Para indicar a Internet Guard Dog las funciones que debe utilizar, marque o quite la marca de las casillas de verificación que se encuentran a la izquierda del nombre de la función en el panel izquierdo del cuadro de diálogo. Haga clic en el nombre de la función en el panel izquierdo para visualizar sus correspondientes opciones de configuración en la página Configuración de protección del panel de la derecha.

Restaura los valores de todas las opciones de todas las funciones de protección (excepto las de Protector de identidad y de Administrar contraseñas) con los valores iniciales de Internet Guard Dog. Al restaurar los valores predeterminados, Internet Guard Dog no modifica el estado activado o desactivado de las funciones de protección (como, por ejemplo, Planificador o Bloqueador de cookies).

Cierre el cuadro de diálogo **Configuración de protección** sin guardar los cambios realizados en la configuración.

Guarda los cambios realizados en cualquier página de Configuración de protección y cierra el cuadro de diálogo **Configuración de protección**.

Ofrece información acerca de los valores de esta página y acerca de lo que controlan.

Seleccione el modo en el que desea que funcione Internet Guard Dog al iniciar Windows.

Muestra la pantalla de bienvenida de McAfee mientras Internet Guard Dog se está cargando en la memoria del equipo.

Inicia la parte de supervisión del programa Internet Guard Dog cada vez que se inicia Windows.

Para controlar el acceso a Internet Guard Dog, asigne una contraseña que proteja este programa. Es posible que ya lo haya hecho durante la Entrevista de Internet Guard Dog; en tal caso, aquí podrá modificar la contraseña. Si no ha asignado ninguna contraseña, puede hacerlo ahora. Es recomendable asignar una contraseña a Internet Guard Dog, ya que aumentará la protección de sus datos privados y confidenciales frente a cualquier persona que pueda utilizar el equipo.

Solicita la contraseña de Internet Guard Dog cada vez que se inicia Windows.

Si no ha creado una contraseña o si desea modificar la contraseña existente, haga clic en **Cambiar contraseña**.

Crea una nueva contraseña de Internet Guard Dog o modifica la contraseña existente.

Mientras Internet Guard Dog supervisa el equipo, el programa puede avisarle de situaciones inminentes que puedan dañar sus datos. Si tiene instalada una tarjeta de sonido, Internet Guard Dog emite una alerta sonora, además de mostrar el cuadro de alerta estándar. Para controlar las alertas sonoras, seleccione las opciones correspondientes en el cuadro de grupo **Efectos de sonido**.

Lista los sonidos que Internet Guard Dog puede reproducir al mostrar una alerta de privacidad. Seleccione **Silencio** si desea desactivar el sonido. Haga clic en el botón  para escuchar el sonido seleccionado. (Para reproducir un sonido de Internet Guard Dog, es necesario disponer de una tarjeta de sonido y altavoces.)

Lista los sonidos que Internet Guard Dog puede reproducir al mostrar una alerta de seguridad. Seleccione **Silencio** si desea desactivar el sonