). Aparecerá entonces un cuadro de diálogo en el que puede especificar los elementos adicionales que desea explorar.

 Para editar los elementos que aparecen en la lista, haga clic en **Editar**.

 Para eliminar un elemento de la lista, selecciónelo y haga clic en **Eliminar**.

4 Seleccione la casilla **Incluir subcarpetas** si desea explorar las subcarpetas, junto con las carpetas de nivel superior.

5 Haga clic en uno de los botones para indicar si se deben explorar todos los archivos. o sólo los archivos de programas.

 Si selecciona la opción **Sólo archivos de programa**, haga clic en **Extensiones** para ver una lista con las extensiones de nombre de archivo que explorará VirusScan. Puede editar esa lista.

6 Seleccione la casilla **Archivos comprimidos** para incluir archivos creados con programas de compresión LHA, LZEXE, PkLite, PkZip o WinZip. Dado que VirusScan descomprime estos tipos de archivo en memoria antes de comprobar si tienen virus, esta opción aumenta el tiempo necesario para realizar una exploración.

7 Haga clic en la casilla denominada **Reanudar exploración desde donde se interrumpió ScreenScan** si desea que ScreenScan continúe la exploración que empezó en un período anterior de aparición del protector de pantalla y que fue interrumpida por un movimiento del ratón o la presión de una tecla.

8 Haga clic en **Avanzada** para definir las propiedades de exploración.

 Utilice la pestaña deslizante para fijar los niveles de prioridad de la exploración en relación con otros programas que puedan estar ejecutándose mientras el protector de pantalla está activo.

 Seleccione **Activar registro de actividades de ScreenScan** si desea conservar un registro de estas actividades de exploración.

 Haga clic en **Examinar** para seleccionar una carpeta en la que guardar el archivo de registro.

 Haga clic en **Aceptar** cuando haya terminado de configurar las opciones avanzadas. Al hacerlo, volverá a la página de propiedades de ScreenScan.

9 Cuando haya terminado:

 Haga clic en **Aplicar** para guardar las opciones de detección que haya elegido sin salir de la página de propiedades **Programa** o

 Haga clic en **Aceptar** para guardar los cambios efectuados en esta u otras páginas de propiedades y cerrar el cuadro de diálogo Propiedades de VirusScan o

 Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar los cambios efectuados.

VirusScan proporciona dos modalidades de exploración requerida : **Clásica** y **Avanzada.**

A continuación se comparan las posibilidades de configuración de cada uno de estos tipos:

Característica	**Clásica**	**Avanzada**
Selección de la ubicación a explorar	Ubicación única	Múltiples ubicaciones
Selección de tipos de archivo a incluir	Sí	Sí
Definición de acciones automáticas para todos los virus que se detecten	Sí	Sí
Posibilidad de que el usuario seleccione una acción en particular para cada uno de los virus que se detecten	No	Sí
Selección del método de aviso de que se ha detectado un virus	Sí	Sí
Creación de un archivo de registro en el que registrar los eventos de las exploraciones	VShield selecciona los eventos	El usuario selecciona los eventos
Visualización del archivo de definición de virus	Sí	Sí
Exclusión de determinadas carpetas de la exploración	No	Sí
Protección mediante contraseña de las opciones de configuración seleccionadas	No	Sí
Acceso al Planificador con el que se puede crear una planificación para las exploraciones	No	Sí

Otros temas asociados

Para configurar y realizar una exploración requerida en una unidad de disco local o de red:

1 Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.
2 Seleccione **Programas → McAfee VirusScan → Consola de McAfee VirusScan**. Aparecerá entonces el programa de inicio de **McAfee**.
3 Seleccione **Explorar.** Aparecerá entonces la pantalla de **McAfee Virus Scan**. Como opción predeterminada, se abre con las páginas de configuración de exploración **Clásica**.

» Para confirmar que se encuentra en la página de Exploración clásica, seleccione el menú **Herramientas**. Si aparece la palabra **Avanzada** en el menú, es que en la actualidad está en la página de exploración **Clásica**.

» Si en el menú aparece la palabra **Clásica**, es que se encuentra en la página de exploración **Avanzada**. Seleccione la opción **Clásica** para configurar una exploración clásica.

Si desea realizar una exploración avanzada, vea el apartado Realización de una exploración avanzada requerida

4 Seleccione la pestaña **Dónde y qué**. Como opción predeterminada, VirusScan asume que desea explorar la unidad **C:**. Si desea explorar una unidad de disco distinta, haga clic en **Examinar** y seleccione una unidad de disco local o de red.
5 A continuación, seleccione la casilla **Incluir subcarpetas** si desea explorar las subcarpetas junto con las carpetas de nivel superior.
6 Haga clic en uno de los botones para indicar si desea explorar todos los archivos o sólo los archivos de programa.

» Si selecciona **Sólo archivos de programa**, haga clic en **Extensiones** para ver una lista con las extensiones de nombre de archivo que VirusScan explorará. Puede editar esa lista.

7 Seleccione la casilla **Archivos comprimidos** para incluir en la exploración los archivos creados con los programas LHA, LZEXE, PkLite, PkZip o WinZip. Dado que VirusScan descomprime este tipo de archivos en memoria antes de comprobar si contienen o no virus, esta opción hace aumentar el tiempo necesario para realizar una exploración.
8 Active la exploración o continúe configurando el programa:

» Haga clic en **Explorar ahora** para iniciar inmediatamente la exploración,

» Haga clic en **Detener** para interrumpir una exploración que ya ha comenzado.

» Haga clic en **Nueva exploración** para reemplazar sus opciones de configuración por las opciones predeterminadas de **VirusScan**.

O

» Seleccione otra pestaña y continúe configurando el programa.

{button ,JI(`vscan4.HLP',`Classic_Scan_Action_Tab')}

{button ,JI(`vscan4.HLP',`Classic_Scan_Report_Tab')}

1 Seleccione la pestaña **Acción** para especificar de qué forma debe actuar VirusScan cuando detecte un virus. Como opción predeterminada, aparece seleccionada la acción **Consultar antes de actuar**.

2 Haga clic en la flecha abajo si desea seleccionar otra acción como respuesta de VirusScan ante la detección de un virus. Las opciones que aparecen en **Acciones posibles** dependen de la respuesta que seleccione:

 Si deja la respuesta predeterminada, **Consultar antes de actuar**, tendrá la oportunidad de seleccionar cualquiera de las opciones cuando se detecte un virus. Si selecciona otra opción en la lista desplegable, esa acción se ejecutará automáticamente cada vez que se detecte un virus.

 Si selecciona la opción **Mover los archivos infectados automáticamente**, tendrá que indicar la ubicación y nombre de la carpeta de destino de esos archivos.

 Si selecciona las opciones **Limpiar los archivos infectados automáticamente**, **Borrar los archivos infectados automáticamente**, o **Continuar exploración**, aparecerá un mensaje que describe la opción elegida.

3 Inicie la exploración o continúe configurando el programa:

 Haga clic en **Explorar ahora** para iniciar inmediatamente la exploración,

 Haga clic en **Detener** para interrumpir una exploración que ya ha comenzado.

 Haga clic en **Nueva exploración** para reemplazar sus opciones de configuración por las opciones predeterminadas de **VirusScan**.

O

 Seleccione otra pestaña para continuar con la configuración.

{button ,JI(`vscan4.HLP',`Classic_Where_and_What_Tab')}

{button ,JI(`vscan4.HLP',`Classic_Scan_Report_Tab')}

1. Seleccione la pestaña **Informe** para especificar de qué forma desea que VirusScan le informe que ha detectado un virus y para crear un archivo de registro en el que queden registradas todas las actividades de exploración.
2. Si ha seleccionado previamente la opción **Consultar antes de actuar** en la pestaña **Acción**, VirusScan necesita saber cómo debe avisar de la detección de un virus: mediante un mensaje que aparece en pantalla, mediante un tono o con ambos. Como opción predeterminada, aparecerá en color gris el mensaje del cuadro de texto.

   » Para cambiar el mensaje, seleccione la casilla **Mostrar mensaje personalizado** y escriba un nuevo mensaje.

   » Para no emitir el tono, borre la marca de la casilla **Emitir señal audible**.
3. Puede hacer cambios en las características del archivo de registro. VirusScan crea un archivo denominado VSCLog.txt, con un tamaño máximo de 100 KB, en el que quedan registradas todas las opciones de informe disponibles que aparecen en la pantalla. La ubicación predeterminada del archivo de registro es C:\Archivos de programa\Network Associates\McAfee Virus Scan\. Si desea cambiar estas opciones predeterminadas, puede:

   » Borrar la marca de la casilla Registrar en archivo, con lo que se interrumpe toda actividad de registro.

   » Escribir un nuevo nombre o ruta de acceso del archivo de texto que se genera. VirusScan sólo generará un archivo de texto sin formato.

   » Haga clic en **Examinar** para seleccionar una ubicación para el archivo.

   » Borrar la marca de la casilla **Limitar tamaño de archivo de registro** para eliminar cualquier límite de tamaño.

   » Cambiar el tamaño máximo del archivo de registro.

   » Borrar la marca de las casillas de cualquiera de los elementos del informe que no esté interesado en que quede registrado.
4. Inicie la exploración o continúe configurando el programa:

   » Haga clic en **Explorar ahora** para iniciar inmediatamente la exploración,

   » Haga clic en **Detener** para interrumpir una exploración que ya ha comenzado.

   » Haga clic en **Nueva exploración** para reemplazar sus opciones de configuración por las opciones predeterminadas de **VirusScan**.

O

   » Seleccione otra pestaña para continuar con la configuración.

{button ,JI(`vscan4.HLP',`Classic_Where_and_What_Tab')}
{button ,JI(`vscan4.HLP',`Classic_Scan_Action_Tab')}

Para configurar y realizar una exploración requerida de una unidad de disco local o de red:

1 Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.

2 Seleccione **Programas → McAfee VirusScan → Consola de McAfee VirusScan**. Aparecerá entonces el programa de inicio de **McAfee**.

3 Seleccione **Explorar.** Aparecerá entonces la pantalla de **McAfee Virus Scan**. Como opción predeterminada, se abre con las páginas de configuración de exploración **Clásica**.

» Para confirmar que se encuentra en la página de Exploración clásica, seleccione el menú **Herramientas**. Si aparece la palabra **Avanzada** en el menú, es que en la actualidad está en la página de exploración **Clásica**.

» Seleccione la opción **Avanzada** para configurar una exploración avanzada.

Si desea realizar una exploración **Clásica**, vea el apartado Realización de una exploración clásica requerida

4 Seleccione la pestaña **Detección**. Como opción predeterminada, VirusScan asumes que desea explorar todas las unidades fijas de disco.

5 Si desea explorar otras ubicaciones adicionales, haga clic en **Agregar**. Aparecerá entonces la pantalla **Agregar elemento a la exploración**.

» **Vea la nota**

6 Seleccione el botón que describe las ubicaciones adicionales que desea explorar.

» Si desea explorar varias unidades de disco conectadas a su equipo, haga clic en la opción **Seleccionar elemento para explorar**. A continuación, haga clic en

» y seleccione el ámbito de la exploración. Puede incluir todas las unidades conectadas a su equipo, todas las unidades desmontables, todas las unidades fijas o todas las unidades de red.

» Si desea explorar una ubicación determinada, haga clic en **Seleccionar unidad o carpeta para explorar**. A continuación, haga clic en **Examinar** y seleccione la unidad de disco o carpeta que desea incluir en la exploración. Después, seleccione la casilla **Incluir subcarpetas** si desea incluir las subcarpetas en la exploración.

7 Cuando haya terminado, haga clic en **Aceptar** para guardar los cambios efectuados y cerrar el cuadro de diálogo.

8 Haga clic en uno de los botones para indicar si se debe explorar todos los archivos o sólo los archivos de programa.

» Si selecciona la opción **Sólo archivos de programa**, haga clic en **Extensiones** para ver la lista de extensiones de nombre de archivo que VirusScan explorará. Puede editar esa lista.

9 Seleccione la casilla **Archivos comprimidos** para incluir en la exploración archivos creados con los programas LHA, LZEXE, PkLite, PkZip o WinZip. Dado que VirusScan descomprime este tipo de archivos en memoria antes de comprobar si tienen virus o no, esta opción puede aumentar el tiempo necesario para realizar una exploración.

10 Haga clic en **Analizador de macros** para incluir en la exploración las macros de Microsoft Office. Si desea más detalles, vea el apartado Exploración con el Analizador de macros.

11 Inicie la exploración o continúe configurando el programa:

» Haga clic en **Explorar ahora** para iniciar inmediatamente la exploración,

» Haga clic en **Detener** para interrumpir una exploración que ya ha comenzado.

» Haga clic en **Nueva exploración** para reemplazar sus opciones de configuración por las opciones predeterminadas de **VirusScan**.

O

» Seleccione otra pestaña para continuar con la configuración.

{button ,JI(`vscan4.HLP',`Advanced_Scan_Action_Tab')} Pestaña Acción
{button ,JI(`vscan4.HLP',`Advanced_Scan_Alert_Tab')} Pestaña Alerta
{button ,JI(`vscan4.HLP',`Advanced_Scan_Report_Tab')} Pestaña Informe
{button ,JI(`vscan4.HLP',`Advanced_Scan_Exclusion_Tab')} Pestaña Exclusión

1 Seleccione la pestaña **Acción** para especificar de qué forma debe actuar VirusScan cuando detecte un virus. Como opción predeterminada, aparece seleccionada la acción **Consultar antes de actuar**.

2 Haga clic en la flecha abajo si desea seleccionar otra acción como respuesta de VirusScan ante la detección de un virus. Las opciones que aparecen en **Acciones posibles** dependen de la respuesta que seleccione:

 Si deja la respuesta predeterminada, **Consultar antes de actuar**, tendrá la oportunidad de seleccionar cualquiera de las opciones cuando se detecte un virus. Si selecciona otra opción en la lista desplegable, esa acción se ejecutará automáticamente cada vez que se detecte un virus.

 Si selecciona la opción **Mover los archivos infectados automáticamente**, tendrá que indicar la ubicación y nombre de la carpeta de destino de esos archivos.

 Si selecciona las opciones **Limpiar los archivos infectados automáticamente**, **Borrar los archivos infectados automáticamente**, o **Continuar exploración**, aparecerá un mensaje que describe la opción elegida.

3 Inicie la exploración o continúe configurando el programa:

 Haga clic en **Explorar ahora** para iniciar inmediatamente la exploración,

 Haga clic en **Detener** para interrumpir una exploración que ya ha comenzado.

 Haga clic en **Nueva exploración** para reemplazar sus opciones de configuración por las opciones predeterminadas de **VirusScan**.

O

 Seleccione otra pestaña para continuar con la configuración.

{button ,JI(`vscan4.HLP',`Advanced_Detection_Tab')} Pestaña Detección

{button ,JI(`vscan4.HLP',`Advanced_Scan_Alert_Tab')} Pestaña Alerta

{button ,JI(`vscan4.HLP',`Advanced_Scan_Report_Tab')} Pestaña Informe

{button ,JI(`vscan4.HLP',`Advanced_Scan_Exclusion_Tab')} Pestaña Exclusión

1 Seleccione la pestaña **Alerta** si desea que VirusScan envíe un mensaje cuando detecte un virus.

2 Seleccione la casilla **Enviar alerta de red** si desea enviar una alerta a un servidor de la red. Al hacerlo, se activa el botón **Examinar** y puede elegir la ubicación de destino de la alerta de red. Una vez seleccionada, la ruta de esa ubicación aparecerá en el cuadro de texto.

3 Seleccione la casilla **DMI** para enviar el aviso a aplicaciones de gestión de red o de gestión de escritorio que cumplen con la especificación DMI (Interfaz de administración de escritorio**)**.

4 Si se ha seleccionado previamente la opción Consultar antes de actuar en la pestaña **Acción**, VirusScan necesita saber de qué forma debe avisar de la detección del virus: mediante un mensaje en pantalla, con un tono o mediante ambos. Como opción predeterminada, el mensaje que aparece en el cuadro de texto tiene color gris.

 Para cambiar el mensaje, seleccione la casilla **Mostrar mensaje personalizado** y escriba un nuevo mensaje.

 Para omitir el tono, borre la marca de la casilla **Emitir señal audible**.

5 Inicie la exploración o continúe configurando el programa:

 Haga clic en **Explorar ahora** para iniciar inmediatamente la exploración,

 Haga clic en **Detener** para interrumpir una exploración que ya ha comenzado.

 Haga clic en **Nueva exploración** para reemplazar sus opciones de configuración por las opciones predeterminadas de **VirusScan**.

O

 Seleccione otra pestaña para continuar con la configuración.

{button ,JI(`vscan4.HLP',`Advanced_Detection_Tab')} Pestaña Detección

{button ,JI(`vscan4.HLP',`Advanced_Scan_Action_Tab')} Pestaña Acción

{button ,JI(`vscan4.HLP',`Advanced_Scan_Report_Tab')} Pestaña Informe

{button ,JI(`vscan4.HLP',`Advanced_Scan_Exclusion_Tab')} Pestaña Exclusión

1. Seleccione la pestaña **Informe** si desea que VirusScan conserve un registro de sus actividades de exploración. Como opción predeterminada, VirusScan crea un archivo de nombre VSCLog.txt, con un tamaño máximo de 100 KB, en el que registra todas las opciones de informe disponibles que aparecen en pantalla. La ubicación predeterminada del archivo de registro es C:\Archivos de programa\Network Associates\McAfee Virus Scan\. Si desea cambiar estas opciones predeterminadas, puede:

   - Borrar la marca de la casilla Registrar en archivo, con lo que se interrumpe toda actividad de registro.
   - Escribir un nuevo nombre o ruta de acceso del archivo de texto que se genera. VirusScan sólo generará un archivo de texto sin formato.
   - Haga clic en **Examinar** para seleccionar una ubicación para el archivo.
   - Borrar la marca de la casilla **Limitar tamaño de archivo de registro** para eliminar cualquier límite de tamaño.
   - Cambiar el tamaño máximo del archivo de registro.
   - Borrar la marca de las casillas de cualquiera de los elementos del informe que no esté interesado en ver registrado.

2. Inicie la exploración o continúe configurando el programa:

   - Haga clic en **Explorar ahora** para iniciar inmediatamente la exploración,
   - Haga clic en **Detener** para interrumpir una exploración que ya ha comenzado.
   - Haga clic en **Nueva exploración** para reemplazar sus opciones de configuración por las opciones predeterminadas de **VirusScan**.

O

   - Seleccione otra pestaña para continuar con la configuración.

{button ,JI(`vscan4.HLP',`Advanced_Detection_Tab')} Pestaña Detección
{button ,JI(`vscan4.HLP',`Advanced_Scan_Action_Tab')} Pestaña Acción
{button ,JI(`vscan4.HLP',`Advanced_Scan_Alert_Tab')} Pestaña Alerta
{button ,JI(`vscan4.HLP',`Advanced_Scan_Exclusion_Tab')} Pestaña Exclusión

1 Seleccione la pestaña **Exclusión** para especificar carpetas que deben quedar excluidas de la exploración en busca de virus. Como opción predeterminada, VirusScan no explora los archivos de la carpeta Papelera de reciclaje.

 Seleccione la opción **Agregar** para especificar una carpeta que deba excluirse. Tiene además la opción de incluir las subcarpetas y especificar si la exclusión es para las exploraciones de archivos o la exploración de sector de arranque.

 Seleccione **Editar…** para modificar las instrucciones relativas a la carpeta seleccionada que ya aparece en la lista de exclusiones.

 Seleccione **Eliminar** para borrar la carpeta seleccionada de la lista.

2 Inicie la exploración o continúe configurando el programa:

 Haga clic en **Explorar ahora** para iniciar inmediatamente la exploración,

 Haga clic en **Detener** para interrumpir una exploración que ya ha comenzado.

 Haga clic en **Nueva exploración** para reemplazar sus opciones de configuración por las opciones predeterminadas de **VirusScan**.

O

 Seleccione otra pestaña para continuar con la configuración.

{button ,JI(`vscan4.HLP',`Advanced_Detection_Tab')} Pestaña Detección

{button ,JI(`vscan4.HLP',`Advanced_Scan_Action_Tab')} Pestaña Acción

{button ,JI(`vscan4.HLP',`Advanced_Scan_Alert_Tab')} Pestaña Alerta

{button ,JI(`vscan4.HLP',`Advanced_Scan_Report_Tab')} Pestaña Informe

Como opción predeterminada, VirusScan explora las unidades locales de discos cada vez que se inicia el equipo. Esa exploración se realiza conforme a la configuración predeterminada de exploración que se incluye en la versión de VirusScan instalada en su equipo.

Además, VirusScan ofrece otras tres configuraciones predeterminadas de exploración. Cada una de ellas se puede planificar y activar en cualquier momento. Además, puede definir y planificar todas las exploraciones adicionales que desee. El

Planificador de VirusScan controla estas características. Para acceder al **Planificador**, haga clic en  en la bandeja del sistema situada en la esquina inferior derecha de la pantalla. Aparecerá entonces el Planificador de VirusScan. Otra opción consiste en hacer clic en **Inicio**, en la esquina inferior izquierda de la pantalla y seleccionar a continuación **Programas → McAfee VirusScan → Consola VirusScan → Planificar**

{button ,JI(`VScan4.hlp',`Scheduling_Scanning_Tasks')} Planificación de las tareas de exploración%Scheduling_Scanning_Tasks

{button ,JI(`vscan4.HLP',`Creating_New_Tasks')} Creación de nuevas tareas%Creating_New_Tasks

Para planificar tareas de exploración:

1 Haga clic en  en la bandeja del sistema, en la esquina inferior derecha de la pantalla. Aparecerá entonces el Planificador de VirusScan. Otra opción para accedar al Planificador consiste en hacer clic en **Inicio**, en la esquina inferior izquierda de la pantalla. A continuación, seleccione **Programas → McAfee VirusScan → Consola VirusScan → Planificar**

2 Haga doble clic en la tarea que desea planificar. Aparecerán entonces las páginas **Propiedades de tarea** de la exploración seleccionada.

3 Seleccione la pestaña **Programa**.

4 De un nombre a la tarea que la describa con claridad.

» Si configura una tarea que ya aparece en la lista del Planificador, el cuadro Descripción muestra el nombre de la tarea seleccionada. Puede cambiar esa descripción si lo desea.

» Si se trata de crear una nueva tarea, el cuadro Descripción está vacío. Escriba un nombre que describa la tarea.

5 El cuadro de texto **Programa** muestra la ruta del archivo del programa de exploración, Scan32.exe. Si ha instalado VirusShield en una ubicación distinta a la predeterminada para su instalación, haga clic en **Examinar** para buscarla y seleccione el archivo.

6 El cuadro de texto **Iniciar en** muestra la ruta de la carpeta que contiene el archivo Scan32.exe. Si el archivo está en otra carpeta, haga clic en **Examinar** para buscarla y seleccionarla.

7 El cuadro de texto **Parámetros** permite a los usuarios avanzados incorporar opciones de conmutación para este y otros programas.

8 Haga clic en la flecha abajo, en el cuadro de texto **Ejecutar**, si desea que el explorador se ejecute en una ventana maximizada o minimizada, en lugar de en una ventana normal.

9 Haga clic en **Configurar** para especificar las propiedades de la exploración planificada. Aparecerán entonces las páginas **Propiedades de McAfee VirusScan**. Vea el apartado de Configuración de propiedades de VirusScan si desea tener más información.

10 Inicie la exploración o continúe configurando el programa:

» Haga clic en **Ejecutar ahora** si desea realizar inmediatamente la exploración.

O

» Seleccione la pestaña **Planificar** para continuar con la configuración.

O

» Haga clic en la pestaña **Estado** para ver información acerca de la exploración planificada.

11 Cuando haya terminado:

» Haga clic en **Aplicar** para guardar las opciones de detección seleccionadas sin salir de la página de propiedades **Programa** o

» Haga clic en **Aceptar** para guardar los cambios efectuados en esta y otras páginas de propiedades y cerrar a continuación el cuadro de diálogo Propiedades de VirusScan o

» Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar los cambios efectuados.

1. Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.
2. Seleccione **Programas → McAfee VirusScan → Consola VirusScan → Planificar** Aparecerá entonces el Planificador.
3. Haga doble clic en la tarea que desea planificar. Aparecerán entonces las páginas **Propiedades de tarea** correspondientes a la exploración seleccionada.
4. Seleccione la pestaña **Planificar**.
5. Haga clic en la casilla **Activar**.
6. En la parte **Ejecutar** de la pantalla, seleccione el botón que representa la frecuencia con las que desea ejecutar la exploración.
7. En la parte **Iniciar a** de la pantalla, seleccione los días de la semana en que desea realizar la exploración, escribiendo la hora en el cuadro de texto.
8. Inicie la exploración o continúe configurando el programa:

    Haga clic en **Ejecutar ahora**, en la pestaña **Programa**, si desea realizar inmediatamente la exploración, o examine las opciones de configuración ya seleccionadas.

O

    Haga clic en la pestaña **Estado** para ver información acerca de la ejecución planificada.

9. Cuando haya terminado:

    Haga clic en **Aplicar** para guardar las opciones de detección seleccionadas sin salir de la página de propiedades **Programa** o

    Haga clic en **Aceptar** para guardar los cambios efectuados en esta u otras páginas de propiedades y cerrar a continuación el cuadro de diálogo Propiedades de VirusScan o

    Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar cambio alguno.

Hay dos métodos para agregar una nueva tarea planificada. El primero supone crearla desde el principio. Mientras que el otro consiste en copiar una tarea existente, cambiarla de nombre y cambiar su configuración.

Método 1-Crear una nueva tarea:

1 Seleccione la opción de menú **Tarea → Nueva tarea** o haga clic en  , en la barra de herramientas. Aparecerán entonces las páginas **Propiedades de Tarea**, con el cuadro Descripción vacío.

2 Escriba un nombre que describa la tarea.

3 Vea el apartado Planificación de las tareas de exploración (a partir del Paso 4), donde encontrará las restantes instrucciones.

Método 2-Copiar una tarea existente:

1 Seleccione una tarea existente. A continuación, haga clic con el botón derecho en **→Copiar**. Después, haga clic con el botón derecho en **→ Pegar**. Aparecerán entonces las páginas **Propiedades de tarea**.

 **Vea la nota**

2 Sustituya el nombre por una nueva descripción de la tarea.

3 Vea el apartado Planificación de las tareas de exploración (a partir del Paso 4), donde encontrará las restantes instrucciones.

Configuración de las propiedades de VirusScan

Para configurar exploraciones requeridas de VirusScan en unidades de disco locales o de red:

1 Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.

2 Seleccione **Programas → McAfee VirusScan → Consola VirusScan → Planificar**. Aparecerá entonces el Planificador de Virus Scan.

3 Haga clic en el icono  de la barra de herramientas del Planificador. Aparecerán entonces las páginas **Propiedades de McAfee VirusScan**.

O

Haga doble clic en la descripción de la exploración que desea configurar. Aparecerán entonces las páginas **Propiedades de tarea** de la exploración seleccionada. A continuación, haga clic en **Configurar**. Aparecerán entonces las páginas **Propiedades de McAfee VirusScan**.

4 Configure las propiedades en cada una de las pestañas.

{button ,JI(`vscan4.HLP',`Configuring_VirusScan_Detection_Properties')} Pestaña Detección

{button ,JI(`vscan4.HLP',`Configuring_VirusScan_Action_Properties')} Pestaña Acción

{button ,JI(`vscan4.HLP',`Configuring_VirusScan_Alert_Properties')} Pestaña Alerta

{button ,JI(`vscan4.HLP',`Configuring_System_Scan_Report_Properties')} Pestaña Informe

{button ,JI(`vscan4.HLP',`Configuring_VirusScan_Exclusion_Properties')} Pestaña Exclusión

{button ,JI(`vscan4.HLP',`Configuring_VirusScan_Security')} Pestaña Seguridad

 Otros temas asociados

1 Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.

2 Seleccione **Programas → McAfee VirusScan → Consola VirusScan → Planificar**. Aparecerá entonces el Planificador de Virus Scan.

3 Seleccione una tarea *que no sea* **McAfee VShield**. Si desea información acerca de la configuración de **VShield**, vea el apartado Configuración de los módulos de VShield

4 Haga clic en el icono  , en la barra de herramientas del Planificador. Aparecerán entonces las páginas **Propiedades de McAfee VirusScan**.

O

Haga doble clic en la descripción de la exploración que desea configurar. Aparecerán entonces las páginas **Propiedades de tarea** de la exploración seleccionada. A continuación, haga clic en **Configurar**. Aparecerán entonces las páginas **Propiedades de McAfee VirusScan**.

5 Seleccione la pestaña **Detección**. Como opción predeterminada, VirusScan asume que desea explorar la unidad **C:**.

6 Si desea explorar otras ubicaciones adicionales, haga clic en **Agregar**. Aparecerá entonces la pantalla **Agregar elemento a la exploración**.

Vea la nota

7 Seleccione el botón que describe las ubicaciones adicionales.

Si desea explorar varias unidades de disco conectadas al equipo, haga clic en **Seleccionar elemento para explorar**.

Si desea explorar una ubicación determinada, haga clic en **Seleccionar unidad o carpeta para explorar**.

8 Si ha elegido la opción **Seleccionar elemento a explorar**, haga clic en y seleccione el ámbito de la exploración. Puede incluir todas las unidades de disco conectadas al equipo, todas las unidades desmontables, todas las unidades fijas o todas las unidades de red.

O

Si ha elegido **Seleccionar unidad o carpeta para explorar**, haga clic en **Examinar** y seleccione la unidad o carpeta que desea incluir. A continuación, seleccione la casilla **Incluir subcarpetas** si desea incluir las subcarpetas en la exploración.

9 Cuando haya terminado, haga clic en **Aceptar** para guardar los cambios efectuados y cerrar el cuadro de diálogo.

10 En la parte **Qué explorar** de la pantalla, seleccione cualquiera o todas las casillas.

Seleccione la casilla **Explorar memoria** para incluir en la exploración la búsqueda de virus residentes en memoria. Estos virus quedan en memoria después de que se ejecutan y siguen afectando a otros archivos.

Seleccione la casilla **Explorar sectores de arranque** para incluir en la exploración la búsqueda de virus que se introducen en el sector de arranque. El sector de arranque es la primer división lógica de un disco duro o un disquete. El BIOS de su equipo examina ese sector poco después de iniciar el sistema en busca de los archivos y programas que necesita para iniciar el funcionamiento del equipo.

Seleccione la casilla **Archivos comprimidos** para incluir en la exploración los archivos creados con los programas LHA, LZEXE, PkLite, PkZip o WinZip. Dado que VirusScan descomprime en memoria este tipo de archivos antes de determinar si tienen o no virus, esta opción aumenta el tiempo necesario para realizar una exploración.

Seleccione la casilla **Iniciar automáticamente** si desea que la exploración comience sin hacer ninguna pregunta al usuario, basándose exclusivamente en las opciones seleccionadas en el **Planificador**. Vea el apartado de Planificación de exploraciones requeridas para ejecución automática si desea más información.

11 A continuación, en la parte **Qué explorar** de la pantalla, haga clic en uno de los botones para indicar si se deben explorar todos los archivos o sólo los archivos de Programa.

Si selecciona **Sólo archivos de programa**, haga clic en **Extensiones** para ver una lista con las extensiones de nombre de archivo que VirusScan explorará. Puede editar esa lista.

12 Haga clic en **Analizador de macros** para configurar la Exploración con el Analizador de macros.

13 Haga clic en **Aplicar** para guardar los cambios efectuados sin cerrar el cuadro de diálogo. Así termina la configuración de la página de propiedades **Detección**.

14 Haga clic en otra pestaña para continuar.

Vea la nota

1 Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.

2 Seleccione **Programas → McAfee VirusScan → Consola VirusScan → Planificar**. Aparecerá entonces el Planificador de Virus Scan.

3 Seleccione una tarea *que no sea* **McAfee VShield**. Si desea información acerca de la configuración de **VShield**, vea el apartado Configuración de los módulos de VShield

4 Haga clic en el icono  , en la barra de herramientas del Planificador. Aparecerán entonces las páginas **Propiedades de McAfee VirusScan**.

O

Haga doble clic en la descripción de la exploración que desea configurar. Aparecerán entonces las páginas **Propiedades de tarea** de la exploración seleccionada. A continuación, haga clic en **Configurar**. Aparecerán entonces las páginas **Propiedades de McAfee VirusScan**.

5 Seleccione la pestaña **Acción** para especificar de qué forma debe actuar VirusScan cuando detecta un virus. Como opción predeterminada, aparece seleccionada la opción **Consultar antes de actuar**.

6 Haga clic en la flecha abajo si desea seleccionar una respuesta distinta de VirusScan ante la detección de un virus. Las opciones que aparecen en **Acciones posibles** cambiarán en función de la acción que seleccione. Si deja la respuesta predeterminada **Consultar antes de actuar**, tendrá la oportunidad de seleccionar cualquiera de las acciones posibles cada vez que se detecte un virus. Si selecciona una de las otras opciones en la lista de desplegable, esa opción se ejecutará automáticamente cada vez que se detecte un virus.

 Si deja seleccionada la opción **Consultar antes de actuar**, deseleccione todas las posibles acciones que no desea dejar al usuario. Deje sólo seleccionadas las casillas de las opciones que desea ofrecer.

 Si selecciona la opción **Mover los archivos infectados automáticamente**, se le pedirá que indique la ubicación y nombre de destino de los archivos.

 Si selecciona las opciones **Limpiar los archivos infectados automáticamente**, **Borrar los archivos infectados automáticamente** o **Continuar exploración**, aparecerá un mensaje que explica la opción elegida.

7 Haga clic en **Aplicar** para guardar los cambios efectuados sin cerrar el cuadro de diálogo. Así termina la configuración de la página de propiedades **Acción**.

8 Haga clic en otra pestaña para continuar.

 **Vea la nota**

1 Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.

2 Seleccione **Programas → McAfee VirusScan → Consola VirusScan → Planificar**. Aparecerá entonces el Planificador de Virus Scan.

3 Seleccione una tarea *que no sea* **McAfee VShield**. Si desea información acerca de la configuración de **VShield**, vea el apartado Configuración de los módulos de VShield

4 Haga clic en el icono  , en la barra de herramientas del Planificador. Aparecerán entonces las páginas **Propiedades de McAfee VirusScan**.

O

Haga doble clic en la descripción de la exploración que desea configurar. Aparecerán entonces las páginas **Propiedades de tarea** de la exploración seleccionada. A continuación, haga clic en **Configurar**. Aparecerán entonces las páginas **Propiedades de McAfee VirusScan**.

5 Seleccione la pestaña **Alerta** si desea que VirusScan envíe un mensaje cuando detecte un virus.

6 Seleccione la casilla **Enviar alerta de red** si desea que la alerta se envíe a un servidor de la red. Al hacerlo se activará el botón **Examinar** y podrá buscar la ubicación de destino para la alerta de red. Cuando la haya seleccionado, la ruta de esa ubicación aparecerá en el cuadro de texto.

7 Seleccione la casilla **DMI** para enviar el aviso a aplicaciones de gestión de red o de escritorio que cumplen con la especificación DMI (Interfaz de administración de escritorio).

8 Si ha seleccionado previamente la opción **Consultar antes de actuar** en la pestaña **Acción**, VirusScan necesita saber de qué forma debe avisar cuando detecte un virus: mediante un mensaje en pantalla, con un tono o con ambos. Como opción predeterminada, el mensaje que aparece en el cuadro de texto tiene color gris.

- Para cambiar el mensaje, seleccione la casilla **Mostrar mensaje personalizado** y escriba un nuevo mensaje.
- Para omitir el tono, borre la marca de la casilla **Emitir señal audible**.

9 Haga clic en **Aplicar** para guardar los cambios efectuados sin cerrar el cuadro de diálogo. Así termina la configuración de la página de propiedades **Detección**.

10 Haga clic en otra pestaña para continuar.

Vea la nota

1. Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.
2. Seleccione **Programas → McAfee VirusScan → Consola VirusScan → Planificar**. Aparecerá entonces el Planificador de Virus Scan.
3. Seleccione una tarea *que no sea* **McAfee VShield**. Si desea información acerca de la configuración de **VShield**, vea el apartado Configuración de los módulos de VShield
4. Haga clic en el icono  , en la barra de herramientas del Planificador. Aparecerán entonces las páginas **Propiedades de McAfee VirusScan**.

   O

   Haga doble clic en la descripción de la exploración que desea configurar. Aparecerán entonces las páginas **Propiedades de tarea** de la exploración seleccionada. A continuación, haga clic en **Configurar**. Aparecerán entonces las páginas **Propiedades de McAfee VirusScan**.
5. Seleccione la pestaña **Informe** si desea que VirusScan conserve un registro de sus actividades de exploración. Como opción predeterminada, VirusScan crea un archivo de nombre VSCLog.txt, con un tamaño máximo de 100 KB, en el que registra todas las opciones de informe disponibles que aparecen en pantalla. La ubicación predeterminada del archivo de registro es C:\Archivos de programa\Network Associates\McAfee Virus Scan\. Si desea cambiar estas opciones predeterminadas, puede:

   » Borrar la marca de la casilla **Registrar en archivo**, con lo que se interrumpe toda actividad de registro.

   » Escribir un nuevo nombre o ruta de acceso del archivo de texto que se genera. VirusScan sólo generará un archivo de texto sin formato.

   » Haga clic en **Examinar** para seleccionar una ubicación para el archivo.

   » Borrar la marca de la casilla **Limitar tamaño de archivo de registro** para eliminar cualquier límite de tamaño.

   » Cambiar el tamaño máximo del archivo de registro.

   » Borrar la marca de las casillas de cualquiera de los elementos del informe que no esté interesado en ver registrado.
6. Haga clic en **Aplicar** para guardar los cambios efectuados sin cerrar el cuadro de diálogo. Así termina la configuración de la página de propiedades **Informe**.
7. Haga clic en otra pestaña para continuar.

» **Vea la nota**

1. Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.
2. Seleccione **Programas → McAfee VirusScan → Consola VirusScan → Planificar**. Aparecerá entonces el Planificador de Virus Scan.
3. Seleccione una tarea *que no sea* **McAfee VShield**. Si desea información acerca de la configuración de **VShield**, vea el apartado Configuración de los módulos de VShield
4. Haga clic en el icono  , en la barra de herramientas del Planificador. Aparecerán entonces las páginas **Propiedades de McAfee VirusScan**.

   O

   Haga doble clic en la descripción de la exploración que desea configurar. Aparecerán entonces las páginas **Propiedades de tarea** de la exploración seleccionada. A continuación, haga clic en **Configurar**. Aparecerán entonces las páginas **Propiedades de McAfee VirusScan**.
5. Seleccione la pestaña **Exclusión** para especificar carpetas que deben quedar excluidas de la exploración en busca de virus. Como opción predeterminada, VirusScan no explora los archivos de la carpeta Papelera de reciclaje.

   Seleccione la opción **Agregar...** para especificar una carpeta que deba excluirse. Tiene además la opción de incluir las subcarpetas y especificar si la exclusión es para las exploraciones de archivos o la exploración de sector de arranque.

   Seleccione **Editar…** para modificar las instrucciones relativas a la carpeta seleccionada que ya aparece en la lista de exclusiones.

   Seleccione **Eliminar** para borrar la carpeta seleccionada de la lista.
6. Haga clic en **Aplicar** para guardar los cambios efectuados sin cerrar el cuadro de diálogo. Así termina la configuración de la página de propiedades **Detección**.
7. Haga clic en otra pestaña para continuar.

Vea la nota

1 Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.

2 Seleccione **Programas → McAfee VirusScan → Consola VirusScan → Planificar**. Aparecerá entonces el Planificador de Virus Scan.

4 Haga clic en el icono  , en la barra de herramientas del Planificador. Aparecerán entonces las páginas **Propiedades de McAfee VirusScan**.

O

Haga doble clic en la descripción de la exploración que desea configurar. Aparecerán entonces las páginas **Propiedades de tarea** de la exploración seleccionada. A continuación, haga clic en **Configurar**. Aparecerán entonces las páginas **Propiedades de McAfee VirusScan**.

4 Seleccione la pestaña **Seguridad**.

5 Seleccione la página o páginas que desea proteger mediante contraseña.

 El gráfico de un candado abierto pasa a un candado cerrado para indicar que la opción queda "bloqueada".

 El botón Contraseña se activa.

 Se activa también la casilla Mantener opciones de seguridad.

6 Haga clic en **Contraseña**. Al hacerlo se abrirá el cuadro de diálogo **Especificar contraseña**.

7 Escriba una contraseña. A continuación, vuelva a escribir la misma contraseña exactamente igual que la escribió por primera vez.

8 Haga clic en **Aceptar**.

9 Si se trata de configurar una tarea que se creó copiando una tarea ya existente, seleccione la casilla **Mantener opciones de seguridad** para aplicar a la nueva tarea las mismas opciones de seguridad que tenía la tarea original. La casilla se activa al seleccionar una de las páginas de propiedades relacionadas con la protección mediante contraseña.

10 Haga clic en **Aplicar** para guardar los cambios efectuados sin cerrar el cuadro de diálogo. Así termina la configuración de la página de propiedades **Seguridad**.

11 Haga clic en otra pestaña para continuar.

 **Vea la nota**

 Información acerca de seguridad en exploraciones relacionadas con acceso o en Internet

Indique las páginas de propiedades (pestañas) que necesitan ser protegidas mediante contraseña.

1 Seleccione la página (o páginas) de propiedades a proteger mediante contraseña.

2 Haga clic en **Contraseña** para especificar una contraseña.

3 Haga clic en **Aceptar** cuando haya terminado.

Bloquee el acceso a un URL que sospeche que contiene objetos de ActiveX o Java dañinos.

1 Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.

2 Seleccione **Programas → McAfee VirusScan → Consola VirusScan → VShield.** Aparecerán entonces las páginas de propiedades de VShield**.**

{button ,JI(`vscan4.HLP',`Navigate_to_the_VShield_Configuration_Pages')} Haga clic aquí para ver otras formas de acceder a las páginas de propiedades de VShield.

3 Seleccione **Filtro de Internet** en el cuadro de componentes que aparece en el lado izquierdo de las páginas de configuración. Al hacerlo, aparecerán las páginas de propiedades **Filtro de Internet**.

4 Seleccione la pestaña **Detección**.

5 Asegúrese que está seleccionada la casilla **Activar Java & ActiveX**.

6 Seleccione la casilla **URL de Internet que se bloquearán**, situada cerca de la parte inferior de la pantalla.

7 Haga clic en el botón **Configurar** que aparece al lado. Al hacerlo, se abrirá el cuadro de diálogo **URL prohibidas**.

8 Haga clic en **Agregar**. Al hacerlo, se abrirá el cuadro de diálogo Agregar URL.

9 Escriba el URL que desea en el cuadro de texto.

10 Haga clic en **Aceptar**. El nombre del URL prohibido aparecerá entonces en el cuadro de diálogo URL prohibidos.

11 Haga clic en **Aceptar**

12 Haga clic en **Aplicar** si desea guardar los cambios efectuados y continuar con la configuración. Si ha terminado la configuración, haga clic en **Aceptar** para guardar los cambios y cerrar las páginas de propiedades.

Bloquee el acceso a una dirección IP de Internet que sospeche que contiene objetos de ActiveX o Java dañinos.

1 Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.

2 Seleccione **Programas → McAfee VirusScan → Consola VirusScan → VShield.** Aparecerán entonces las páginas de propiedades de VShield.

{button ,JI(`vscan4.HLP',`Navigate_to_the_VShield_Configuration_Pages')} Haga clic aquí para ver otras formas de acceder a las páginas de propiedades de VShield.

3 Seleccione **Filtro de Internet** en el cuadro de componentes que aparece en el lado izquierdo de las páginas de configuración. Al hacerlo, aparecerán las páginas de propiedades **Filtro de Internet**.

4 Seleccione la pestaña **Detección**.

5 Asegúrese que está seleccionada la casilla **Activar Java & ActiveX**.

6 Seleccione la casilla **Direcciones IP que se bloquearán** situada cerca de la parte inferior de la pantalla.

7 Haga clic en el botón **Configurar** que aparece al lado. Al hacerlo se abrirá el cuadro de diálogo **Direcciones IP prohibidas**.

8 Haga clic en **Agregar**. Al hacerlo, se abrirá el cuadro de diálogo **Agregar dirección IP**.

9 Escriba la dirección en el cuadro de texto de dirección IP.

10 Escriba la Subred en el cuadro de texto de Máscara de subred.

11 Haga clic en **Aceptar**. Al hacerlo, la dirección aparecerá en el cuadro de diálogo **Direcciones IP prohibidas**.

12 Haga clic en **Aceptar**

13 Haga clic en **Aplicar** si desea guardar los cambios efectuados y continuar con la configuración. Si ha terminado de hacer cambios en la configuración, haga clic en **Aceptar** para guardar los cambios y cerrar las páginas de propiedades.

Una vez que se ha activado y configurado,  aparece en la bandeja del sistema, en la esquina inferior derecha de la pantalla, en la misma ubicación que contiene la hora actual. Así se indica que VShield está operando en segundo plano, controlando y explorando el correo electrónico que recibe, los archivos que descarga o los objetos de Java y ActiveX que se encuentra. Para activar o desactivar la actividad de exploración o para ver un resumen de las acciones:

1 Haga doble clic en el icono de VirusScan para acceder a las páginas del cuadro de diálogo Estado.

2 Haga clic en la pestaña que corresponde al componente del programa que desea activar o desactivar o cuyo funcionamiento desea comprobar.

VShield informa acerca del número de archivos que ha explorado, movido o borrado y del número de archivos infectados que han encontrado los componentes de Exploración de correo electrónico y Explorador de elementos descargados. En cuanto a objetos de Java y ActiveX o sitios de Internet, VShield informa del número de elementos que ha explorado y del número de los que ha "prohibido" o evitado el acceso. Si ha activado su función de registro, VirusScan registra también esta misma información en el archivo de registro de cada componente del programa.

3 Haga clic en **Activar** para iniciar el componente del programa. Para desactivarlo, haga clic en **Desactivar**.

 **Vea la nota**

4 Haga clic en **Propiedades** para acceder al cuadro de diálogo Propiedades de VirusScan, donde se pueden definir las opciones que indican a VirusScan cómo debe realizar cada tipo de exploración.

5 Haga clic en **Cerrar** para cerrar el cuadro de diálogo de Estado de VShield.

El componente VShield incluye cuatro módulos que se pueden configurar previamente para que realicen exploraciones cada vez que se produzca un evento determinado, como puede ser la apertura de un archivo o un archivo adjunto de correo electrónico. Esos módulos son los siguientes:

- Explorador del sistema (para exploraciones relacionadas con accesos)
- Exploración de correo electrónico (para exploraciones relacionadas con accesos)
- Explorador de elementos descargados
- Filtro de Internet.

Puede configurar cada uno de estos componentes o utilizar el Asistente del Explorador para definir sus propiedades.

Vea la nota

Utilizando el Asistente:

1 Haga clic con el botón derecho en de la bandeja del sistema, en la esquina inferior derecha de la pantalla, en el mismo lugar en que aparece la hora actual.

2 En el menú que aparecerá, seleccione **Propiedades**. A continuación, seleccione **Explorador del sistema** o cualquiera de los otros módulos que aparecen en la lista. Al hacerlo, aparecerán las páginas de propiedades para exploraciones relacionadas con accesos.

3 Haga clic en **Asistente**, la opción que aparece debajo de la lista de módulos. Al hacerlo aparecerá el **Asistente** de configuración.

4 Siga las instrucciones que irán apareciendo en pantalla.

Configuración manual de los módulos:

1 Haga clic con el botón derecho en de la bandeja del sistema, en la esquina inferior derecha de la pantalla, en el mismo lugar en que aparece la hora actual.

2 En el menú que aparecerá, seleccione **Propiedades**. A continuación, seleccione el módulo que desea configurar. Aparecerán entonces las páginas de propiedades relacionadas con la exploración asociada a accesos y correspondientes al módulo que desea configurar. Vea el apartado Cómo llegar a las páginas de configuración de VShield si desea tener más información acerca de otras formas de acceder a las páginas de propiedades de **VShield**.

3 Seleccione las opciones que desea para el módulo seleccionado en cada una de las pestañas o seleccione otro módulo en la lista situada en la parte izquierda de la pantalla. Haga clic en un botón de los siguientes para ver instrucciones acerca de la configuración de cada uno de los módulos:

{button ,JI(`vscan4.HLP',`Configuring_System_Scan_Properties')} Explorador del sistema

{button ,JI(`vscan4.HLP',`Configuring_On_Access_E-Mail_Scan_Properties')} Exploración de correo electrónico

{button ,JI(`vscan4.HLP',`Configuring_Download_Scan_Properties')} Explorador de elementos descargados

{button ,JI(`vscan4.HLP',`Configuring_Internet_Filter_Properties')} Filtro de Internet

{button ,JI(`vscan4.HLP',`Configuring_VShield_Security_Properties')} Seguridad

4 Si desea configurar otro módulo, selecciónelo en el cuadro que aparece en la parte izquierda de la pantalla y repita el Paso 3 hasta que haya terminado la configuración.

5 Cuando haya terminado.

Haga clic en **Aplicar** para guardar las opciones de detección seleccionadas sin salir de la página de propiedades correspondiente o

Haga clic en **Aceptar** para guardar los cambios efectuados en esta u otras páginas de propiedades y cerrar el cuadro de diálogo Propiedades de VirusScan o

Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar cambio alguno.

1 Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.

2 Seleccione **Programas → McAfee VirusScan → Consola VirusScan → VShield**. Aparecerán entonces las páginas de propiedades de VShield.

{button ,JI(`vscan4.HLP',`Navigate_to_the_VShield_Configuration_Pages')} Haga clic aquí para ver otras formas de acceder a las páginas de propiedades de VShield.

3 Seleccione **Exploración de correo electrónico** entre los componentes del programa que aparecen en la parte izquierda de la pantalla de configuración de VShield.

Al hacerlo, aparecerán las páginas de configuración de la Exploración de correo electrónico.

Como opción predeterminada, aparecerá en primer lugar la pestaña **Detección**.

4 Haga clic en la casilla **Activar la exploración de los archivos adjuntos al correo**. Al hacerlo, se activará el resto de la página de propiedades.

5 Configure las propiedades en cada una de las pestañas.

Vea la nota

{button ,JI(`vscan4.HLP',`Configuring_On_Access_E_mail_Scan_Detection_Properties')} Pestaña Detección

{button ,JI(`vscan4.HLP',`Configuring_On_Access_E_mail_Scan_Action_Properties')} Pestaña Acción

{button ,JI(`vscan4.HLP',`Configuring_On_Access_E_mail_Scan_Alert_Properties')} Pestaña Alerta

{button ,JI(`vscan4.HLP',`Configuring_On_Access_E_mail_Scan_Report_Properties')} Pestaña Informe

Otros temas asociados

Haga clic en uno de los siguientes botones para obtener información relacionada con el software específico de correo electrónico que utiliza:

{button ,JI(`vscan4.HLP',`Configuring_a_Microsoft_Exchange_(MAPI)_E-mail_Client')} Microsoft Exchange (MAPI)

{button ,JI(`vscan4.HLP',`Configuring_Lotus_cc:Mail')} Lotus cc:Mail

{button ,JI(`vscan4.HLP',`Configuring_a_POP-3_Internet_Mail_Client')} Cliente de correo de Internet POP-3

Las siguientes instrucciones sólo son aplicables a la ***exploración asociada a accesos*** de correo electrónico recibido a través de ***Microsoft Exchange o de otro programa que cumpla con el estándar MAPI***, como puede ser Microsoft Outlook, e incluso Lotus cc:Mail 8.

» Si desea más información acerca de la ***exploración requerida*** de correo electrónico, vea el apartado de Configuración de las propiedades de la exploración de correo electrónico requerida

» Si desea más información acerca de la ***exploración asociada a accesos*** de correo electrónico recibido a través de un cliente de correo ***POP-3 o proxy***, como America Online, Eudora Light, Netscape y Outlook Express, vea el apartado de Configuración de un cliente de correo de Internet POP-3

Nota: Si su programa de correo electrónico está en un dominio de red distinto a aquel en que normalmente inicia una sesión para las actividades normales, habrá que proporcionar el nombre de usuario de correo electrónico y la contraseña cada vez que se inicie o reinicie el sistema.

1 Haga clic en la casilla **Activar la exploración de archivos adjuntos al correo**.

2 Seleccione la casilla **Microsoft Exchange (MAPI)**.

3 Haga clic en las opciones **Todo el correo nuevo** o **Carpeta seleccionada** para especificar qué correo electrónico debe explorarse.

4 Si elige la opción **Carpeta seleccionada**, haga clic en **Examinar** para seleccionar la carpeta que contiene el correo electrónico que desea explorar.

5 Haga clic en uno de los botones de la sección **Archivos adjuntos** de la pantalla para indicar si deben explorarse todos los archivos adjuntos de correo o sólo los archivos de programa.

6 Si selecciona **Sólo archivos de programa**, haga clic en **Extensiones** para ver una lista con las extensiones que de nombre de archivo que VirusScan explorará. Puede editar esa lista.

7 Seleccione la casilla de **Archivos comprimidos** si desea incluir en la exploración los archivos creados con los programas LHA, LZEXE, PkLite, PkZip o WinZip. Dado que VirusScan descomprime los archivos de este tipo en memoria antes de comprobar si tienen o no virus, esta opción puede aumentar el tiempo necesario para realizar una exploración.

8 Haga clic en **Aplicar** para guardar los cambios efectuados sin cerrar el cuadro de diálogo. Así termina la configuración de la página de propiedades **Detección**.

9 Haga clic en otra pestaña para continuar.

» **Vea la nota**

Se puede acceder a la exploración de correo electrónico requerida a través de la barra de herramientas o el menú Herramientas de los programas de correo electrónico que cumplen el estándar MAPI, como puede ser Microsoft Outlook.

Seleccione **Herramientas → Propiedades de la Exploración de correo electrónico** o haga clic en  . Al hacerlo, aparecerán las páginas **Propiedades de la Exploración de correo electrónico**.

Configure las propiedades en cada una de las pestañas.

{button ,JI(`vscan4.HLP',`Configuring_On_Demand_E_mail_Scan_Detection_Properties')} Pestaña Detección

{button ,JI(`vscan4.HLP',`Configuring_On_Demand_E_mail_Scan_Action_Properties')} Pestaña Acción

{button ,JI(`vscan4.HLP',`Configuring_On_Demand_E_mail_Scan_Alert_Properties')} Pestaña Alerta

{button ,JI(`vscan4.HLP',`Configuring_On_Demand_E_mail_Scan_Report_Properties')} Pestaña Informe

Usuarios de Microsoft Exchange, vean la Nota

Seleccione la pestaña **Detección**. Como opción predeterminada, esta es la pestaña activa cuando se entra en las páginas **Propiedades de la Exploración de correo electrónico requerida**.

1 Seleccione **Explorar todos los mensajes** o **Explorar sólo los mensajes no leídos**.

2 Haga clic en uno de los botones de la sección de **Archivos adjuntos** de la pantalla para indicar si se debe explorar todos los archivos adjuntos al correo o sólo los archivos de programa.

3 Si selecciona **Sólo archivos de programa**, haga clic en **Extensiones** para ver una lista con todas las extensiones de nombre de archivo que VirusScan explorará. Puede editar esa lista.

4 Seleccione la casilla **Archivos comprimidos** para incluir en la exploración los archivos creados con los programas LHA, LZEXE, PkLite, PkZip o WinZip. Dado que VirusScan descomprime este tipo de archivos en memoria antes de comprobar si tiene o no virus, esta opción puede aumentar el tiempo necesario para realizar la exploración del correo electrónico.

5 Haga clic en **Aplicar** para guardar los cambios efectuados sin cerrar el cuadro de diálogo. Así termina la configuración de la página de propiedades **Detección**.

6 Haga clic en otra pestaña para continuar.

1. Seleccione la pestaña **Acción** para especificar de qué forma debe actuar VirusScan cuando detecte un virus. Como opción predeterminada, la respuesta seleccionada es **Consultar antes de actuar**.
2. Haga clic en la flecha abajo si desea seleccionar una respuesta distinta de VirusScan ante la detección de un virus. Las opciones que aparecen en **Acciones posibles** cambiarán en función de la acción que seleccione. Si deja la respuesta predeterminada **Consultar antes de actuar**, tendrá la oportunidad de seleccionar cualquiera de las acciones posibles cada vez que se detecte un virus. Si selecciona una de las otras opciones en la lista de desplegable, esa opción se ejecutará automáticamente cada vez que se detecte un virus.

   Si deja seleccionada la opción **Consultar antes de actuar**, deseleccione todas las posibles acciones que no desea dejar al usuario. Deje sólo seleccionadas las casillas de las opciones que desea ofrecer.

   Si selecciona la opción **Limpiar los archivos adjuntos infectados automáticamente**, VirusScan tratará de eliminar el virus del archivo adjunto al correo. Si no puede limpiar el virus, generará un mensaje que indica que el virus no se puede eliminar. En esas circunstancias, McAfee aconseja que no trate de acceder al archivo infectado, sino que lo borre. Si es necesario, póngase en contacto con el remitente y pida que le envíe una copia del archivo adjunto que no esté infectada.

   Si selecciona la opción **Mover los archivos adjuntos infectados automáticamente**, se le pedirá que indique la ubicación y nombre de la carpeta de destino de los archivos.

   Si selecciona las opciones **Borrar los archivos adjuntos infectados automáticamente** o **Continuar exploración**, aparecerá un mensaje que explica la opción elegida.
3. Si selecciona la opción **Consultar antes de actuar**, VirusScan necesitará saber de qué forma debe avisar que ha detectado un virus: mediante un mensaje en pantalla, con un tono o con ambos. Como opción predeterminada, el mensaje que aparece en el cuadro de texto pasa a tener color gris.

   Para cambiar el mensaje, seleccione la casilla **Mostrar mensaje personalizado** y escriba un nuevo mensaje.

   Para omitir el tono, borre la marca de la casilla **Emitir señal audible**.
4. Haga clic en **Aplicar** para guardar los cambios efectuados sin cerrar el cuadro de diálogo. Así termina la configuración de la página de propiedades **Acción**.
5. Haga clic en otra pestaña para continuar.

Vea la nota

1. Seleccione la pestaña **Alerta** si desea que VirusScan envíe un mensaje de aviso cuando detecte un virus.
2. Seleccione la casilla **Enviar alerta de red** si desea que la alerta se envíe a un servidor de la red. Al hacerlo, se activará el botón **Examinar** y se puede buscar la ubicación de destino de la alerta de red. Cuando se haya seleccionado, la ruta de esa ubicación aparecerá en el cuadro de texto.
3. Si desea enviar alertas de correo electrónico, seleccione **Enviar mensaje de respuesta al remitente** y/o **Enviar mensaje de alerta al usuario**.
4. Haga clic en el botón **Configurar** correspondiente a su elección para designar al destinatario (o destinatarios) y preparar el mensaje.
5. Haga clic en **Aplicar** para guardar los cambios efectuados sin cerrar el cuadro de diálogo. Así termina la configuración de la página de propiedades **Alerta**.
6. Haga clic en otra pestaña para continuar.

 **Vea la nota**

1. Seleccione la pestaña **Informe** si desea que VirusScan conserve un registro de sus actividades de exploración. Como opción predeterminada, VirusScan crea un archivo de nombre WebEmail.txt, con un tamaño máximo de 100 KB, en el que registra todas las opciones de informe disponibles que aparecen en pantalla. La ubicación predeterminada del archivo de registro es C:\Archivos de programa\Network Associates\McAfee Virus Scan\. Si desea cambiar estas opciones predeterminadas, puede:

   - Borrar la marca de la casilla **Registrar en archivo**, con lo que se interrumpe toda actividad de registro.
   - Escribir un nuevo nombre o ruta de acceso del archivo de texto que se genera. VirusScan sólo generará un archivo de texto sin formato.
   - Haga clic en **Examinar** para seleccionar una ubicación para el archivo.
   - Borrar la marca de la casilla **Limitar tamaño de archivo de registro** para eliminar cualquier límite de tamaño.
   - Cambiar el tamaño máximo del archivo de registro.
   - Borrar la marca de las casillas de cualquiera de los elementos del informe que no esté interesado en ver registrado.

2. Haga clic en **Aplicar** para guardar los cambios efectuados sin cerrar el cuadro de diálogo. Así termina la configuración de la página de propiedades **Informe**.
3. Haga clic en otra pestaña para continuar.

Vea la nota

Se puede acceder a la **Exploración de correo electrónico** para exploraciones de correo electrónico requeridas a través de las barras de herramientas o del menú Herramientas de los programas de correo electrónico que cumplen con el estándar MAPI, como por ejemplo Microsoft Outlook.

Seleccione **Herramientas → Explorar en busca de virus** o haga clic en  . La pantalla de estado de la **Exploración de correo electrónico** aparecerá entonces e inmediatamente comenzará la actividad de exploración. En esa pantalla hay botones que permiten hacer una pausa, detener y reiniciar la actividad de exploración.

 **Vea la nota**

La versión más reciente de Lotus cc:Mail cumple con el estándar MAPI para programas de correo electrónico. Las versiones anteriores no eran compatibles con MAPI.

» Si utiliza Lotus cc:Mail 8, vea el apartado de Configuración de un cliente de correo electrónico (MAPI) de Microsoft Exchange

» Si utiliza una versión anterior de cc:Mail, es necesario realizar una instalación Personalizada de VirusScan, seleccionando **Lotus cc:Mail** durante el proceso de instalación. Las siguientes instrucciones sólo son aplicables a este caso.

1 Haga clic en la casilla **Activar la exploración de los archivos adjuntos al correo**.

2 Haga clic en la casilla **Activar correo corporativo**.

3 Seleccione el botón **Lotus cc:Mail**.

4 En la sección **Comprobar cada … segundos**, escriba la frecuencia, en segundos, con que desea que VShield compruebe si se ha recibido nuevo correo. Esta operación debe hacerse, al menos, con una frecuencia doble a la que utiliza el servidor de correo electrónico para comprobar si hay nuevo correo.

5 Haga clic en uno de los botones de la sección de **Archivos adjuntos** de la pantalla para indicar si se deben explorar todos los archivos adjuntos al correo o sólo los archivo de programa.

6 Si selecciona **Sólo archivos de programa**, haga clic en **Extensiones** para ver la lista con las extensiones de nombre de archivo que VirusScan explorará. Puede editar esa lista.

7 Seleccione la casilla de **Archivos comprimidos** si desea incluir en la exploración los archivos creados con los programas LHA, LZEXE, PkLite, PkZip o WinZip. Dado que VirusScan descomprime este tipo de archivos en memoria antes de comprobar si tiene o no virus, esta opción puede aumentar el tiempo necesario para realizar la exploración del correo electrónico.

8 Haga clic en **Aplicar** para guardar los cambios efectuados sin cerrar el cuadro de diálogo. Así termina la configuración de la página de propiedades **Detección**.

9 Haga clic en otra pestaña para continuar.

» **Vea la nota**

Las siguientes instrucciones corresponden a ***exploraciones asociadas a accesos*** de correo electrónico recibido a través de un ***cliente de correo POP-3 o proxy***, como pueden ser America Online, Eudora Light, Netscape y Outlook Express.

» Si desea información acerca de la exploración asociada a accesos de correo electrónico recibido a través de ***Microsoft Exchange u otro programa que cumpla con el estándar MAPI***, como puede ser Microsoft Outlook o Lotus cc:Mail 8, vea el apartado Configuración de un cliente de correo electrónico (MAPI) de Microsoft Exchange.

» Es el módulo **Explorador de elementos descargados** y no **Exploración de correo electrónico**, el que controla la exploración de archivos adjuntos que se reciben mediante esos programas. Al seleccionar **Correo Internet**, se activa automáticamente el **Explorador de elementos descargados**

1 Seleccione la casilla **Correo Internet**.

2 Borre la marca de la casilla **Activar la exploración de los archivos adjuntos al correo**.

3 Haga clic en **Aplicar** para guardar los cambios efectuados sin cerrar el cuadro de diálogo.

4 Seleccione la pestaña Explorador de elementos descargados para configurar las propiedades de exploración de archivos descargados, entre los que se incluyen los archivos adjuntos al correo que se recibe a través de un cliente POP-3.

» **Vea la nota**

1. Seleccione la pestaña **Acción** para especificar de qué forma debe actuar VirusScan cuando detecte un virus. Como opción predeterminada, la respuesta seleccionada es **Consultar antes de actuar**.
2. Haga clic en la flecha abajo si desea seleccionar una respuesta distinta de VirusScan ante la detección de un virus. Las opciones que aparecen en **Acciones posibles** cambiarán en función de la acción que seleccione. Si deja la respuesta predeterminada **Consultar antes de actuar**, tendrá la oportunidad de seleccionar cualquiera de las acciones posibles cada vez que se detecte un virus. Si selecciona una de las otras opciones en la lista de desplegable, esa opción se ejecutará automáticamente cada vez que se detecte un virus.

 Si deja seleccionada la opción **Consultar antes de actuar**, deseleccione todas las posibles acciones que no desea dejar al usuario. Deje sólo seleccionadas las casillas de las opciones que desea ofrecer.

 Si selecciona la opción **Mover los archivos infectados a una carpeta**, se le pedirá que indique la ubicación y nombre de la carpeta de destino de los archivos.

 Si selecciona las opciones **Borrar los archivos infectados** o **Continuar exploración**, aparecerá un mensaje que explica la opción elegida.

3. Si selecciona la opción **Consultar antes de actuar**, VirusScan necesitará saber de qué forma debe avisar que ha detectado un virus: mediante un mensaje en pantalla, con un tono o con ambos. Como opción predeterminada, el mensaje que aparece en el cuadro de texto pasa a tener color gris.

 Para cambiar el mensaje, seleccione la casilla **Mostrar mensaje personalizado** y escriba un nuevo mensaje.

 Para omitir el tono, borre la marca de la casilla **Emitir señal audible**.

4. Haga clic en **Aplicar** para guardar los cambios efectuados sin cerrar el cuadro de diálogo. Así termina la configuración de la página de propiedades **Acción**.
5. Haga clic en otra pestaña para continuar.

 **Vea la nota**

1. Seleccione la pestaña **Alerta** si desea que VirusScan envíe un mensaje de aviso cuando detecte un virus.
2. Seleccione la casilla **Enviar alerta de red** si desea que la alerta se envíe a un servidor de la red. Al hacerlo, se activará el botón **Examinar** y se puede buscar la ubicación de destino de la alerta de red. Cuando se haya seleccionado, la ruta de esa ubicación aparecerá en el cuadro de texto.
3. Si desea enviar alertas de correo electrónico, seleccione **Enviar mensaje de respuesta al remitente** y/o **Enviar mensaje de alerta al usuario**.
4. Haga clic en el botón **Configurar** correspondiente a su elección para designar al destinatario (o destinatarios) y preparar el mensaje.
5. Haga clic en **Aplicar** para guardar los cambios efectuados sin cerrar el cuadro de diálogo. Así termina la configuración de la página de propiedades **Alerta**.
6. Haga clic en otra pestaña para continuar.

 **Vea la nota**

1 Seleccione la pestaña **Informe** si desea que VirusScan conserve un registro de sus actividades de exploración. Como opción predeterminada, VirusScan crea un archivo de nombre WebEmail.txt, con un tamaño máximo de 100 KB, en el que registra todas las opciones de informe disponibles que aparecen en pantalla. La ubicación predeterminada del archivo de registro es C:\Archivos de programa\Network Associates\McAfee Virus Scan\. Si desea cambiar estas opciones predeterminadas, puede:

- Borrar la marca de la casilla **Registrar en archivo**, con lo que se interrumpe toda actividad de registro.
- Escribir un nuevo nombre o ruta de acceso del archivo de texto que se genera. VirusScan sólo generará un archivo de texto sin formato.
- Hacer clic en **Examinar** para seleccionar una ubicación para el archivo.
- Borrar la marca de la casilla **Limitar tamaño de archivo de registro** para eliminar cualquier límite de tamaño.
- Cambiar el tamaño máximo del archivo de registro.
- Borrar la marca de las casillas de cualquiera de los elementos del informe que no esté interesado en ver registrado.

2 Haga clic en **Aplicar** para guardar los cambios efectuados sin cerrar el cuadro de diálogo. Así termina la configuración de la página de propiedades **Informe**.

3 Haga clic en otra pestaña para continuar.

Vea la nota

Para configurar VirusScan para Windows 95 y Windows 98 de forma que busque virus en archivos de una unidad de disco local o de red:

1 Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.

2 Seleccione **Programas → McAfee VirusScan → Consola VirusScan → VShield**. Al hacerlo aparecerán las páginas de propiedades de VShield.

{button ,JI(`vscan4.HLP',`Navigate_to_the_VShield_Configuration_Pages')} Haga clic aquí para ver otras formas de acceder a las páginas de propiedades de VShield.

3 Seleccione **Explorador del sistema** entre los componentes del programa que aparecen en la parte izquierda de la pantalla de configuración.

 Como opción predeterminada, esta es la primera pantalla que aparece al abrir la característica de configuración de VirusScan

 La casilla **Activar exploración de sistema** está seleccionada y el resto de la página de propiedades está activada.

 Si no desea que el Explorador del sistema explore las unidades de disco locales o de red, borre la marca de la casilla **Explorador del sistema**.

 Si desea que el Explorador del sistema explore las unidades de disco locales o de red, configure las propiedades en cada una de las siguientes pestañas.

{button ,JI(`vscan4.HLP',`Configuring_System_Scan_Detection_Properties')} Pestaña Detección

{button ,JI(`vscan4.HLP',`Configuring_System_Scan_Action_Properties')} Pestaña Acción

{button ,JI(`vscan4.HLP',`Configuring_System_Scan_Alert_Properties')} Pestaña Alerta

{button ,JI(`vscan4.HLP',`Configuring_System_Scan_Report_Properties')} Pestaña Informe

{button ,JI(`vscan4.HLP',`Configuring_System_Scan_Exclusion_Properties')} Pestaña Exclusión

 Otros temas asociados

1. Como opción predeterminada, los archivos se exploran cuando se ejecutan, copian, crean o cambian de nombre. Si desea excluir alguno de estos eventos de forma que no activen la exploración asociada a accesos, borre la marca de la casilla correspondiente en la sección **Explorar archivos** de la pantalla.
2. Como opción predeterminada, el sector de arranque del disquete se explora cuando se entra en la unidad de disquete y cuando se apaga el sistema. Si desea excluir alguno de estos eventos de forma que no activen la exploración, borre la marca de la correspondiente casilla en la sección **Explorar disquetes** de la pantalla.
3. Haga clic un botón de la sección **Qué explorar** de la pantalla para indicar si se deben explorar todos los archivos o sólo los archivos de programa.

    Si selecciona **Sólo archivos de programa**, haga clic en **Extensiones** para ver una lista con las extensiones de nombre de archivo que VirusScan explorará. Puede editar esa lista haciendo clic en **Agregar** o **Borrar**.
4. Seleccione la casilla de **Archivos comprimidos** para incluir en la exploración los archivos creados con los programas LHA, LZEXE, PkLite, PkZip o WinZip. Dado que VirusScan descomprime este tipo de archivos en memoria antes de comprobar si tienen virus o no, esta opción puede aumentar el tiempo necesario para realizar una exploración.
5. Como opción predeterminada, el Explorador del sistema se carga cuando se inicia el sistema, puede desactivarse y está representado por un icono que aparece en la barra de tareas. Puede cambiar cualquiera de esas opciones, borrando la marca de la casilla correspondiente en la sección **General** de la pantalla.
6. Haga clic en **Analizador de macros** para configurar la Exploración con el Analizador de macros.
7. Haga clic en **Aplicar** para guardar los cambios efectuados sin cerrar el cuadro de diálogo. Así termina la configuración de la página de propiedades **Detección**.
8. Haga clic en otra pestaña para continuar.

 **Vea la nota**

1 Seleccione la pestaña **Acción** para especificar de qué forma debe actuar VirusScan cuando detecta un virus. Como opción predeterminada, aparece seleccionada la opción **Consultar antes de actuar**.

2 Haga clic en la flecha abajo si desea seleccionar una respuesta distinta de VirusScan ante la detección de un virus. Las opciones que aparecen en **Acciones posibles** cambiarán en función de la acción que seleccione. Si deja la respuesta predeterminada **Consultar antes de actuar**, tendrá la oportunidad de seleccionar cualquiera de las acciones posibles cada vez que se detecte un virus. Si selecciona una de las otras opciones en la lista de desplegable, esa opción se ejecutará automáticamente cada vez que se detecte un virus.

 Si deja seleccionada la opción **Consultar antes de actuar**, deseleccione todas las posibles acciones que no desea dejar al usuario. Deje sólo seleccionadas las casillas de las opciones que desea ofrecer.

 Si selecciona la opción **Mover los archivos infectados automáticamente**, se le pedirá que indique la ubicación y nombre de destino de los archivos.

 Si selecciona la opción **Limpiar los archivos infectados automáticamente**, **Borrar los archivos infectados automáticamente** o **Denegar acceso a los archivos infectados y continuar**, aparecerá un mensaje que describe la opción elegida.

3 Haga clic en **Aplicar** para guardar los cambios efectuados sin cerrar el cuadro de diálogo. Así termina la configuración de la página de propiedades **Acción**.

4 Haga clic en otra pestaña para continuar.

 **Vea la nota**

1 Seleccione la pestaña **Alerta** si desea que VirusScan envíe un mensaje cuando detecte un virus.

2 Seleccione la casilla **Enviar alerta de red** si desea que la alerta se envíe a un servidor de la red. Al hacerlo se activará el botón **Examinar** y podrá buscar la ubicación de destino para la alerta de red. Cuando la haya seleccionado, la ruta de esa ubicación aparecerá en el cuadro de texto.

3 Seleccione la casilla **DMI** para enviar el aviso a aplicaciones de gestión de red o de escritorio que cumplen con la especificación DMI (Interfaz de administración de escritorio).

4 Si ha seleccionado previamente la opción **Consultar antes de actuar** en la pestaña **Acción**, VirusScan necesita saber de qué forma debe avisar cuando detecte un virus: mediante un mensaje en pantalla, con un tono o con ambos. Como opción predeterminada, el mensaje que aparece en el cuadro de texto tiene color gris.

 Para cambiar el mensaje, seleccione la casilla **Mostrar mensaje personalizado** y escriba un nuevo mensaje.

 Para omitir el tono, borre la marca de la casilla **Emitir señal audible**.

5 Haga clic en **Aplicar** para guardar los cambios efectuados sin cerrar el cuadro de diálogo. Así termina la configuración de la página de propiedades **Alerta**.

6 Haga clic en otra pestaña para continuar.

 **Vea la nota**

1. Seleccione la pestaña **Informe** si desea que VirusScan conserve un registro de sus actividades de exploración. Como opción predeterminada, VirusScan crea un archivo de nombre VSHLog.txt, con un tamaño máximo de 100 KB, en el que registra todas las opciones de informe disponibles que aparecen en pantalla. La ubicación predeterminada del archivo de registro es C:\Archivos de programa\Network Associates\McAfee Virus Scan\. Si desea cambiar estas opciones predeterminadas, puede:

   - Borrar la marca de la casilla **Registrar en archivo**, con lo que se interrumpe toda actividad de registro.
   - Escribir un nuevo nombre o ruta de acceso del archivo de texto que se genera. VirusScan sólo generará un archivo de texto sin formato.
   - Haga clic en **Examinar** para seleccionar una ubicación para el archivo.
   - Borrar la marca de la casilla **Limitar tamaño de archivo de registro** para eliminar cualquier límite de tamaño.
   - Cambiar el tamaño máximo del archivo de registro.
   - Borrar la marca de las casillas de cualquiera de los elementos del informe que no esté interesado en ver registrado.

2. Haga clic en **Aplicar** para guardar los cambios efectuados sin cerrar el cuadro de diálogo. Así termina la configuración de la página de propiedades **Informe**.
3. Haga clic en otra pestaña para continuar.

Vea la nota

1 Seleccione la pestaña **Exclusión** para especificar carpetas que deben quedar excluidas de la exploración en busca de virus. Como opción predeterminada, VirusScan no explora los archivos de la carpeta Papelera de reciclaje.

 Seleccione la opción **Agregar** para especificar una carpeta que deba excluirse. Tiene además la opción de incluir las subcarpetas y especificar si la exclusión es para las exploraciones de archivos o la exploración de sector de arranque.

 Seleccione **Editar** para modificar las instrucciones relativas a la carpeta seleccionada que ya aparece en la lista de exclusiones.

 Seleccione **Eliminar** para borrar la carpeta seleccionada de la lista.

2 Haga clic en **Aplicar** para guardar los cambios efectuados sin cerrar el cuadro de diálogo. Así termina la configuración de la página de propiedades **Detección**.

3 Haga clic en otra pestaña para continuar.

 **Vea la nota**

Para configurar VirusScan para Windows 95 y Windows 98 de forma que busque virus en los archivos descargados de Internet, incluyendo archivos adjuntos al correo recibido mediante America Online, Eudora Light, Netscape Mail y otros clientes de correo POP-3 o proxy:

1 Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.

2 Seleccione **Programas → McAfee VirusScan → Consola VirusScan → VShield**. Al hacerlo, aparecerán las páginas de propiedades de VShield.

{button ,JI(`vscan4.HLP',`Navigate_to_the_VShield_Configuration_Pages')} Haga clic aquí para ver otras formas de acceder a las páginas de propiedades de VShield.

3 Seleccione **Explorador de elementos descargados** entre los componentes de programa que aparecen en la parte izquierda de la pantalla de configuración de VShield.

Al hacerlo, aparecerán las páginas de propiedades **Explorador de elementos descargados**.

Como opción predeterminada, se muestra en primer lugar la pestaña **Detección**.

4 Haga clic en la casilla **Activar exploración de elementos descargados de Internet**. El resto de la página de propiedades se activará.

Vea la nota

{button ,JI(`vscan4.HLP',`Configure_Download_Detection_Properties')} Pestaña Detección

{button ,JI(`vscan4.HLP',`Configuring_Download_Action_Properties')} Pestaña Acción

{button ,JI(`vscan4.HLP',`Configuring_Download_Alert_Properties')} Pestaña Alerta

{button ,JI(`vscan4.HLP',`Configuring_Download_Report_Properties')} Pestaña Informe

Otros temas asociados

1 Haga clic en un botón de la sección **Archivos adjuntos** de la pantalla para indicar si se deben explorar todos los archivos o sólo los archivos de programa.

   Si selecciona la opción **Sólo archivos de programa**, haga clic en **Extensiones** para ver la lista con las extensiones de nombre de archivo que VirusScan explorará. Puede editar esa lista.

2 Seleccione la casilla **Explorar archivos comprimidos** para incluir en la exploración los archivos creados con los programas LHA, LZEXE, PkLite, PkZip o WinZip. Dado que VirusScan descomprime este tipo de archivos en memoria antes de buscar si tienen o no virus, esta opción puede aumentar el tiempo necesario para la exploración de los archivos descargados.

3 Haga clic en **Aplicar** para guardar los cambios efectuados sin cerrar el cuadro de diálogo. Así termina la configuración de la página de propiedades **Detección**.

4 Haga clic en otra pestaña para continuar

Vea la nota

1 Seleccione la pestaña **Acción** para especificar de qué forma debe actuar VirusScan cuando detecte un virus. Como opción predeterminada, aparece como respuesta seleccionada **Continuar exploración**.

2 Haga clic en la flecha abajo si desea seleccionar una respuesta distinta de VirusScan ante la detección de un virus. Las opciones que aparecen en **Acciones posibles** cambiarán en función de la acción que seleccione. Si deja la respuesta predeterminada **Consultar antes de actuar**, tendrá la oportunidad de seleccionar cualquiera de las acciones posibles cada vez que se detecte un virus. Si selecciona una de las otras opciones en la lista de desplegable, esa opción se ejecutará automáticamente cada vez que se detecte un virus.

 Si deja la respuesta predeterminada, **Continuar exploración,** aparecerá un mensaje que describe la acción elegida.

 Si deja seleccionada la opción **Consultar antes de actuar**, deseleccione todas las posibles acciones que no desea dejar al usuario. Deje sólo seleccionadas las casillas de las opciones que desea ofrecer.

 Si selecciona la opción **Mover los archivos infectados a una carpeta**, se le pedirá que indique la ubicación y nombre de la carpeta de destino de los archivos.

 Si selecciona las opciones **Borrar los archivos infectados** o **Continuar exploración**, aparecerá un mensaje que explica la opción elegida.

3 Si selecciona la opción **Consultar antes de actuar**, VirusScan necesitará saber de qué forma debe avisar que ha detectado un virus: mediante un mensaje en pantalla, con un tono o con ambos. Como opción predeterminada, el mensaje que aparece en el cuadro de texto pasa a tener color gris.

 Para cambiar el mensaje, seleccione la casilla **Mostrar mensaje personalizado** y escriba un nuevo mensaje.

 Para omitir el tono, borre la marca de la casilla **Emitir señal audible**.

4 Haga clic en **Aplicar** para guardar los cambios efectuados sin cerrar el cuadro de diálogo. Así termina la configuración de la página de propiedades **Acción**.

5 Haga clic en otra pestaña para continuar.

 **Vea la nota**

1. Seleccione la pestaña **Alerta** si desea que VirusScan envíe un mensaje cuando detecte un virus.
2. Seleccione la casilla **Enviar alerta de red** si desea que la alerta se envíe a un servidor de la red. Al hacerlo, se activará el botón **Examinar** y podrá buscar una ubicación de destino para la alerta de red. Una vez seleccionada, la ruta de esa ubicación aparecerá en el cuadro de texto.
3. Haga clic en **Aplicar** para guardar los cambios efectuados sin cerrar el cuadro de diálogo. Así termina la configuración de la página de propiedades **Alerta**.
4. Haga clic en otra pestaña para continuar.

 **Vea la nota**

1. Seleccione la pestaña **Informe** si desea que VirusScan conserve un registro de sus actividades de exploración. Como opción predeterminada, VirusScan crea un archivo de nombre WebInet.txt, con un tamaño máximo de 100 KB, en el que registra todas las opciones de informe disponibles que aparecen en pantalla. La ubicación predeterminada del archivo de registro es C:\Archivos de programa\Network Associates\McAfee Virus Scan\. Si desea cambiar estas opciones predeterminadas, puede:

   - Borrar la marca de la casilla **Registrar en archivo**, con lo que se interrumpe toda actividad de registro.
   - Escribir un nuevo nombre o ruta de acceso del archivo de texto que se genera. VirusScan sólo generará un archivo de texto sin formato.
   - Hacer clic en **Examinar** para seleccionar una ubicación para el archivo.
   - Borrar la marca de la casilla **Limitar tamaño de archivo de registro** para eliminar cualquier límite de tamaño.
   - Cambiar el tamaño máximo del archivo de registro.
   - Borrar la marca de las casillas de cualquiera de los elementos del informe que no esté interesado en ver registrado.
2. Cuando haya terminado la configuración de este componente de programa, y de todos los demás, haga clic en **Aceptar**.
3. Haga clic en **Aplicar** para guardar los cambios efectuados sin cerrar el cuadro de diálogo. Así termina la configuración de la página de propiedades **Informe**.
4. Haga clic en otra pestaña para continuar.

Vea la nota

Para configurar VirusScan de forma que filtre los objetos de Java y ActiveX potencialmente dañinos o para que impida el acceso a sitios Internet peligrosos:

1. Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.
2. Seleccione **Programas → McAfee VirusScan → Consola VirusScan → VShield.** Al hacerlo, aparecerán las páginas de propiedades de VShield.

   {button ,JI(`vscan4.HLP',`Navigate_to_the_VShield_Configuration_Pages')} Haga clic aquí para ver otras formas de acceder a las páginas de propiedades de VShield.
3. Seleccione **Filtro de Internet** entre los componentes de programa que aparecen en la parte izquierda de la pantalla de configuración de VShield.

    Al hacerlo, aparecerán las páginas de configuración de Filtro de Internet.

    Como opción predeterminada, aparece en primer lugar la pestaña **Detección**.
4. Haga clic en la casilla **Activar filtro Java & ActiveX**. Al hacerlo, se activará el resto de la página de propiedades.
5. Configure las propiedades en cada una de las siguientes pestañas.

   {button ,JI(`vscan4.HLP',`Configuring_Internet_Filter_Detection_Properties')} Pestaña Detección

   {button ,JI(`vscan4.HLP',`Configuring_Internet_Filter_Action_Properties')} Pestaña Acción

   {button ,JI(`vscan4.HLP',`Configuring_Internet_Filter_Alert_Properties')} Pestaña Alerta

   {button ,JI(`vscan4.HLP',`Configuring_Internet_Filter_Report_Properties')} Pestaña Informe

 Otros temas asociados

1. Seleccione la casilla **Controles ActiveX** y/o la casilla **Clases Java** para incluirlos en la exploración.
2. Haga clic en el botón **Configurar**, que aparece junto a **Direcciones IP**, si desea prohibir el acceso a una dirección IP de Internet en particular. Si no hay ninguna dirección IP que desee prohibir, borre la marca de la casilla **Direcciones IP que se bloquearán**.
3. Haga clic en el botón **Configurar**, que aparece junto a **Nombres de host de Internet que se bloquearán**, si desea prohibir el acceso a un dominio de Internet determinado. Si no hay ningún dominio de Internet que desee prohibir, borre la marca de la casilla **Nombres de host de Internet que se bloquearán**.
4. Haga clic en **Aplicar** para guardar los cambios efectuados sin cerrar el cuadro de diálogo. Así termina la configuración de la página de propiedades **Detección**.
5. Haga clic en otra pestaña para continuar

 **Vea la nota**

1 Seleccione la pestaña **Acción** para especificar de qué forma debe actuar VirusScan cuando detecte un virus. Como opción predeterminada, aparece como respuesta seleccionada **Consultar antes de actuar**. También tiene la posibilidad, si prefiere que no se le pregunte que acción debe tomarse cada vez que se encuentre un virus en un objeto de ActiveX o Java, de hacer clic en la flecha abajo y seleccionar la opción **Denegar el acceso a los objetos**.

2 Si selecciona la opción **Consultar antes de actuar**, VirusScan necesitará saber cómo debe avisar cuando detecte un virus: mediante un mensaje en pantalla, con un tono o con ambos. Como opción predeterminada, el mensaje que aparece en el cuadro de texto pasa a tener color gris.

   Para cambiar el mensaje, seleccione la casilla **Mostrar mensaje personalizado** y escriba un nuevo mensaje.

   Para omitir el tono, borre la marca de la casilla **Emitir señal audible**.

3 Haga clic en **Aplicar** para guardar los cambios efectuados sin cerrar el cuadro de diálogo. Así termina la configuración de la página de propiedades **Acción**.

4 Haga clic en otra pestaña para continuar

Vea la nota

1. Seleccione la pestaña **Alerta** si desea que VirusScan envíe un mensaje cuando detecte un virus.
2. Seleccione la casilla **Enviar alerta de red** si desea que la alerta se envíe a un servidor de la red. Al hacerlo, se activará el botón **Examinar** y podrá buscar una ubicación de destino para la alerta de red. Una vez seleccionada, la ruta de esa ubicación aparecerá en el cuadro de texto.
3. Haga clic en **Aplicar** para guardar los cambios efectuados sin cerrar el cuadro de diálogo. Así termina la configuración de la página de propiedades **Alerta**.
4. Haga clic en otra pestaña para continuar.

 **Vea la nota**

1. Seleccione la pestaña **Informe** si desea que VirusScan conserve un registro de sus actividades de exploración. Como opción predeterminada, VirusScan crea un archivo de nombre WebFiltrl.txt, con un tamaño máximo de 100 KB, en el que registra todas las opciones de informe disponibles que aparecen en pantalla. La ubicación predeterminada del archivo de registro es C:\Archivos de programa\Network Associates\McAfee Virus Scan\. Si desea cambiar estas opciones predeterminadas, puede:

   - Borrar la marca de la casilla **Registrar en archivo**, con lo que se interrumpe toda actividad de registro.
   - Escribir un nuevo nombre o ruta de acceso del archivo de texto que se genera. VirusScan sólo generará un archivo de texto sin formato.
   - Hacer clic en **Examinar** para seleccionar una ubicación para el archivo.
   - Borrar la marca de la casilla **Limitar tamaño de archivo de registro** para eliminar cualquier límite de tamaño.
   - Cambiar el tamaño máximo del archivo de registro.
   - Borrar la marca de las casillas de cualquiera de los elementos del informe que no esté interesado en ver registrado.
2. Haga clic en **Aplicar** para guardar los cambios efectuados sin cerrar el cuadro de diálogo. Así termina la configuración de la página de propiedades **Informe**.
3. Haga clic en otra pestaña para continuar.

Vea la nota

Para configurar VShield de forma que queden protegidas mediante contraseña las páginas de configuración que se seleccionen y no puedan hacerse en ellas cambios no autorizados:

1 Seleccione Seguridad entre los componentes de programa que aparecen en la parte izquierda de la pantalla de configuración. Al hacerlo, aparecerán las páginas de configuración de Seguridad. Como opción predeterminada, aparece en primer lugar la pestaña **Contraseña** y está seleccionada la opción **Bloquear sólo opciones seleccionadas**.

Vea la nota

2 Puede seleccionar también la opción Bloquear todas las opciones de la página de propiedades. En ese caso, nadie podrá cambiar ninguna de las opciones seleccionadas en todas las páginas de configuración, sin utilizar previamente la contraseña que indique. Si deja seleccionada la opción Bloquear sólo opciones seleccionadas, puede indicar qué opciones desea proteger mediante contraseña para cada componente de programa: Explorador del sistema, Exploración de correo electrónico, Explorador de elementos descargados y Filtro de Internet.

3 Si desea proteger mediante contraseña alguna o todas las opciones, escriba una contraseña.

4 Vuelva a escribir la contraseña exactamente igual que la escribió anteriormente.

5 Haga clic en Aplicar para guardar su contraseña.

6 Seleccione la pestaña correspondiente al componente de programa que contiene las opciones que desea proteger mediante contraseña. Aparecerá entonces una lista de opciones.

7 Seleccione las páginas que desea proteger mediante contraseña. El símbolo gráfico pasará de un candado abierto a uno cerrado, para indicar que la opción queda ‘‘bloqueada’’.

8 Cuando haya terminado de seleccionar opciones para ese componente de programa, haga clic en Aplicar para guardar los cambios efectuados.

9 Repita los pasos 6 a 8 para cada componente de programa, hasta que termine de seleccionar opciones a proteger.

10 Haga clic en Aceptar.

11 Cuando haya terminado de configurar este componente de programa y los restantes, haga clic en **Aceptar**.

Otros temas asociados

Las "firmas" de los virus, o secuencias de código características, que VirusScan busca sólo suelen aparecer en archivos adjuntos al correo electrónico y no en los propios mensajes de correo. Aunque el código de un virus pudiera aparecer en el texto de un mensaje de correo electrónico, debido quizá a un error en la transmisión del correo, ese virus no podría nunca infectar su equipo ya que el software de correo electrónico transmite los mensajes con formato de texto. Para que la secuencia de código se comporte como un virus es necesario que pueda ejecutarse como un programa o como parte de otro programa.

Para detectar virus incluidos en el correo electrónico:

1 Abra la página correspondiente de propiedades de la Exploración de correo electrónico

Para exploraciones asociadas a accesos

§ Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.

§ Seleccione **Programas → McAfee VirusScan → Iniciador de McAfee VirusScan → Vshield**. Al hacerlo, aparecerán las páginas de propiedades de VShield.

§ Seleccione **Exploración de correo electrónico** en el cuadro de componentes que aparece en la parte izquierda de las páginas de configuración. Al hacerlo, aparecerán las páginas de propiedades asociadas a accesos de la Exploración de correo electrónico.

Para exploraciones requeridas

§ Abra Microsoft Outlook u otro cliente de correo electrónico de Microsoft Exchange.

§ Seleccione **Herramientas → Propiedades de la Exploración de correo electrónico** o haga clic en  , en la barra de herramientas.

§ Al hacerlo, aparecerán las páginas de propiedades de la Exploración de correo electrónico requerida.

2 Seleccione la pestaña **Detección**. Como opción predeterminada, esta será la pestaña activa al acceder las páginas de propiedades **Exploración de correo electrónico** .

3 Seleccione la casilla **Activar la exploración de los archivos adjuntos al correo**.

4 Seleccione el botón que representa el tipo de sistema de correo electrónico que utiliza, MAPI o cc:Mail:

» Si utiliza Lotus cc:Mail 8 seleccione Microsoft Mail (MAPI). Lotus cc:Mail 8 cumple con el estándar MAPI.

» Si utiliza AOL, Eudora Light, Netscape o cualquier otro cliente de correo POP-3 o proxy, utilice el componente de VirusScan **Explorador de elementos descargados**, en lugar del componente **Exploración de correo electrónico**, para configurar las opciones preferidas de exploración en busca de virus.

5 Indique a VirusScan en dónde o con qué frecuencia debe comprobar si hay correo:

» Si utiliza Microsoft Mail (MAPI):

- Haga clic en **Todo el correo nuevo**. para buscar virus en todos los archivos adjuntos al correo que entren en su buzón; o
- Haga clic en **Seleccionar carpeta** para explorar todos los archivos adjuntos a mensajes que se encuentren en una ubicación determinada. A continuación, haga clic en **Examinar** para elegir la carpeta en la que VirusScan debe efectuar la búsqueda.

» Si utiliza Lotus cc:Mail, sólo hay que indicar a VirusScan con qué frecuencia debe explorar los archivos adjuntos al correo electrónico recibido en busca de virus. En el cuadro de texto correspondiente, escriba el número de segundos que VirusScan debe esperar antes de realizar una exploración.

6 Indique a VirusScan qué archivos adjuntos debe explorar:

» Elija la opción **Todos los archivos adjuntos** para que VirusScan busque virus en todos los archivos adjuntos a los mensajes de correo electrónico. Aunque esta opción es la que proporciona la máxima protección, puede afectar al rendimiento de su equipo si recibe gran cantidad de correo electrónico.

» Elija la opción **Sólo archivos de programa** para explorar únicamente aquellos archivos adjuntos que son susceptibles de tener virus.

» Haga clic en **Extensiones** para ver una lista con los tipos de archivo que son susceptibles de tener virus.

» Para cambiar la lista de extensiones de nombre de archivo que utiliza VirusScan uses, vea el apartado Agregar una extensión de archivo de programa

7 Seleccione la casilla de **Archivos comprimidos** si desea que VirusScan busque virus en archivos comprimidos creados con los programas LHA, LZEXE, PkLite, PkZip o WinZip. Dado que VirusScan descomprime estos archivos en memoria antes de realizar la exploración, esta opción puede aumentar el tiempo necesario para realizar la exploración del correo electrónico.

8 Cuando haya terminado:

» Haga clic en **Aplicar** para guardar las opciones de detección elegidas sin salir de la página de propiedades

Exploración de correo electrónico o

Haga clic en **Aceptar** para guardar los cambios efectuados en esta y otras páginas de propiedades y cerrar el cuadro de diálogo Propiedades de VirusScan o

Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar cambio alguno.

Otros temas asociados

Para indicar a VirusScan qué debe hacer con los virus que encuentre incluidos en el correo electrónico:

1 Abra la página correspondiente de propiedades de la Exploración de correo electrónico

Para exploraciones asociadas a accesos	**Para exploraciones requeridas**
§ Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.	§ Abra Microsoft Outlook u otro cliente de correo electrónico de Microsoft Exchange.
§ Seleccione **Programas → McAfee VirusScan → Iniciador de McAfee VirusScan → VShield**. Al hacerlo, aparecerán las páginas de propiedades de VShield.	§ Seleccione **Herramientas → Propiedades de la Exploración de correo electrónico** o haga clic en  , en la barra de herramientas.
§ Seleccione **Exploración de correo electrónico** en el cuadro de componentes que aparece en la parte izquierda de las páginas de configuración. Al hacerlo, aparecerán las páginas de propiedades asociadas a accesos de la Exploración de correo electrónico.	§ Al hacerlo, aparecerán las páginas de propiedades de la Exploración de correo electrónico requerida.

2 Seleccione la pestaña **Acción**.

3 Haga clic en  para seleccionar la acción a tomar. Las opciones son:

 **Consultar antes de actuar**. Cuando se detecta un virus, VirusScan presenta un cuadro de alerta e que pregunta cómo desea tratar el virus detectado. Utilice esta opción si desea decidir individualmente de qué forma quiere tratar cada virus. Si desea actuar con todos los virus de la misma forma y automáticamente, elija otra opción.

 **Mover los archivos infectados automáticamente**. VirusScan mueve todos los archivos adjuntos infectados al archivo de cuarentena que le indique.

 **Limpiar los archivos infectados automáticamente**. Esta opción sólo está disponible en el caso de exploraciones de correo electrónico requeridas. VirusScan tratará de limpiar el virus y le avisará si no puede hacerlo.

 **Borrar los archivos infectados automáticamente**. VirusScan borra los archivos infectados cuando los detecta.

 **Continuar exploración**. VirusScan ignora los archivos infectados y continúa la exploración.

4 Dependiendo de la respuesta seleccionada en el Paso 4, las **Acciones posibles** que aparecen varían:

 Si elige la opción **Consultar antes de actuar**, debe seleccionar qué acciones deben estar disponibles para utilizar cuando se detecte el virus.

- A continuación, seleccione la pestaña **Alerta**. Estará activada la parte inferior de la pantalla, que aparece identificada con el nombre **Si está seleccionado 'Consultar antes de actuar'**. El cuadro de texto muestra el mensaje predeterminado que VirusScan mostrará cuando detecte un virus.
- Seleccione **Mostrar mensaje personalizado** para editar el mensaje.
- Como opción predeterminada, VirusScan emite un tono cuando pregunta que acción debe tomar. Si no desea que se escuche el tono, borre la marca de la casilla **Emitir señal audible**.

 Si elige la opción **Mover los archivos infectados automáticamente**, haga clic en **Examinar** para seleccionar una carpeta de destino para los archivos en cuarentena.

 Si elige las opciones **Limpiar los archivos infectados automáticamente**, **Borrar los archivos infectados automáticamente** o **Continuar exploración**, aparecerá un mensaje que describe la opción elegida.

5 Cuando haya terminado:

 Haga clic en **Aplicar** para guardar las opciones de alerta elegidas sin salir de la página de propiedades **Exploración de correo electrónico** o

 Haga clic en **Aceptar** para guardar los cambios efectuados en esta y otras páginas de propiedades y cerrar el cuadro de diálogo Propiedades de VirusScan o

 Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar cambio alguno.

 Otros temas asociados

VirusScan para Windows 95 y Windows 98 le ofrece tres formas para avisar a otros acerca de los virus que ha encontrado en el correo electrónico. Haga clic en los puntos que aparecen a continuación para saber cómo puede:

{button ,JI(`VScan4.hlp',`Notifying_sender_of_e_mail_infection')} Avisar a la persona que le envío un mensaje con un archivo adjunto infectado

{button ,JI(`VScan4.hlp',`Notifying_othere_mail_users_aboutl_infection')} Avisar a otros usuarios de correo electrónico acerca de un archivo adjunto infectado

{button ,JI(`VScan4.hlp',`Notifying_the_network_administrator_about_infected_e_mail')} Avisar al administrador de la red acerca de un archivo adjunto infectado

Para preparar la respuesta estándar que se enviará a la persona que envió un mensaje con un archivo adjunto infectado:

1 Abra la página de propiedades correspondiente de la Exploración de correo electrónico

Para exploraciones asociadas a accesos	**Para exploraciones requeridas**
§ Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.	§ Abra Microsoft Outlook u otro cliente de correo electrónico de Microsoft Exchange.
§ Seleccione **Programas → McAfee VirusScan → Iniciador de McAfee VirusScan → VShield**. Al hacerlo, aparecerán las páginas de propiedades de VShield.	§ Seleccione **Herramientas → Propiedades de la Exploración de correo electrónico** o haga clic en  , en la barra de herramientas.
§ Seleccione **Exploración de correo electrónico** en el cuadro de componentes que aparece en la parte izquierda de las páginas de configuración. Al hacerlo, aparecerán las páginas de propiedades asociadas a accesos de la Exploración de correo electrónico.	§ Al hacerlo, aparecerán las páginas de propiedades de la Exploración de correo electrónico requerida.

2 Seleccione la pestaña **Alerta**.

3 Utilice la sección **Alerta de correo electrónico** que aparece en la parte central de la pantalla.

4 Seleccione **Enviar mensaje de respuesta al remitente**.

5 Haga clic en **Configurar**. Al hacerlo, aparecerá la pantalla de **Configuración de mensaje de respuesta**.

6 VirusScan selecciona automáticamente como destinatario al remitente del mensaje infectado, e identifica el virus y el archivo infectado en el área que aparece inmediatamente debajo de la línea de asunto.

7 Para enviar una copia de este mensaje a otras personas, escriba una dirección de correo electrónico en el cuadro de texto identificado como **CC:** o haga clic en **CC:** para elegir un destinatario en la libreta de direcciones o el directorio de usuarios de su sistema de correo

8 Escriba un texto adecuado en la sección **Asunto** y en la parte dedicada al mensaje en la pantalla.

9 Haga clic en **Aceptar** para guardar el mensaje. Al hacerlo, volverá a la pestaña **Alerta**.

10 Cuando haya terminado:

 Haga clic en **Aplicar** para guardar las opciones de detección elegidas sin salir de la página de propiedades **Exploración de correo electrónico** o

 Haga clic en **Aceptar** para guardar los cambios efectuados en esta y otras páginas de propiedades y cerrar el cuadro de diálogo Propiedades de VirusScan o

 Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar cambio alguno.

Para preparar un mensaje de aviso para otros usuarios de correo electrónico acerca del archivo adjunto infectado:

1 Abra la página de propiedades correspondiente de la Exploración de correo electrónico

Para exploraciones asociadas a accesos

§ Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.

§ Seleccione **Programas → McAfee VirusScan → Iniciador de McAfee VirusScan → VShield**. Al hacerlo, aparecerán las páginas de propiedades de VShield.

§ Seleccione **Exploración de correo electrónico** en el cuadro de componentes que aparece en la parte izquierda de las páginas de configuración. Al hacerlo, aparecerán las páginas de propiedades asociadas a accesos de la Exploración de correo electrónico.

Para exploraciones requeridas

§ Abra Microsoft Outlook u otro cliente de correo electrónico de Microsoft Exchange.

§ Seleccione **Herramientas → Propiedades de la Exploración de correo electrónico** o haga clic en  , en la barra de herramientas.

§ Al hacerlo, aparecerán las páginas de propiedades de la Exploración de correo electrónico requerida.

2 Seleccione la pestaña **Alerta**.

3 Utilice la sección **Alerta de correo electrónico** que aparece en la parte central de la pantalla.

4 Seleccione **Enviar mensaje de alerta al usuario**.

5 Haga clic en **Configurar**. Al hacerlo, aparecerá la pantalla **Configuración del mensaje de respuesta**.

6 Escriba una dirección de correo electrónico en el cuadro de texto identificado como **A**, o haga clic en el botón **A** y seleccione un destinatario en la libreta de direcciones o el directorio de usuarios del sistema de correo electrónico. Virus identifica el virus y el archivo afectado en la zona que aparece inmediatamente debajo de la línea de asunto.

7 Para enviar una copia de este mensaje a otra persona, escriba una dirección de correo electrónico en el cuadro de texto identificado como **CC:** o haga clic en **CC:** para elegir un destinatario en la libreta de direcciones o el directorio de usuarios del sistema de correo electrónico.

8 Escriba un texto adecuado en la sección de **Asunto** y en la sección de mensaje de la pantalla.

9 Haga clic en **Aceptar** para guardar el mensaje. Al hacerlo, volverá a la pestaña **Alerta**.

10 Cuando haya terminado:

 Haga clic en **Aplicar** para guardar las opciones de detección elegidas sin salir de la página de propiedades **Exploración de correo electrónico** o

 Haga clic en **Aceptar** para guardar los cambios efectuados en esta y otras páginas de propiedades y cerrar el cuadro de diálogo Propiedades de VirusScan o

 Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar cambio alguno.

VirusScan opera conjuntamente con un servidor de red que ejecute el programa NetShield de Network Associates para avisar al administrador de la red cuando se detecte un virus. Este aviso consiste en un formulario de informe o en una ‘‘alerta de red’’ que genera automáticamente VirusScan y envía a una ubicación específica para que las lea NetShield.

1 Abra la página correspondiente de propiedades de la Exploración de correo electrónico

Para exploraciones asociadas a accesos	**Para exploraciones requeridas**
§ Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.	§ Abra Microsoft Outlook u otro cliente de correo electrónico de Microsoft Exchange.
§ Seleccione **Programas → McAfee VirusScan → Iniciador de McAfee VirusScan → VShield**. Al hacerlo, aparecerán las páginas de propiedades de VShield.	§ Seleccione **Herramientas → Propiedades de la Exploración de correo electrónico** o haga clic en  , en la barra de herramientas.
§ Seleccione **Explorador de correo electrónico** en el cuadro de componentes que aparece en la parte izquierda de las páginas de configuración. Al hacerlo, aparecerán las páginas de propiedades asociadas a accesos de la Exploración de correo electrónico.	§ Al hacerlo, aparecerán las páginas de propiedades de la Exploración de correo electrónico requerida.

2 Seleccione la pestaña **Alerta**.

3 Utilice la sección **Alerta de red** que se encuentra en la parte central de la pantalla.

4 Seleccione **Enviar alerta de red**.

5 Haga clic en **Examinar**. Al hacerlo, aparecerá el cuadro de diálogo **Buscar carpeta**.

6 Seleccione la carpeta en la que NetShield debe buscar los mensajes de advertencia.

7 Haga clic en **Aceptar**. Al hacerlo, volverá a la pestaña **Alerta**.

8 Cuando haya terminado:

 Haga clic en **Aplicar** para guardar las opciones de detección que ha elegido sin salir de la página de propiedades **Exploración de correo electrónico** o

 Haga clic en **Aceptar** para guardar los cambios efectuados en esta y otras páginas de propiedades, cerrando el cuadro de diálogo Propiedades de VirusScan o

 Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar cambio alguno.

VirusScan puede registrar las acciones que realiza cuando explora el correo electrónico en busca de archivos adjuntos infectados, además de otros datos útiles para el control de las infecciones. Esta información se guarda en un archivo de texto al cual se puede acceder con cualquier programa estándar de tratamiento de texto. La información existente en el archivo de registro permite conocer el número de archivos que ha examinado VirusScan, determinar qué archivos contenían virus y saber los parámetros de configuración de VirusScan que se utilizaron para detectar y responder a esas infecciones. Es aconsejable, por tanto, activar esta función.

1 Abra la página de propiedades correspondiente de la Exploración de correo electrónico

Para exploraciones asociadas a accesos	**Para exploraciones requeridas**
§ Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.	§ Abra Microsoft Outlook u otro cliente de correo electrónico de Microsoft Exchange.
§ Seleccione **Programas → McAfee VirusScan → Iniciador de McAfee VirusScan → VShield**. Al hacerlo, aparecerán las páginas de propiedades de VShield.	§ Seleccione **Herramientas → Propiedades de la Exploración de correo electrónico** o haga clic en  , en la barra de herramientas.
§ Seleccione **Explorador de correo electrónico** en el cuadro de componentes que aparece en la parte izquierda de las páginas de configuración. Al hacerlo, aparecerán las páginas de propiedades asociadas a accesos de la Exploración de correo electrónico.	§ Al hacerlo, aparecerán las páginas de propiedades de la Exploración de correo electrónico requerida.

2 Seleccione la pestaña **Informe**.

3 Seleccione **Registrar en archivo**. Todas las opciones en pantalla aparecerán activadas. En el cuadro de texto aparece el nombre del archivo de registro de actividades. Como opción predeterminada, el archivo se guarda en la carpeta McAfee VirusScan.

4 Si desea utilizar un nombre de archivo o carpeta distintos, haga clic en **Examinar**. Al hacerlo, aparecerá el cuadro de diálogo **Nombre de archivo del registro de actividad**.

5 Seleccione la carpeta en que desea guardar el archivo de registro:

 Como opción predeterminada, el archivo de registro se denomina **WebEmail.txt**

 Puede cambiar el nombre del archivo escribiendo un nombre nuevo en el cuadro **Nombre de archivo**.

 No cambie la extensión de nombre de archivo (**.txt**) que aparece en el cuadro **Tipo de archivo**.

 Puede seleccionar una nueva carpeta. Si esta nueva carpeta no existe, se le preguntará si desea crearla.

6 Haga clic en **Abrir**. Al hacerlo, volverá a la página **Informe**. La ruta del archivo de registro aparecerá entonces en el cuadro de texto. Cuando VirusScan guarda datos de una operación de exploración en el archivo de registro, el archivo se crea en la ubicación en que se guardó inicialmente. Para ver el archivo de registro, ábralo con cualquier editor de texto estándar, como puede ser el Bloc de notas o WordPad.

7 Para reducir el tamaño del registro de archivo, seleccione la casilla Limitar tamaño de archivo de registro. A continuación, escriba un valor para el tamaño del archivo (en kilobytes) en el cuadro de texto correspondiente.

8 Seleccione las casillas que aparecen junto a cada conjunto de datos que desea que VirusScan recoja y registre.

9 Haga clic en **Aceptar**. Al hacerlo, volverá a la pestaña **Informe**.

10 Cuando haya terminado:

 Haga clic en **Aplicar** para guardar las opciones de detección elegidas sin salir de la página de propiedades **Exploración de correo electrónico** o

 Haga clic en **Aceptar** para guardar los cambios efectuados en esta y otras páginas de propiedades, cerrando el cuadro de diálogo Propiedades de VirusScan o

 Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar cambio alguno.

 Otros temas asociados

El componente Descarga de Internet de VirusScan puede detectar firmas de virus que aparezcan en archivos descargados de Internet. Entre esos archivos se incluyen los archivos adjuntos a mensajes de correo electrónico que se descargan de AOL, Eudora Light, Netscape o de cualquier otro cliente de correo POP-3 o proxy (si utiliza Microsoft Mail o Lotus cc:Mail, para configurar sus preferencias debe utilizar el componente **Explorador de correo electrónico** en vez del componente **Explorador de elementos descargados**).

1 Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.

2 Seleccione **Programas → McAfee VirusScan → Consola VirusScan → VShield**. Al hacerlo, aparecerán las páginas de propiedades de VShield.

{button ,JI(`vscan4.HLP',`Navigate_to_the_VShield_Configuration_Pages')} Haga clic aquí para ver otras formas de acceder a las páginas de propiedades de VShield.

3 Seleccione Explorador de elementos descargados en el cuadro de componentes que aparece en la parte izquierda de las páginas de configuración. Al hacerlo, aparecerán las páginas de propiedades **Explorador de elementos descargados**.

4 Seleccione la casilla **Activar exploración de elementos descargados de Internet**.

5 Seleccione la pestaña Detección. Como opción predeterminada, esta pestaña se activa cuando se entra en las páginas de propiedades **Explorador de elementos descargados**.

6 Indique a VirusScan qué archivos debe explorar:

» Seleccione la opción **Todos los archivos** para que VirusScan busque virus en todos los archivos descargados y en todos los archivos adjuntos a mensajes de correo electrónico recibidos a través de AOL, Eudora Light, Netscape o cualquier otro cliente de correo POP-3 o proxy. Aunque esta opción proporciona la máxima protección, puede afectar al rendimiento de su equipo si recibe gran cantidad de correo electrónico.

» Seleccione la opción **Sólo archivos de programa** para explorar únicamente aquellos archivos adjuntos que tengan más posibilidades de estar infectados con virus.

» Haga clic en **Extensiones** para ver una lista con los tipos de archivos descargados que tiene más posibilidades de estar infectados con virus.

» Para cambiar la lista de extensiones de nombre de archivo que utiliza VirusScan, vea el apartado Agregar una extensión de archivo de programa.

7 Seleccione la casilla de Archivos comprimidos para que VirusScan busque virus en los archivos comprimidos creados con los programas LHA, LZEXE, PkLite, PkZip o WinZip. Dado que VirusScan descomprime estos archivos en memoria antes de explorarlos, esta opción puede aumentar el tiempo necesario para explorar los archivos descargados.

8 Cuando haya terminado:

» Haga clic en **Aplicar** para guardar las opciones de detección elegidas sin salir de la página de propiedades **Explorador de elementos descargados** o

» Haga clic en **Aceptar** para guardar los cambios efectuados en esta y otras páginas de propiedades, cerrando el cuadro de diálogo Propiedades de VirusScan o

» Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar cambio alguno.

» Otros temas asociados

Para indicar a VShield qué debe hacer con los virus que encuentre en archivos descargados:

1 Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.v

2 Seleccione **Programas → McAfee VirusScan → Consola VirusScan → VShield**. Al hacerlo, aparecerán las páginas de propiedades de VShield.

{button ,JI(`vscan4.HLP',`Navigate_to_the_VShield_Configuration_Pages')} Haga clic aquí para ver otras formas de acceder a las páginas de propiedades de VShield.

3 Seleccione el **Explorador de elementos descargados** entre los componentes que aparecen en el cuadro situado en la parte izquierda de las páginas de configuración. Al hacerlo, aparecerán las páginas de propiedades del Explorador de elementos descargados.

4 Seleccione la pestaña **Acción**.

5 Haga clic en » para seleccionar la acción a tomar. Las opciones disponibles son:

» **Consultar antes de actuar**. Cuando se detecta un virus, VirusScan presenta un cuadro de alerta en que pregunta cómo desea tratar el virus detectado. Utilice esta opción si desea decidir individualmente de qué forma quiere tratar cada virus. Si desea actuar con todos los virus de la misma forma y automáticamente, elija otra opción.

» **Mover los archivos infectados a una carpeta**. VirusScan mueve todos los archivos adjuntos infectados al archivo de cuarentena que le indique.

» **Borrar los archivos infectados automáticamente**. VirusScan borra los archivos infectados cuando los detecta.

» **Continuar exploración**. VirusScan ignora los archivos infectados y continúa la exploración.

6 Dependiendo de la respuesta seleccionada en el Paso 4, las **Acciones posibles** que aparecen varían:

» Si elige la opción **Consultar antes de actuar**, debe seleccionar qué acciones deben estar disponibles para utilizar cuando se detecte el virus.

- A continuación, seleccione la pestaña **Alerta**. Estará activada la parte inferior de la pantalla, que aparece identificada con el nombre **Si está seleccionado 'Consultar antes de actuar'**. El cuadro de texto muestra el mensaje predeterminado que VirusScan mostrará cuando detecte un virus.
- Seleccione **Mostrar mensaje personalizado** para editar el mensaje.
- Como opción predeterminada, VirusScan emite un tono cuando pregunta que acción debe tomar. Si no desea que se escuche el tono, borre la marca de la casilla **Emitir señal audible**.

» Si elige la opción **Mover los archivos infectados a una carpeta**, haga clic en **Examinar** para seleccionar una carpeta de destino para los archivos en cuarentena.

» Si elige las opciones **Borrar los archivos infectados** o **Continuar exploración**, aparecerá un mensaje que describe la opción elegida.

7 Cuando haya terminado:

» Haga clic en **Aplicar** para guardar las opciones de detección elegidas sin salir de la página de propiedades **Explorador de elementos descargados** o

» Haga clic en **Aceptar** para guardar los cambios efectuados en esta y otras páginas de propiedades, cerrando el cuadro de diálogo Propiedades de VirusScan o

» Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar cambio alguno.

» Otros temas asociados

VirusScan opera conjuntamente con un servidor de red que ejecute el programa NetShield de Network Associates para avisar al administrador de la red cuando se detecte un virus. Este aviso consiste en un formulario de informe o en una ‘‘alerta de red’’ que genera automáticamente VirusScan y envía a una ubicación específica para que las lea NetShield.

1 Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.

2 Seleccione **Programas → McAfee VirusScan → Consola VirusScan → VShield**. Al hacerlo, aparecerán las páginas de propiedades de VShield.

{button ,JI(`vscan4.HLP',`Navigate_to_the_VShield_Configuration_Pages')} Haga clic aquí para ver otras formas de acceder a las páginas de propiedades de VShield.

3 Seleccione **Descarga de Internet** en el cuadro de componentes situado en la parte izquierda de las páginas de configuración. Al hacerlo, aparecerán las páginas de propiedades **Explorador de elementos descargados**.

4 Seleccione la pestaña **Alerta**.

5 Seleccione **Enviar alerta de red**.

6 Haga clic en **Examinar**. Al hacerlo, aparecerá el cuadro de diálogo **Buscar carpeta**.

7 Seleccione la carpeta en la que NetShield debe buscar los mensajes de advertencia.

8 Haga clic en **Aceptar**. Al hacerlo, volverá a la pestaña **Alerta**.

9 Cuando haya terminado:

» Haga clic en **Aplicar** para guardar las opciones de detección que ha elegido sin salir de la página de propiedades **Explorador de elementos descargados** o

» Haga clic en **Aceptar** para guardar los cambios efectuados en esta y otras páginas de propiedades, cerrando el cuadro de diálogo Propiedades de VirusScan o

» Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar cambio alguno.

» Otros temas asociados

VirusScan puede registrar las acciones que realiza cuando explora los anexos infectados, además de otros datos útiles para el control de las infecciones. Esta información se guarda en un archivo de texto al cual se puede acceder con cualquier programa estándar de tratamiento de texto. La información existente en el archivo de registro permite conocer el número de archivos que ha examinado VirusScan, determinar qué archivos contenían virus y saber los parámetros de configuración de VirusScan que se utilizaron para detectar y responder a esas infecciones. Es aconsejable, por tanto, activar esta función.

1 Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.

2 Seleccione **Programas → McAfee VirusScan → Consola VirusScan → VShield**. Al hacerlo, aparecerán las páginas de propiedades de VShield.

{button ,JI(`vscan4.HLP',`Navigate_to_the_VShield_Configuration_Pages')} Haga clic aquí para ver otras formas de acceder a las páginas de propiedades de VShield.

3 Seleccione **Explorador de elementos descargados** en el cuadro de componentes situado en la parte izquierda de las páginas de configuración. Al hacerlo, aparecerán las páginas de propiedades **Explorador de elementos descargados**.

4 Seleccione la pestaña **Informe**.

5 Seleccione **Registrar en archivo**. Todas las opciones en pantalla aparecerán activadas. En el cuadro de texto aparece el nombre del archivo de registro de actividades. Como opción predeterminada, el archivo se guarda en la carpeta McAfee VirusScan.

6 Si desea utilizar un nombre de archivo o carpeta distintos, haga clic en **Examinar**. Al hacerlo, aparecerá el cuadro de diálogo **Nombre de archivo del registro de actividad**.

7 Seleccione la carpeta en que desea guardar el archivo de registro:

» Como opción predeterminada, el archivo de registro se denomina **Weblnet.txt**

» Puede cambiar el nombre del archivo escribiendo un nombre nuevo en el cuadro **Nombre de archivo**.

» No cambie la extensión de nombre de archivo (**.txt**) que aparece en el cuadro **Tipo de archivo**.

» Puede seleccionar una nueva carpeta. Si esta nueva carpeta no existe, se le preguntará si desea crearla.

8 Haga clic en **Abrir**. Al hacerlo, volverá a la página **Informe**. La ruta del archivo de registro aparecerá entonces en el cuadro de texto. Cuando VirusScan guarda datos de una operación de exploración en el archivo de registro, el archivo se crea en la ubicación en que se guardó inicialmente. Para ver el archivo de registro, ábralo con cualquier editor de texto estándar, como puede ser el Bloc de notas o WordPad.

9 Para reducir el tamaño del registro de archivo, seleccione la casilla Limitar tamaño de archivo de registro. A continuación, escriba un valor para el tamaño del archivo (en kilobytes) en el cuadro de texto correspondiente.

10 Seleccione las casillas que aparecen junto a cada conjunto de datos que desea que VirusScan recoja y registre.

11 Haga clic en **Aceptar**. Al hacerlo, volverá a la pestaña **Informe**.

12 Cuando haya terminado:

» Haga clic en **Aplicar** para guardar las opciones de detección elegidas sin salir de la página de propiedades **Explorador de elementos descargados** o

» Haga clic en **Aceptar** para guardar los cambios efectuados en esta y otras páginas de propiedades, cerrando el cuadro de diálogo Propiedades de VirusScan o

» Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar cambio alguno.

» Otros temas asociados

Las clases de Java y los controles de ActiveX son programas pequeños y de uso específico escritos en el lenguaje de programación Java, desarrollado por Sun Microsystems, o desarrollados con la tecnología ActiveX de Microsoft. Estos programas u "objetos" se utilizan a menudo como componentes para crear programas de mayor tamaño piezas. o sirven para dotar de nuevas funciones a programas ya existentes. Muchos sitios web utilizan clases de Java o controles de ActiveX para incluir elementos animados en formularios, para ejecutar consultas y para manipular datos.

Ambas tecnologías incluyen sistemas de seguridad diseñados para proteger al usuario de pérdidas de datos y otras clases de daños. Sin embargo, un programador puede lograr utilizar las características de Java o ActiveX para conocer detalles acerca del contenido real del disco duro o para dañar los datos que contiene. VirusScan para Windows 95 y Windows 98 incluye una base de datos con clases y controles que se sabe que son dañinos, y puede impedir que actúen.

Para explorar los objetos de Java o ActiveX que puede encontrar al visitar un sitio web:

1 Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.

2 Seleccione **Programas → McAfee VirusScan → Consola VirusScan → VShield.** Al hacerlo, aparecerán las páginas de propiedades de VShield.

{button ,JI(`vscan4.HLP',`Navigate_to_the_VShield_Configuration_Pages')} Haga clic aquí para ver otras formas de acceder a las páginas de propiedades de VShield.

3 Seleccione Filtro de Internet en el cuadro de componentes situado en la parte izquierda de las páginas de configuración. Al hacerlo, aparecerán las páginas de propiedades **Filtro de Internet**.

4 Seleccione la casilla Activar los filtros Java & ActiveX.

5 Indique a VirusScan qué objetos debe explorar.

» Seleccione la casilla **Controles ActiveX** para que explore en busca de controles dañinos ActiveX u OCX.

» Seleccione la casilla **Clases Java** para que explore en busca de clases de Java dañinas o de subprogramas escritos en Java.

6 Cuando haya terminado:

» Haga clic en **Aplicar** para guardar las opciones de detección elegidas sin salir de la página de propiedades **Filtro de Internet** o

» Haga clic en **Aceptar** para guardar los cambios efectuados en esta y otras páginas de propiedades, cerrando el cuadro de diálogo Propiedades de VirusScan o

» Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar cambio alguno.

» Otros temas asociados

VirusScan ofrece varias posibilidades de actuación cuando encuentra objetos potencialmente dañinos:

1 Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.

2 Seleccione **Programas → McAfee VirusScan → Consola VirusScan → VShield.** Al hacerlo, aparecerán las páginas de propiedades de VShield.

{button ,JI(`vscan4.HLP',`Navigate_to_the_VShield_Configuration_Pages')} Haga clic aquí para ver otras formas de acceder a las páginas de propiedades de VShield.

3 Seleccione Filtro de Internet en el cuadro de componentes situado en la parte izquierda de las páginas de configuración. Al hacerlo, aparecerán las páginas de propiedades **Filtro de Internet**.

4 Seleccione la casilla Activar los filtros Java & ActiveX.

5 Haga clic en la pestaña Acción.

6 Haga clic en » para seleccionar la acción a tomar. Las opciones disponibles son:

- § Consultar antes de actuar.
- § Denegar el acceso a los objetos.

7 Si elige la opción **Consultar antes de actuar**, seleccione a continuación la pestaña **Alerta**. La parte inferior de la pantalla, identificada como **Si está seleccionado 'Consultar antes de actuar'**, estará activa. En el cuadro de texto aparecerá el mensaje predeterminado que VirusScan muestra al detectar un virus.

- § Seleccione **Mostrar mensaje personalizado** para editar el mensaje.
- § Como opción predeterminada, VirusScan hace sonar un tono cuando pide que se seleccione la acción a tomar. Si no quiere que suene ese tono, borre la marca de la casilla **Emitir señal audible**.

8 Cuando haya terminado:

» Haga clic en **Aplicar** para guardar las opciones de detección elegidas sin salir de las páginas de propiedades **Filtro de Internet** o

» Haga clic en **Aceptar** para guardar los cambios efectuados en esta y otras páginas de propiedades, cerrando el cuadro de diálogo Propiedades de VirusScan o

» Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar cambio alguno.

» Otros temas asociados

VirusScan opera conjuntamente con un servidor de red que ejecute el programa NetShield de Network Associates para avisar al administrador de la red cuando se detecte un virus. Este aviso consiste en un formulario de informe o en una ‘‘alerta de red’’ que genera automáticamente VirusScan y envía a una ubicación específica para que las lea NetShield.

1 Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.

2 Seleccione **Programas → McAfee VirusScan → Consola VirusScan → VShield**. Al hacerlo, aparecerán las páginas de propiedades de VShield.

{button ,JI(`vscan4.HLP',`Navigate_to_the_VShield_Configuration_Pages')} Haga clic aquí para ver otras formas de aaceder a las páginas de propiedades de VShield.

3 Seleccione **Filtro de Internet** en el cuadro de componentes situado en la parte izquierda de las páginas de configuración. Al hacerlo, aparecerán las páginas de propiedades **Filtro de Internet**.

4 Seleccione la pestaña **Alerta**.

5 Seleccione **Enviar alerta de red**.

6 Haga clic en **Examinar**. Al hacerlo, aparecerá el cuadro de diálogo **Buscar carpeta**.

7 Seleccione la carpeta en la que NetShield debe buscar los mensajes de advertencia.

8 Haga clic en **Aceptar**. Al hacerlo, volverá a la pestaña **Alerta**.

9 Cuando haya terminado:

» Haga clic en **Aplicar** para guardar las opciones de detección que ha elegido sin salir de la página de propiedades **Filtro de Internet** o

» Haga clic en **Aceptar** para guardar los cambios efectuados en esta y otras páginas de propiedades, cerrando el cuadro de diálogo Propiedades de VirusScan o

» Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar cambio alguno.

» Otros temas asociados

VirusScan puede registrar las acciones que realiza cuando encuentra un objeto de Java o ActiveX potencialmente dañino. Esta información se guarda en un archivo de texto que se puede abrir con cualquier programa estándar de tratamiento de texto. La información existente en el archivo de registro permite conocer el número de objetos que ha examinado VirusScan, determinar qué objetos eran potencialmente dañinos y saber los parámetros de configuración de VirusScan que se utilizaron para detectar y responder a esas infecciones. Es aconsejable, por tanto, activar esta función.

1 Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.

2 Seleccione **Programas → McAfee VirusScan → Consola VirusScan → VShield**. Al hacerlo, aparecerán las páginas de propiedades de VShield.

{button ,JI(`vscan4.HLP',`Navigate_to_the_VShield_Configuration_Pages')} Haga clic aquí para ver otras formas de acceder a las páginas de propiedades de VShield.

3 Seleccione Filtro de Internet en el cuadro de componentes situado en la parte izquierda de las páginas de configuración. Al hacerlo, aparecerán las páginas de propiedades **Filtro de Internet**.

4 Seleccione la pestaña Informe.

5 Seleccione Registrar en archivo. Todas las opciones en pantalla aparecerán activadas. En el cuadro de texto aparece el nombre del archivo de registro de actividades. Como opción predeterminada, el archivo se guarda en la carpeta McAfee VirusScan.

6 Si desea utilizar un nombre de archivo o carpeta distintos, haga clic en **Examinar**. Al hacerlo, aparecerá el cuadro de diálogo **Nombre de archivo del registro de actividad**.

7 Seleccione la carpeta en que desea guardar el archivo de registro:

» Como opción predeterminada, el archivo de registro se denomina **WebFiltr.txt**

» Puede cambiar el nombre del archivo escribiendo un nombre nuevo en el cuadro **Nombre de archivo**.

» No cambie la extensión de nombre de archivo (**.txt**) que aparece en el cuadro **Tipo de archivo**.

» Puede seleccionar una nueva carpeta. Si esta nueva carpeta no existe, se le preguntará si desea crearla.

8 Haga clic en **Abrir**. Al hacerlo, volverá a la página **Informe**. La ruta del archivo de registro aparecerá entonces en el cuadro de texto. Cuando VirusScan guarda datos de una operación de exploración en el archivo de registro, el archivo se crea en la ubicación en que se guardó inicialmente. Para ver el archivo de registro, ábralo con cualquier editor de texto estándar, como puede ser el Bloc de notas o WordPad.

9 Para reducir el tamaño del registro de archivo, seleccione la casilla Limitar tamaño de archivo de registro. A continuación, escriba un valor para el tamaño del archivo (en kilobytes) en el cuadro de texto correspondiente.

10 Seleccione las casillas que aparecen junto a cada conjunto de datos que desea que VirusScan recoja y registre.

11 Haga clic en **Aceptar**. Al hacerlo, volverá a la pestaña **Informe**.

12 Cuando haya terminado:

» Haga clic en **Aplicar** para guardar las opciones de detección elegidas sin salir de la página de propiedades **Filtro de Internet** o

» Haga clic en **Aceptar** para guardar los cambios efectuados en esta y otras páginas de propiedades, cerrando el cuadro de diálogo Propiedades de VirusScan o

» Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar cambio alguno.

» Otros temas asociados

Si VirusScan detecta un virus en memoria, realice las siguientes operaciones:

1 Salga de todos los programas y apague el equipo completamente. No use el botón de reinicio ni la combinación de teclas **Ctrl+Alt+Supr** para reiniciar el equipo.

2 Inserte el Disco de emergencia en la unidad de disquete. Vea el apartado, Creación de un disco de emergencia .

3 Encienda el equipo.

4 Siga las instrucciones que irán apareciendo en pantalla y elimine todos los virus encontrados.

 Si aparece el mensaje **Rastros de virus en memoria**, vea la información adicional disponible en el apartado Lista de mensajes de la página web de Network Associates. Seleccione en esa lista **Rastros de virus en memoria**.

 Si VirusScan puede eliminar con éxito todos los virus de la memoria, apague el equipo, extraiga el disquete de emergencia y vuelva a encender su equipo. Recupere el archivo borrado a partir de una copia de seguridad. Para prevenir una nueva infección, explore los disquetes inmediatamente después de insertarlos en la unidad de disquetes.

 Si VirusScan no puede eliminar el virus de la memoria, aparecerá el mensaje **No se pudo eliminar el virus**. Realice una nueva exploración siguiendo las instrucciones que aparecen en el apartado Realización de una exploración clásica requerida o Realización de una exploración avanzada requerida. Seleccione **Borrar los archivos infectados automáticamente** en la pestaña **Acción**.

O

 Realice una exploración desde la línea de comandos del DOS utilizando el comando **SCAN /DEL**.

El Disco de emergencia es un componente esencial de cualquier programa de prevención de virus. Si el sistema se infecta, no se tiene acceso al disco duro o no se puede cargar Windows, el Disco de emergencia le permitirá arrancar su equipo en un entorno limpio.

1 Tenga preparado un disquete de 3.5" (alta densidad) con formato, que incluya ya los archivos de sistema necesarios para arrancar el equipo.

   Hay dos sistemas para dar formato a un disquete de sistema.

   {button ,JI(`vscan4.HLP',`Formatting_a_Diskette_from_the_DOS_Command_Line')} Desde la **Línea de comandos del DOS**.

   {button ,JI(`vscan4.HLP',`Formatting_a_Diskette_from_My_Computer_or_Windows_Explorer')} Desde **Mi PC** o el **Explorador de Windows**

2 Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.

3 Seleccione **Programas → McAfee VirusScan → McAfee Consola VirusScan**. Al hacerlo, aparecerá la pantalla de introducción de McAfee.

4 Haga clic en **Herramientas**. Aparecerá entonces la caja de herramientas.

5 Haga clic en **Disco de emergencia**. Aparecerá la pantalla de la Utilidad de creación del Disco de emergencia de McAfee.

6 Haga clic en **Continuar**. Se le indicará que debe insertar el disquete en la unidad A: de su equipo.

7 Haga clic en **Aceptar**. La utilidad de disco de emergencia explorará el disquete en busca de virus y copiará en él los archivos necesarios para realizar una exploración del sistema en busca de virus. Un cuadro de diálogo le informará cuando haya terminado el proceso.

8 Haga clic en **Aceptar**.

9 Extraiga el disquete de la unidad A:, protéjalo contra escritura y etiquételo como **Disco de emergencia de VirusScan.**

10 Pruebe el Disco de emergencia apagando el sistema y reiniciándolo con el Disco de emergencia insertado en la unidad de disquete.

   - Este reinicio debe hacerse en frío, es decir que debe apagar completamente su sistema antes de reiniciarlo.
   - No utilice el botón **Reiniciar** del menú **Inicio** → **Apagar el sistema**.
   - No utilice el botón de reinicio de su equipo.

Al proteger contra escritura un disquete se impide que los datos que contiene se dañen o sobrescriban inadvertidamente. Además, reduce la vulnerabilidad del disquete a infecciones con virus dado que no aceptará ningún dato adicional mientras esté protegido contra escritura.

Para proteger contra escritura un disquete de 3.5":

1 Sujete el disquete de forma que:

    la flecha que indica la dirección en que debe insertarse el disquete en la unidad de disquetes quede apuntándole.

    el lado que tiene la etiqueta quede en el extremo más alejado de usted.

2 Encuentre un pequeño orificio de forma rectangular en la esquina superior izquierda del disquete, dentro de ese orificio hay una pequeña pestaña de plástico. Si no se ve la pestaña de plástico y el orificio está abierto, el disquete ya está protegido contra escritura.

3 Deslice hacia arriba la pestaña de plástico, hacia el borde del disquete, para dejar abierto el orificio. El disquete quedará así protegido contra escritura.

La pantalla de inicio permite llegar a los componentes principales de VirusScan para Windows 95 y Windows 98, al tiempo que ofrece información importante y sugerencias acerca del estado y configuración del programa y sus componentes.

Para acceder a un componente:

1 Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.

2 Seleccione **Programas → McAfee VirusScan → McAfee Consola VirusScan.** Aparecerá la pantalla de inicio de VirusScan.

3 Haga clic en **Explorar** para configurar y realizar exploraciones requeridas. Vea el apartado Configuración de las propiedades de VirusScan si desea más información.

4 Haga clic en **VShield** para configurar las exploraciones asociadas a accesos. La operación de exploración se produce cuando la inicia un evento y en las condiciones que se seleccionen. Vea el apartado Configuración de las propiedades del explorador del sistema si desea más información.

5 Haga clic en **Planificar** para definir una planificación de exploraciones automáticas. Vea el apartado Planificación de exploraciones requeridas y otras tareas de ejecución automática si desea más información.

6 Haga clic en **Herramientas** para acceder a:

 el Asistente **Enviar a McAfee**, que facilita la notificación a Network Associates cuando se encuentran nuevos virus.

 la utilidad de creación del **Disco de emergencia**. Vea el apartado Creación de un disco de emergencia si desea más información.

 un enlace a la **Biblioteca de documentación técnica y de Información acerca de virus** de Network Associates. Vea el apartado Acceso a información acerca de virus y a la biblioteca de documentación técnica si desea más información.

MAPI (Interfaz de programación de aplicaciones de mensajería)

MAPI es un estándar de Microsoft que regula la forma en que las aplicaciones de comunicaciones transfieren entre ellas datos. Para instalar y trabajar con aplicaciones que cumplen con el estándar MAPI, debe primero configurar Mensajería de Windows, un componente estándar de Windows. Si desea conocer más detalles, consulte la documentación de Microsoft Exchange.

Si ha encontrado algo que sospecha puede tratarse de un virus nuevo o no identificado, envíe el archivo infectado al equipo de emergencia (Anti-Virus Emergency Response Team) de McAfee Labs para su análisis, utilizando para ello el Asistente **Enviar a McAfee**. Tenga en cuenta que Network Associates se reserva el derecho a utilizar la información que nos proporcione de la forma que estime adecuada, sin que al hacerlo incurra en ninguna obligación.

1 Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.

2 Seleccione **Programas → McAfee VirusScan → Iniciador de McAfee VirusScan.** Aparecerá la pantalla de inicio de VirusScan.

3 Haga clic en **Herramientas.** Aparecerá un menú con las herramientas disponibles.

4 Haga clic en **Enviar a McAfee.** Aparecerá el Asistente McAfee Labs A.V.E.R.T.

5 Haga clic en **Siguiente**. Aparecerá una página en la que puede escribir un mensaje al equipo de emergencia (A.V.E.R.T). Si lo desea, incluya sus datos personales de contacto. Esta información, aunque útil, es opcional.

6 Haga clic en **Siguiente**. Aparecerá entonces una lista de elementos a enviar.

7 Haga clic en **Agregar** para seleccionar el archivo o archivos a enviar.

 Otra posibilidad consiste en arrastrar los archivos desde **Mi PC** o el **Explorador de Windows** para colocarlos en el cuadro de lista.

 Si desea borrar un archivo de la lista, selecciónelo y haga clic en **Borrar**.

8 Haga clic en Siguiente. Aparecerá la página **Seleccionar las opciones de carga**.

9 Seleccione Eliminar datos del archivo, si desea conservar la confidencialidad de sus datos.

10 Si se encuentra fuera de los Estados Unidos de América, sustituya la dirección predeterminada de correo electrónico por la que corresponda a su zona.

11 Haga clic en Siguiente. Aparecerá la página del subsistema de correo electrónico.

 Si lo requiere la configuración de su sistema, seleccione SMTP y escriba el nombre de su servidor SMTP.

 Seleccione la opción Enviar correo a través de MAPI, si utiliza un servidor de correo que cumpla con el estándar MAPI (como por ejemplo, Microsoft Outlook).

12 Haga clic en **Finalizar** para enviar el archivo.

{button ,JI(`vscan4.HLP',`Reporting_New_Viruses_or_Objects')} Haga clic aquí si desea información adicional para notificaciones acerca de virus nuevos y objetos peligrosos.

Utilice la página del Explorador de elementos descargados para hacer que VirusScan examine todo el correo recibido a través de America Online, Eudora Light, Netscape, Internet Explorer y otras aplicaciones cliente de correo compatibles. Si utiliza VirusScan en su domicilio, los parámetros de configuración de esa página servirán para cubrir las necesidades más habituales de exploración de correo electrónico.

Utilice la página Exploración de correo electrónico para explorar el correo recibido a través de cc:Mail, Microsoft Exchange y otros programas de correo que cumplen con el estándar MAPI. Normalmente, aunque no siempre, estos programas de correo se utilizan para recibir correo a través de una red de área local o en un entorno similar.

Lotus cc:Mail 8 cumple con el estándar MAPI. Las versiones anteriores no.

En cualquier momento puede:

- hacer clic en **Aceptar**, en la parte inferior de la pantalla, para guardar los cambios efectuados y cerrar el cuadro de diálogo o
- hacer clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar los cambios efectuados o
- hacer clic en **Aplicar** para guardar los cambios efectuados sin salir del cuadro de diálogo.

Network Associates no puede garantizar que los archivos .DAT de VirusScan que se incluyen en esta versión son compatibles con versiones anteriores de VirusScan o WebScan.

Network Associates aconseja que utilice una denominación URL del sitio, en lugar de su dirección IP, para agregarlo a la lista de sitios *prohibidos* de VirusScan. Una dirección URL es normalmente más fiable a la hora de controlar la ubicación actual de un sitio en Internet que una dirección IP fija, ya que el sistema servidor de nombres de dominio da acceso a la dirección actual de un sitio, incluso en el caso de que haya cambiado de dirección.

Para poder conectar con Network Associates debe disponer de una cuenta de acceso telefónico o de conexión directa con un proveedor de servicios de Internet. Póngase en contacto con un proveedor de servicios de Internet para obtener más detalles acerca de esas cuentas.

Póngase en contacto directamente con cada fabricante para conocer más detalles acerca de las opciones de acceso con el software cliente FTP (protocolo de transferencia de archivos) y otros sistemas para obtener el software del explorador.

Su acceso a estas actualizaciones tiene las restricciones legales que impongan los términos del acuerdo de mantenimiento que se citan en el archivo README.1ST que acompaña al software y que se describen en detalle en el acuerdo de licencia del software.

Si el componente de programa está activo, el botón tiene la opción **Desactivar**. Si el componente de programa está inactivo, el mismo botón tiene la opción **Activar**.

El uso del mismo botón para activar o desactivar un componente de programa es similar a la operación de selección y borrado de la marca de la casilla **Activar** en la página de propiedades del componente.

Para cambiar las opciones asociadas a un elemento que ya aparece en la lista, selecciónelo y haga clic en **Editar**. Al hacerlo, aparecerá la pantalla **Editar elemento a explorar**.

Para eliminar un elemento de la lista, selecciónelo y haga clic en **Eliminar**.

Otro sistema para acceder a la página **Propiedades de actualización/ampliación automáticas** consiste en seleccionar **AutoUpgrade** o **AutoUpdate** en el cuadro de lista del **Planificador**. A continuación, haga clic en el icono  , en la barra de herramientas.

Hay dos sistemas para copiar una tarea:

1 Seleccione una tarea. A continuación, seleccione en el menú **Edición → Copiar**. A continuación, seleccione en el menú **Edición → Pegar**.

O

2 Seleccione una tarea. A continuación, pulse las teclas **Ctrl + C** del teclado. A continuación, pulse las teclas **Ctrl +V**.

Estas instrucciones no son aplicables a exploraciones requeridas con VirusScan (scan32.exe). Para configurar las exploraciones requeridas, vea el apartado Configuración de las propiedades de VirusScan

Para dar formato al disquete que se usará como Disco de emergencia, utilizando la línea de comandos de DOS:

1 Inserte un disquete en la unidad **A:** del equipo.

2 Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.

3 Seleccione **Programas**.

4 Seleccione **MS-DOS**. Aparecerá la pantalla de línea de comandos de DOS, con el directorio **C:\Windows** como directorio actual.

5 Escriba **FORMAT A:/S /U** y pulse la tecla **Intro**. DOS da formato al disquete y copia en él los archivos de sistema necesarios.

6 Cuando termina la operación de dar formato y vuelve a aparecer el símbolo del sistema **C:\ Windows**, escriba **EXIT** para cerrar la pantalla de línea de comandos de MS-DOS.

Si recibe correo electrónico a través de America Online, Eudora Light, Netscape Mail y otros clientes de correo POP-3 o proxy, debe activar el **Explorador de elementos descargados** si desea explorar los archivos adjuntos al correo.

Algunos clientes de correo de Microsoft Exchange no pueden mostrar los iconos de la barra de herramientas. Sin embargo, las opciones de **Propiedades de la Exploración de correo electrónico** y de **Explorar en busca de virus** siguen estando disponibles en el menú **Herramientas** de la aplicación.

1. Desinstalar VirusScan.
2. Instalar Microsoft Exchange
3. Volver a instalar VirusScan.

El procedimiento de actualización incluye además opciones para la actualización del software VirusScan.

Para dar formato a un disquete que se utilizará como Disco de emergencia, utilizando **Mi PC** o el **Explorador de Windows**:

1. Inserte un disquete en la unidad **A:** de su equipo.
2. Con **Mi PC** o el **Explorador de Windows**, seleccione la unidad **A:**.
3. Haga clic con el botón derecho y seleccione la opción **Dar formato**. Aparecerá el cuadro de diálogo **Formatear**.
4. En la parte **Tipo de formato** del cuadro de diálogo, seleccione **Completo**.
5. En la parte **Otras opciones** del cuadro de diálogo, seleccione **Copiar archivos de sistema**.
6. Haga clic en **Inicio**. Windows dará formato al disquete y copiará en él los archivos de sistema necesarios.

Hay tres formas de llegar a las páginas de configuración de propiedades de VShield.

Desde el programa de inicio de VirusScan:

1. Haga clic en **Inicio,** en la esquina inferior izquierda de la pantalla.
2. Seleccione **Programas → McAfee VirusScan → Consola VirusScan → VShield.** Al hacerlo, aparecerán las páginas de propiedades de VShield.

Desde las páginas de Estado de VShield:

1. Haga clic con el botón derecho en el icono  de la bandeja del sistema, en la esquina inferior derecha de la pantalla (en el mismo lugar en que aparece la hora actual).
2. Seleccione **Estado**. Aparecerá la pantalla de **Estado de VShield**.
3. Haga clic en **Propiedades**. Al hacerlo, aparecerán las páginas de propiedades de VShield.

Desde el menú Propiedades

1. Haga clic con el botón derecho en el icono  de la bandeja del sistema, en la esquina inferior derecha de la pantalla.
2. Seleccione **Propiedades**. Aparecerá entonces un submenú en el que puede seleccionar la página de propiedades que desea ver.

Desde el Planificador:

1. Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.
2. Seleccione **Programas → McAfee VirusScan → Consola VirusScan → Planificar**. Aparecerá la pantalla del Planificador de VirusScan.
3. Seleccione **McAfee VShield** en la lista de tareas.
4. Haga clic en el icono  . Al hacerlo, aparecerán las páginas de propiedades de VShield.

El sector de arranque es la primer división lógica de un disco duro o disquete. El BIOS de su equipo busca en ese sector, inmediatamente después de encender el equipo, los archivos y programas que necesita para iniciar el sistema.

Un virus de arranque se copia a si mismo desde el sector de arranque de una unidad de disco al de otra (por ejemplo, desde un disquete a un disco duro).

Un virus de archivo se incrusta en un programa ejecutable. Cuando se ejecuta el programa, el virus se incrusta en otros programas ejecutables.

Un virus de ocultación se esconde para evitar su detección. Puede ser un virus de arranque o un virus de archivo.

Un virus multipartito actúa al tiempo como un virus de arranque y como un virus de archivo, ya que infecta sectores de arranque de discos y archivos ejecutables.

Los virus mutantes cambian sus firmas de código para evitar ser detectados. Muchos virus mutantes son además virus encriptados.

Los virus encriptados codifican parte de su firma de código para evitar ser detectados. Muchos virus encriptados son además virus mutantes.

Los virus polimórficos actúan de forma parecida a como lo hacen los virus mutantes, aunque cada vez que un virus polimórfico se copia a si mismo, cambia ligeramente su firma de código para evitar ser detectado.

Es un virus escrito en lenguaje de programación de macros o incrustado en las macros que forman parte de los archivos de datos de un programa. Por ejemplo, los archivos de datos de Microsoft Word y Microsoft Excel, así como los archivos de plantillas de esos programas, pueden incluir ese tipo de virus.

Vea el apartado dedicado a la Exploración con el Analizador de macros si desea más información acerca del sistema para evaluar la posibilidad de que una macro de una aplicación de Microsoft Office se trate en realidad de un virus.

Es uno de los métodos estándar para especificar la ubicación de un objeto en Internet. En VirusScan para Windows 95 y Windows 98, los URL se denominan también **Nombres de host** o **Dominios**.

www.nai.com/ ies un ejemplo de URL.

Otro método de localizar un sitio Internet consiste en utilizar su Dirección IP.

Es la dirección Internet del host definida mediante IP (protocolo de Internet). Normalmente se representa en un formato numérico separado por puntos.

128.121.4.5. ies un ejemplo de dirección IP.

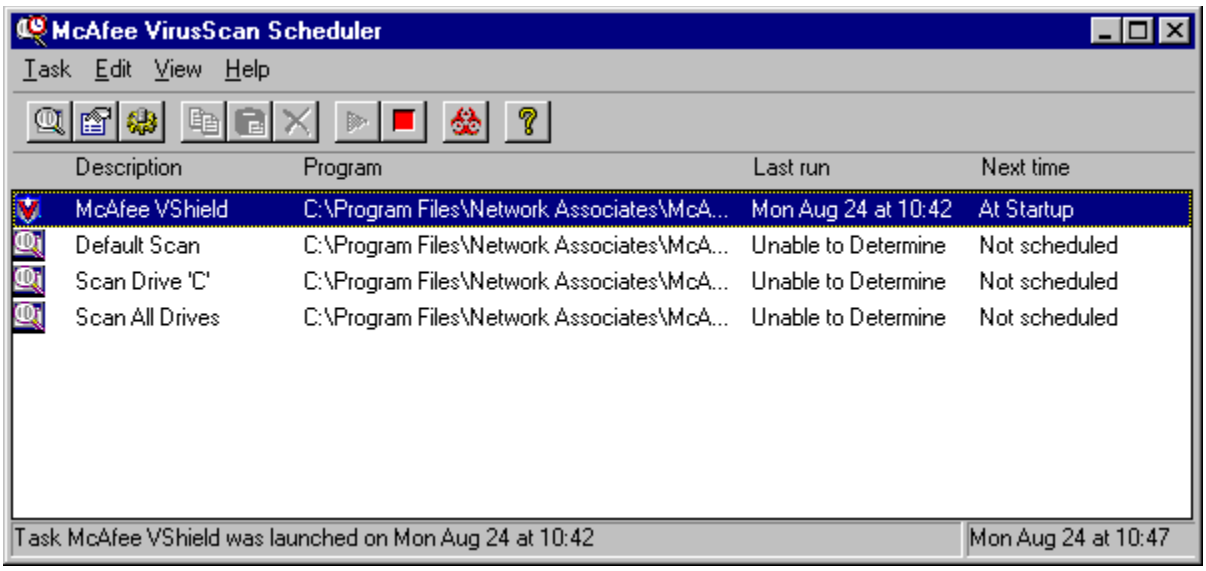
Otro método para localizar un sitio Internet consiste en utilizar su URL.

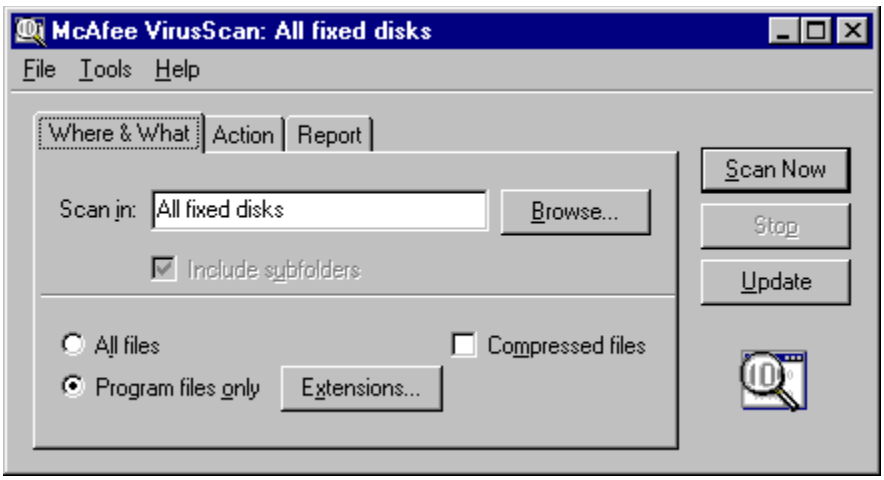
Es el período de tiempo que VirusScan sigue activo en la memoria del equipo. Una sesión de exploración termina cuando sale del programa VirusScan o reinicia el equipo.

Son las secuencias de código características de los virus. VirusScan busca esas cadenas. Pueden encontrase en archivos ejecutables, en archivos descargados de Internet o incrustados en archivos adjuntos a mensajes de correo electrónico. Para que operen como un virus, la secuencia de código debe ser capaz de ejecutarse como un programa o como parte de otro programa.

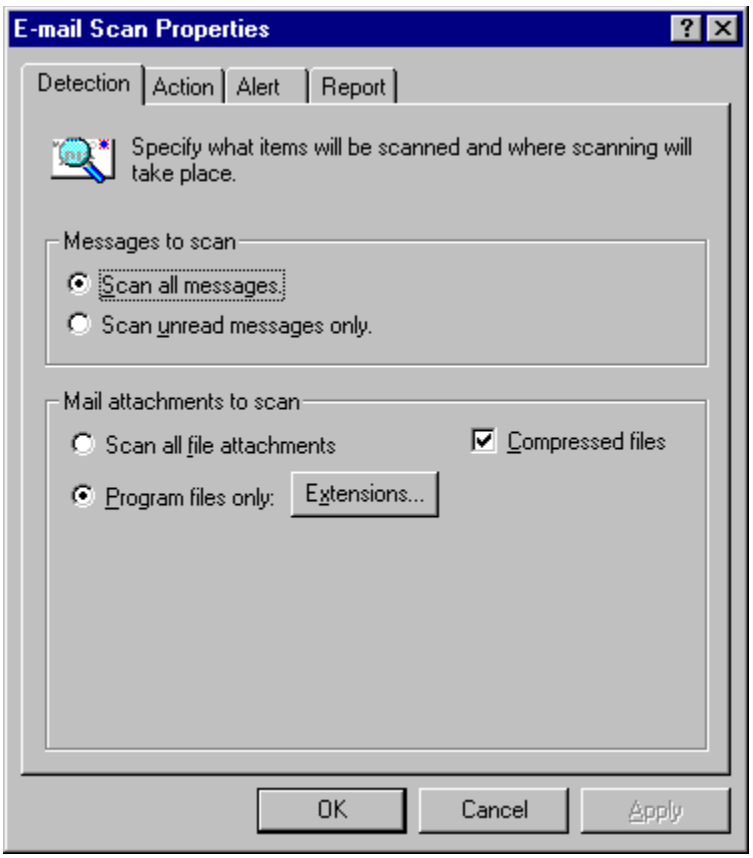
Es un control ActiveX que incluye una interfaz de usuario.


System Scan Properties
System Scan
E-Mail Scan
Download Scan
Internet Filter
Security
Detection
Action
Alert
Report
Exclusion
Define the events that trigger scanning and the kinds of files to scan.
Enable System scan
Scan files on
Run
Create
Copy
Rename
Scan floppies on
Access
Shutdown
What to scan
All files
Compressed files
Program files only
Extensions...
General
System scan can be disabled
Show icon in the Taskbar
Macro Hunter...
Wizard...
OK
Cancel
Apply


McAfee VirusScan Scheduler
Task Edit View Help
Description Program Last run Next time
McAfee VShield C:\Program Files\Network Associates\McA... Mon Aug 24 at 10:42 At Startup
Default Scan C:\Program Files\Network Associates\McA... Unable to Determine Not scheduled
Scan Drive 'C' C:\Program Files\Network Associates\McA... Unable to Determine Not scheduled
Scan All Drives C:\Program Files\Network Associates\McA... Unable to Determine Not scheduled
Task McAfee VShield was launched on Mon Aug 24 at 10:42
Mon Aug 24 at 10:47


McAfee VirusScan: All fixed disks
File
Tools
Help
Where & What
Action
Report
Scan in:
All fixed disks
Browse...
Include subfolders
All files
Compressed files
Program files only
Extensions...
Scan Now
Stop
Update


Scan
VShield
Schedule
Tools
VirusScan
MCAFEE
Update
Since Last
Update


E-mail Scan Properties
Detection
Action
Alert
Report
Specify what items will be scanned and where scanning will take place.
Messages to scan
Scan all messages
Scan unread messages only.
Mail attachments to scan
Scan all file attachments
Compressed files
Program files only:
Extensions...
OK
Cancel
Apply

 Seleccione una carpeta. A continuación, haga clic en **Aceptar**.

 Seleccione una carpeta. A continuación, haga clic en **Aceptar**.

 Haga clic en **Cancelar** para interrumpir este proceso.

 Haga clic en **Cancelar** para interrumpir este proceso.

 Escriba su contraseña y haga clic en **Aceptar**.

 Escriba su contraseña y haga clic en **Aceptar**.

 Haga clic en este botón para cerrar el cuadro de diálogo sin iniciar una sesión.

 Utilice esta pantalla para crear un registro con las actividades de exploración. Haga clic con el botón derecho en cualquiera de las opciones para ver información adicional.

 Seleccione esta casilla para activar el registro de actividades. A continuación, haga clic en **Examinar** para seleccionar un archivo para el registro. Una vez seleccionado, la ruta del archivo aparecerá en el cuadro de texto. Entonces, puede fijar el tamaño máximo del archivo de registro.

 Seleccione la casilla **Registrar en archivo**, que aparece arriba, para activar el registro de actividades. A continuación, haga clic en **Examinar** para seleccionar un archivo para el registro. Una vez seleccionado, la ruta del archivo aparecerá en este cuadro de texto.

 Haga clic en este botón para seleccionar el archivo en el que se creará el registro. Cuando lo seleccione, la ruta del archivo de registro aparecerá en el cuadro de texto.

 Seleccione esta casilla si desea limitar el tamaño del archivo de registro. A continuación, en el cuadro de texto, escriba el tamaño máximo, en kilobytes, del archivo de registro. Puede utilizar

 para seleccionar el número de kilobytes o escribir un número utilizando el teclado.

Borre la marca de esta casilla para desactivar la limitación de tamaño del archivo de registro.

 Escriba el tamaño máximo, en kilobytes, del archivo de registro. Puede utilizar
 para seleccionar el número de kilobytes o escribir un número utilizando el teclado.

 Escriba el tamaño máximo, en kilobytes, del archivo de registro. Puede utilizar
 para seleccionar el número de kilobytes o escribir un número utilizando el teclado.

 Seleccione cualquiera o todas estas casillas para registrar la información asociada a ellas en su archivo de registro.

 Seleccione esta casilla para registrar los nombres de las variedades de virus que se hayan encontrado durante una sesión de exploración y el número de veces que se ha encontrado cada una de ellas.

Borre la marca de esta casilla para desactivar el registro de los tipos de virus.

 Seleccione esta casilla para registrar el número de archivos infectados que se han limpiado durante una sesión de exploración. Borre la marca de esta casilla para desactivar el registro de virus limpiados.

 Seleccione esta casilla para registrar el número de archivos infectados que se han borrado durante una sesión de exploración. Borre la marca de esta casilla para desactivar el registro de archivos infectados borrados.

 Seleccione esta casilla para registrar el número de archivos infectados que se han movido a un directorio de cuarentena durante una sesión de exploración.

Borre la marca de esta casilla para desactivar el registro de archivos infectados que han cambiado de ubicación.

 Seleccione esta casilla para registrar los parámetros de configuración elegidos para esta sesión de exploración. Borre la marca de esta casilla para desactivar el registro de los parámetros de configuración de la sesión.

 Seleccione esta casilla para crear un resumen de las acciones tomadas durante esta sesión de exploración, resumen en el que se incluyen:

- El número de archivos explorados en busca de virus.
- El número de archivos infectados limpiados.
- El número de archivos infectados borrados.
- El número de archivos infectados movidos.
- Otra información acerca de las opciones de configuración usadas.

Borre la marca de esta casilla para desactivar el registro de la información de resumen de la sesión.

 Seleccione esta casilla para registrar la fecha y hora en que comenzó la sesión de exploración.
Borre la marca de esta casilla para desactivar el registro de la fecha y hora.

 Seleccione esta casilla para registrar el nombre del usuario que realizó la exploración.
Borre la marca de esta casilla para desactivar el registro del nombre del usuario.

 Activa la actividad de registro, crea un archivo de registro y especifica su tamaño máximo.

 Utilice esta pantalla para excluir de la exploración determinados objetos, como archivos, carpetas y unidades de disco. Utilice los botones situados en la parte inferior de la pantalla para **Agregar** objetos adicionales a la lista; **Editar** objetos que ya están en la lista y **Eliminar** elementos de la lista.

 Este cuadro muestra los archivos , carpetas y unidades de disco que se excluyen de la exploración en busca de virus. Para agregar elementos a esa lista se usa el cuadro de diálogo **Agregar Excluir elemento**, que aparece al hacer clic en **Agregar**, en la parte inferior de la pantalla. En el cuadro que aparece a continuación se muestra información acerca del elemento, entre la que se incluye su **nombre**; si también están excluidos o no sus **subcarpetas**; y si el elemento está excluido **de** la exploración de archivos, la exploración del sector de arranque o de ambas.

 Este cuadro muestra los archivos , carpetas y unidades de disco que se excluyen de la exploración en busca de virus. Para agregar elementos a esa lista se usa el cuadro de diálogo **Agregar Excluir elemento**, que aparece al hacer clic en **Agregar**, en la parte inferior de la pantalla. En el cuadro que aparece a continuación se muestra información acerca del elemento, entre la que se incluye su **nombre**; si también están excluidos o no sus **subcarpetas**; y si el elemento está excluido **de** la exploración de archivos, la exploración del sector de arranque o de ambas.

 Este cuadro muestra los archivos , carpetas y unidades de disco que se excluyen de la exploración en busca de virus. Para agregar elementos a esa lista se usa el cuadro de diálogo **Agregar Excluir elemento**, que aparece al hacer clic en **Agregar**, en la parte inferior de la pantalla. En el cuadro que aparece a continuación se muestra información acerca del elemento, entre la que se incluye su **nombre**; si también están excluidos o no sus **subcarpetas**; y si el elemento está excluido **de** la exploración de archivos, la exploración del sector de arranque o de ambas.

 Este cuadro muestra los archivos , carpetas y unidades de disco que se excluyen de la exploración en busca de virus. Para agregar elementos a esa lista se usa el cuadro de diálogo **Agregar Excluir elemento**, que aparece al hacer clic en **Agregar**, en la parte inferior de la pantalla. En el cuadro que aparece a continuación se muestra información acerca del elemento, entre la que se incluye su **nombre**; si también están excluidos o no sus **subcarpetas**; y si el elemento está excluido **de** la exploración de archivos, la exploración del sector de arranque o de ambas.

 Haga clic en este botón para abrir el cuadro de diálogo **Agregar Excluir elemento**.

 Haga clic en este botón para abrir el cuadro de diálogo **Abrir Excluir elemento**.

 Haga clic en este botón para borrar el elemento seleccionado en la lista de elementos excluidos, que aparece arriba.

 Dependiendo de la frecuencia seleccionada en la parte **Ejecutar** de la pantalla, esta parte de la pantalla muestra las opciones de reloj y calendario entre las que puede elegir. Escriba la hora, minutos, día del mes y año, que desee. Los nombres de los meses se pueden seleccionar en una lista desplegable. Los nombres de los días se pueden seleccionar en listas desplegables o seleccionarlos al hacer clic en los botones correspondientes.

 Haga clic en este botón para buscar y seleccionar el archivo del programa de exploración, Scan32.exe. Una vez seleccionado, la ruta del archivo aparecerá en el cuadro de texto.

 Haga clic en este botón para buscar y seleccionar la carpeta que contiene el archivo del programa de exploración, Scan32.exe. Una vez seleccionada, la ruta del archivo aparecerá en el cuadro de texto.

 Haga clic en este botón para configurar la tarea.

 Haga clic en este botón para realizar ahora la tarea seleccionada, basándose en las propiedades y opciones de configuración seleccionadas.

- Si seleccionó la casilla **Iniciar automáticamente** en la página de propiedades de Detección de VirusScan, la exploración comenzará inmediatamente (si desea más detalles, vea el tema de Ayuda **Configuración de las propiedades de detección requerida de VirusScan**).
- Si no seleccionó la casilla **Iniciar automáticamente**, aparecerá la pantalla de inicio de exploración requerida. Desde esa pantalla puede iniciar la exploración.

 Haga clic en este botón para detener la exploración en curso.

 El programa se puede ejecutar en una ventana normal, en una ventana maximizada o en una ventana minimizada. Haga clic en  para seleccionar una de estas opciones.

 Muestra la descripción de la tarea seleccionada. Para cambiar la descripción, edite el contenido del cuadro de texto y haga clic en **Aplicar**. Haga clic en **Aceptar** para ver cambiar la descripción en la pantalla del **Planificador**.

 Utilice este cuadro de texto para especificar parámetros adicionales que desea aplicar a la ejecución del archivo. Este cuadro puede quedar vacío.

 Esta ventana muestra la ruta del archivo del programa de exploración, Scan32.exe. Si ha instalado VirusScan para Windows 95 y Windows 98 en una ubicación distinta a la predeterminada para la instalación, haga clic en **Examinar** para buscar y seleccionar el archivo.

 Esta ventana muestra la ruta del archivo del programa de exploración, Scan32.exe. Si ha instalado VirusScan para Windows 95 y Windows 98 en una ubicación distinta a la predeterminada para la instalación, haga clic en **Examinar** para buscar y seleccionar la carpeta que contiene el archivo Scan32.exe.

 Haga clic en este botón para activar **VShield**, el componente de exploración asociada a accesos

 Haga clic en este botón para desactivar **VShield**, el componente de exploración asociada a accesos

Haga clic en este botón para definir una contraseña que protegerá las opciones de actualización (Actualizar y Ampliar).

 Seleccione esta casilla para activar la planificación de la tarea seleccionada en la pantalla del **Planificador**.

 Seleccione este botón si desea que la exploración se efectúe sólo una vez. La parte **Iniciar a** de la pantalla le permite fijar la fecha y hora de comienzo de la exploración.

 Seleccione este botón si desea que la exploración se efectúe cada hora. La parte **Iniciar a** de la pantalla le permite fijar los minutos a que debe comenzar la exploración.

 Seleccione este botón si desea que la exploración se efectúe una vez al día. La parte **Iniciar a** de la pantalla le permite fijar los días de la semana y la hora de comienzo de la exploración.

 Seleccione este botón si desea que la exploración se efectúe una vez al día. La parte **Iniciar a** de la pantalla le permite fijar los días de la semana y la hora de comienzo de la exploración.

 Seleccione este botón si desea que la exploración se efectúe una vez al mes. La parte **Iniciar a** de la pantalla le permite fijar el día del mes y la hora de comienzo de la exploración.

 Especifica la siguiente vez que se ejecutará la tarea, en función de las opciones seleccionadas en la pestaña **Planificar**.

 Especifica la última vez que se ejecutó la tarea.

 Muestra el número de elementos infectados que se identificaron la última vez que se ejecutó la tarea seleccionada.

 Muestra el número de archivos infectados que fueron limpiados la última vez que se ejecutó la tarea seleccionada.

 Muestra el número de archivos infectados que fueron eliminados la última vez que se ejecutó la tarea seleccionada.

 Muestra el número de archivos infectados que fueron movidos a una carpeta de cuarentena la última vez que se ejecutó la tarea seleccionada.

 Muestra el número de archivos que se exploraron la última vez que se ejecutó la tarea seleccionada.

 Seleccione la frecuencia de ejecución de la tarea planificada. Dependiendo del valor que seleccione, la parte **Iniciar a** de la pantalla muestra las opciones correspondientes de reloj y calendario para que las pueda seleccionar.

 Cuando haya terminado de examinar la información acerca del virus, haga clic en este botón para cerrar el cuadro de diálogo.

 Información acerca del virus:

- La parte superior de la pantalla muestra la información de identificación del virus.
- La parte inferior de la pantalla describe sus características.

 Muestra el nombre del virus seleccionado.

 Muestra el nombre del virus seleccionado.

 Muestra los tipos de archivos que pueden ser infectados por este virus.

 Muestra los tipos de archivos que pueden ser infectados por este virus.

 Muestra el número de bytes que ocupa el virus.

 Muestra el número de bytes que ocupa el virus.

 Información acerca del virus:

- La parte superior de la pantalla muestra la información de identificación del virus.
- La parte inferior de la pantalla describe sus características.

- Algunos virus quedan en memoria después de ejecutarse y siguen infectando otros archivos.

 VirusScan selecciona este cuadro si el virus encripta parte de su firma de código para evitar ser detectado.

 VirusScan selecciona este cuadro si el virus evita ser detectado cambiando ligeramente su firma de código cada vez que se copia a si mismo.

 VirusScan selecciona este cuadro si el virus puede ser limpiado.

 VirusScan selecciona este cuadro si el virus está escrito en un lenguaje para macros o está incrustado en macros incluidas en archivos de datos de programas. Por ejemplo, los archivos de datos y los archivos de plantillas de Microsoft Word y Microsoft Excel pueden incluir estos virus.

 Haga clic en este botón para pasar al virus anterior en la lista.

 Haga clic en este botón para pasar al virus siguiente en la lista.

 Pueden ser necesarios unos segundos para que se cargue la lista de virus.

 Haga clic en este botón para cancelar la carga de la lista de virus.

 Escriba en este cuadro el nombre de un virus que desee encontrar en la lista de virus. Cuando haya terminado, haga clic en **Cerrar**.

 Escriba en el cuadro el nombre de un virus que desee encontrar en la lista de virus.

 Después de encontrar un virus determinado, haga clic en este botón para cerrar el cuadro de diálogo .

 Seleccione una carpeta. A continuación, haga clic en **Aceptar**.

 Seleccione una carpeta. A continuación, haga clic en **Aceptar**.

 Haga clic en **Cancelar** para interrumpir este proceso.

 Cuando haya terminado, haga clic en **Aceptar**.

 Muestra la ruta de acceso del último archivo local o de red explorado.

 Muestra el número de archivos locales o de red explorados.

 Muestra el número de archivos locales o de red en los que VShield ha detectado un virus durante la última exploración.

 Muestra el número de archivos infectados que se han limpiado durante la última exploración.

 Muestra el número de archivos locales o de red infectado que se han borrado durante la última exploración.

 Muestra el número de archivos locales o de red infectados que se han movido a una carpeta de cuarentena durante la última exploración.

 Haga clic en este botón para activar o desactivar este componente de programa.

Si el componente se está ejecutando, el botón mostrará la opción **Desactivar**. Si el componente no se ejecuta, el botón mostrará la opción **Activar**.

 Haga clic en este botón para configurar las páginas de propiedades de VShield.

 Haga clic aquí para cerrar este cuadro de diálogo.

 Muestra la dirección IP del último sitio web o Internet examinado.

 Muestra el nombre de la última clase de Java o control de ActiveX examinado.

 Muestra el número de subprogramas de Java examinados durante la última exploración.

 Muestra el número de subprogramas de Java prohibidos durante la última exploración.

 Muestra el número de controles de ActiveX examinados durante la última exploración.

 Muestra el número de controles ActiveX prohibidos durante la última exploración.

 Muestra el número de sitios Internet incluidos en la última exploración.

 Muestra el número de sitios Internet a los que VShield prohibió el acceso en la última exploración.

 Haga clic en este botón para desactivar la actividad de exploración descrita en la pestaña que aparece en la parte superior de esta página.

 Haga clic en este botón para configurar las páginas de propiedades de VShield.

 Haga clic aquí para cerrar este cuadro de diálogo.

 Muestra el último archivo adjunto al correo que se ha examinado durante la última exploración.

 Muestra el número de elementos de correo que se han examinado durante la última exploración.

 Muestra el número de elementos de correo electrónico infectados que se han encontrado durante la última exploración.

 Muestra el número de elementos de correo electrónico infectados que se han borrado durante la última exploración.

 Muestra el número de elementos de correo electrónico infectados que se han movido a una carpeta de cuarentena durante la última exploración.

 Haga clic en este botón para activar o desactivar este componente de programa.
Si el componente se está ejecutando, el botón mostrará la opción **Desactivar**. Si el componente no se ejecuta, el botón mostrará la opción **Activar**

 Haga clic en este botón para configurar las páginas de propiedades de VShield.

 Haga clic en este botón para cerrar este cuadro de diálogo.

 Muestra el último archivo descargado de Internet examinado durante la última exploración.

 Muestra el número de archivos descargados de Internet que se han examinado durante la última exploración.

 Muestra el número de archivos descargados de Internet infectados que se han encontrado durante la última exploración.

 Muestra el número de archivos descargados de Internet infectados que se han borrado durante la última exploración.

 Muestra el número de archivos descargados de Internet infectados que se han movido a una carpeta de cuarentena durante la última exploración.

 Haga clic en este botón para activar o desactivar este componente de programa.

Si el componente se está ejecutando, el botón mostrará la opción **Desactivar**. Si el componente no se ejecuta, el botón mostrará la opción **Activar**

 Haga clic en este botón para configurar las páginas de propiedades de VShield.

 Haga clic en este botón para cerrar este cuadro de diálogo.

 Pueden ser necesarios unos segundos para cargar la lista de virus.

 Haga clic en este botón para cancelar la carga de la lista de virus.

 Escriba el nombre de un virus en este cuadro para encontrarlo en la lista de virus.

 Después de encontrar un virus determinado, haga clic en este botón para cerrar el cuadro de diálogo .

 Muestra el nombre del virus seleccionado.

 Muestra los tipos de archivos que puede infectar este virus.

 Muestra el número de bytes que ocupa el virus.

- Algunos virus permanecen en memoria después de ejecutarse y siguen infectando a otros archivos.

 VirusScan selecciona este cuadro si el virus encripta parte de su firma de código para evitar ser detectado.

 VirusScan selecciona este cuadro si el virus evita la detección cambiando ligeramente su firma de código cada vez que se copia a si mismo.

 VirusScan selecciona este cuadro si es posible limpiar el virus.

 VirusScan selecciona este cuadro si el virus está escrito en un lenguaje para macros o está incrustado en macros incluidas en archivos de datos de un programa. Por ejemplo, los archivos de datos y archivos de plantillas de Microsoft Word y Microsoft Excel pueden incluir este tipo de virus.

 Cuando haya terminado de examinar la información acerca del virus, haga clic en este botón para cerrar el cuadro de diálogo .

 Haga clic en este botón para pasar al virus anterior de la lista.

 Haga clic en este botón para pasar al siguiente virus de la lista.

Haga clic en este botón para cerrar el cuadro de diálogo de la Lista de virus.

Haga clic en este botón para ver información detallada acerca del virus seleccionado.

Haga clic en este botón para encontrar un virus determinado en la lista de virus.

Desplace la pantalla para ver la lista completa de definiciones de los virus incluidos actualmente en los archivos .DAT de su equipo.

Muestra el número de identificación de los archivos de identificación de virus que utiliza su sistema.

Muestra la fecha en que se creó el archivo de definición de virus de su sistema.

Muestra la versión del programa de exploración de virus que utiliza actualmente su sistema.

 Esta pantalla muestra información importante para los usuarios de la versión de evaluación de la Exploración de correo electrónico. Haga clic en **Aceptar** cuando haya terminado de examinar su contenido.

 Esta pantalla muestra información importante para los usuarios de la versión de evaluación de la Exploración de correo electrónico. Haga clic en **Aceptar** cuando haya terminado de examinar su contenido.

 Esta pantalla muestra información importante que identifica su copia de la Exploración de correo electrónico. Haga clic en **Aceptar** cuando haya terminado de examinar su contenido.

 Esta pantalla muestra información importante que identifica su copia de la Exploración de correo electrónico. Haga clic en **Aceptar** cuando haya terminado de examinar su contenido.

 Seleccione este botón para indicar que deben explorarse todos los mensajes de correo electrónico que haya recibido.

 Seleccione este botón para indicar que deben explorarse sólo aquellos mensajes de correo electrónico que aún no se hayan leído.

 Seleccione este botón para indicar que se deben explorar todos los archivos adjuntos al correo electrónico recibido.

 Seleccione este botón para limitar la exploración sólo a los archivos de programa que haya recibido. A continuación, haga clic en **Extensiones** para ver la lista de tipos de archivo que son más susceptibles de tener virus.

 Si ha elegido la opción **Sólo archivos de programa**, haga clic en este botón para ver la lista de tipos de archivo que son más susceptibles de tener virus.

 Seleccione esta casilla para incluir en la exploración los archivos comprimidos con los programas LHA, LZEXE, PkLite, PkZip o WinZip.

Borre la marca de esta casilla para desactivar la exploración de archivos comprimidos.

 Haga clic en
 para seleccionar la acción que debe tomar la Exploración de correo electrónico cuando detecte un virus. Dependiendo de la opción que elija, la sección de **Acciones posibles** mostrará:

- otras opciones adicionales o
- una ventana de texto para escribir información adicional o
- un mensaje que describe el resultado de la opción seleccionada.

 Seleccione esta casilla para tener la oportunidad de limpiar el correo electrónico infectado cuando se encuentre un virus. Cuando está seleccionada, esta opción aparece como un botón en el cuadro de diálogo de Advertencia de correo electrónico.

 Seleccione esta casilla para tener la posibilidad de borrar el correo electrónico infectado cuando la Exploración de correo electrónico lo detecte en su sistema.

Cuando está seleccionada, esta opción aparece como un botón en el cuadro de diálogo de Advertencia de correo electrónico.

 Seleccione esta casilla para tener la posibilidad de ignorar el correo electrónico infectado y continuar con la exploración. Cuando está seleccionada, esta opción aparece como un botón en el cuadro de diálogo de Advertencia de correo electrónico.

 Seleccione esta casilla para tener la posibilidad de detener inmediatamente la exploración.
Cuando está seleccionada, esta opción aparece como un botón en el cuadro de diálogo de Advertencia de correo electrónico.

 Seleccione esta casilla para tener la posibilidad de mover el correo electrónico infectado a un directorio de cuarentena. A continuación, haga clic en **Examinar** para seleccionar la ubicación a la que deben moverse los archivos infectados.

Cuando está seleccionada, esta opción aparece como un botón en el cuadro de diálogo de Advertencia de correo electrónico.

 Haga clic en este botón para seleccionar el archivo de cuarentena al que debe moverse el correo electrónico infectado.

 Haga clic en **Examinar** para seleccionar el archivo de cuarentena al que debe moverse el correo electrónico infectado. Cuando lo haya seleccionado, la ruta del archivo de cuarentena aparecerá en este cuadro.

 Dependiendo de la acción a tomar que seleccione en la lista desplegable, la sección de **Acciones posibles** mostrará:

- opciones adicionales o
- una ventana de texto para escribir información adicional o
- un mensaje que describe el resultado de la acción seleccionada.

Seleccione la casilla **Enviar alerta de red** para alertar al administrador de la red por medio de NetShield cuando se detecte un virus en el correo electrónico recibido. A continuación, haga clic en **Examinar** para seleccionar el servidor que debe recibir el mensaje de centralización de alertas. Cuando lo haya seleccionado, la ruta de la carpeta del mensaje aparecerá en el cuadro de texto.

NetShield es una solución anti-virus para servidores de Network Associates.

Borre la marca de esta casilla para desactivar la alerta de red.

 Seleccione la casilla **Enviar alerta de red** para alertar al administrador de la red por medio de NetShield cuando se detecte un virus en un archivo adjunto al correo electrónico recibido. A continuación, haga clic en **Examinar** para seleccionar el servidor que debe recibir el mensaje de centralización de alertas. Cuando lo haya seleccionado, la ruta de la carpeta del mensaje aparecerá en el cuadro de texto.

NetShield es una solución anti-virus para servidores de Network Associates.

 Haga clic en este botón para abrir el cuadro de diálogo **Buscar carpeta**, en donde puede seleccionar un servidor de destino para los mensajes de centralización de alertas. Cuando lo haya seleccionado, la ruta de la carpeta de mensajes aparecerá en el cuadro de texto.

 Seleccione esta casilla para enviar una notificación aplicaciones de gestión de red o de gestión de escritorio que cumplan con el estándar DMI (Interfaz de administración de escritorio).

 Seleccione esta casilla si desea crear un mensaje personalizado que presentará la Exploración de correo electrónico cuando detecte un virus en el correo electrónico recibido. A continuación, escriba el mensaje en el cuadro de texto, que aparece debajo. Cuando se selecciona esta opción, el mensaje aparecerá como un texto de advertencia en el cuadro de diálogo de Alerta de la Exploración de correo electrónico.

Borre la marca de esta casilla para desactivar el mensaje personalizado.

 Seleccione esta casilla si desea que la Exploración de correo electrónico emita un tono cuando detecte un virus en el correo electrónico recibido.

Borre la marca de esta casilla para desactivar el tono audible.

» Vea el mensaje que presenta la Exploración de correo electrónico cuando detecta un virus o redacte uno nuevo.

 Seleccione esta casilla para activar el registro de actividades para exploraciones de correo electrónico requeridas. A continuación, haga clic en **Examinar** para seleccionar el archivo de registro. Cuando lo haya seleccionado, aparecerá en el cuadro de texto la ruta del archivo. A continuación, puede fijar el tamaño máximo del archivo de registro.

Seleccione la casilla **Registrar en archivo** para activar el registro de actividades para exploraciones de correo electrónico requeridas. A continuación, haga clic en **Examinar** para seleccionar una carpeta en la que se creará el archivo de registro. Cuando la haya seleccionado, aparecerá en este cuadro de texto la ruta del archivo.

 Seleccione esta casilla si desea limitar el tamaño del archivo de registro. A continuación, escriba en el cuadro de texto el tamaño máximo, en kilobytes, del archivo de registro. Puede utilizar la
 para seleccionar el número de kilobytes o escribir el número con el teclado.

Borre la marca de esta casilla para desactivar la limitación de tamaño del archivo de registro.

 Escriba el tamaño máximo del archivo de registro, en kilobytes. Puede usar
 para seleccionar el número de kilobytes o escribir el número con el teclado.

 Escriba el tamaño máximo del archivo de registro, en kilobytes. Puede usar
 para seleccionar el número de kilobytes o escribir el número con el teclado.

 Escriba el tamaño máximo del archivo de registro, en kilobytes. Puede usar
 para seleccionar el número de kilobytes o escribir el número con el teclado.

 Haga clic en este botón para seleccionar el archivo en el que se creará el registro de actividades. Cuando lo haya seleccionado, aparecerá en el cuadro de texto la ruta del archivo.

 Seleccione esta casilla para registrar los nombres de las variedades de virus que se han encontrado durante una sesión de exploración y el número de veces que se ha encontrado cada una de ellas.

Borre la marca de esta casilla para desactivar el registro de las variedades de virus.

 Seleccione esta casilla para registrar el número de archivos infectados que se han limpiado durante una sesión de exploración. Borre la marca de esta casilla para desactivar el registro de virus limpiados.

 Seleccione esta casilla para registrar el número de archivos infectados que se han borrado durante una sesión de exploración. Borre la marca de esta casilla para desactivar el registro de archivos infectados borrados.

 Seleccione esta casilla para registrar el número de archivos infectados que se han movido a un directorio de cuarentena durante una sesión de exploración.

Borre la marca de esta casilla para desactivar el registro de archivos infectados que se han cambiado de ubicación.

 Seleccione esta casilla para registrar los parámetros de configuración seleccionados para esta sesión de exploración requerida. Borre la marca de esta casilla para desactivar el registro de los parámetros de configuración de la sesión.

 Seleccione esta casilla para generar un resumen de las acciones tomadas durante la sesión de exploración. En esa información se incluyen:

- El número de archivos examinados en busca de virus.
- El número de archivos infectados que se han limpiado.
- El número de archivos infectados que se han borrado.
- El número de archivos infectados que se han movido.
- Otros datos acerca de los parámetros de configuración seleccionados.

Borre la marca de esta casilla para desactivar el registro de datos resumen de la sesión.

 Seleccione esta casilla para registrar la fecha y hora a que comenzó la sesión de exploración requerida.
Borre la marca de esta casilla para desactivar el registro de la fecha y hora.

 Seleccione esta casilla para registrar el nombre del usuario que realizó la exploración requerida.
Borre la marca de esta casilla para desactivar el registro del nombre de usuario.

 Escriba la extensión del tipo de archivo que desea explorar en busca de virus. No incluya el punto que normalmente precede a la extensión de nombre de archivo.

 Haga clic en este botón para guardar los cambios efectuados y cerrar el cuadro de diálogo .

 Haga clic en este botón para cerrar el cuadro de diálogo sin guardar cambio alguno de los efectuados.

 Haga clic en este botón para guardar los cambios efectuados y cerrar el cuadro de diálogo.

 Haga clic en este botón para cerrar el cuadro de diálogo sin guardar cambio alguno de los efectuados.

 Haga clic en este botón para abrir el cuadro de diálogo **Agregar extensión de archivos de programa**.

 Haga clic en este botón para borrar de la lista una extensión de archivo de programa seleccionada.

 Haga clic en este botón para recuperar las extensiones de nombre de archivo predeterminadas. Al hacerlo, se borrarán de la lista todas las extensiones que hayan agregado los usuarios.

 Este cuadro muestra una lista con las extensiones de todos los tipos de archivo que se exploran en busca de virus.

- Para agregar una extensión, haga clic en **Agregar**. Aparecerá entonces el cuadro de diálogo **Agregar extensión de archivos de programa**.
- Para borrar una extensión de la lista, selecciónela y haga clic en **Borrar**.
- Para recuperar la lista de extensiones predeterminadas, eliminando las que hayan agregado los usuarios, haga clic en **Predeterminadas**.

 Esta pantalla muestra información detallada de identificación del archivo infectado, su ubicación y sus atributos.

 Describe el tipo de archivo del archivo infectado.

 Muestra la ruta del archivo infectado.

 Muestra el número de bytes del archivo infectado.

 Muestra el nombre DOS del archivo, ocho caracteres más tres caracteres de extensión. Los nombre largos de archivo se truncarán.

 Muestra la fecha en que se creó el archivo infectado.

 Muestra la fecha en que modificó por última vez el archivo infectado.

 Identifica el elemento de correo electrónico infectado por medio de su asunto.

 Identifica el elemento de correo electrónico infectado por medio de su asunto.

 Identifica el elemento adjunto al correo electrónico infectado por medio de su asunto.

 Identifica el archivo adjunto al correo electrónico infectado por medio de su nombre de archivo.

 Identifica el nombre del virus detectado.

 Identifica el nombre del virus detectado.

 Muestra el mensaje predeterminado de la Exploración de correo electrónico o el mensaje alternativo que se haya especificado en la pestaña **Alerta**.

 Haga clic en este botón para ignorar el correo electrónico infectado identificado en esta pantalla y continuar con la exploración.

 Haga clic en este botón para detener las operaciones de exploración inmediatamente.

 Haga clic en este botón para limpiar el correo electrónico infectado identificado en esta pantalla.

 Haga clic en este botón para borrar el correo electrónico infectado identificado en esta pantalla.

 Haga clic en este botón para mover el correo electrónico infectado identificado en esta pantalla a una carpeta de cuarentena.

 Haga clic en este botón para ver información adicional acerca del virus identificado en esta pantalla.

 Indica el estado actual del virus.

 Muestra el nombre del virus que infecta el archivo.

 Muestra los tipos de archivo que pueden ser infectados por este virus.

 Muestra el número de bytes que ocupa el virus.

 VirusScan selecciona esta casilla si el virus permanece en memoria después de ejecutarse y sigue infectando otros archivos.

 VirusScan selecciona esta casilla si el virus encripta parte de su firma de código para evitar ser detectado.

 VirusScan selecciona esta casilla si el virus evita ser detectado cambiando ligeramente su firma de código cada vez que se copia si mismo.

 VirusScan selecciona esta casilla si el virus puede ser limpiado.

 Seleccione esta casilla para activar el registro de VShield. A continuación, haga clic en **Examinar** para seleccionar un archivo para el registro. Cuando lo haya seleccionado, aparecerá en el cuadro de texto la ruta del archivo. Puede fijar un límite de tamaño máximo para el archivo de registro.

Seleccione la casilla **Registrar en archivo**, para activar el registro de VShield. A continuación, haga clic en **Examinar** para seleccionar un archivo para el registro. Cuando lo haya seleccionado, aparecerá en el cuadro de texto la ruta del archivo de registro.

 Haga clic en este botón para seleccionar un archivo para el registro. Cuando lo haya seleccionado, aparecerá en el cuadro de texto la ruta del archivo de registro.

Seleccione esta casilla si desea limitar el tamaño del archivo de registro. A continuación, escriba en el cuadro de el tamaño máximo, en kilobytes, del archivo de registro. Puede usar para seleccionar el número de kilobytes o escribir el número con el teclado.

Borre la marca de esta casilla para desactivar la limitación de tamaño del archivo de registro.

 Escriba el tamaño máximo, en kilobytes, del archivo de registro. Puede usar la
 para seleccionar el número de kilobytes o escribir el número con el teclado.

 Escriba el tamaño máximo, en kilobytes, del archivo de registro. Puede usar
 para seleccionar el número de kilobytes o escribir el número con el teclado.

 Seleccione cualquiera o todas las casillas para registrar la información asociada a cada una de ellas en el archivo de registro.

 Seleccione esta casilla para registrar los nombres de las variedades de virus que VShield ha encontrado durante una sesión de exploración y el número de veces que ha encontrado cada una de ellas.

Borre la marca de esta casilla para desactivar el registro de las variedades de virus.

 Seleccione esta casilla para registrar el número de archivos infectados que VShield ha limpiado durante una sesión de exploración.

Borre la marca de esta casilla para desactivar el registro de virus limpiados.

Seleccione esta casilla para registrar el número de archivos infectados que VShield ha borrado durante una sesión de exploración.

Borre la marca de esta casilla para desactivar el registro de archivos infectados borrados.

 Seleccione esta casilla para registrar el número de archivos infectados que VShield ha movido a un directorio de cuarentena durante una sesión de exploración.

Borre la marca de esta casilla para desactivar el registro de cambio de ubicación de archivos infectados.

 Seleccione esta casilla para registrar los parámetros de configuración seleccionados para esta sesión de exploración. Borre la marca de esta casilla para desactivar el registro de los parámetros de configuración de la sesión.

 Seleccione esta casilla para generar un resumen de las acciones de VShield durante esta sesión de exploración. Esta información incluye:

- El número de archivos examinados en busca de virus.
- El número de archivos infectados que se han limpiado.
- El número de archivos infectados que se han borrado.
- El número de archivos infectados que se han movido.
- Otros datos acerca de los parámetros de configuración de VShield.
- Borre la marca de esta casilla para desactivar el registro de los datos resumen de la sesión.

 Seleccione esta casilla para registrar la fecha y hora en que comenzó la sesión de exploración.
Borre la marca de esta casilla para desactivar el registro de fecha y hora.

 Seleccione esta casilla para registrar el nombre del usuario que realizó la exploración.
Borre la marca de esta casilla para desactivar el registro del nombre del usuario.

Utilice esta pantalla para seleccionar las opciones que desea proteger frente a cambios no autorizados.
Puede seleccionar todas las opciones que aparecen en el cuadro de listo cualquier opción individual. A la izquierda de las páginas protegidas aparecerá .

 Seleccione las páginas de propiedades de VShield que desea proteger frente a cambios no autorizados.
Puede seleccionar todas las opciones que aparecen en el cuadro de listo cualquier opción individual. A la izquierda de las páginas protegidas aparecerá  .

 Haga clic en este botón para guardar los cambios efectuados y cerrar el cuadro de diálogo.

 Haga clic en este botón para cerrar el cuadro de diálogo sin guardar cambio alguno.

 Haga clic en este botón para escribir su contraseña.

 Haga clic en este botón para obtener Ayuda adaptada al contexto usando esta pantalla.

 Escriba una contraseña fácil de recordar.

 Escriba una contraseña fácil de recordar.

 Vuelva a escribir la contraseña exactamente igual que la escribió anteriormente.

 Vuelva a escribir la contraseña exactamente igual que la escribió anteriormente.

 Haga clic en este botón para guardar su contraseña y cerrar el cuadro de diálogo.

 Haga clic en este botón para cerrar el cuadro de diálogo sin guardar su contraseña.

 Después de escribir una contraseña válida, haga clic en este botón para abrir las pantallas del sistema de seguridad de protección mediante contraseña.

 Haga clic en este botón para cerrar el cuadro de diálogo sin guardar los cambios efectuados.

 Escriba la contraseña que controla el acceso al sistema de seguridad de protección mediante contraseña de VShield.

 Escriba la contraseña que controla el acceso al sistema de seguridad de protección mediante contraseña de VShield.

 Haga clic en este botón para guardar los cambios efectuados y cerrar el cuadro de diálogo.

 Haga clic en este botón para cerrar el cuadro de diálogo sin guardar los cambios efectuados.

 Haga clic en este botón para obtener Ayuda adaptada al contexto usando esta pantalla.

 Haga clic en **Examinar** para buscar la unidad de disco o carpeta que desea agregar a la exploración. Cuando la haya seleccionado, la ruta aparecerá en este cuadro de texto.

 Seleccione esta casilla para incluir en la exploración todas las subcarpetas existentes en la ubicación seleccionada para la exploración.

 Haga clic en este botón para buscar la unidad de disco o carpeta que se desea agregar a la exploración. Cuando la haya seleccionado, la ruta aparecerá en el cuadro de texto anterior.

 Seleccione este botón si desea agregar todos los elementos de:

- Mi PC
- todas las unidades de disco desmontables
- todas las unidades de disco fijas
- todas las unidades de disco de red.

A continuación, haga clic en  y seleccione uno de los tipos de elemento disponibles.

 Seleccione este botón si desea seleccionar una unidad de disco o carpeta a agregar a la exploración. A continuación, haga clic en **Examinar** para buscar la unidad de disco o carpeta que desea agregar a la exploración. Cuando la haya seleccionado, la ruta aparecerá en el cuadro de texto.

 Haga clic en
 y seleccione uno de los tipos de elemento disponibles:

- Mi PC
- todas las unidades de disco desmontables
- todas las unidades de disco fijas
- todas las unidades de disco de red.

 Seleccione un elemento a explorar o una unidad de disco/carpeta a explorar.

- Si desea seleccionar un elemento, haga clic en  y seleccione uno de los tipos de elemento disponibles.
- Si desea seleccionar una unidad de disco o carpeta, haga clic en **Examinar** para buscarla. Cuando la haya seleccionado, la ruta aparecerá en el cuadro de texto.
- Si desea incluir las subcarpetas existentes en la ubicación seleccionada, seleccione la casilla **Incluir subcarpetas**.

Cuando haya terminado, haga clic en **Aceptar** para guardar los cambios efectuados y cerrar el cuadro de diálogo.

 Seleccione esta casilla para activar la exploración con el **Analizador de macros**. Esta característica evalúa la probabilidad de que una macro de una de las aplicaciones de Microsoft Office se trate en realidad de un virus.

Utilice la pestaña deslizante para ajustar el umbral de sensibilidad que define una macro como virus.

- Un valor bajo reduce el número de macros que se identifican como virus.
- Un valor alto aumenta el número de macros que se identifican como virus.
- El valor máximo hace que todas las macros de Microsoft Office se consideren virus.

ADVERTENCIA: Si selecciona el valor máximo y tiene seleccionada también la opción **Eliminar todas las macros al limpiar documentos infectados**, se borrarán todas las macros de los documentos de Microsoft Office.

 Utilice la pestaña deslizante para ajustar el umbral de sensibilidad que define una macro como virus.

- Un valor bajo reduce el número de macros que se identifican como virus.
- Un valor alto aumenta el número de macros que se identifican como virus.
- El valor máximo hace que todas las macros de Microsoft Office se consideren virus.

ADVERTENCIA: Si selecciona el valor máximo y tiene seleccionada también la opción **Eliminar todas las macros al limpiar documentos infectados**, se borrarán todas las macros de los documentos de Microsoft Office.

 Utilice la pestaña deslizante para ajustar el umbral de sensibilidad que define una macro como virus.

- Un valor bajo reduce el número de macros que se identifican como virus.
- Un valor alto aumenta el número de macros que se identifican como virus.
- El valor máximo hace que todas las macros de Microsoft Office se consideren virus.

ADVERTENCIA: Si selecciona el valor máximo y tiene seleccionada también la opción **Eliminar todas las macros al limpiar documentos infectados**, se borrarán todas las macros de los documentos de Microsoft Office.

 Utilice la pestaña deslizante para ajustar el umbral de sensibilidad que define una macro como virus.

- Un valor bajo reduce el número de macros que se identifican como virus.
- Un valor alto aumenta el número de macros que se identifican como virus.
- El valor máximo hace que todas las macros de Microsoft Office se consideren virus.

ADVERTENCIA: Si selecciona el valor máximo y tiene seleccionada también la opción **Eliminar todas las macros al limpiar documentos infectados**, se borrarán todas las macros de los documentos de Microsoft Office.

 Utilice la pestaña deslizante para ajustar el umbral de sensibilidad que define una macro como virus.

- Un valor bajo reduce el número de macros que se identifican como virus.
- Un valor alto aumenta el número de macros que se identifican como virus.
- El valor máximo hace que todas las macros de Microsoft Office se consideren virus.

ADVERTENCIA: Si selecciona el valor máximo y tiene seleccionada también la opción **Eliminar todas las macros al limpiar documentos infectados**, se borrarán todas las macros de los documentos de Microsoft Office.

 Seleccione esta casilla para borrar las macros de los documentos de Microsoft Office infectados al tiempo que se limpian. Borre la marca de esta casilla para desactivar el borrado de las macros.

ADVERTENCIA: Si selecciona el valor máximo y tiene seleccionada también la opción **Eliminar todas las macros al limpiar documentos infectados**, se borrarán todas las macros de los documentos de Microsoft Office.

 Utilice la pestaña deslizante para ajustar el umbral de sensibilidad que define una macro como virus.

- Un valor bajo reduce el número de macros que se identifican como virus.
- Un valor alto aumenta el número de macros que se identifican como virus.
- El valor máximo hace que todas las macros de Microsoft Office se consideren virus.

ADVERTENCIA: Si selecciona el valor máximo y tiene seleccionada también la opción **Eliminar todas las macros al limpiar documentos infectados**, se borrarán todas las macros de los documentos de Microsoft Office.

 Haga clic en este botón para guardar los cambios efectuados y cerrar el cuadro de diálogo.

 Haga clic en este botón para cerrar el cuadro de diálogo sin guardar cambio alguno de los efectuados.

 Haga clic en este botón para obtener Ayuda adaptada al contexto usando esta pantalla.

 Utilice esta pantalla para activar y configurar el **Analizador de macros**. Esta característica evalúa la de que una macro de una de las aplicaciones de Microsoft Office se trate en realidad de un virus.

Utilice la pestaña deslizante para ajustar el umbral de sensibilidad que define una macro como virus.

- Un valor bajo reduce el número de macros que se identifican como virus.
- Un valor alto aumenta el número de macros que se identifican como virus.
- El valor máximo hace que todas las macros de Microsoft Office se consideren virus.

ADVERTENCIA: Si selecciona el valor máximo y tiene seleccionada también la opción **Eliminar todas las macros al limpiar documentos infectados**, se borrarán todas las macros de los documentos de Microsoft Office.

 Este cuadro muestra una lista de archivos, carpetas y unidades de disco que se han incluido en la detección en busca de virus. VShield presenta información acerca del elemento, incluyendo su **nombre**; si se incluyen o no su **subcarpetas**; y su tipo.

- Para agregar elementos a la lista, haga clic en **Agregar** (en la parte inferior de la pantalla).
- Para editar elementos, haga clic en **Abrir**.
- Para eliminar un elemento de la lista, seleccione el elemento y haga clic en **Eliminar**.

 Este cuadro muestra una lista de archivos, carpetas y unidades de disco que se han incluido en la detección en busca de virus. VShield presenta información acerca del elemento, incluyendo su **nombre**; si se incluyen o no su **subcarpetas**; y su tipo.

- Para agregar elementos a la lista, haga clic en **Agregar** (en la parte inferior de la pantalla).
- Para editar elementos, haga clic en **Editar**.
- Para eliminar un elemento de la lista, seleccione el elemento y haga clic en **Eliminar**.

 Este cuadro muestra una lista de archivos, carpetas y unidades de disco que se han incluido en la detección en busca de virus. VShield presenta información acerca del elemento, incluyendo su **nombre**; si se incluyen o no su **subcarpetas**; y su tipo.

- Para agregar elementos a la lista, haga clic en **Agregar** (en la parte inferior de la pantalla).
- Para editar elementos, haga clic en **Editar**.
- Para eliminar un elemento de la lista, seleccione el elemento y haga clic en **Eliminar**.

 Este cuadro muestra una lista de archivos, carpetas y unidades de disco que se han incluido en la detección en busca de virus. VShield presenta información acerca del elemento, incluyendo su **nombre**; si se incluyen o no su **subcarpetas**; y su tipo.

- Para agregar elementos a la lista, haga clic en **Agregar** (en la parte inferior de la pantalla).
- Para editar elementos, haga clic en **Editar**.
- Para eliminar un elemento de la lista, seleccione el elemento y haga clic en **Eliminar**.

 Haga clic en este botón para agrega un elemento a la lista anterior.

 Haga clic en este botón para editar un elemento de la lista anterior.

 Haga clic en este botón para borrar un elemento de la lista anterior.

 Elija que archivos desea explorar.

- Elija la opción **Todos los archivos** para examinar cada archivo.
- Elija la opción **Sólo archivos de programa** para examinar sólo aquellos archivos que son más susceptibles de tener un virus. Para ver la lista de archivos que VirusScan considera como más susceptibles, haga clic en **Extensiones**.
- Seleccione la casilla **Archivos comprimidos** para incluir en la exploración los archivos .**zip** y otros tipos de archivos comprimidos.

 Seleccione este botón para especificar la exploración de todos los archivos y de todos los tipos de archivos.

 Seleccione este botón para limitar la exploración sólo a los archivos de programa. A continuación, haga clic en **Extensiones** para ver la lista de tipos de archivo que son más susceptibles de tener un virus.

 Haga clic en este botón para ver la lista de tipos de archivo que es más probable de tener un virus.

 Seleccione esta casilla para incluir en la exploración los archivos comprimidos creados con los programas LHA, LZEXE, PkLite, PkZip o WinZip.

Borre la marca de esta casilla para desactivar la exploración de archivos comprimidos.

 Haga clic en este botón para configurar el **Analizador de macros**. Esta característica evalúa la probabilidad de que una macro de una aplicación de Microsoft Office se trate en realidad de un virus.

Utilice la pestaña deslizante para ajustar el umbral de sensibilidad que define una macro como virus.

- Un valor bajo reduce el número de macros que se identifican como virus.
- Un valor alto aumenta el número de macros que se identifican como virus.
- El valor máximo hace que todas las macros de Microsoft Office se consideren virus.

ADVERTENCIA: Si selecciona el valor máximo y tiene seleccionada también la opción **Eliminar todas las macros al limpiar documentos infectados**, se borrarán todas las macros de los documentos de Microsoft Office.

 Haga clic en
 para seleccionar la acción que debe tomar VShield cuando detecte un virus.
Dependiendo de la opción que elija, la sección de **Acciones posibles** mostrará:

- otras opciones adicionales o
- una ventana de texto para escribir información adicional o
- un mensaje que describe el resultado de la opción seleccionada.

Haga clic con el botón derecho en cualquiera de esas opciones para ver más detalles.

Si selecciona **Consultar antes de actuar** en la lista desplegable, tendrá que indicar en la pestaña **Alerta** si desea o no que VShield genere un mensaje de aviso o haga sonar un tono. Puede crear un mensaje personalizado y/o especificar que se emita un tono audible cuando se detecte un virus.

 Haga clic en
 para seleccionar la acción que debe tomar VShield cuando detecte un virus.
Dependiendo de la opción que elija, la sección de **Acciones posibles** mostrará:

- otras opciones adicionales o
- una ventana de texto para escribir información adicional o
- un mensaje que describe el resultado de la opción seleccionada.

 Dependiendo de la opción que elija, la sección de **Acciones posibles** mostrará:

- otras opciones adicionales o
- una ventana de texto para escribir información adicional o
- un mensaje que describe el resultado de la opción seleccionada.

Haga clic con el botón derecho en cualquiera de esas opciones para ver más detalles.

Si selecciona **Consultar antes de actuar** en la lista desplegable, tendrá que indicar en la pestaña **Alerta** si desea que VShield genere un mensaje de aviso, haga sonar un tono o ambas acciones. Esas selecciones se efectúan en la sección **Si está seleccionado 'Consultar antes de actuar'**, en la parte inferior de la pantalla.

 Haga clic en **Examinar** para seleccionar el archivo de cuarentena en el que se debe guardar el archivo infectado.

 Dependiendo de la opción que elija en la lista desplegable, la sección de **Acciones posibles** mostrará:

- otras opciones adicionales o
- una ventana de texto para escribir información adicional o
- un mensaje que describe el resultado de la opción seleccionada.

 Seleccione esta casilla para tener la oportunidad de limpiar los archivos infectados cuando se detecte un virus. Cuando la haya seleccionado, esta opción aparecerá como un botón en el cuadro de diálogo de Alerta de VShield.

 Seleccione esta casilla para tener la oportunidad de borrar los archivos infectados cuando se detecte un virus. Cuando la haya seleccionado, esta opción aparecerá como un botón en el cuadro de diálogo de Alerta de VShield.

 Seleccione esta casilla para tener la oportunidad de excluir este archivo de la exploración.
Cuando la haya seleccionado, esta opción aparecerá como un botón en el cuadro de diálogo de Alerta de VShield.

 Seleccione esta casilla para tener la oportunidad de mover los archivos infectados a un directorio de cuarentena. A continuación, haga clic **Examinar** para seleccionar la ubicación a la que deben moverse los archivos infectados.

Cuando la haya seleccionado, esta opción aparecerá como un botón en el cuadro de diálogo de Alerta de VShield.

 Seleccione esta casilla para tener la oportunidad de ignorar los archivos infectados y continuar con la exploración. Cuando la haya seleccionado, esta opción aparecerá como un botón en el cuadro de diálogo de Alerta de VShield.

 Seleccione esta casilla para tener la oportunidad de parar la exploración de inmediato.
Cuando la haya seleccionado, esta opción aparecerá como un botón en el cuadro de diálogo de Alerta de VShield.

 Haga clic en este botón para seleccionar el directorio de cuarentena al que enviar el archivo infectado.

 Este cuadro muestra una lista de archivos, carpetas y unidades de disco que se han excluido de la detección en busca de virus. Los elementos se agregan a esa lista mediante el cuadro de diálogo **Agregar Excluir elemento**, que pasa a estar disponible al hacer clic en **Agregar** (en la parte inferior de la pantalla). En el cuadro inferior se presenta información acerca del elemento, entre la que se incluye su **nombre**, si sus **subcarpetas** están excluidas o no y si la exclusión es **de** la exploración de archivos, la exploración del sector de arranque o de ambas.

 Este cuadro muestra una lista de archivos, carpetas y unidades de disco que se han excluido de la detección en busca de virus. Los elementos se agregan a esa lista mediante el cuadro de diálogo **Agregar Excluir elemento**, que pasa a estar disponible al hacer clic en **Agregar** (en la parte inferior de la pantalla). En el cuadro inferior se presenta información acerca del elemento, entre la que se incluye su **nombre**, si sus **subcarpetas** están excluidas o no y si la exclusión es **de** la exploración de archivos, la exploración del sector de arranque o de ambas.

 Este cuadro muestra una lista de archivos, carpetas y unidades de disco que se han excluido de la detección en busca de virus. Los elementos se agregan a esa lista mediante el cuadro de diálogo **Agregar Excluir elemento**, que pasa a estar disponible al hacer clic en **Agregar** (en la parte inferior de la pantalla). En el cuadro inferior se presenta información acerca del elemento, entre la que se incluye su **nombre**, si sus **subcarpetas** están excluidas o no y si la exclusión es **de** la exploración de archivos, la exploración del sector de arranque o de ambas.

 Este cuadro muestra una lista de archivos, carpetas y unidades de disco que se han excluido de la detección en busca de virus. Los elementos se agregan a esa lista mediante el cuadro de diálogo **Agregar Excluir elemento**, que pasa a estar disponible al hacer clic en **Agregar** (en la parte inferior de la pantalla). En el cuadro inferior se presenta información acerca del elemento, entre la que se incluye su **nombre**, si sus **subcarpetas** están excluidas o no y si la exclusión es **de** la exploración de archivos, la exploración de sectores de arranque o de ambas.

 Haga clic en este botón para abrir el cuadro de diálogo **Agregar Excluir elemento**.

 Haga clic en este botón para abrir el cuadro de diálogo **Editar Excluir elemento**.

 Haga clic en este botón para borrar un elemento seleccionado en la lista de elementos excluidos.

Seleccione la casilla **Enviar alerta de red** para alertar al administrador de la red, por medio de NetShield, cuando VShield encuentre un archivo infectado. A continuación, haga clic en **Examinar** para seleccionar el servidor de destino del mensaje de centralización de alertas. Cuando lo haya seleccionado, la ruta de la carpeta de mensajes aparecerá en el cuadro de texto.

NetShield es una solución anti-virus de Network Associates para servidores.

Borre la marca de esta casilla para desactivar la alerta de red.

Seleccione la casilla **Enviar alerta de red** para alertar al administrador de la red, por medio de NetShield, cuando VShield encuentre un archivo infectado. A continuación, haga clic en **Examinar** para seleccionar el servidor de destino del mensaje de centralización de alertas. Cuando lo haya seleccionado, la ruta de la carpeta de mensajes aparecerá en el cuadro de texto.

NetShield es una solución anti-virus de Network Associates para servidores.

 Haga clic en este botón para abrir el cuadro de diálogo **Buscar carpeta**, en el que puede seleccionar el servidor de destino del mensaje de centralización de alertas. Cuando lo haya seleccionado, la ruta de la carpeta de mensajes aparecerá en el cuadro de texto.

 Si ha seleccionado la opción **Consultar antes de actuar** en la pestaña **Acción**, debe indicar si desea que VShield genere un mensaje, emita un tono o ambos.

 Seleccione esta casilla si desea que VShield emita un tono cuando encuentre un archivo infectado. Borre la marca de esta casilla para desactivar el tono audible.

 Seleccione esta casilla si desea preparar un mensaje personalizado que VShield presentará cuando encuentre un virus. A continuación, escriba el mensaje en el cuadro de texto. Cuando la haya seleccionado, esta opción presentará el mensaje personalizado como texto de alerta en el cuadro de diálogo de Alerta de VShield.

Borre la marca de esta casilla para desactivar el mensaje personalizado.

 Vea el mensaje que se mostrará cuando se detecte un virus o redacte uno nuevo.

 Seleccione esta casilla para enviar un aviso a aplicaciones de gestión de red o de gestión de escritorio que cumplen con el estándar DMI (Interfaz de administración de escritorio).

 Haga clic en **Examinar** para seleccionar una carpeta que desea excluir de la exploración en busca de virus. Cuando la haya seleccionado, la ruta de la carpeta aparecerá en este cuadro de texto.

 Haga clic en **Examinar** para seleccionar una carpeta que desea excluir de la exploración en busca de virus. Cuando la haya seleccionado, la ruta de la carpeta aparecerá en este cuadro de texto.

 Haga clic en este botón para seleccionar una carpeta que desea excluir de la exploración en busca de virus. Cuando la haya seleccionado, la ruta de la carpeta aparecerá en este cuadro de texto.

 Seleccione esta casilla para excluir de la exploración en busca de virus todas las subcarpetas asociadas a la carpeta seleccionada para ser excluida.

 Seleccione una o ambas casillas para especificar si el archivo o carpeta indicado debe excluirse de la **Exploración de archivos**, de la **Exploración de sectores de arranque** o de ambas.

 Seleccione esta casilla para excluir el archivo o carpeta anterior solamente de la **Exploración de archivos**.

 Seleccione esta casilla para excluir el archivo o carpeta anterior solamente de la **Exploración de sectores de arranque**.

 Haga clic en este botón para guardar los cambios efectuados y cerrar el cuadro de diálogo.

 Haga clic en este botón para cerrar el cuadro de diálogo sin guardar cambio alguno de los efectuados.

 Haga clic en este botón para guardar los cambios efectuados y cerrar el cuadro de diálogo .

 Haga clic en este botón para cerrar el cuadro de diálogo sin guardar cambio alguno de los efectuados.

 Escriba la extensión del tipo de archivo que desea explorar en busca de virus. No incluya el punto que normalmente precede a las extensiones de nombre de archivo.

 Escriba la extensión del tipo de archivo que desea explorar en busca de virus. No incluya el punto que normalmente precede a las extensiones de nombre de archivo.

 Haga clic en este botón para cerrar el cuadro de diálogo y guardar los cambios efectuados.

 Haga clic en este botón para cerrar el cuadro de diálogo y guardar los cambios efectuados.

 Haga clic en este botón para abrir el cuadro de diálogo **Agregar extensión de archivos de programa**.

 Haga clic en este botón para borrar de la lista la extensión de archivo de programa seleccionada.

 Haga clic en este botón para recuperar las extensiones de nombre de archivo predeterminadas que utiliza VShield. Todas las extensiones que hayan agregado los usuarios, se borrarán de la lista.

 Este cuadro presenta una lista con las extensiones de todos los tipos de archivo que se exploran en busca de virus.

- Para agregar una extensión, haga clic en **Agregar**. Al hacerlo, aparecerá el cuadro de diálogo **Agregar extensión de archivos de programa**.
- Para borra de la lista una extensión, seleccione la extensión y haga clic en **Borrar**.
- Para recuperar la lista de extensiones predeterminadas que utiliza VShield, eliminando las extensiones que han ido agregando los usuarios, haga clic en **Predeterminadas**.

 Este cuadro muestra una lista con las extensiones de todos los tipos de archivo que se exploran en busca de virus.

- Para agregar una extensión, haga clic en **Agregar**. Al hacerlo, aparecerá el cuadro de diálogo **Agregar extensión de archivos de programa**.
- Para borra de la lista una extensión, seleccione la extensión y haga clic en **Borrar**.
- Para recuperar la lista de extensiones predeterminadas que utiliza VShield, eliminando las extensiones que han ido agregando los usuarios, haga clic en **Predeterminadas**.

 Utilice esta pantalla para definir los parámetros de configuración de la exploración en busca de virus. Haga clic con el botón derecho en cualquiera de las opciones si desea ver más detalles.

 Este cuadro muestra una lista de archivos, carpetas y unidades de disco que se han incluido en la detección en busca de virus. Presenta información acerca del elemento, incluyendo su **nombre** y si se incluyen o no sus **subcarpetas**.

- Para agregar elementos a la lista, haga clic en **Agregar** (en la parte inferior de la pantalla).
- Para editar elementos, haga clic en **Editar**.
- Para eliminar un elemento de la lista, seleccione el elemento y haga clic en **Eliminar**.

 Este cuadro muestra una lista de archivos, carpetas y unidades de disco que se han incluido en la detección en busca de virus. Presenta información acerca del elemento, incluyendo su **nombre** y si se incluyen o no sus **subcarpetas**.

- Para agregar elementos a la lista, haga clic en **Agregar** (en la parte inferior de la pantalla).
- Para editar elementos, haga clic en **Editar**.
- Para eliminar un elemento de la lista, seleccione el elemento y haga clic en **Eliminar**.

 Este cuadro muestra una lista de archivos, carpetas y unidades de disco que se han incluido en la detección en busca de virus. Presenta información acerca del elemento, incluyendo su **nombre** y si se incluyen o no sus **subcarpetas**.

- Para agregar elementos a la lista, haga clic en **Agregar** (en la parte inferior de la pantalla).
- Para editar elementos, haga clic en **Editar**.
- Para eliminar un elemento de la lista, seleccione el elemento y haga clic en **Eliminar**.

 Haga clic en este botón para agregar un elemento a la lista anterior.

 Haga clic en este botón para editar un elemento de la lista anterior.

 Haga clic en este botón para borrar un elemento de la lista anterior.

 Elija los archivos que desea explorar. Haga clic con el botón derecho en cualquiera de las opciones para ver más detalles.

 Seleccione este botón para especificar que se deben explorar todos los archivos.

 Seleccione este botón para limitar la exploración solamente a los archivos de programa. A continuación, haga clic en **Extensiones** para ver la lista de tipos de archivo que VShield considera que son más susceptibles de tener un virus.

 Haga clic en este botón para ver la lista de tipos de archivo que VShield considera que son más susceptibles de tener un virus.

 Seleccione esta casilla para incluir en la exploración los archivos comprimidos creados con los programas LHA, LZEXE, PkLite, PkZip o WinZip.

Borre la marca de esta casilla para desactivar la exploración de archivos comprimidos.

 Seleccione esta casilla si desea que la exploración comience tan pronto como se ejecute la tarea en la pantalla del Planificador de VShield, al hacer clic en

 , seleccionar las opciones de menú **Tarea>>Inicio** o al pulsar las teclas Alt + S.

Borre la marca de esta casilla su prefiere que la tarea de exploración no se ejecute hasta que haga clic en el botón **Explorar ahora**.

 Seleccione esta casilla para incluir en la exploración la búsqueda de virus residentes en memoria. Se trata de virus que permanecen en memoria después de ejecutarse y siguen afectando a otros archivos.

 Seleccione esta casilla para incluir en la exploración la búsqueda de virus en los sectores de arranque. El sector de arranque es la primera división lógica de un disco duro o disquete. El BIOS del sistema busca en ese sector, inmediatamente después de arrancar el equipo, los archivos y programas que necesita para iniciar el sistema.

 Haga clic en este botón para configurar el **Analizador de macros**. Esta característica evalúa la probabilidad de que una macro de una aplicación de Microsoft Office se trate en realidad de un virus.

Utilice la pestaña deslizante para ajustar el umbral de sensibilidad que define una macro como virus.

- Un valor bajo reduce el número de macros que se identifican como virus.
- Un valor alto aumenta el número de macros que se identifican como virus.
- El valor máximo hace que todas las macros de Microsoft Office se consideren virus.

ADVERTENCIA: Si selecciona el valor máximo y tiene seleccionada también la opción **Eliminar todas las macros al limpiar documentos infectados**, se borrarán todas las macros de los documentos de Microsoft Office.

 Escriba una contraseña fácil de recordar.

 Escriba una contraseña fácil de recordar.

 Vuelva a escribir la contraseña exactamente igual que la escribió anteriormente.

 Vuelva a escribir la contraseña exactamente igual que la escribió anteriormente.

 Haga clic en este botón para guardar la contraseña y cerrar el cuadro de diálogo.

 Haga clic en este botón para cerrar el cuadro de diálogo sin guardar la contraseña.

 Escriba su contraseña y haga clic en **Aceptar**.

 Escriba su contraseña y haga clic en **Aceptar**.

 Haga clic en este botón para continuar el proceso de desactivación de la protección mediante contraseña.

 Haga clic en este botón para cerrar el cuadro de diálogo sin desactivar la protección mediante contraseña.

 Haga clic en este botón para guardar los parámetros de configuración sin cerrar el cuadro de diálogo.

 Haga clic en este botón para cerrar el cuadro de diálogo sin guardar cambio alguno de los efectuados.

 Haga clic en este botón para guardar los cambios efectuados y cerrar el cuadro de diálogo.

Utilice esta pantalla para definir los parámetros de configuración para la exploración de archivos y el control de VShield.

Especifique los eventos que activarán la exploración.
Seleccione una o todas las opciones (eventos):

- al ejecutar un archivo ejecutable.
- al copiar un archivo.
- al crear un archivo.
- al cambiar de nombre un archivo.

 Seleccione esta casilla para explorar los archivos ejecutables cuando se ejecutan.
Borre la marca de esta casilla para desactivar la exploración de archivos ejecutables cuando se ejecutan.

 Seleccione esta casilla para explorar los archivos cuando se copian.
Borre la marca de esta casilla para desactivar la exploración cuando se copian los archivos.

 Seleccione esta casilla para explorar los archivos cuando se crean.
Borre la marca de esta casilla para desactivar la exploración de los archivos cuando se crean.

 Seleccione esta casilla para explorar los archivos cuando cambian de nombre.
Borre la marca de esta casilla para desactivar la exploración de los archivos cuando cambian de nombre.

Especifique los eventos que activan la exploración del sector de arranque de disquetes.
Seleccione una o ambas opciones (eventos):

- al abrir un disquete insertado en la unidad de disquete.
- al apagar el sistema con un disquete insertado.

 Seleccione esta casilla para explorar el sector de arranque del disquete cuando se llega a su contenido.
Borre la marca de esta casilla para desactivar la exploración de disquetes cuando se llega a su contenido.

 Seleccione esta casilla para explorar el sector de arranque del disquete al apagar el sistema con el disquete insertado. Borre la marca de esta casilla para desactivar la exploración de disquetes al apagar el sistema.

 Elija qué archivos desea explorar.

- Seleccione la opción **Todos los archivos** para examinar cada uno de los archivos.
- Seleccione la opción **Sólo archivos de programa** para examinar sólo los archivos susceptibles de estar infectados. Para ver la lista de archivos que VShield considera que son más susceptibles de tener un virus, haga clic en **Extensiones**.
- Seleccione la casilla **Archivos comprimidos** para incluir en la exploración los archivo del tipo **.zip** y otros tipos de archivos comprimidos.

 Seleccione este botón para especificar que deben explorarse todos los archivos.

 Seleccione este botón para limitar la exploración solamente a los archivos de programa. A continuación, haga clic en **Extensiones** para ver una lista con los tipos de archivo más susceptibles de tener un virus.

 Haga clic en este botón para ver una lista con los tipos de archivo que son más susceptibles de tener un virus.

 Seleccione esta casilla para incluir en la exploración los archivos comprimidos creados con los programas LHA, LZEXE, PkLite, PkZip o WinZip.

Borre la marca de esta casilla para desactivar la exploración de archivos comprimidos.

Seleccione las opciones de inicio, desactivación y presentación del icono.

Seleccione una o todas las opciones siguientes:

- activar la protección anti-virus al iniciar el sistema.
- permitir al usuario la desactivación de VShield desde la barra de tareas o el Planificador.
- mostrar el icono de VShield en la barra de tareas.

 Seleccione esta casilla para activar VShield cuando se inicia el equipo.
Borre la marca de esta casilla para desactivar la activación en el inicio.

 Seleccione esta casilla para permitir que VShield se desactive desde la barra de tareas o el Planificador. Borre la marca de esta casilla para impedir la desactivación de VShield.

 Seleccione esta casilla para mostrar el icono de VShield en la barra de tareas.

 Haga clic en este botón para configurar el **Analizador de macros**. Esta característica evalúa la probabilidad de que una macro de una aplicación de Microsoft Office se trate en realidad de un virus.

Utilice la pestaña deslizante para ajustar el umbral de sensibilidad que define una macro como virus.

- Un valor bajo reduce el número de macros que se identifican como virus.
- Un valor alto aumenta el número de macros que se identifican como virus.
- El valor máximo hace que todas las macros de Microsoft Office se consideren virus.

ADVERTENCIA: Si selecciona el valor máximo y tiene seleccionada también la opción **Eliminar todas las macros al limpiar documentos infectados**, se borrarán todas las macros de los documentos de Microsoft Office.

 Seleccione esta casilla para activar la exploración del **Analizador de macros**. Esta característica evalúa la probabilidad de que una macro de una aplicación de Microsoft Office se trate en realidad de un virus.

Utilice la pestaña deslizante para ajustar el umbral de sensibilidad que define una macro como virus.

- Un valor bajo reduce el número de macros que se identifican como virus.
- Un valor alto aumenta el número de macros que se identifican como virus.
- El valor máximo hace que todas las macros de Microsoft Office se consideren virus.

ADVERTENCIA: Si selecciona el valor máximo y tiene seleccionada también la opción **Eliminar todas las macros al limpiar documentos infectados**, se borrarán todas las macros de los documentos de Microsoft Office.

 Utilice la pestaña deslizante para ajustar el umbral de sensibilidad que define una macro como virus.

- Un valor bajo reduce el número de macros que se identifican como virus.
- Un valor alto aumenta el número de macros que se identifican como virus.

 Seleccione esta casilla para borrar las macros de los documentos infectados de Microsoft Office, al mismo tiempo que se limpian.

Borre la marca de esta casilla para desactivar el borrado de macros.

 Haga clic en este botón para guardar los cambios efectuados y cerrar el cuadro de diálogo.

 Haga clic en este botón para cerrar el cuadro de diálogo sin guardar cambio alguno de los efectuados.

 Haga clic en este botón para obtener Ayuda adaptada al contexto usando esta pantalla.

 Utilice esta pantalla para especificar las acciones que debe tomar VShield cuando encuentre un virus. Haga clic con el botón derecho en cualquiera de las opciones para ver más detalles.

 Haga clic en
 para seleccionar la acción que debe tomar VShield cuando encuentre un virus.
Dependiendo de la acción a tomar que seleccione en la lista desplegable, la sección de **Acciones posibles** mostrará:

- opciones adicionales o
- una ventana de texto para escribir información adicional o
- un mensaje que describe el resultado de la acción seleccionada.

Haga clic con el botón derecho en cualquiera de las opciones para ver más detalles.

Si selecciona **Consultar antes de actuar** en la lista desplegable, tendrá que indicar en la pestaña **Alerta** si desea que VShield genere un mensaje de aviso, haga sonar un tono o ambas acciones. Puede preparar un mensaje personalizado y/o especificar que se emita un tono audible cuando se encuentre un virus.

 Haga clic en
 para seleccionar la acción que debe tomar VShield cuando encuentre un virus.
Dependiendo de la acción a tomar que seleccione en la lista desplegable, la sección de **Acciones posibles** mostrará:

- opciones adicionales o
- una ventana de texto para escribir información adicional o
- un mensaje que describe el resultado de la acción seleccionada.

 Seleccione esta casilla para tener la oportunidad de limpiar los archivos infectados cuando se encuentre un virus. Cuando la haya seleccionado, esta opción aparecerá como un botón en el cuadro de diálogo de Alerta de VShield.

 Seleccione esta casilla para tener la oportunidad de borrar de su sistema los archivos infectados cuando VShield los detecte. Cuando la haya seleccionado, esta opción aparecerá como un botón en el cuadro de diálogo de Alerta de VShield.

 Seleccione esta casilla para tener la oportunidad de excluir de la exploración un archivo en el que se ha encontrado un virus. Cuando la haya seleccionado, esta opción aparecerá como un botón en el cuadro de diálogo de Alerta de VShield.

 Seleccione esta casilla para tener la oportunidad de ignorar los archivos infectados y continuar con la exploración. Cuando la haya seleccionado, esta opción aparecerá como un botón en el cuadro de diálogo de Alerta de VShield.

 Seleccione esta casilla para tener la oportunidad de detener inmediatamente la exploración.
Cuando la haya seleccionado, esta opción aparecerá como un botón en el cuadro de diálogo de Alerta de VShield.

 Seleccione esta casilla para tener la oportunidad de mover los archivos infectados a un directorio de cuarentena. A continuación, haga clic en **Examinar** para seleccionar la ubicación a la que se deben mover los archivos infectados.

Cuando la haya seleccionado, esta opción aparecerá como un botón en el cuadro de diálogo de Alerta de VShield.

 Haga clic en
 para seleccionar la acción que debe tomar VShield cuando encuentre un virus.
Dependiendo de la acción a tomar que seleccione en la lista desplegable, la sección de **Acciones posibles** mostrará:

- opciones adicionales o
- una ventana de texto para escribir información adicional o
- un mensaje que describe el resultado de la acción seleccionada.

Haga clic con el botón derecho en cualquiera de las opciones para ver más detalles.

Si selecciona **Consultar antes de actuar** en la lista desplegable, tendrá que indicar en la pestaña **Alerta** si desea que VShield genere un mensaje de aviso, haga sonar un tono o ambas acciones. Puede preparar un mensaje personalizado y/o especificar que se emita un tono audible cuando se encuentre un virus.

 Haga clic en este botón para seleccionar el directorio de cuarentena al que se deben mover los archivos infectados.

 Haga clic en el botón **Examinar** para seleccionar el directorio de cuarentena al que se deben mover los archivos infectados.

 Dependiendo de la acción a tomar que seleccione en la lista desplegable, la sección de **Acciones posibles** mostrará:

- opciones adicionales o
- una ventana de texto para escribir información adicional o
- un mensaje que describe el resultado de la acción seleccionada.

Utilice esta pantalla para avisar al administrador de la red, por medio de NetShield, cuando VShield encuentre un archivo infectado:

- Seleccione la casilla **Enviar alerta de red**.
- Haga clic en **Examinar** para seleccionar una carpeta de red, (directorio) al que se enviará la alerta. Cuando la haya seleccionado, la ruta de la carpeta de mensajes aparecerá en el cuadro de texto.

NetShield es una solución anti-virus de Network Associates para servidores

Seleccione la casilla **Enviar alerta de red** para avisar al administrador de red, por medio de NetShield, cuando VShield encuentre un archivo infectado. A continuación, haga clic en **Examinar** para seleccionar un servidor de destino para los mensajes de centralización de alertas. Cuando lo haya seleccionado, la ruta de la carpeta de mensajes aparecerá en el cuadro de texto.

NetShield es una solución anti-virus de Network Associates para servidores.

Borre la marca de esta casilla para desactivar la alerta de red.

Seleccione la casilla **Enviar alerta de red** para avisar al administrador de red, por medio de NetShield, cuando VShield encuentre un archivo infectado. A continuación, haga clic en **Examinar** para seleccionar un servidor de destino para los mensajes de centralización de alertas. Cuando lo haya seleccionado, la ruta de la carpeta de mensajes aparecerá en el cuadro de texto.

NetShield es una solución anti-virus de Network Associates para servidores.

 Haga clic en este botón para abrir el cuadro de diálogo **Buscar carpeta**, en el que puede seleccionar un servidor de destino para los mensajes de centralización de alertas. Cuando lo haya seleccionado, la ruta de la carpeta de mensajes aparecerá en el cuadro de texto.

 Si ha seleccionado la opción **Consultar antes de actuar** en la pestaña **Acción**, deberá indicar si desea que VShield genere un mensaje, haga sonar un tono o ambos.

 Seleccione esta casilla si desea que VShield haga sonar un tono cuando encuentre un archivo infectado. Borre la marca de esta casilla para desactivar el tono audible.

 Seleccione esta casilla si desea preparar un mensaje personalizado que VShield presentará cuando encuentre un virus. A continuación, escriba el mensaje en el cuadro de texto. Cuando la haya seleccionado, esta opción presentará el mensaje personalizado como mensaje de alerta en el cuadro de diálogo de Alerta de VShield.

Borre la marca de esta casilla para desactivar el mensaje personalizado.

 Vea el mensaje que se presentará cuando se detecte un virus o redacte uno nuevo.

Seleccione la casilla **Enviar alerta de red** para avisar al administrador de red, por medio de NetShield, cuando VShield encuentre un archivo infectado. A continuación, haga clic en **Examinar** para seleccionar un servidor de destino para los mensajes de centralización de alertas. Cuando lo haya seleccionado, la ruta de la carpeta de mensajes aparecerá en el cuadro de texto.

Si ha seleccionado la opción **Consultar antes de actuar** en la pestaña **Acción**, indique, en la parte inferior de la pantalla, si desea que VShield genere un mensaje, haga sonar un tono o ambos.

NetShield es una solución anti-virus de Network Associates para servidores.

 Seleccione esta casilla para enviar un aviso a aplicaciones de gestión de red o de gestión de escritorio que cumplan con el estándar DMI (Interfaz de administración de escritorio).

 Utilice esta pantalla para crear un registro de actividades de exploración. Haga clic con el botón derecho en cualquiera de las opciones para ver más detalles.

 Seleccione esta casilla para activar el registro de actividades de VShield. A continuación, haga clic en **Examinar** para seleccionar un archivo para el registro. Cuando lo haya seleccionado, aparecerá en el cuadro de texto la ruta del archivo. Entonces podrá fijar el tamaño máximo del archivo de registro.

 Seleccione la casilla **Registrar en archivo** para activar el registro de actividades de VShield. A continuación, haga clic en **Examinar** para seleccionar un archivo para el registro. Cuando lo haya seleccionado, aparecerá en este cuadro de texto la ruta del archivo.

 Haga clic en este botón para seleccionar el archivo en que se creará el registro. Cuando lo haya seleccionado, aparecerá en el cuadro de texto la ruta del archivo de registro.

Seleccione esta casilla si desea limitar el tamaño del archivo de registro. A continuación, escriba en el cuadro de texto el tamaño máximo, en kilobytes, del archivo de registro. Puede utilizar para seleccionar el número de kilobytes o escribir el número con el teclado.

Borre la marca de esta casilla para desactivar la limitación de tamaño del archivo de registro.

 Escriba el tamaño máximo, en kilobytes, del archivo de registro. Puede utilizar
 para seleccionar el número de kilobytes o escribir el número con el teclado.

 Escriba el tamaño máximo, en kilobytes, del archivo de registro. Puede utilizar
 para seleccionar el número de kilobytes o escribir el número con el teclado.

 Seleccione cualquiera o todas estas casillas para registrar en el archivo de registro la información asociada a cada una de ellas.

 Seleccione esta casilla para registrar los nombres de las variedades de virus que VShield encuentre durante una sesión de exploración y el número de veces que encuentra cada una de ellas.

Borre la marca de esta casilla para desactivar el registro de las variedades de virus.

 Seleccione esta casilla para registrar el número de archivos infectados que VShield ha limpiado durante una sesión de exploración.

Borre la marca de esta casilla para desactivar el registro de virus limpiados.

Seleccione esta casilla para registrar el número de archivos infectados que VShield ha borrado durante una sesión de exploración.

Borre la marca de esta casilla para desactivar el registro de archivos infectados borrados.

 Seleccione esta casilla para registrar el número de archivos infectados que VShield ha movido a un directorio de cuarentena durante una sesión de exploración.

Borre la marca de esta casilla para desactivar el registro de archivos infectados que han cambiado de ubicación.

 Seleccione esta casilla para registrar los parámetros de configuración seleccionados para esta sesión de exploración. Borre la marca de esta casilla para desactivar el registro de los parámetros de configuración de la sesión.

Seleccione esta casilla para generar un resumen de las acciones que ha tomado VShield durante esta sesión de exploración, información que incluye:

- El número de archivos que se han examinado en busca de virus.
- El número de archivos infectados que se han limpiado.
- El número de archivos infectados que se han borrado.
- El número de archivos infectados que se han movido.
- Otros datos acerca de los parámetros de configuración de VShield.
- Borre la marca de esta casilla para desactivar el registro de la información de resumen de la sesión.

 Seleccione esta casilla para registrar la fecha y hora en que comenzó la sesión de exploración.
Borre la marca de esta casilla para desactivar el registro de fecha y hora.

 Seleccione esta casilla para registrar el nombre del usuario que realizó la exploración.
Borre la marca de esta casilla para desactivar el registro del nombre del usuario.

 Active el registro de actividades, cree un archivo de registro y especifique su tamaño máximo.

 Utilice esta pantalla para excluir objetos, como archivos, carpetas y unidades de disco, de la exploración en busca de virus. Utilice los botones que aparecen en la parte inferior de la pantalla para **Agregar** objetos adicionales a la lista, **Editar** objetos que ya aparecen en la lista y **Eliminar** elementos de la lista.

 Este cuadro muestra una lista de archivos, carpetas y unidades de disco que se han excluido de la detección en busca de virus. Los elementos se agregan a esa lista mediante el cuadro de diálogo **Agregar Excluir elemento**, que pasa a estar disponible al hacer clic en **Agregar** (en la parte inferior de la pantalla). En el cuadro inferior se presenta información acerca del elemento, entre la que se incluye su **nombre**, si sus **subcarpetas** están excluidas o no y si la exclusión es **de** la exploración de archivos, la exploración de sectores de arranque o de ambas.

 Este cuadro muestra una lista de archivos, carpetas y unidades de disco que se han excluido de la detección en busca de virus. Los elementos se agregan a esa lista mediante el cuadro de diálogo **Agregar Excluir elemento**, que pasa a estar disponible al hacer clic en **Agregar** (en la parte inferior de la pantalla). En el cuadro inferior se presenta información acerca del elemento, entre la que se incluye su **nombre**, si sus **subcarpetas** están excluidas o no y si la exclusión es **de** la exploración de archivos, la exploración de sectores de arranque o de ambas.

 Este cuadro muestra una lista de archivos, carpetas y unidades de disco que se han excluido de la detección en busca de virus. Los elementos se agregan a esa lista mediante el cuadro de diálogo **Agregar Excluir elemento**, que pasa a estar disponible al hacer clic en **Agregar** (en la parte inferior de la pantalla). En el cuadro inferior se presenta información acerca del elemento, entre la que se incluye su **nombre**, si sus **subcarpetas** están excluidas o no y si la exclusión es **de** la exploración de archivos, la exploración de sectores de arranque o de ambas.

 Este cuadro muestra una lista de archivos, carpetas y unidades de disco que se han excluido de la detección en busca de virus. Los elementos se agregan a esa lista mediante el cuadro de diálogo **Agregar Excluir elemento**, que pasa a estar disponible al hacer clic en **Agregar** (en la parte inferior de la pantalla). En el cuadro inferior se presenta información acerca del elemento, entre la que se incluye su **nombre**, si sus **subcarpetas** están excluidas o no y si la exclusión es **de** la exploración de archivos, la exploración de sectores de arranque o de ambas.

 Haga clic en este botón para abrir el cuadro de diálogo **Agregar Excluir elemento**.

 Haga clic en este botón para abrir el cuadro de diálogo **Editar Excluir elemento**.

 Haga clic en este botón Para borrar de la lista de elementos excluidos el elemento seleccionado.

 Utilice esta pantalla para seleccionar las opciones de VShield que desea proteger frente a cambios no autorizados. Puede seleccionar todas las opciones que aparecen ene el cuadro de lista o cualquier opción individual. A la izquierda de las páginas protegidas aparece  .

 Seleccione las opciones de VShield que desea proteger frente a cambios no autorizados.
Puede seleccionar todas las opciones que aparecen ene el cuadro de lista o cualquier opción individual. A la izquierda de las páginas protegidas aparece  .

 Haga clic en este botón para escribir su contraseña.

 Al configurar una tarea que se creó copiando una tarea ya existente, seleccione esta casilla para aplicar las opciones de seguridad de la tarea original a la nueva tarea. La casilla se activará cuando seleccione una de las páginas de propiedades para que quede protegida mediante contraseña.

 Haga clic en este botón para guardar los cambios efectuados y cerrar el cuadro de diálogo.

 Haga clic en este botón para cerrar el cuadro de diálogo sin guardar cambio alguno.

 Escriba la extensión del tipo de archivo que desea explorar en busca de virus. No incluya el punto que normalmente precede a las extensiones de nombre de archivo.

 Escriba la extensión del tipo de archivo que desea explorar en busca de virus. No incluya el punto que normalmente precede a las extensiones de nombre de archivo.

 Haga clic en este botón para cerrar el cuadro de diálogo y guardar los cambios efectuados.

 Haga clic en este botón para cerrar el cuadro de diálogo y guardar los cambios efectuados.

 Haga clic en este botón para abrir el cuadro de diálogo **Agregar extensión de archivos de programa**.

 Haga clic en este botón para borrar de la lista la extensión de archivo de programa seleccionada.

 Haga clic en este botón para recuperar las extensiones predeterminadas. Todas las extensiones que hayan ido agregando los usuarios, se borrarán de la lista.

 Este cuadro muestra una lista con las extensiones de todos los tipos de archivo que se exploran en busca de virus.

- Para agregar una extensión, haga clic en **Agregar**. Al hacerlo, aparecerá el cuadro de diálogo **Agregar extensión de archivos de programa**.
- Para borra de la lista una extensión, seleccione la extensión y haga clic en **Borrar**.
- Para recuperar la lista de extensiones predeterminadas que utiliza VShield, eliminando las extensiones que hayan ido agregando los usuarios, haga clic en **Predeterminadas**.

 Este cuadro muestra una lista con las extensiones de todos los tipos de archivo que se exploran en busca de virus.

- Para agregar una extensión, haga clic en **Agregar**. Al hacerlo, aparecerá el cuadro de diálogo **Agregar extensión de archivos de programa**.
- Para borra de la lista una extensión, seleccione la extensión y haga clic en **Borrar**.
- Para recuperar la lista de extensiones predeterminadas que utiliza VShield, eliminando las extensiones que hayan ido agregando los usuarios, haga clic en **Predeterminadas**.

 Haga clic en **Examinar** para seleccionar una carpeta que desee excluir de la exploración en busca de virus. Cuando la haya seleccionado, la ruta de la carpeta aparecerá en este cuadro de texto.

 Haga clic en **Examinar** para seleccionar una carpeta que desee excluir de la exploración en busca de virus. Cuando la haya seleccionado, la ruta de la carpeta aparecerá en este cuadro de texto.

 Haga clic en este botón para seleccionar una carpeta que desee excluir de la exploración en busca de virus. Cuando la haya seleccionado, la ruta de la carpeta aparecerá en el cuadro de texto.

 Seleccione esta casilla para excluir de la exploración en busca de virus todas las subcarpetas asociadas a la carpeta que se desea excluir.

 Seleccione una o ambas casillas para especificar si la carpeta o archivo especificado debe excluirse de la **Exploración de archivos**, de la **Exploración de sectores de arranque** o de ambas.

 Seleccione esta casilla para excluir el archivo a carpeta indicado solamente de la **Exploración de archivos**.

 Seleccione esta casilla para excluir el archivo o carpeta indicado solamente de la **Exploración de sectores de arranque**.

 Haga clic en este botón para guardar los cambios efectuados y cerrar el cuadro de diálogo.

 Haga clic en este botón para cerrar el cuadro de diálogo sin guardar cambio alguno de los efectuados.

 Seleccione un elemento a explorar o una unidad de disco/carpeta a explorar.

- Si desea seleccionar un elemento, haga clic en  y seleccione uno de los tipos de elemento disponibles.
- Si desea seleccionar una unidad de disco o carpeta, haga clic en **Examinar** para buscarla. Cuando la haya seleccionado, la ruta aparecerá en el cuadro de texto.
- Si desea incluir las subcarpetas existentes en la ubicación seleccionada, seleccione la casilla **Incluir subcarpetas**.

 Haga clic en este botón para cerrar el cuadro de diálogo sin guardar cambio alguno.

 Haga clic en este botón para obtener Ayuda adaptada al contexto utilizando esta pantalla.

 Haga clic en **Examinar** para buscar la unidad de disco o carpeta que desea incluir en la exploración. Cuando la haya seleccionado, la ruta aparecerá en este cuadro de texto.

 Seleccione esta casilla para incluir en la exploración todas las subcarpetas existentes en la ubicación seleccionada para la exploración.

 Haga clic en este botón para buscar la unidad de disco o carpeta que desea incluir en la exploración. Cuando la haya seleccionado, la ruta aparecerá en este cuadro de texto.

 Seleccione este botón si desea agregar todos los elementos:

- de Mi PC
- de todas las unidades de disco desmontables
- de todas las unidades disco fijas
- de todas las unidades de red.

A continuación, haga clic en  y seleccione uno de los tipos de elemento disponibles.

 Seleccione este botón si desea seleccionar una unidad de disco o carpeta a incluir en la exploración. A continuación, haga clic en **Examinar** para buscar la unidad de disco o carpeta que desea incluir en la exploración. Cuando la haya seleccionado, la ruta aparecerá en este cuadro de texto.

Haga clic en
y seleccione uno de los tipos de elemento disponibles:

- Mi PC
- Todas las unidades de disco desmontables
- Todas las unidades disco fijas
- Todas las unidades de red.

» Este cuadro muestra información importante acerca de las condiciones de utilización de este producto.

 Esta pantalla muestra información importante de identificación de su copia de VShield. Haga clic en **Aceptar** cuando haya terminado de examinar su contenido.

 Esta pantalla muestra información importante de identificación de su copia de VShield. Haga clic en **Aceptar** cuando haya terminado de examinar su contenido.

 Esta pantalla muestra información importante de identificación de su copia de VShield. Haga clic en **Aceptar** cuando haya terminado de examinar su contenido.

 Esta pantalla muestra información importante de identificación de su copia de VShield. Haga clic en **Aceptar** cuando haya terminado de examinar su contenido.

 Esta pantalla muestra información importante de identificación de su copia de VShield. Haga clic en **Aceptar** cuando haya terminado de examinar su contenido.

 Esta pantalla muestra información importante de identificación de su copia de VShield. Haga clic en **Aceptar** cuando haya terminado de examinar su contenido.

 Esta pantalla muestra información importante de identificación de su copia de VShield. Haga clic en **Aceptar** cuando haya terminado de examinar su contenido.

 Esta pantalla muestra información importante de identificación de su copia de VShield. Haga clic en **Aceptar** cuando haya terminado de examinar su contenido.

 Esta pantalla muestra información importante para los usuarios de la versión de evaluación de VirusScan para Windows 95 y Windows 98. Haga clic en **Aceptar** cuando haya terminado de examinar su contenido.

 Esta pantalla muestra información importante para los usuarios de la versión de evaluación de VirusScan para Windows 95 y Windows 98. Haga clic en **Aceptar** cuando haya terminado de examinar su contenido.

 Esta pantalla muestra información importante para los usuarios de la versión de evaluación de VirusScan para Windows 95 y Windows 98. Haga clic en **Aceptar** cuando haya terminado de examinar su contenido.

 Esta pantalla muestra información importante para los usuarios de la versión de evaluación de VirusScan para Windows 95 y Windows 98. Haga clic en **Aceptar** cuando haya terminado de examinar su contenido.

 Esta pantalla muestra información importante para los usuarios de la versión de evaluación de VirusScan para Windows 95 y Windows 98. Haga clic en **Aceptar** cuando haya terminado de examinar su contenido.

 Esta pantalla muestra información importante para los usuarios de la versión de evaluación de VirusScan para Windows 95 y Windows 98. Haga clic en **Aceptar** cuando haya terminado de examinar su contenido.

 Esta pantalla muestra información importante para los usuarios de la versión de evaluación de VirusScan para Windows 95 y Windows 98. Haga clic en **Aceptar** cuando haya terminado de examinar su contenido.

 Esta pantalla muestra información importante para los usuarios de la versión de evaluación de VirusScan para Windows 95 y Windows 98. Haga clic en **Aceptar** cuando haya terminado de examinar su contenido.

 Muestra la ruta del último archivo explorado.

 Muestra el número de archivos que VShield ha examinado durante la última exploración.

 Muestra el número de archivos infectados que se han limpiado durante la última exploración.

 Muestra el número de archivos infectados que se han movido a una carpeta de cuarentena durante la última exploración.

 Muestra el número de archivos infectados que se han movido a una carpeta de cuarentena durante la última exploración.

 Esta pantalla muestra un resumen con los resultados de la última exploración de VShield.

- Haga clic en **Propiedades** para configurar las actividades de exploración.
- Haga clic con el botón derecho en cualquiera de los valores numéricos si desea ver más detalles.

 Haga clic aquí para cerrar este cuadro de diálogo.

 Haga clic en este botón para activar o desactivar este componente de programa.

Si el componente se está ejecutando, el botón mostrará la opción **Desactivar**. Si el componente no se ejecuta, el botón mostrará la opción **Activar**

 Muestra el nombre de la última clase de Java o control de ActiveX explorado.

 Muestra el nombre de la última clase de Java o control de ActiveX explorado.

 Muestra la dirección IP del último sitio web o Internet examinado.

 Los números que aparecen a la derecha indican el número de subprogramas de Java que VShield ha examinado durante la última exploración y el número de ellos que ha prohibido.

 Los números que aparecen a la derecha indican el número de controles ActiveX que VShield ha examinado durante la última exploración y el número de ellos que ha prohibido.

 Los números que aparecen a la derecha indican el número de sitios Internet que VShield ha examinado durante la última exploración y el número de ellos que ha prohibido.

 Los valores siguientes indican el número de subprogramas de Java, controles de ActiveX y sitios Internet que se han prohibido durante la última exploración.

 Muestra el número de sitios Internet que se han prohibido durante la última exploración.

 Muestra el número de sitios Internet que se han examinado durante la última exploración.

 Muestra el número subprogramas de Java que se han examinado durante la última exploración.

 Los valores siguientes indican el número de subprogramas de Java, controles de ActiveX y sitios Internet que se han examinado durante la última exploración.

 Muestra la dirección IP del último sitio web o Internet examinado.

 Esta pantalla muestra un resumen de la última actividad de filtrado de Internet realizada.

- Haga clic en **Propiedades** para configurar las actividades de exploración.
- Haga clic con el botón derecho en cualquiera de las etiquetas o valores numéricos para ver más detalles.

 Haga clic aquí para cerrar este cuadro de diálogo.

 Haga clic en este botón para desactivar la actividad de exploración descrita en la pestaña que aparece en la parte superior de la página.

 Muestra la dirección IP del último sitio web o de Internet examinado.

 Muestra información de resumen acerca del número de objetos y sitios de Internet que se han explorado y el número que se han prohibido durante la última exploración.

 Muestra el número de controles ActiveX que se han explorado durante la última exploración.

 Muestra el número de subprogramas de Java que se han prohibido durante la última exploración.

 Muestra el número de controles de ActiveX que se han prohibido durante la última exploración.

 Muestra el nombre del último archivo recibido de Internet.

 Esta pantalla muestra un resumen con los resultados de la última exploración de correo electrónico o elementos descargados de Internet.

- Haga clic en **Propiedades** para configurar las actividades de exploración.
- Haga clic con el botón derecho en cualquiera de los valores numéricos para ver más detalles.

 Haga clic en este botón para cerrar este cuadro de diálogo.

 Haga clic en este botón para activar o desactivar este componente de programa.

Si el componente se está ejecutando, el botón mostrará la opción **Desactivar**. Si el componente no se ejecuta, el botón mostrará la opción **Activar**.

 Muestra el número de archivos adjuntos al correo electrónico o archivos descargados que se han incluido en la última exploración.

 Muestra el nombre del último archivo recibido de Internet.

 Muestra información de resumen acerca del número de archivos adjuntos a correo electrónico y otros archivos descargados de Internet que se han explorado, los que estaban infectados, los que se han borrado y los que se han movido a un directorio de cuarentena.

 Muestra el número de archivos adjuntos al correo y de archivos descargados infectados que se han detectado durante la última exploración.

 Muestra el número de archivos adjuntos al correo y de archivos descargados infectados que se han borrado durante la última exploración.

 Muestra el número de archivos adjuntos al correo y de archivos descargados infectados que se han movido al directorio de cuarentena durante la última exploración.

Para ver una lista de virus definidos en los archivos .DAT instalados en su equipo:

1 Haga clic en **Inicio**, en la esquina inferior izquierda de la pantalla.

2 Seleccione **Programas → McAfee VirusScan → McAfee Consola VirusScan.** Aparecerá la pantalla de inicio del programa VirusScan.

3 Haga clic en **Herramientas → Info acerca de virus.** Aparecerá la lista de virus definidos en los archivos de datos instalados en su equipo.

Si desea más información acerca de cómo mantener actualizados sus archivos de datos, vea el apartado Actualización de los archivos de datos de VirusScan.

 Seleccione esta casilla para Microsoft Mail o para cualquier cliente de correo electrónico que cumpla con MAPI, incluido Lotus cc:Mail 8, que cumple con MAPI.

Si utiliza America Online, Eudora Light, Netscape o cualquier otro cliente de correo electrónico POP-3 o proxy, seleccione Internet Mail y utilice el módulo **Explorador de elementos descargados** de VShield en vez de **Exploración de correo electrónico** para configurar sus preferencias de exploración de virus.

 Seleccione este botón para Microsoft Mail o para cualquier cliente de correo electrónico que cumpla con MAPI, incluido Lotus cc:Mail 8, que cumple con MAPI.

Si utiliza America Online, Eudora Light, Netscape, o cualquier otro cliente de correo electrónico POP-3 o proxy, seleccione **Correo Internet** y utilice el módulo **Explorador de elementos descargados** de VShield en vez de **Exploración de correo electrónico** para configurar sus preferencias de exploración de virus.

 Seleccione este botón para especificar la exploración al entrar en todos los anexos que reciba con su correo.

 Seleccione este botón para limitar la exploración al entrar sólo en los archivos de programa que reciba. A continuación, haga clic en **Extensiones** para ver una lista de los tipos de archivos que sean más susceptibles de infectarse con un virus.

 Si ha elegido **Sólo archivos de programa**, haga clic en este botón para ver una lista de los tipos de archivos que sean más susceptibles de infectarse con un virus.

Seleccione la casilla **Enviar alerta de red** para enviar una alerta al administrador de red a través de NetShield cada vez que se encuentre un archivo infectado. A continuación, haga clic en **Examinar** para seleccionar el servidor que va a recibir el Mensaje de centralización de alertas. Una vez seleccionado, la ruta de la carpeta del mensaje aparecerá en el cuadro de texto.

NetShield es una solución anti-virus para servidor de Network Associates.

Borre la marca de esta casilla para desactivar la alerta de red.

Seleccione la casilla **Enviar alerta de red** para enviar una alerta al administrador de red a través de NetShield cada vez que VShield encuentre un archivo infectado. A continuación, haga clic en **Examinar** para seleccionar el servidor que va a recibir el Mensaje de centralización de alertas. Una vez seleccionado, la ruta de la carpeta del mensaje aparecerá en el cuadro de texto.

NetShield es una solución anti-virus para servidor de Network Associates.

 Seleccione esta casilla para enviar un mensaje de alerta a la persona que le envió el mensaje que contenía el virus. VShield enviará un mensaje de alerta estándar cada vez que detecte un virus. Para ver o componer su propio mensaje, haga clic en **Configurar**.

Borre la marca de esta casilla para desactivar la respuesta al remitente.

 Seleccione esta casilla para enviar una notificación a las aplicaciones de administración de escritorio o de administración de red que cumplan con el estándar Interfaz de administración de escritorio.

 Seleccione esta casilla para activar la actividad de registro. A continuación, haga clic en **Examinar** para seleccionar el archivo de registro. Una vez seleccionado, la ruta del archivo aparecerá en el cuadro de texto. Usted puede definir el tamaño máximo del archivo de registro.

 Seleccione la casilla **Registrar en archivo** para activar la actividad de registro. A continuación, haga clic en **Examinar** para seleccionar la carpeta en la que se creará el archivo de registro. Una vez seleccionada, la ruta del archivo aparecerá en el cuadro de texto.

 Introduzca el tamaño máximo, en kilobytes, del archivo de registro. Puede utilizar
 para seleccionar el número de kilobytes o escribirlo con el teclado.

 Seleccione esta casilla para registrar los valores que elija para esta sesión de exploración.
Borre la marca de esta casilla para desactivar el registro de los valores de la sesión.

 Seleccione esta casilla para enviar una notificación a las aplicaciones de administración de escritorio o de administración de red que cumplan con el estándar Interfaz de administración de escritorio.

 Seleccione esta casilla para explorar en busca de clases de Java perjudiciales cuando se visiten sitios de Internet. VShield compara las clases de Java que encuentre con una base de datos de clases conocidas como causantes de daños. Le alerta cuando encuentra una clase de Java potencialmente dañina.

 Seleccione esta casilla para indicar a VShield que impida al software del examinador visitar los sitios de Internet que designe con una dirección IP.

A continuación, haga clic en **Configurar** para ver o agregar a la lista que VShield utiliza para identificar direcciones IP peligrosas.

 Haga clic en
 para seleccionar la forma en la que quiere que VShield responda cuando encuentre un virus. En la sección **Acciones posibles** se mostrará un mensaje que describe el resultado de la respuesta seleccionada.

Seleccione la casilla **Enviar alerta de red** para alertar al administrador de la red a través de NetShield cuando VShield encuentre un archivo infectado. A continuación, haga clic en **Examinar** para seleccionar el servidor que va a recibir el Mensaje de centralización de alertas. Una vez seleccionada, la ruta de la carpeta del mensaje aparecerá en este cuadro de texto.

NetShield es la solución anti-virus para servidor de Network Associates.

Borre la marca de esta casilla para desactivar la alerta de red.

Seleccione la casilla **Enviar alerta de red** para alertar al administrador de la red a través de NetShield cuando VShield encuentre un archivo infectado. A continuación, haga clic en **Examinar** para seleccionar el servidor que va a recibir el Mensaje de centralización de alertas. Una vez seleccionada, la ruta de la carpeta del mensaje aparecerá en este cuadro de texto.

NetShield es la solución anti-virus para servidor de Network Associates.

» Vea el mensaje que se mostrará al detectar un virus o cree uno nuevo.

 Seleccione la casilla **Registrar en archivo** anterior para activar la actividad de registro. A continuación, haga clic en **Examinar** para seleccionar el archivo en el que se va a crear el registro. Una vez seleccionado, la ruta del archivo de registro aparecerá en este cuadro de texto.

 Introduzca el tamaño máximo, en kilobytes, del archivo de registro. Puede utilizar
 para seleccionar el número de kilobytes o escribir el número desde el teclado.

 Haga clic en esta casilla para activar la protección mediante contraseña de las páginas de propiedades.

 Seleccione este botón para proteger mediante contraseña toda la configuración y las opciones que haya seleccionado.

 Seleccione este botón para proteger mediante contraseña sólo las opciones que especifique. Haga clic en cada pestaña para ver una lista de las páginas de propiedades que quizá quiera proteger mediante contraseña.

 Haga clic en este botón para introducir una contraseña que proteja las configuraciones y opciones que ha seleccionado.

 Vuelva a introducir la contraseña que ha escrito anteriormente.

 Use esta pantalla para definir los parámetros para exploración de virus de correo electrónico. Haga clic con el botón derecho en cualquiera de las opciones para obtener información adicional.

 Seleccione esta casilla para hacer una exploración de virus en los archivos de correo electrónico que reciba de Internet a través de Lotus cc:Mail, Microsoft Mail o cualquier cliente de correo electrónico que cumpla con MAPI.

Borre la marca de esta casilla para desactivar la exploración en el correo electrónico.

 Seleccione el tipo de programa que utiliza para recibir correo electrónico desde Internet.

- Seleccione **Correo Microsoft (MAPI)** para Microsoft Mail o cualquier cliente de correo electrónico que cumpla con MAPI, incluido Lotus cc:Mail 8.
- Seleccione **cc:Mail** para Lotus cc:Mail 6 o 7. No seleccione este botón para Lotus cc:Mail 8, que cumple con MAPI.

Si utiliza America Online, Eudora Light, Netscape o cualquier otro cliente de correo electrónico POP-3 o proxy, utilice el módulo **Explorador de elementos descargados** en vez del módulo **Exploración de correo electrónico** para configurar sus preferencias de exploración de virus.

 Seleccione este botón para Microsoft Mail o cualquier cliente de correo electrónico que cumpla con MAPI, incluido Lotus cc:Mail 8.

- Si utiliza Lotus cc:Mail 8, seleccione **Correo Microsoft (MAPI)**. Lotus cc:Mail 8 cumple con MAPI.
- Si utiliza America Online, Eudora Light, Netscape o cualquier otro cliente de correo electrónico POP-3 o proxy, utilice el módulo **Explorador de elementos descargados** en vez del módulo **Exploración de correo electrónico** para configurar sus preferencias de exploración de virus.

 Seleccione este botón para Lotus cc:Mail 6 o 7.

- Si utiliza Lotus cc:Mail 8, seleccione **Correo Microsoft (MAPI)** en su lugar. Lotus cc:Mail 8 cumple con MAPI.
- Si utiliza America Online, Eudora Light, Netscape o cualquier otro cliente de correo electrónico POP-3 o proxy, utilice el módulo **Explorador de elementos descargados** en vez del módulo **Exploración de correo electrónico** para configurar sus preferencias de exploración de virus.

 Especifique qué elementos de correo electrónico se van a explorar y con qué frecuencia se va a comprobar el correo nuevo.

 Seleccione este botón para especificar la exploración de todo el correo electrónico nuevo.

 Seleccione este botón para especificar la exploración del correo electrónico nuevo de una carpeta concreta. A continuación, haga clic en el

contiguo para examinar la carpeta que contiene el correo que se va a explorar.

Si aún no se ha registrado en el sistema de correo electrónico, se le pedirá que elija un perfil de usuario para utilizar con Microsoft Mail o un sistema de correo que cumpla con MAPI. Vea la documentación acerca de la Mensajería de Microsoft para obtener más detalles.

 Si ha elegido **Seleccionar carpeta**, haga clic en este botón para examinar la carpeta que contiene el correo que se va a explorar.

 En el cuadro de texto, introduzca la frecuencia, en segundos, con la que se va a comprobar el servidor de correo para ver si ha llegado correo electrónico nuevo. Ésta debe duplicar aproximadamente la frecuencia con la que el servidor de correo comprueba el correo nuevo.

Puede utilizar  para seleccionar el número de segundos o escribir el número desde el teclado.

Introduzca la frecuencia, en segundos, con la que VShield debe comprobar el servidor de correo para ver si ha llegado correo electrónico nuevo. Ésta debe duplicar aproximadamente la frecuencia con la que el servidor de correo comprueba el correo nuevo.

Puede utilizar para seleccionar el número de segundos o escribir el número desde el teclado.

Introduzca la frecuencia, en segundos, con la que VShield debe comprobar el servidor de correo para ver si ha llegado correo electrónico nuevo. Ésta debe duplicar aproximadamente la frecuencia con la que el servidor de correo comprueba el correo nuevo.

Puede utilizar para seleccionar el número de segundos o escribir el número desde el teclado.

 En el cuadro de texto, introduzca la frecuencia, en segundos, con la que VShield debe comprobar el servidor de correo para ver si ha llegado correo electrónico nuevo. Ésta debe duplicar aproximadamente la frecuencia con la que el servidor de correo comprueba el correo nuevo.

Puede utilizar  para seleccionar el número de segundos o escribir el número desde el teclado.

 Elija qué archivos desea explorar de entre los que recibe por correo electrónico.

- Elija **Todos los archivos adjuntos** para examinar todos los mensajes que reciba.
- Elija **Sólo archivos de programa** para examinar sólo aquellos archivos más susceptibles de infectarse. Haga clic en **Extensiones** para ver una lista de archivos susceptibles.
- Seleccione la casilla **Archivos comprimidos** para incluir la exploración de archivos **.zip** u otros tipos de archivos comprimidos.

 Si ha elegido **Sólo archivos de programa**, haga clic en este botón para ver la lista de los tipos de archivo más susceptibles de infectarse con un virus.

 Seleccione esta casilla para incluir la exploración de archivos comprimidos con LHA, LZEXE, PkLite, PkZip o WinZip. Borre la marca de esta casilla para desactivar la exploración de archivos comprimidos.

 Seleccione este botón para Microsoft Mail o cualquier cliente de correo electrónico que cumpla con MAPI.

- Si utiliza Lotus cc:Mail 8, seleccione **Correo Microsoft (MAPI)**. Lotus cc:Mail 8 cumple con MAPI.'
- Si utiliza una versión de Lotus cc:Mail anterior a la versión 8, debe realizar una instalación personalizada de VirusScan para Windows 95 y Windows 98.
- Si utiliza America Online, Eudora Light, Netscape o cualquier otro cliente de correo electrónico POP-3 o proxy, utilice el módulo **Explorador de elementos descargados** en vez del módulo **Exploración de correo electrónico** para configurar sus preferencias de exploración de virus.

 Seleccione este botón si utiliza America Online, Eudora Light, Netscape o cualquier otro cliente de correo electrónico POP-3 o proxy. VShield utiliza las opciones que elija en la página de propiedades **Explorador de elementos descargados** para controlar la exploración de los anexos recibidos a través de estos clientes de correo electrónico.

 Si va a utilizar una versión de cc:Mail anterior a la versión 8, debe seleccionar esta casilla para activar la selección de cc:Mail como servidor de correo.

Haga clic en este botón para explorar todos los mensajes del buzón de entrada, incluidos los ya leídos o explorados.

Haga clic en este botón para limitar la exploración sólo a aquellos mensajes del buzón de entrada que aún no ha leído.

 Haga clic en
 para seleccionar una respuesta a la detección del virus.
Dependiendo de la respuesta que elija de la lista desplegable, en la sección **Acciones posibles** se mostrará:

- opciones adicionales o
- una ventana de texto para introducir información adicional o
- un mensaje que describa el resultado de la acción seleccionada.

Haga clic con el botón derecho en cualquiera de las opciones para obtener información adicional.

Si selecciona **Consultar antes de actuar** en la lista desplegable, tendrá que indicar en la pestaña **Alerta** si prefiere un mensaje o un tono cuando se detecte un virus.

 Haga clic en
 para seleccionar una respuesta a la detección de un virus.
Dependiendo de la selección, en la sección **Acciones posibles** se mostrará:

- opciones adicionales o
- una ventana de texto para introducir información adicional o
- un mensaje que describa el resultado de la acción seleccionada.

 Dependiendo de la respuesta que seleccione, en la sección **Acciones posibles** se mostrará:

- opciones adicionales o
- una ventana de texto para introducir información adicional o
- un mensaje que describa el resultado de la acción seleccionada.

Si ha seleccionado **Consultar antes de actuar** en la lista desplegable anterior, debe indicar en la pestaña **Alerta** si prefiere un mensaje, un tono o ambos.

 Seleccione esta casilla para que se le ofrezca la opción de borrar los archivos infectados del sistema cuando se detecten. Una vez seleccionada, esta opción aparece como un botón en el cuadro de diálogo **Alerta**.

 Seleccione esta casilla para que se le ofrezca la opción de ignorar los archivos infectados y continuar con la exploración. Una vez seleccionada, esta opción aparece como un botón en el cuadro de diálogo **Alerta**.

 Seleccione esta casilla para que se le ofrezca la opción de trasladar los archivos infectados a un directorio de cuarentena. A continuación, haga clic en **Examinar** para seleccionar la ubicación a la que va a trasladarse el archivo.
Una vez seleccionada, esta opción aparece como un botón en el cuadro de diálogo **Alerta**.

 Seleccione esta casilla para que se le ofrezca la opción de detener inmediatamente la exploración. Una vez seleccionada, esta opción aparece como un botón en el cuadro de diálogo **Alerta**.

 Seleccione esta casilla para que se le ofrezca la opción de limpiar los archivos infectados cuando se encuentre un virus. Una vez seleccionada, esta opción aparece como un botón en el cuadro de diálogo **Alerta**.

 Haga clic en este botón para seleccionar el archivo de cuarentena en el que va a almacenar el archivo infectado.

 Haga clic en **Examinar** para seleccionar el archivo de cuarentena en el que va a almacenar el archivo infectado.

Dependiendo de la respuesta que seleccione de la lista desplegable, en la sección **Acciones posibles** se mostrará:

- opciones adicionales.
- una ventana de texto para introducir información adicional.
- un mensaje que describa el resultado de la acción seleccionada.

 Utilice esta pantalla para indicar el método para distribuir la información relativa a la detección de virus; a través de la red, del correo electrónico o ambos. Haga clic con el botón derecho sobre cualquiera de las opciones para obtener información adicional.

Seleccione la casilla **Enviar alerta de red** para alertar al administrador de la red a través de NetShield cuando VShield encuentre un archivo infectado. A continuación, haga clic en **Examinar** para seleccionar el servidor que va a recibir el Mensaje de centralización de alertas. Una vez seleccionada, la ruta de la carpeta del mensaje aparecerá en este cuadro de texto.

NetShield es la solución anti-virus para servidor de Network Associates.

Borre la marca de esta casilla para desactivar la alerta de la red.

Seleccione la casilla **Enviar alerta de red** para alertar al administrador de la red a través de NetShield cuando VShield encuentre un archivo infectado. A continuación, haga clic en **Examinar** para seleccionar el servidor que va a recibir el Mensaje de centralización de alertas. Una vez seleccionada, la ruta de la carpeta del mensaje aparecerá en este cuadro de texto.

NetShield es la solución anti-virus para servidor de Network Associates.

 Haga clic en este botón para abrir el cuadro de diálogo **Buscar carpeta**, donde puede seleccionar el servidor que va a recibir el Mensaje de centralización de alertas. Una vez seleccionada, la ruta de la carpeta del mensaje aparecerá en el cuadro de texto.

Seleccione la casilla **Enviar alerta de red** para alertar al administrador de la red a través de NetShield cuando VShield encuentre un archivo infectado. A continuación, haga clic en **Examinar** para seleccionar el servidor que va a recibir el Mensaje de centralización de alertas. Una vez seleccionada, la ruta de la carpeta del mensaje aparecerá en el cuadro de texto.

NetShield es la solución anti-virus para servidor de Network Associates.

 Especifique a qué personas quiere informar del mensaje de correo electrónico infectado con un virus.

- Seleccione la casilla **Enviar mensaje de respuesta al remitente** para enviar un mensaje de alerta a la persona que le envió el correo electrónico infectado.
- Seleccione la casilla **Enviar mensaje de alerta al usuario** para enviar una alerta a otras personas para que estén informadas del correo electrónico infectado.

Después de seleccionar una de las opciones o ambas, haga clic en los botones **Configurar** contiguos para crear y dirigir las alertas de correo electrónico.

 Haga clic en este botón para crear la alerta de correo electrónico:

- proporcionar la dirección de la persona que le envió el correo electrónico infectado;
- ver el mensaje predeterminado o componer su propio mensaje.

 Haga clic en este botón para crear la alerta de correo electrónico:

- proporcionar la dirección de la persona a la que quiere informar del correo electrónico infectado;
- ver el mensaje predeterminado o componer su propio mensaje.

 Si ha seleccionado **Consultar antes de actuar** en la pestaña **Acción**, debe indicar si prefiere un mensaje, un tono o ambos.

 Seleccione esta casilla si quiere oír un tono cuando se encuentre un archivo infectado.
Borre la marca de esta casilla para desactivar el tono audible.

 Seleccione esta casilla si desea diseñar un mensaje personalizado para que se muestre cuando se encuentre un virus. A continuación, escriba el mensaje en el cuadro de texto siguiente. Una vez seleccionada, esta opción muestra el mensaje como texto de alerta en el cuadro de diálogo **Alerta**.

Borre la marca de esta casilla para desactivar el envío de mensajes personalizados.

 Vea el mensaje predeterminado que VShield muestra al detectar un virus o componga un nuevo mensaje.

 Active la actividad de registro, configure un archivo de registro y especifique su tamaño máximo.

 Seleccione esta casilla para activar la actividad de registro. A continuación, haga clic en **Examinar** para seleccionar un archivo para el registro. Una vez seleccionado, la ruta del archivo aparecerá en el cuadro de texto. Ahora puede definir el tamaño máximo del archivo de registro.

Seleccione la casilla **Registrar en archivo** para activar la actividad de registro. A continuación, haga clic en **Examinar** para seleccionar la carpeta en la que se va a crear el archivo de registro. Una vez seleccionada, la ruta del archivo aparecerá en este cuadro de texto.

 Seleccione esta casilla si desea limitar el tamaño del archivo de registro. Luego, introduzca en el cuadro de texto su tamaño máximo, en kilobytes. Puede utilizar
 para seleccionar el número de kilobytes o escribir el número desde el teclado.
Borre la marca de esta casilla para desactivar la limitación de tamaño del archivo de registro.

 Introduzca el tamaño máximo, en kilobytes, del archivo de registro. Puede utilizar
 para seleccionar el número de kilobytes o escribir el número desde el teclado.

 Introduzca el tamaño máximo, en kilobytes, del archivo de registro. Puede utilizar
 para seleccionar el número de kilobytes o escribir el número desde el teclado.

 Introduzca el tamaño máximo, en kilobytes, del archivo de registro. Puede utilizar
 para seleccionar el número de kilobytes o escribir el número desde el teclado.

 Haga clic en este botón para seleccionar el archivo en el que se va a crear el registro. Una vez seleccionado, la ruta del archivo aparecerá en el cuadro de texto.

 Seleccione esta casilla para registrar los nombres de todas las cepas de virus encontradas durante una sesión de exploración y el número de veces que se han encontrado.

Borre la marca de esta casilla para desactivar el registro de cepas de virus.

 Seleccione esta casilla para registrar el número de archivos infectados que se han limpiado durante una sesión de exploración. Borre la marca de esta casilla para desactivar el registro de la limpieza de virus.

 Seleccione esta casilla para registrar el número de archivos infectados que se han borrado durante una sesión de exploración. Borre la marca de esta casilla para desactivar el registro del borrado de archivos infectados.

 Seleccione esta casilla para registrar el número de archivos infectados que se han trasladado a un directorio de cuarentena durante una sesión de exploración.

Borre la marca de esta casilla para desactivar el registro de la reubicación de archivos infectados.

 Seleccione esta casilla para generar un resumen de las acciones realizadas durante esta sesión de exploración, incluidos:

- El número de archivos examinados en busca de virus.
- El número de archivos infectados que se han limpiado.
- El número de archivos infectados que se han borrado.
- El número de archivos infectados que se han trasladado.
- Otra información acerca de los valores de configuración.
- Borre la marca de esta casilla para desactivar el registro de información de resumen de la sesión.

 Seleccione una casilla o todas ellas para registrar la información correspondiente en el archivo de registro.

 Utilice esta pantalla para configurar un registro de las actividades de exploración. Haga clic con el botón derecho en cualquiera de las opciones para obtener información adicional.

 Utilice esta pantalla para seleccionar las opciones de correo electrónico que desea proteger de cambios no autorizados. Puede seleccionar todas las opciones del cuadro de lista o cualquiera de ellas por separado. Aparece  a la izquierda de las páginas protegidas.

 Seleccione las páginas de propiedades de correo electrónico (pestañas) que desea proteger de cambios no autorizados. Puede seleccionar todas las páginas de propiedades del cuadro de lista o cualquiera de ellas por separado. Aparece  a la izquierda de las páginas protegidas.

 Seleccione las páginas de propiedades de exploración del sistema (pestañas) que desea proteger de cambios no autorizados. Puede seleccionar todas las páginas de propiedades del cuadro de lista o cualquiera de ellas por separado. Aparece  a la izquierda de las páginas protegidas.

» Seleccione las páginas de propiedades del filtro de Internet (pestañas) que desea proteger de cambios no autorizados. Puede seleccionar todas las páginas de propiedades del cuadro de lista o cualquiera de ellas por separado. Aparece » a la izquierda de las páginas protegidas.

 En este cuadro de lista se enumeran las extensiones de todos los tipos de archivos explorados en busca de virus.

- Para agregar una extensión, haga clic en **Agregar**. Aparece el cuadro de diálogo **Agregar extensión de archivos de programa**.
- Para borrar una extensión de la lista, selecciónela y haga clic en **Borrar**.
- Para recuperar la lista de extensiones predeterminadas eliminando las que han sido agregadas por los usuarios, haga clic en **Predeterminadas.**

 En este cuadro de lista se enumeran las extensiones de todos los tipos de archivos explorados en busca de virus.

- Para agregar una extensión, haga clic en **Agregar**. Aparece el cuadro de diálogo **Agregar extensión de archivos de programa**.
- Para borrar una extensión de la lista, selecciónela y haga clic en **Borrar**.
- Para recuperar la lista de extensiones predeterminadas eliminando las que han sido agregadas por los usuarios, haga clic en **Predeterminadas**.

 Haga clic en este botón para cerrar el cuadro de diálogo y guardar los cambios que ha realizado.

 Haga clic en este botón para cerrar el cuadro de diálogo y guardar los cambios que ha realizado.

 Haga clic en este botón para abrir el cuadro de diálogo **Agregar extensión de archivos de programa**.

 Haga clic en este botón para borrar una extensión de archivo de programa seleccionada de la lista.

 Haga clic en este botón para recuperar las extensiones predeterminadas. Todas las extensiones que hayan sido agregadas por los usuarios se eliminarán de la lista.

 Escriba el tipo de archivo que se explorará para comprobar si tiene virus. No incluya el punto que suele preceder a la extensión.

 Escriba el tipo de archivo que se explorará para comprobar si tiene virus. No incluya el punto que suele preceder a la extensión.

 Escriba el tipo de archivo que se explorará para comprobar si tiene virus. No incluya el punto que suele preceder a la extensión.

 Haga clic en este botón para guardar los cambios y cerrar el cuadro de diálogo.

 Haga clic en este botón para cerrar el cuadro de diálogo sin guardar los cambios que ha realizado.

 Haga clic en este botón para obtener ayuda sensible al contexto acerca del uso de esta pantalla.

 Escriba la contraseña y haga clic en **Aceptar**.

 Escriba la contraseña y haga clic en **Aceptar**.

 Haga clic en este botón para continuar con el desbloqueo de la protección mediante contraseña.

 Haga clic en este botón para cerrar el cuadro de diálogo sin desbloquear la protección mediante contraseña.

 Haga clic en este botón para abrir Agenda cc:Mail. A continuación, seleccione los usuarios a los que desea enviar la alerta. Si aún no se ha registrado en cc:Mail, verá primero el cuadro de diálogo **Comprobación contraseña cc:Mail**.

 Los nombres de los usuarios a los que desea enviar la alerta aparecerán aquí tras haberlos seleccionado en **Agenda cc:Mail**. Puede escribir los nombres directamente en esta casilla.

 Haga clic en este botón para abrir Agenda cc:Mail. A continuación, seleccione los usuarios a los que desea enviar copias de la alerta.

Si aún no se ha registrado en cc:Mail, verá primero el cuadro de diálogo **Comprobación contraseña cc:Mail**.

 Los nombres de los usuarios a los que desea enviar la alerta aparecerán aquí tras haberlos seleccionado en **Agenda cc:Mail**. Puede escribir los nombres directamente en esta casilla.

 Introduzca un breve resumen del mensaje.

Escriba aquí el mensaje de alerta.

 Haga clic en este botón para guardar la configuración del correo y cerrar el cuadro de diálogo.

 Haga clic en este botón para cerrar el cuadro de diálogo sin guardar los cambios que ha realizado.

Escriba aquí el mensaje de alerta.

 Escriba una contraseña fácil de recordar.

 Escriba una contraseña fácil de recordar.

 Vuelva a escribir la contraseña exactamente como la escribió anteriormente.

 Vuelva a escribir la contraseña exactamente como la escribió anteriormente.

 Haga clic en este botón para guardar la contraseña y cerrar el cuadro de diálogo.

 Haga clic en este botón para cerrar el cuadro de diálogo sin guardar la contraseña.

 Introduzca la contraseña de cc:Mail.

 Introduzca la contraseña de cc:Mail.

 Haga clic en este botón para guardar los cambios y cerrar el cuadro de diálogo.

 Haga clic en este botón para cerrar el cuadro de diálogo sin guardar los cambios.

 Introduzca la identificación de usuario de cc:Mail.

 Introduzca la identificación de usuario de cc:Mail.

 Introduzca la contraseña de cc:Mail.

 Introduzca la contraseña de cc:Mail.

 Introduzca la ruta de cc:Mail.

 Introduzca la ruta de cc:Mail.

 Haga clic en este botón para guardar los cambios y cerrar el cuadro de diálogo.

 Haga clic en este botón para cerrar el cuadro de diálogo sin guardar los cambios.

 Haga clic en este botón para obtener ayuda sensible al contexto acerca del uso de esta pantalla.

 Escriba el nombre de la persona a la que quiere enviar la alerta. A continuación, haga clic en **Agregar** para incluir el nombre en la lista de distribución de la notificación.

 Escriba el nombre de la persona a la que quiere enviar la alerta. A continuación, haga clic en **Agregar** para incluir el nombre en la lista de distribución de la notificación.

 En este cuadro se relacionan los nombres de las personas que se encuentran en la lista de notificación de la alerta de cc:Mail.

 Haga clic en
 para seleccionar un nombre de otra lista de correo.

 Haga clic en
 para seleccionar un nombre de otra lista de correo.

 Haga clic en este botón para agregar el nombre a la lista de distribución de la notificación.

 Haga clic en este botón para borrar un nombre seleccionado de la lista de distribución de la notificación.

 Haga clic en este botón para cerrar el cuadro de diálogo sin guardar los cambios.

 Haga clic en este botón para obtener ayuda sensible al contexto acerca del uso de esta pantalla.

 Seleccione el módulo VShield que quiera configurar.

Utilice esta página para definir las propiedades de:

- la función nombrada en la pestaña
- el componente del programa seleccionado en el cuadro de la parte izquierda de la pantalla.

 Haga clic en este botón para guardar los ajustes sin cerrar el cuadro de diálogo.

 Haga clic en este botón para guardar los cambios y cerrar el cuadro de diálogo.

 Haga clic en este botón para cerrar el cuadro de diálogo sin guardar los cambios que ha realizado.

Utilice esta página para definir las propiedades de:

- la función nombrada en la pestaña
- el componente del programa seleccionado en el cuadro de la parte izquierda de la pantalla.

Utilice esta página para definir las propiedades de:

- la función nombrada en la pestaña
- el componente del programa seleccionado en el cuadro de la parte izquierda de la pantalla.

Utilice esta página para definir las propiedades de:

- la función nombrada en la pestaña
- el componente del programa seleccionado en el cuadro de la parte izquierda de la pantalla.

Utilice esta página para definir las propiedades de:

- la función nombrada en la pestaña
- el componente del programa seleccionado en el cuadro de la parte izquierda de la pantalla.

 Haga clic en este botón para utilizar el **Asistente** como guía para configurar VShield.

 Utilice esta pantalla para configurar un registro de las actividades de exploración. Haga clic con el botón derecho en cualquiera de las opciones para obtener información adicional.

 Active la actividad de registro, configure un archivo de registro y especifique su tamaño máximo.

 Seleccione esta casilla para activar la actividad de registro. A continuación, haga clic en **Examinar** para seleccionar un archivo para el registro. Una vez seleccionado, la ruta del archivo aparecerá en el cuadro de texto. Ahora puede definir el tamaño máximo del archivo de registro.

 Seleccione la casilla **Registrar en archivo** para activar la actividad de registro. A continuación, haga clic en **Examinar** para seleccionar el archivo en el que se creará el registro. Una vez seleccionado, la ruta del archivo de registro aparecerá en este cuadro de texto.

Si desea limitar el tamaño del archivo de registro, seleccione la casilla que tenga esa etiqueta. Luego, introduzca en el cuadro de texto contiguo su tamaño máximo, en kilobytes. Puede utilizar para seleccionar el número de kilobytes o escribir el número desde el teclado.

Borre la marca de la casilla **Limitar tamaño de archivo de registro a** para desactivar la limitación de tamaño del archivo de registro.

 Introduzca el tamaño máximo, en kilobytes, del archivo de registro. Puede utilizar
 para seleccionar el número de kilobytes o escribir el número desde el teclado.

 Introduzca el tamaño máximo, en kilobytes, del archivo de registro. Puede utilizar
 para seleccionar el número de kilobytes o escribir el número desde el teclado.

 Introduzca el tamaño máximo, en kilobytes, del archivo de registro. Puede utilizar
 para seleccionar el número de kilobytes o escribir el número desde el teclado.

 Haga clic en este botón para seleccionar el archivo en el que se va a crear el registro. Una vez seleccionado, la ruta del archivo de registro aparecerá en el cuadro de texto.

 Seleccione una casilla o todas ellas para registrar la información correspondiente en el archivo de registro.

 Seleccione esta casilla para registrar los nombres de todas las cepas de virus encontradas durante una sesión de exploración y el número de veces que se han encontrado.

Borre la marca de esta casilla para desactivar el registro de cepas de virus.

 Seleccione esta casilla para registrar el número de archivos infectados que se han limpiado durante una sesión de exploración. Borre la marca de esta casilla para desactivar el registro de la limpieza de virus.

 Seleccione esta casilla para registrar el número de archivos infectados que se han borrado durante una sesión de exploración. Borre la marca de esta casilla para desactivar el registro del borrado de archivos infectados.

 Seleccione esta casilla para registrar el número de archivos infectados que se han trasladado a un directorio de cuarentena durante una sesión de exploración.

Borre la marca de esta casilla para desactivar el registro de la reubicación de archivos infectados.

 Seleccione esta casilla para registrar los ajustes que ha seleccionado para esta sesión de exploración.
Borre la marca de esta casilla para desactivar el registro de los ajustes de la sesión.

 Seleccione esta casilla para generar un resumen de las acciones realizadas durante esta sesión de exploración, incluidos:

- El número de archivos examinados en busca de virus.
- El número de archivos infectados que se han limpiado.
- El número de archivos infectados que se han borrado.
- El número de archivos infectados que se han trasladado.
- Otra información acerca de los valores de configuración.
- Borre la marca de esta casilla para desactivar el registro de información de resumen.

 Haga clic en
 para seleccionar una respuesta cuando se encuentre un virus.
Dependiendo de la selección, en la sección **Acciones posibles** se mostrará:

- opciones adicionales o
- una ventana de texto para introducir información adicional o
- un mensaje que describa el resultado de la acción seleccionada.

 Seleccione esta casilla para que se le ofrezca la opción de limpiar los archivos infectados cuando se encuentre un virus. Una vez seleccionada, esta opción aparece como un botón en el cuadro de diálogo **Alerta**.

 Seleccione esta casilla para que se le ofrezca la opción de borrar los archivos infectados del sistema cuando se detecten. Una vez seleccionada, esta opción aparece como un botón en el cuadro de diálogo **Alerta**.

 Seleccione esta casilla para que se le ofrezca la opción de ignorar los archivos infectados y continuar con la exploración. Una vez seleccionada, esta opción aparece como un botón en el cuadro de diálogo **Alerta**.

 Seleccione esta casilla para que se le ofrezca la opción de trasladar los archivos infectados a un directorio de cuarentena. A continuación, haga clic en **Examinar** para seleccionar la ubicación a la que va a trasladarse el archivo.

Una vez seleccionada, esta opción aparece como un botón en el cuadro de diálogo **Alerta**.

 Haga clic en
 para seleccionar una respuesta cuando se encuentre un virus.
Dependiendo de la respuesta que seleccione en la lista desplegable, en la sección **Acciones posibles** se mostrará:

- opciones adicionales o
- una ventana de texto para introducir información adicional o
- un mensaje que describa el resultado de la acción seleccionada.

Haga clic con el botón derecho en cualquiera de las opciones para obtener información adicional.

Si selecciona **Consultar antes de actuar** en la lista desplegable, debe indicar en la pestaña **Alerta** si prefiere un mensaje o un tono. Puede diseñar un mensaje personalizado, especificar que se emita un tono audible cuando se encuentre un virus o ambos.

 Haga clic en este botón para seleccionar el archivo de cuarentena en el que va a almacenar el archivo infectado.

 Haga clic en **Examinar** para seleccionar el archivo de cuarentena en el que va a almacenar el archivo infectado.

Dependiendo de la respuesta que seleccione en la lista desplegable, en la sección **Acciones posibles** se mostrará:

- opciones adicionales.
- una ventana de texto para introducir información adicional.
- un mensaje que describa el resultado de la acción seleccionada.

 Haga clic en
 para seleccionar una respuesta cuando se encuentre un virus.
Dependiendo de la respuesta que seleccione en la lista desplegable, en la sección **Acciones posibles** se mostrará:

- opciones adicionales o
- una ventana de texto para introducir información adicional o
- un mensaje que describa el resultado de la acción seleccionada.

Haga clic con el botón derecho en cualquiera de las opciones para obtener información adicional.

Si selecciona **Consultar antes de actuar** en la lista desplegable, debe indicar en la pestaña **Alerta** si prefiere un mensaje o un tono. Puede diseñar un mensaje personalizado, especificar que se emita un tono audible cuando se encuentre un virus o ambos.

 Utilice esta pantalla para especificar una respuesta cuando se encuentre un virus. Haga clic con el botón derecho en cualquiera de las opciones para obtener información adicional.

Utilice esta pantalla para alertar al administrador de la red a través de NetShield cuando VShield encuentre un archivo infectado:

- Seleccione la casilla **Enviar alerta de red**.
- Haga clic en **Examinar** para seleccionar la carpeta de red (directorio) en la que se va a ubicar la alerta. Una vez seleccionada, la ruta de la carpeta del mensaje aparecerá en el cuadro de texto.

NetShield es la solución anti-virus para servidor de Network Associates.

 Seleccione la casilla **Enviar alerta de red** para alertar al administrador de la red a través de NetShield cuando VShield encuentre un archivo infectado. A continuación, haga clic en **Examinar** para seleccionar el servidor que va a recibir el Mensaje de centralización de alertas. Una vez seleccionado, la ruta de la carpeta del mensaje aparecerá en el cuadro de texto.

Si ha seleccionado **Consultar antes de actuar** en la pestaña **Acción**, indique en la parte inferior de la pantalla si desea un mensaje, un tono o ambos.

NetShield es la solución anti-virus para servidor de Network Associates.

Seleccione la casilla **Enviar alerta de red** para alertar al administrador de la red a través de NetShield cuando VShield encuentre un archivo infectado. A continuación, haga clic en **Examinar** para seleccionar el servidor que va a recibir el Mensaje de centralización de alertas. Una vez seleccionado, la ruta de la carpeta del mensaje aparecerá en el cuadro de texto.

NetShield es la solución anti-virus para servidor de Network Associates.

Borre la marca de esta casilla para desactivar la alerta de red.

» Seleccione la casilla **Enviar alerta de red** para alertar al administrador de la red a través de NetShield cuando VShield encuentre un archivo infectado. A continuación, haga clic en **Examinar** para seleccionar un servidor que reciba el Mensaje de centralización de alertas. Una vez seleccionada, la ruta de la carpeta del mensaje aparecerá en este cuadro de texto.

NetShield es la solución anti-virus para servidor de Network Associates.

 Haga clic en este botón para abrir el cuadro de diálogo **Buscar carpeta**, donde puede seleccionar el servidor que va a recibir el Mensaje de centralización de alertas. Una vez seleccionado, la ruta de la carpeta del mensaje aparecerá en el cuadro de texto.

 Si ha seleccionado **Consultar antes de actuar** en la pestaña **Acción**, debe indicar si prefiere un mensaje, un tono o ambos.

 Seleccione esta casilla si quiere oír un tono cuando se encuentre un archivo infectado.
Borre la marca de esta casilla para desactivar el tono audible.

 Seleccione esta casilla si desea diseñar un mensaje personalizado para que se muestre al encontrar un virus. A continuación, escriba el mensaje en el cuadro de texto siguiente. Una vez seleccionada, esta opción mostrará el mensaje como texto de alerta en el cuadro de diálogo **Alerta**.

Borre la marca de esta casilla para desactivar el envío de mensajes personalizados.

 Vea el mensaje que muestra VShield al detectar un virus o cree un nuevo mensaje.

 Utilice esta pantalla para definir los parámetros para la exploración de virus en los archivos que ha descargado de Internet. Haga clic con el botón derecho en cualquiera de las opciones para obtener información adicional.

 Seleccione esta casilla para realizar exploraciones de virus en los archivos que ha descargado de Internet:

- incluido el correo electrónico recibido a través de America Online, Eudora Light, Netscape o cualquier otro cliente de correo electrónico POP-3 o proxy.
- sin incluir el correo electrónico recibido a través de Lotus cc:Mail, Microsoft Mail o cualquier cliente de correo electrónico que cumpla con MAPI. La exploración de estos mensajes de correo electrónico se controla mediante el módulo **Exploración de correo electrónico**, no mediante el módulo **Descarga de Internet**.

Borre la marca de esta casilla para desactivar la exploración mediante Descarga de Internet.

 Elija qué archivos desea explorar de entre los descargados de Internet.

- Elija **Todos los archivos** para examinar todos los archivos que reciba.
- Elija **Sólo archivos de programa** para examinar sólo aquellos archivos más susceptibles de infectarse. Haga clic en **Extensiones** para ver una lista de los archivos susceptibles.
- Seleccione la casilla **Archivos comprimidos** para incluir la exploración de archivos **.zip** u otros tipos de archivos comprimidos.

 Seleccione este botón para especificar la exploración de todos los archivos descargados de Internet.

 Seleccione este botón para especificar la exploración sólo de los archivos de programa.

 Haga clic en este botón para ver una lista de los tipos de archivo más susceptibles de infectarse con un virus.

 Seleccione esta casilla para incluir la exploración de los archivos comprimidos con LHA, LZEXE, PkLite, PkZip o WinZip. Borre la marca de esta casilla para desactivar la exploración de archivos comprimidos.

Utilice esta pantalla para seleccionar las opciones de descarga que quiere proteger de cambios no autorizados.

Puede seleccionar todas las opciones del cuadro de lista o cualquiera de ellas por separado. Aparece a la izquierda de las páginas protegidas.

 Seleccione las páginas de propiedades de Exploración de elementos descargados (pestañas) que desea proteger de cambios no autorizados.

Puede seleccionar todas las páginas de propiedades del cuadro de lista o cualquiera de ellas por separado. Aparece  a la izquierda de las páginas protegidas.

 Utilice esta pantalla para definir los parámetros para la exploración de archivos y el control de VShield.

 Seleccione esta casilla para realizar una exploración de virus en cualquier archivo, excepto de Internet y correo electrónico. Borre la marca de esta casilla para desactivar exploración de virus.

 Especifique el evento que va a activar la exploración.
Seleccione todas las opciones de eventos o cualquiera de ellas:

- cuando se ejecuta un archivo ejecutable.
- cuando se copia un archivo.
- cuando se crea un archivo.
- cuando se renombra un archivo.

 Seleccione esta casilla para explorar los archivos ejecutables durante su ejecución.
Borre la marca de esta casilla para desactivar la exploración durante la ejecución de los archivos ejecutables.

 Seleccione esta casilla para explorar los archivos durante su copiado.
Borre la marca de esta casilla para desactivar la exploración durante el copiado de los archivos.

 Seleccione esta casilla para explorar los archivos durante su creación.
Borre la marca de esta casilla para desactivar la exploración durante la creación de los archivos.

 Seleccione esta casilla para explorar los archivos durante su renombrado.
Borre la marca de esta casilla para desactivar la exploración durante el renombrado de los archivos.

Especifique el evento que va a activar la exploración en el sector de arranque de un disquete.
Seleccione una de las opciones de eventos o ambas:

- cuando se entra en un disco de la unidad de disquetes.
- cuando se apaga el sistema.

 Seleccione esta casilla para explorar el sector de arranque de un disquete cuando se entra en el disco.
Borre la marca de esta casilla para desactivar la exploración en el sector de arranque del disquete cuando se entra.

 Seleccione esta casilla para explorar el sector de arranque de un disquete cuando se apaga el sistema.
Borre la marca de esta casilla para desactivar la exploración en el sector de arranque del disquete cuando se apaga el sistema.

 Elija qué archivos desea explorar.

- Elija **Todos los archivos** para examinar todos los archivos.
- Elija **Sólo archivos de programa** para examinar sólo aquellos archivos más susceptibles de infectarse. Haga clic en **Extensiones** para ver una lista de los archivos susceptibles.
- Seleccione la casilla **Archivos comprimidos** para incluir la exploración de archivos **.zip** u otros tipos de archivos comprimidos.

 Seleccione este botón para especificar la exploración de todos los archivos.

 Seleccione este botón para limitar la exploración sólo a los archivos de programa. A continuación, haga clic en **Extensiones** para ver una lista de los tipos de archivos más susceptibles de infectarse con un virus.

 Haga clic en este botón para ver una lista de los tipos de archivo más susceptibles de infectarse con un virus.

 Seleccione esta casilla para incluir la exploración de los archivos comprimidos con LHA, LZEXE, PkLite, PkZip o WinZip. Borre la marca de esta casilla para desactivar la exploración de archivos comprimidos.

 Seleccione las opciones de arranque, desactivación y visualización de icono.
Seleccione todas las opciones o cualquiera de ellas:

- § active la protección anti-virus cuando arranque el sistema.
- § permita al usuario desactivar VShield desde la barra de tareas o el planificador.
- § muestre el icono de VShield en la barra de tareas.

 Seleccione esta casilla para permitir la desactivación de VShield desde la barra de tareas o el planificador. Borre la marca de esta casilla para permitir la desactivación de VShield.

 Seleccione esta casilla para mostrar el icono de VShield en la barra de tareas.

 Haga clic en este botón para configurar **Analizador de macros**, función que evalúa la probabilidad de que una macro de una aplicación de Microsoft Office sea un virus.

 Utilice esta pantalla para especificar la forma en la que quiere que VShield responda cuando encuentre un virus. Haga clic con el botón derecho en cualquiera de las opciones para obtener información adicional.

 Haga clic en
 para seleccionar la forma en la que quiere que VShield responda cuando encuentre un virus. Dependiendo de la selección, en la sección **Acciones posibles** se mostrará:

- opciones adicionales o
- una ventana de texto para introducir información adicional o
- un mensaje que describa el resultado de la acción seleccionada.

 Haga clic en
 para seleccionar una respuesta cuando se encuentre un virus. Dependiendo de la selección, en la sección **Acciones posibles** se mostrará:

- opciones adicionales o
- una ventana de texto para introducir información adicional o
- un mensaje que describa el resultado de la acción seleccionada.

 Seleccione esta casilla para que se le ofrezca la opción de limpiar los archivos infectados cuando se encuentre un virus. Una vez seleccionada, esta opción aparece como un botón en el cuadro de diálogo **Alerta** de VShield.

 Seleccione esta casilla para que se le ofrezca la opción de borrar los archivos infectados del sistema cuando se detecten. Una vez seleccionada, esta opción aparece como un botón en el cuadro de diálogo **Alerta** de VShield.

 Seleccione esta casilla para que se le ofrezca la opción de excluir del procedimiento de exploración un archivo en el que se ha encontrado un virus.

Una vez seleccionada, esta opción aparece como un botón en el cuadro de diálogo **Alerta** de VShield.

 Seleccione esta casilla para que se le ofrezca la opción de entrar en un archivo, incluso cuando VShield haya encontrado un virus en él.

Una vez seleccionada, esta opción aparece como un botón en el cuadro de diálogo **Alerta** de VShield.

 Seleccione esta casilla para que se le ofrezca la opción de impedir la entrada en un archivo en el que se ha encontrado un virus.

Una vez seleccionada, esta opción aparece como un botón en el cuadro de diálogo **Alerta** de VShield.

Dependiendo de la acción que haya seleccionado de la lista desplegable, en esta sección se mostrará:

- opciones adicionales o
- una ventana de texto para introducir información adicional o
- un mensaje que describa el resultado de la acción seleccionada.

 Haga clic en este botón para seleccionar el archivo de cuarentena en el que se va a almacenar el archivo infectado.

 Haga clic en **Examinar** para seleccionar el archivo de cuarentena en el que se va a almacenar el archivo infectado.

Dependiendo de la acción que haya seleccionado de la lista desplegable, en esta sección se mostrará:

- opciones adicionales o
- una ventana de texto para introducir información adicional o
- un mensaje que describa el resultado de la acción seleccionada.

Utilice esta pantalla para alertar al administrador de la red a través de NetShield cuando VShield encuentre un archivo infectado:

- Seleccione la casilla **Enviar alerta de red**.
- Haga clic en **Examinar** para seleccionar la carpeta de red (directorio) en la que se va a ubicar la alerta. Una vez seleccionada, la ruta de la carpeta del mensaje aparecerá en el cuadro de texto.

NetShield es la solución anti-virus para servidor de Network Associates.

Seleccione la casilla **Enviar alerta de red** para alertar al administrador de la red a través de NetShield cuando VShield detecte un archivo infectado. A continuación, haga clic en **Examinar** para seleccionar el servidor que va a recibir el Mensaje de centralización de alertas. Una vez seleccionado, la ruta de la carpeta del mensaje aparecerá en el cuadro de texto.

NetShield es la solución anti-virus para servidor de Network Associates.

Borre la marca de esta casilla para desactivar la alerta de red.

Seleccione la casilla **Enviar alerta de red** para alertar al administrador de la red a través de NetShield cuando VShield encuentre un archivo infectado. A continuación, haga clic en **Examinar** para seleccionar el servidor que va a recibir el Mensaje de centralización de alertas. Una vez seleccionado, la ruta de la carpeta del mensaje aparecerá en este cuadro de texto.

NetShield es la solución anti-virus para servidor de Network Associates.

 Haga clic en este botón para abrir el cuadro de diálogo **Buscar carpeta**, donde puede seleccionar el servidor que va a recibir el Mensaje de centralización de alertas. Una vez seleccionado, la ruta de la carpeta del mensaje aparecerá en el cuadro de texto.

 Si ha seleccionado **Consultar antes de actuar** en la pestaña **Acción**, debe indicar si prefiere un mensaje, un tono o ambos.

 Seleccione esta casilla si quiere que VShield emita un tono cuando encuentre un archivo infectado.
Borre la marca de esta casilla para desactivar el tono audible.

 Seleccione esta casilla si desea diseñar un mensaje personalizado para que VShield lo muestre al encontrar un virus. A continuación, escriba el mensaje en el cuadro de texto siguiente. Una vez seleccionada, esta opción mostrará el mensaje como texto de alerta en el cuadro de diálogo **Alerta** de VShield.

Borre la marca de esta casilla para desactivar el envío de mensajes personalizados.

» Vea el mensaje que muestra VShield al detectar un virus o cree uno nuevo.

 Seleccione la casilla **Enviar alerta de red** para alertar al administrador de la red a través de NetShield cuando VShield encuentre un archivo infectado. A continuación, haga clic en **Examinar** para seleccionar el servidor que va a recibir el Mensaje de centralización de alertas. Una vez seleccionado, la ruta de la carpeta del mensaje aparecerá en el cuadro de texto.

Si ha seleccionado **Consultar antes de actuar** en la pestaña **Acción**, indique en la parte inferior de la pantalla si desea un mensaje, un tono o ambos.

NetShield es la solución anti-virus para servidor de Network Associates.

 Seleccione esta casilla para enviar una notificación a las aplicaciones de administración de escritorio o de administración de red que cumplan con el estándar Interfaz de administración de escritorio.

 Utilice esta pantalla para configurar un registro de las actividades de exploración. Haga clic con el botón derecho en cualquiera de las opciones para obtener información adicional.

 Seleccione esta casilla para activar la actividad de registro. A continuación, haga clic en **Examinar** para seleccionar un archivo para el registro. Una vez seleccionado, la ruta del archivo aparecerá en el cuadro de texto. Ahora puede definir el tamaño máximo del archivo de registro.

 Seleccione la casilla **Registrar en archivo** anterior para activar la actividad de registro de descarga. A continuación, haga clic en **Examinar** para seleccionar el archivo en el que se va a crear el registro. Una vez seleccionado, la ruta del archivo de registro aparecerá en este cuadro de texto.

 Haga clic en este botón para seleccionar el archivo en el que se va a crear el registro. Una vez seleccionado, la ruta del archivo de registro aparecerá en el cuadro de texto.

 Seleccione esta casilla si desea limitar el tamaño del archivo de registro. A continuación, introduzca en el cuadro de texto su tamaño máximo, en kilobytes. Puede utilizar  para seleccionar el número de kilobytes o escribir el número desde el teclado.

Borre la marca de esta casilla para desactivar la limitación de tamaño del archivo de registro.

 Introduzca el tamaño máximo, en kilobytes, del archivo de registro. Puede utilizar
 para seleccionar el número de kilobytes o escribir el número desde el teclado.

 Introduzca el tamaño máximo, en kilobytes, del archivo de registro. Puede utilizar
 para seleccionar el número de kilobytes o escribir el número desde el teclado.

 Seleccione una casilla o todas ellas para registrar la información correspondiente en el archivo de registro.

 Seleccione esta casilla para registrar los nombres de todas las cepas de virus encontradas durante una sesión de exploración y el número de veces que se han encontrado.

Borre la marca de esta casilla para desactivar el registro de cepas de virus.

 Seleccione esta casilla para registrar el número de archivos infectados que se han limpiado durante una sesión de exploración. Borre la marca de esta casilla para desactivar el registro de la limpieza de virus.

 Seleccione esta casilla para registrar el número de archivos infectados que se han borrado durante una sesión de exploración. Borre la marca de esta casilla para desactivar el registro del borrado de archivos infectados.

 Seleccione esta casilla para registrar el número de archivos infectados que se han trasladado a un directorio de cuarentena durante una sesión de exploración.

Borre la marca de esta casilla para desactivar el registro de la reubicación de archivos infectados.

 Seleccione esta casilla para registrar los ajustes que ha seleccionado para esta sesión de exploración.
Borre la marca de esta casilla para desactivar el registro de los ajustes de la sesión.

 Seleccione esta casilla para generar un resumen de las acciones realizadas durante esta sesión de exploración, incluidos:

- El número de archivos examinados en busca de virus.
- El número de archivos infectados que se han limpiado.
- El número de archivos infectados que se han borrado.
- El número de archivos infectados que se han trasladado.
- Otra información acerca de los ajustes de exploración.
- Borre la marca de esta casilla para desactivar el registro de información de resumen de la sesión.

 Seleccione esta casilla para registrar la fecha y hora a las que comenzó la sesión de exploración.
Borre la marca de esta casilla para desactivar el registro de fecha y hora.

 Seleccione esta casilla para registrar el nombre del usuario que realizó la exploración.
Borre la marca de esta casilla para desactivar el registro del nombre del usuario.

 Active la actividad de registro, configure un archivo de registro y especifique su tamaño máximo.

 Utilice esta pantalla para excluir objetos tales como archivos, carpetas y unidades de la detección de virus. Utilice los botones de la parte inferior de la pantalla para **Agregar** objetos adicionales a la lista; **Editar** objetos que ha están en la lista y **Eliminar** elementos de la lista.

 En este cuadro se enumeran los archivos, carpetas y unidades que se excluyen de la detección de virus. Agregue los elementos a la lista utilizando el cuadro de diálogo **Agregar Excluir elemento**, que está disponible al hacer clic en **Agregar** de la parte inferior de la pantalla. La información acerca del elemento se muestra en el cuadro inferior e incluye el **nombre** del elemento; si sus **subcarpetas** están excluidas y si el elemento está excluido **de** la Exploración de archivos, la Exploración de sectores de arranque o ambas.

 En este cuadro se enumeran los archivos, carpetas y unidades que se excluyen de la detección de virus. Los elementos se agregan a la lista utilizando el cuadro de diálogo **Agregar Excluir elemento**, que está disponible al hacer clic en **Agregar** de la parte inferior de la pantalla. La información acerca del elemento se muestra en el cuadro inferior e incluye el **nombre** del elemento; si sus **subcarpetas** están excluidas y si el elemento está excluido **de** la Exploración de archivos, la Exploración de sectores de arranque o ambas.

 En este cuadro se enumeran los archivos, carpetas y unidades que se excluyen de la detección de virus. Los elementos se agregan a la lista utilizando el cuadro de diálogo **Agregar Excluir elemento**, que está disponible al hacer clic en **Agregar** de la parte inferior de la pantalla. La información acerca del elemento se muestra en el cuadro inferior e incluye el **nombre** del elemento; si sus **subcarpetas** están excluidas y si el elemento está excluido **de** la Exploración de archivos, la Exploración de sectores de arranque o ambas.

 En este cuadro se enumeran los archivos, carpetas y unidades que se excluyen de la detección de virus. Los elementos se agregan a la lista utilizando el cuadro de diálogo **Agregar Excluir elemento**, que está disponible al hacer clic en **Agregar** de la parte inferior de la pantalla. La información acerca del elemento se muestra en el cuadro inferior e incluye el **nombre** del elemento; si sus **subcarpetas** están excluidas y si el elemento está excluido **de** la Exploración de archivos, la Exploración de sectores de arranque o ambas.

 Haga clic en este botón para abrir el cuadro de diálogo **Agregar Excluir elemento**.

 Haga clic en este botón para abrir el cuadro de diálogo **Editar Excluir elemento**.

 Haga clic en este botón para borrar un elemento seleccionado de la lista de elementos excluidos anterior.

 Seleccione las páginas de propiedades (pestañas) que desea proteger de cambios no autorizados.

Puede seleccionar todas las páginas de propiedades del cuadro de lista o cualquiera de ellas por separado. Aparece  a la izquierda de las páginas protegidas.

 Haga clic en **Examinar** para seleccionar una carpeta que se va a excluir de la exploración de virus. Una vez seleccionada, la ruta de la carpeta aparecerá en este cuadro de texto.

 Haga clic en **Examinar** para seleccionar una carpeta que se va a excluir de la exploración de virus. Una vez seleccionada, la ruta de la carpeta aparecerá en este cuadro de texto.

 Haga clic en este botón para seleccionar una carpeta que se va a excluir de la exploración de virus. Una vez seleccionada, la ruta de la carpeta aparecerá en el cuadro de texto.

 Seleccione esta casilla para excluir de la exploración de virus todas las subcarpetas asociadas con la carpeta designada para excluirse.

 Seleccione esta casilla para excluir el archivo o carpeta anterior solamente de **Exploración de archivos**.

 Seleccione esta casilla para excluir el archivo o carpeta anterior solamente de **Exploración de sectores de arranque**.

 Seleccione una casilla o ambas para especificar si el archivo o carpeta designados anteriormente van a excluirse de **Exploración de archivos**, de **Exploración de sectores de arranque** o de ambos.

 Haga clic en este botón para guardar los cambios y cerrar el cuadro de diálogo.

 Haga clic en este botón para cerrar el cuadro de diálogo sin guardar los cambios que ha realizado.

 Utilice esta pantalla para indicar a VShield que explore las clases de Java y los controles de ActiveX perjudiciales o los sitios de Internet peligrosos.

 Seleccione esta casilla para explorar las clases de Java perjudiciales, los controles de ActiveX o los sitios de Internet peligrosos.

Borre la marca de esta casilla para desactivar la exploración de Java, ActiveX u otras funciones de Internet peligrosas.

Seleccione las casillas para indicar a VShield qué objetos perjudiciales debe bloquear cuando se visiten sitios de Internet. Puede optar por bloquear los controles de ActiveX y las clases de Java o cada objeto por separado.

Seleccione esta casilla para explorar los controles de ActiveX perjudiciales cuando se visiten sitios de Internet.
VShield compara los controles de ActiveX que encuentre con una base de datos de controles conocidos como causantes de daños. Le alerta cuando encuentre un control de ActiveX potencialmente dañino.

Seleccione esta casilla para explorar los controles de ActiveX perjudiciales cuando se visiten sitios de Internet.
VShield compara los controles de ActiveX que encuentre con una base de datos de controles conocidos como causantes de daños. Le alerta cuando encuentre un control de ActiveX potencialmente dañino.

 Seleccione esta casilla para explorar en busca de clases de Java perjudiciales cuando se visiten sitios Internet.
VShield compara las clases de Java que encuentre con una base de datos de clases conocidas como causantes de daños. Le alerta cuando encuentra una clase de Java potencialmente dañina.

 Seleccione estas casillas para indicar a VShield que impida al software del examinador visitar los sitios de Internet peligrosos. Puede optar por identificar los sitios peligrosos con direcciones IP numéricas, con nombres de host (URL o dominios) o con ambos métodos. Haga clic en **Configurar** a la derecha de cada casilla para ver o agregar a la lista que VShield utiliza para identificar los sitios de Internet peligrosos.

 Haga clic en este botón para ver o agregar a la lista de direcciones IP que VShield utiliza para identificar los sitios de Internet peligrosos.

 Seleccione esta casilla para indicar a VShield que impida al software del examinador visitar los sitios de Internet que designe con un URL (Uniform Resource Locator) o un nombre de dominio.

A continuación, haga clic en **Configurar** para ver o agregar a la lista que VShield utiliza para identificar los sitios de Internet peligrosos.

 Haga clic en este botón para ver o agregar a la lista de URL o dominios que VShield utiliza para identificar los sitios de Internet peligrosos.

 Utilice esta pantalla para especificar una respuesta cuando se encuentre un virus. Haga clic con el botón derecho en cualquiera de las opciones para obtener información adicional.

 Haga clic en
 para seleccionar una respuesta de VShield al encontrar un virus. En la sección **Acciones posibles** se mostrará un mensaje que describa el resultado de la acción seleccionada.

 Haga clic en
 para seleccionar una respuesta de VShield al encontrar un virus. En la sección **Acciones posibles** se mostrará un mensaje que describa el resultado de la acción seleccionada.

 Haga clic en
 para seleccionar una respuesta de VShield al encontrar un virus. En la sección **Acciones posibles** se mostrará un mensaje que describa el resultado de la acción seleccionada.

 Haga clic en
 para seleccionar una respuesta de VShield al encontrar un virus. En la sección **Acciones posibles** se mostrará un mensaje que describa el resultado de la acción seleccionada.

 Utilice esta pantalla para configurar un registro de las actividades de exploración. Haga clic con el botón derecho en cualquiera de las opciones para obtener información adicional.

 Active la actividad de registro, configure un archivo de registro y especifique su tamaño máximo.

 Seleccione esta casilla para activar la actividad de registro. A continuación, haga clic en **Examinar** para seleccionar un archivo para el registro. Una vez seleccionado, la ruta del archivo aparecerá en el cuadro de texto. Ahora puede definir el tamaño máximo del archivo de registro.

 Seleccione la casilla **Registrar en archivo** anterior para activar la actividad de registro. A continuación, haga clic en **Examinar** para seleccionar el archivo en el que se va a crear el registro. Una vez seleccionado, la ruta del archivo de registro aparecerá en este cuadro de texto.

 Seleccione esta casilla si desea limitar el tamaño del archivo de registro. A continuación, introduzca en el cuadro de texto su tamaño máximo, en kilobytes. Puede utilizar  para seleccionar el número de kilobytes o escribir el número desde el teclado.

Borre la marca de esta casilla para desactivar la limitación de tamaño del archivo de registro.

 Introduzca el tamaño máximo, en kilobytes, del archivo de registro. Puede utilizar
 para seleccionar el número de kilobytes o escribir el número desde el teclado.

 Introduzca el tamaño máximo, en kilobytes, del archivo de registro. Puede utilizar
 para seleccionar el número de kilobytes o escribir el número desde el teclado.

 Introduzca el tamaño máximo, en kilobytes, del archivo de registro. Puede utilizar
 para seleccionar el número de kilobytes o escribir el número desde el teclado.

 Haga clic en este botón para seleccionar el archivo en el que se va a crear el registro. Una vez seleccionado, la ruta del archivo de registro aparecerá en el cuadro de texto.

Utilice esta pantalla para alertar al administrador de la red a través de NetShield cuando VShield encuentre un archivo infectado:

- Seleccione la casilla **Enviar alerta de red**.
- Haga clic en **Examinar** para seleccionar la carpeta de red en la que se va a ubicar la alerta. Una vez seleccionada, la ruta de la carpeta del mensaje aparecerá en el cuadro de texto.

NetShield es la solución anti-virus para servidor de Network Associates.

 Haga clic en este botón para abrir el cuadro de diálogo **Buscar carpeta**, donde puede seleccionar el servidor que va a recibir el Mensaje de centralización de alertas. Una vez seleccionado, la ruta de la carpeta del mensaje aparecerá en el cuadro de texto.

 Seleccione la casilla **Enviar alerta de red** para alertar al administrador de la red a través de NetShield cuando VShield encuentre un archivo infectado. A continuación, haga clic en **Examinar** para seleccionar el servidor que va a recibir el Mensaje de centralización de alertas. Una vez seleccionado, la ruta de la carpeta del mensaje aparecerá en el cuadro de texto.

Si ha seleccionado **Consultar antes de actuar** en la pestaña **Acción**, indique en la parte inferior de la pantalla si desea un mensaje, un tono o ambos.

NetShield es la solución anti-virus para servidor de Network Associates.

 Si ha seleccionado **Consultar antes de actuar** en la pestaña **Acción**, debe indicar si prefiere un mensaje, un tono o ambos.

 Seleccione esta casilla si quiere oír un tono cuando se encuentre un archivo infectado.
Borre la marca de esta casilla para desactivar el tono audible.

 Seleccione esta casilla si desea diseñar un mensaje personalizado para que se muestre al encontrar un virus. A continuación, escriba el mensaje en el cuadro de texto siguiente. Una vez seleccionada, esta opción mostrará el mensaje como texto de alerta en el cuadro de diálogo **Alerta**.

Borre la marca de esta casilla para desactivar el envío de mensajes personalizados.

» Vea el mensaje que se mostrará al detectar un virus o cree uno nuevo.

 Seleccione esta casilla para enviar una notificación a las aplicaciones de administración de escritorio o de administración de red que cumplan con el estándar Interfaz de administración de escritorio.

 Haga clic en este botón para guardar los cambios y cerrar el cuadro de diálogo.

 Haga clic en este botón para cerrar el cuadro de diálogo sin guardar los cambios que ha realizado.

 Haga clic en este botón para abrir el cuadro de diálogo **Agregar dirección de dominio**.

 Haga clic en este botón para borrar una dirección de dominio seleccionada de la lista de direcciones prohibidas.

 En este cuadro se enumeran las direcciones de dominio prohibidas.

- Para prohibir una dirección de dominio, haga clic en **Agregar**. Aparece el cuadro de diálogo **Agregar dirección de dominio**.
- Para borrar una dirección de dominio de la lista de direcciones prohibidas, selecciónela y haga clic en **Borrar**.

 Haga clic en este botón para guardar el cambio y cerrar el cuadro de diálogo.

 Haga clic en este botón para cerrar el cuadro de diálogo sin guardar los cambios que ha realizado.

 Haga clic en este botón para abrir el cuadro de diálogo **Agregar dirección IP**.

 Haga clic en este botón para borrar una dirección IP seleccionada de la lista de direcciones prohibidas.

En este cuadro se enumeran las direcciones IP prohibidas.

- Para prohibir una dirección IP, haga clic en **Agregar**. Aparece el cuadro de diálogo **Agregar dirección IP**.
- Para borrar una dirección IP de la lista de direcciones prohibidas, selecciónela y haga clic en **Borrar**.

 Escriba el URL que se va a agregar a la lista de direcciones de dominio prohibidas.

 Escriba el URL que se va a agregar a la lista de direcciones de dominio prohibidas.

 Haga clic en este botón para guardar los cambios y cerrar el cuadro de diálogo.

 Haga clic en este botón para cerrar el cuadro de diálogo sin guardar los cambios que ha realizado.

 Haga clic en este botón para obtener ayuda sensible al contexto acerca del uso de esta pantalla.

En los siguientes cuadros, identifique la dirección IP y la máscara de subred cuyo acceso se va a bloquear.

 Escriba la dirección IP que se va a agregar a la lista de direcciones IP prohibidas.

 Escriba la máscara de subred de la dirección IP que se va a agregar a la lista de direcciones IP prohibidas.

 Haga clic en este botón para guardar los cambios y cerrar el cuadro de diálogo.

 Haga clic en este botón para cerrar el cuadro de diálogo sin guardar los cambios que ha realizado.

 Haga clic en este botón para obtener ayuda sensible al contexto acerca del uso de esta pantalla.

 Seleccione esta casilla para activar la protección mediante contraseña.

 Indique si desea proteger todas las páginas de propiedades o sólo las que ha seleccionado.

- **Páginas de propiedades** son las pantallas en las que puede seleccionar la configuración y las opciones.
- Haga clic en cada pestaña para ver una lista de las páginas de propiedades que quizá quiera proteger mediante contraseña.

 Seleccione este botón para proteger mediante contraseña todas las selecciones de configuración y opciones que ha realizado.

 Seleccione este botón para proteger mediante contraseña sólo las opciones que especifique. Haga clic en cada pestaña para ver una lista de las páginas de propiedades que quizá quiera proteger mediante contraseña.

 Introduzca una contraseña para proteger las configuraciones y opciones que haya seleccionado.

 Introduzca una contraseña para proteger las configuraciones y opciones que haya seleccionado.

 Introduzca una contraseña para proteger las configuraciones y opciones que haya seleccionado.

 Vuelva a escribir la contraseña que haya introducido.

 Vuelva a escribir la contraseña que haya introducido.

» Seleccione las páginas de propiedades del filtro de Internet (pestañas) que desea proteger de cambios no autorizados. Puede seleccionar todas las páginas de propiedades del cuadro de lista o cualquiera de ellas por separado. Aparece » a la izquierda de las páginas protegidas.

 Utilice esta pantalla para activar y configurar el **Analizador de macros**, función que evalúa la probabilidad de que una macro de una aplicación de Microsoft Office sea un virus.

 Seleccione esta casilla para activar **Analizador de macros**, función que evalúa la probabilidad de que una característica no reconocida de una aplicación de Microsoft Office sea un virus.

Utilice la pestaña deslizante para definir el umbral de sensibilidad para definir una macro como virus.

- Un ajuste bajo minimiza el número de macros interpretadas como virus.
- Un ajuste alto maximiza el número de macros interpretadas como virus.

 Utilice la pestaña deslizante para ajustar el umbral de sensibilidad para definir una macro como virus.

- Un ajuste bajo minimiza el número de macros interpretadas como virus.
- Un ajuste alto maximiza el número de macros interpretadas como virus.

 Utilice la pestaña deslizante para ajustar el umbral de sensibilidad para definir una macro como virus.

- Un ajuste bajo minimiza el número de macros interpretadas como virus.
- Un ajuste alto maximiza el número de macros interpretadas como virus.

 Utilice la pestaña deslizante para ajustar el umbral de sensibilidad para definir una macro como virus.

- Un ajuste bajo minimiza el número de macros interpretadas como virus.
- Un ajuste alto maximiza el número de macros interpretadas como virus.

 Utilice la pestaña deslizante para ajustar el umbral de sensibilidad para definir una macro como virus.

- Un ajuste bajo minimiza el número de macros interpretadas como virus.
- Un ajuste alto maximiza el número de macros interpretadas como virus.

 Utilice la pestaña deslizante para ajustar el umbral de sensibilidad para definir una macro como virus.

- Un ajuste bajo minimiza el número de macros interpretadas como virus.
- Un ajuste alto maximiza el número de macros interpretadas como virus.

 Seleccione esta casilla para borrar las macros de los documentos de Microsoft Office infectados al limpiarlos. Borre la marca de esta casilla para desactivar el borrado de macros.

 Haga clic en este botón para guardar los cambios y cerrar el cuadro de diálogo.

 Haga clic en este botón para cerrar el cuadro de diálogo sin guardar los cambios que ha realizado.

 Haga clic en este botón para obtener ayuda sensible al contexto acerca del uso de esta pantalla.

 Esta pantalla muestra información importante para identificar la copia de VirusScan para Windows 95 y Windows 98. Haga clic en **Aceptar** cuando haya visto su contenido.

 Esta pantalla muestra información importante para identificar la copia de VirusScan para Windows 95 y Windows 98. Haga clic en **Aceptar** cuando haya visto su contenido.

 Esta pantalla muestra información importante para identificar la copia de VirusScan para Windows 95 y Windows 98. Haga clic en **Aceptar** cuando haya visto su contenido.

 Esta pantalla muestra información importante para identificar la copia de VirusScan para Windows 95 y Windows 98. Haga clic en **Aceptar** cuando haya visto su contenido.

 Esta pantalla muestra información importante para identificar la copia de VirusScan para Windows 95 y Windows 98. Haga clic en **Aceptar** cuando haya visto su contenido.

 Esta pantalla muestra información importante para identificar la copia de VirusScan para Windows 95 y Windows 98. Haga clic en **Aceptar** cuando haya visto su contenido.

 Esta pantalla muestra información importante para identificar la copia de VirusScan para Windows 95 y Windows 98. Haga clic en **Aceptar** cuando haya visto su contenido.

 Esta pantalla muestra información importante para identificar la copia de VirusScan para Windows 95 y Windows 98. Haga clic en **Aceptar** cuando haya visto su contenido.

 Esta pantalla muestra información importante para identificar la copia de VirusScan para Windows 95 y Windows 98. Haga clic en **Aceptar** cuando haya visto su contenido.

 Esta pantalla muestra información importante para identificar la copia de VirusScan para Windows 95 y Windows 98. Haga clic en **Aceptar** cuando haya visto su contenido.

 En este cuadro de lista se enumeran las extensiones de todos los tipos de archivos explorados en busca de virus.

- Para agregar una extensión, haga clic en **Agregar**. Aparece el cuadro de diálogo **Agregar extensión de archivos de programa**.
- Para borrar una extensión de la lista, selecciónela y haga clic en **Borrar**.
- Para recuperar la lista de extensiones predeterminadas eliminando las que han sido agregadas por los usuarios, haga clic en **Predeterminadas**.

 Haga clic en este botón para guardar los cambios y cerrar el cuadro de diálogo.

 Haga clic en este botón para cerrar el cuadro de diálogo sin guardar los cambios.

 Haga clic en este botón para abrir el cuadro de diálogo **Agregar extensión de archivos de programa**.

 Para borrar de la lista una extensión de archivo de programa, selecciónela. A continuación, haga clic en este botón.

 Haga clic en este botón para recuperar las extensiones predeterminadas. Todas las extensiones que han sido agregadas por los usuarios se eliminan de la lista.

 Escriba la extensión del tipo de archivo que se va a agregar a la lista de tipos incluidos en la exploración. No incluya el punto que suele preceder a la extensión.

 Escriba la extensión del tipo de archivo que se va a agregar a la lista de tipos incluidos en la exploración. No incluya el punto que suele preceder a la extensión.

 Haga clic en este botón para guardar los cambios y cerrar el cuadro de diálogo.

 Haga clic en este botón para cerrar el cuadro de diálogo sin guardar los cambios.

 Esta pantalla muestra información importante para los usuarios de la versión de evaluación de VirusScan para Windows 95 y Windows 98. Haga clic en **Aceptar** cuando haya visto su contenido.

 Esta pantalla muestra información importante para los usuarios de la versión de evaluación de VirusScan para Windows 95 y Windows 98. Haga clic en **Aceptar** cuando haya visto su contenido.

 Esta pantalla muestra información importante para los usuarios de la versión de evaluación de VirusScan para Windows 95 y Windows 98. Haga clic en **Aceptar** cuando haya visto su contenido.

 Esta pantalla muestra información importante para los usuarios de la versión de evaluación de VirusScan para Windows 95 y Windows 98. Haga clic en **Aceptar** cuando haya visto su contenido.

 Esta pantalla muestra información importante para los usuarios de la versión de evaluación de VirusScan para Windows 95 y Windows 98. Haga clic en **Aceptar** cuando haya visto su contenido.

 Esta pantalla muestra información importante para los usuarios de la versión de evaluación de VirusScan para Windows 95 y Windows 98. Haga clic en **Aceptar** cuando haya visto su contenido.

 Esta pantalla muestra información importante para los usuarios de la versión de evaluación de VirusScan para Windows 95 y Windows 98. Haga clic en **Aceptar** cuando haya visto su contenido.

 Esta pantalla muestra información importante para los usuarios de la versión de evaluación de VirusScan para Windows 95 y Windows 98. Haga clic en **Aceptar** cuando haya visto su contenido.

 Esta pantalla muestra información importante para los usuarios de la versión de evaluación de VirusScan para Windows 95 y Windows 98. Haga clic en **Aceptar** cuando haya visto su contenido.

 Esta pantalla muestra información importante para los usuarios de la versión de evaluación de VirusScan para Windows 95 y Windows 98. Haga clic en **Aceptar** cuando haya visto su contenido.

 Esta pantalla muestra información de identificación detallada acerca del archivo infectado, su ubicación y sus atributos.

 Esta pantalla muestra información acerca del archivo infectado.

 Describe el tipo de archivo del archivo infectado.

 Describe el tipo de archivo del archivo infectado.

 Muestra la ruta del archivo infectado.

 Muestra la ruta del archivo infectado.

 Muestra el número de bytes del archivo infectado.

 Muestra el número de bytes del archivo infectado.

 Esta pantalla muestra información de identificación detallada acerca del archivo infectado, su ubicación y sus atributos.

 Muestra el nombre de archivo basándose en la convención de DOS de 8 caracteres mas una extensión de 3 caracteres. Los nombres de archivo largos se cortan.

 Muestra el nombre de archivo basándose en la convención de DOS de 8 caracteres mas una extensión de 3 caracteres. Los nombres de archivo largos se cortan.

 Muestra la fecha de creación del archivo infectado.

 Muestra la fecha de creación del archivo infectado.

 Muestra la fecha de la última modificación del archivo infectado.

 Muestra la fecha de la última modificación del archivo infectado.

 Muestra la fecha en que se abrió, se copió o se ejecutó el archivo infectado por última vez.

 Muestra la fecha en que se abrió, se copió o se ejecutó el archivo infectado por última vez.

 El área siguiente

 VirusScan selecciona este cuadro si el archivo infectado es un archivo de sólo lectura. Consulte la documentación del sistema operativo para ver las definiciones de los atributos del archivo.

 VirusScan selecciona este cuadro si el archivo infectado es un archivo oculto. Consulte la documentación del sistema operativo para ver las definiciones de los atributos del archivo.

 VirusScan selecciona este cuadro si el archivo infectado es un fichero de archivo. Consulte la documentación del sistema operativo para ver las definiciones de los atributos del archivo.

 VirusScan selecciona este cuadro si el archivo infectado es un archivo del sistema. Consulte la documentación del sistema operativo para ver las definiciones de los atributos del archivo.

 VirusScan muestra los atributos del archivo infectado colocando una marca al lado de todos los que sean aplicables.

 Indica la disposición actual del virus.

 Indica la disposición actual del virus.

 Esta pantalla muestra información detallada acerca del virus que VShield ha detectado, incluyendo su nombre, los tipos de archivos a los que afecta y sus características.

 Muestra el nombre del virus que infecta al archivo.

 Muestra el nombre del virus que infecta al archivo.

 Muestra los tipos de archivos susceptibles de infectarse con este virus.

 Muestra los tipos de archivos susceptibles de infectarse con este virus.

 Muestra el número de bytes que ocupa el virus.

 Muestra el número de bytes que ocupa el virus.

 Esta pantalla muestra detallada acerca del virus que VShield ha detectado, incluyendo su nombre, los tipos de archivos a los que afecta y sus características.

» Las casillas seleccionadas describen las características del virus causante de la infección.

 VirusScan selecciona este recuadro si el virus se conserva en la memoria después de ejecutarse y continúa infectando otros archivos.

 VirusScan selecciona este recuadro si el virus encripta parte de su firma codificada para evitar su detección.

 VirusScan selecciona este recuadro si el virus evita su detección cambiando ligeramente su firma codificada cada vez que se copia a sí mismo.

 VirusScan selecciona este recuadro si se puede limpiar el virus.

 Haga clic en uno de los botones siguientes para que tenga lugar la ación descrita. Haga clic con el botón derecho en un botón para ver una descripción de la acción.

 Haga clic en este botón para tratar de limpiar el virus.

 Haga clic en este botón para eliminar el archivo infectado.

 Haga clic en este botón para seleccionar una ubicación de cuarentena para el archivo infectado.

 Haga clic en este botón para iniciar la exploración basándose en las opciones que ha seleccionado en las páginas de propiedades de las pestañas.

 Haga clic en este botón para detener una exploración en curso.

 Haga clic en este botón para actualizar los archivos de datos. Vea Actualización de los archivos de datos de VirusScan para obtener detalles.

 Haga clic en **Examinar** para seleccionar una unidad, disco, carpeta o archivo para explorar. La ubicación seleccionada aparece en el cuadro de texto.

 Haga clic en este botón para seleccionar una unidad, disco, carpeta o archivo para explorar. La ubicación seleccionada aparece en el cuadro de texto.

 Seleccione esta casilla para incluir la exploración de las subcarpetas de la unidad o carpeta seleccionadas.

 Seleccione este botón para especificar la exploración todos los archivos y tipos de archivo.

 Seleccione este botón para limitar la exploración sólo a los archivos de programa. A continuación, haga clic en **Extensiones** para ver una lista de los tipos de archivos más susceptibles de infectarse con un virus.

 Seleccione esta casilla para incluir la exploración de los archivos comprimidos con LHA, LZEXE, PkLite, PkZip o WinZip. Borre la marca de esta casilla para desactivar la exploración de archivos comprimidos.

 Haga clic en este botón para ver una lista de los tipos de archivo más susceptibles de infectarse con un virus.

 En la parte superior de la pantalla, seleccione un disco, unidad, carpeta o archivo para explorar. En la parte inferior de la pantalla, seleccione los tipos de archivos para incluir en la exploración.

 Haga clic en
 para seleccionar una respuesta cuando se detecte un virus. Dependiendo de la selección, en la sección **Acciones posibles** se mostrará:

- opciones adicionales o
- una ventana de texto para introducir información adicional o
- un mensaje que describa el resultado de la acción seleccionada.

 Haga clic en **Examinar** para seleccionar el archivo de cuarentena en el que se va a almacenar el archivo infectado.

 Haga clic en **Examinar** para seleccionar el archivo de cuarentena en el que se va a almacenar el archivo infectado.

 Haga clic en **Examinar** para seleccionar la carpeta de cuarentena en la que se van a almacenar los archivos infectados. La ruta de la carpeta seleccionada aparecerá en el cuadro de texto.

 Haga clic en **Examinar** para seleccionar la carpeta de cuarentena en la que se van a almacenar los archivos infectados. La ruta de la carpeta seleccionada aparecerá aquí.

 Haga clic en este botón para seleccionar la carpeta de cuarentena en la que se van a almacenar los archivos infectados. La ruta de la carpeta seleccionada aparecerá en el cuadro de texto.

 En la parte superior de la pantalla, seleccione el tipo de señal de alerta que prefiere cuando se detecta un virus. En la parte inferior de la pantalla, indique si desea crear un registro de la actividad de exploración. Luego, puede especificar la ubicación del archivo de registro y el tamaño máximo.

 Si ha seleccionado **Consultar antes de actuar** en la pestaña **Acción**, ahora debe indicar si prefiere un mensaje, un tono o ambos. Seleccione esta casilla si quiere que se muestre un mensaje al detectar un virus. A continuación, introduzca un breve mensaje en el cuadro de texto.

Borre la marca de esta casilla para desactivar el envío de mensajes.

» Seleccione la casilla **Mostrar mensaje** si quiere que se muestre un mensaje al detectar un virus. A continuación, introduzca un breve mensaje aquí.

Borre la marca de esta casilla para desactivar el envío de mensajes.

 Si ha seleccionado **Consultar antes de actuar** en la pestaña **Acción**, ahora debe indicar si prefiere un mensaje, un tono o ambos. Seleccione esta casilla si quiere oír un tono audible cuando se encuentre un virus.

Borre la marca de esta casilla para desactivar el tono.

 Seleccione esta casilla para activar la actividad de registro. A continuación, haga clic en **Examinar** para seleccionar un archivo para el registro. Una vez seleccionado, la ruta del archivo aparecerá en el cuadro de texto. Ahora puede definir el tamaño máximo del archivo de registro.

Borre la marca de esta casilla para desactivar el registro de la actividad.

 Seleccione la casilla **Registrar en archivo** para activar la actividad de registro. A continuación, haga clic en **Examinar** para seleccionar un archivo para el registro. Una vez seleccionado, la ruta del archivo aparecerá en este cuadro de texto. Ahora puede definir el tamaño máximo del archivo de registro.

 Haga clic en este botón para seleccionar el archivo en el que se va a crear el registro. Una vez seleccionado, la ruta del archivo de registro aparecerá en el cuadro de texto.

 Seleccione esta casilla si desea limitar el tamaño del archivo de registro. A continuación, introduzca en el cuadro de texto su tamaño máximo, en kilobytes. Puede utilizar
 para seleccionar el número de kilobytes o escribir el número desde el teclado.
Borre la marca de esta casilla para desactivar la limitación de tamaño del archivo de registro.

 Introduzca el tamaño máximo, en kilobytes, del archivo de registro. Puede utilizar
 para seleccionar el número de kilobytes o escribir el número desde el teclado.

 Introduzca el tamaño máximo, en kilobytes, del archivo de registro. Puede utilizar
 para seleccionar el número de kilobytes o escribir el número desde el teclado.

Este cuadro muestra información importante acerca de las condiciones que se aplican al uso de este producto.

 VirusScan utiliza este cuadro para mostrar mensajes. Haga clic en **Aceptar** para cerrar el cuadro.

 VirusScan utiliza este cuadro para mostrar mensajes. Haga clic en **Aceptar** para cerrar el cuadro.

 Haga clic en **Continuar** para seguir con la exploración sin realizar ninguna acción por el momento.

 Haga clic en este botón para detener la exploración sin realizar ninguna acción por el momento.

 Haga clic en este botón para intentar limpiar el virus.

 Haga clic en este botón para eliminar el archivo infectado.

 Haga clic en este botón para seleccionar una ubicación de cuarentena para el archivo infectado.

 Haga clic en este botón para excluir el archivo infectado de la exploración.

 Haga clic en este botón para ver información adicional acerca del virus.

 En esta área aparece el nombre del archivo que contiene el virus.

 En esta área aparece el nombre del archivo que contiene el virus.

 Aquí aparece el nombre del virus que infecta al archivo.

 Aquí aparece el nombre del virus que infecta al archivo.

 Aquí aparece el nombre del virus que infecta al archivo. Haga clic en
 para ver una lista de las macros localizadas dentro de los virus encontrados en aplicaciones de Microsoft Office.

 VirusScan hace una sugerencia acerca de cómo manejar el virus que ha encontrado.

 Muestra el mensaje personalizado que se haya designado para aparecer cuando VirusScan detecte un virus.

 Indica la exploración de virus en la memoria que VirusScan está realizando.

 Haga clic en este botón para cerrar el cuadro de diálogo sin actualizar las definiciones de los virus.

 Haga clic en este botón para asegurar los archivos de definición de virus más actuales de Network Associates.

 Este cuadro enumera los archivos de definición de virus que VirusScan utiliza.

 Este cuadro muestra la antigüedad de las definiciones de virus que se utilizan actualmente.

 Este cuadro muestra la antigüedad de las definiciones de virus que se utilizan actualmente.

 Haga clic en esta casilla para recibir un recordatorio acerca de los archivos de definición de virus antiguos el próximo mes.

 Haga clic en este botón para guardar los cambios y cerrar el cuadro de diálogo.

 Haga clic en este botón para cerrar el cuadro de diálogo sin guardar los cambios.

 Escriba una contraseña fácil de recordar.

 Vuelva a escribir la contraseña exactamente como la escribió anteriormente.

 Después de introducir una contraseña válida, haga clic en este botón para abrir las pantallas de seguridad de protección mediante contraseña.

 Haga clic en este botón para cerrar el cuadro de diálogo sin intentar abrir las pantallas de seguridad de protección mediante contraseña.

 Escriba la contraseña que controla el acceso a la seguridad de protección mediante contraseña de VirusScan.

 Este cuadro muestra las carpetas y archivos disponibles en la unidad seleccionada en el cuadro de texto Unidades de la parte inferior de la pantalla. Para abrir cualquier carpeta o archivo, haga clic en uno de los nombres incluidos en la lista y, a continuación, haga clic en **Aceptar**. También puede hacer doble clic en uno de los nombres incluidos en esta lista para abrirlo.

 Haga clic en
 para seleccionar la unidad local que contiene el archivo que desea abrir.

 Haga clic en
 para seleccionar la unidad local que contiene el archivo que desea abrir.

 Haga clic en este botón para abrir el archivo seleccionado.

 Haga clic en este botón para cerrar el cuadro de diálogo sin abrir un archivo.

 Haga clic en este botón para seleccionar la unidad de red que contiene el archivo que desea abrir.

 Introduzca la identificación de usuario de cc:Mail.

 Introduzca la contraseña de cc:Mail.

 Introduzca la ruta de cc:Mail.

 Introduzca la contraseña de cc:Mail.

 Describe el tipo de archivo del archivo infectado.

 Muestra la ruta del archivo infectado.

 Muestra el número de bytes del archivo infectado.

 Muestra el nombre de archivo basándose en la convención de DOS de 8 caracteres mas una extensión de 3 caracteres. Los nombres de archivo largos se cortan.

 Muestra la fecha de creación del archivo infectado.

 Muestra la fecha de la última modificación del archivo infectado.

 Muestra la fecha en que se abrió, se copió o se ejecutó el archivo infectado por última vez.

 VirusScan selecciona este recuadro si el archivo infectado es un archivo de sólo lectura. Consulte la documentación del sistema operativo para ver las definiciones de los atributos del archivo.

 VirusScan selecciona este recuadro si el archivo infectado es un fichero de archivo. Consulte la documentación del sistema operativo para ver las definiciones de los atributos del archivo.

 VirusScan selecciona este recuadro si el archivo infectado es un archivo oculto. Consulte la documentación del sistema operativo para ver las definiciones de los atributos del archivo.

 Muestra el nombre del archivo infectado.

 Esta área muestra el nombre del archivo infectado y el nombre del virus causante de la infección.

 Esta área muestra el asunto del correo electrónico infectado, el nombre del anexo infectado y el nombre del virus causante de la infección.

Esta área muestra el mensaje de advertencia definido en la página de propiedades **Alerta**.

 Haga clic en este botón para seguir con la exploración sin realizar ninguna acción por el momento.

 Haga clic en este botón para detener la exploración sin realizar ninguna acción por el momento.

 Haga clic en este botón para intentar limpiar el virus.

 Haga clic en este botón para eliminar el archivo infectado.

 Haga clic en este botón para trasladar un archivo infectado a la ubicación de cuarentena designada en la página de propiedades **Acción**.

 Haga clic en este botón para prohibir la aplicación de un objeto ActiveX o Java potencialmente perjudicial o el acceso a un sitio web potencialmente peligroso.

 Haga clic en este botón para ver información adicional acerca del virus identificado.

 Indica la disposición actual del virus.

 Muestra el nombre del virus que infecta al archivo.

 Muestra los tipos de archivos susceptibles de infectarse con este virus.

 Muestra el número de bytes que ocupa el virus.

 VirusScan selecciona este recuadro si el virus se conserva en la memoria después de ejecutarse y continúa infectando otros archivos.

 VirusScan selecciona este recuadro si el virus encripta parte de su firma codificada para evitar su detección.

 VirusScan selecciona este recuadro si el virus evita su detección cambiado ligeramente su firma codificada cada vez que se copia así mismo.

 VirusScan selecciona este recuadro si se puede limpiar el virus.

 Haga clic en este botón para intentar limpiar el virus.

 Haga clic en este botón para eliminar el archivo infectado.

 Haga clic en este botón para seleccionar una ubicación de cuarentena para el archivo infectado.

 VirusScan selecciona este recuadro si el archivo infectado es un archivo del sistema. Consulte la documentación del sistema operativo para ver las definiciones de los atributos del archivo.

 Haga clic en este botón para agregar a la lista de elementos para explorar.

 Para editar un elemento de la lista de elementos para explorar, selecciónelo. A continuación, haga clic en este botón.

 Para borrar un elemento de la lista de elementos para explorar, selecciónelo y, a continuación, haga clic en este botón.

 Este cuadro enumera los elementos para explorar. Éstos pueden agregarse, editarse o eliminarse de la lista mediante los botones situados debajo del cuadro.

 Seleccione esta casilla si quiere que la exploración comience sin recibir ninguna indicación, sino basándose únicamente en las opciones seleccionadas en el **Planificador**. Las tareas planificadas se ejecutan solamente si el **Planificador** está abierto en el momento especificado para la exploración.

 Seleccione esta casilla para incluir en la exploración los virus de sectores de arranque.

El sector de arranque es la primera división lógica del disco duro o el disquete. Justo después de encender la computadora, la BIOS de ésta busca aquí los archivos y programas que necesita para iniciar las operaciones.

 Seleccione esta casilla para incluir en la exploración los virus residentes en la memoria. Estos virus se conservan en la memoria después de ejecutarse y continúan afectando a otros archivos.

 Seleccione esta casilla para activar la actividad de registro. A continuación, haga clic en **Examinar** para seleccionar un archivo para el registro. Una vez seleccionado, la ruta del archivo aparecerá en el cuadro de texto.

 Haga clic en este botón para seleccionar el archivo en el que se va a crear el registro. Una vez seleccionado, la ruta del archivo de registro aparecerá en el cuadro de texto.

Seleccione la casilla **Activar registro en archivo de las actividades de ScreenScan** anterior para activar la actividad de registro. A continuación, haga clic en **Examinar** para seleccionar el archivo en el que se va a crear el registro. Una vez seleccionado, la ruta del archivo de registro aparecerá en este cuadro de texto.

 Utilice la pestaña deslizante para definir cuál es la prioridad de la actividad de exploración respecto a otras actividades que pudieran funcionar mientras se muestra el protector de pantalla (por ejemplo, la desfragmentación del disco).

- Un ajuste bajo da prioridad a otras actividades. La exploración funciona con más lentitud.
- Un ajuste alto da prioridad a la exploración. Las otras actividades funcionan con más lentitud.

 Haga clic en este botón para configurar los ajustes avanzados del explorador, donde puede definir la prioridad de la exploración mientras se muestra el protector de pantalla. También puede definir el archivo en el que se van a registrar las actividades de exploración.

 Seleccione esta casilla para activar la exploración mientras se muestra el protector de pantalla.
Borre la marca de esta casilla para desactivar la exploración mientras se muestra el protector de pantalla.

Haga clic en esta casilla si quiere que ScreenScan continúe la exploración que comenzó durante un intervalo del protector de pantalla anterior, pero que se interrumpió posteriormente debido a un movimiento del mouse o la presión de una tecla.

Si no se selecciona esta casilla, ScreenScan empezará desde el principio cada vez que aparezca el protector de pantalla.

Muestra el nombre de la carpeta que se está explorando actualmente. Si no ha seleccionado una carpeta para explorar, este campo permanece vacío.

Muestra el nombre del archivo que se está explorando actualmente. Si no ha seleccionado un archivo para explorar, este campo permanece vacío.

 Haga clic en este botón para guardar los cambios y cerrar el cuadro de diálogo.

 Haga clic en este botón para cerrar el cuadro de diálogo sin guardar los cambios que ha realizado.

 Haga clic en este botón para guardar los ajustes sin cerrar el cuadro de diálogo.

Seleccione esta casilla si quiere cargar VShield cada vez que se arranque o rearranque el sistema.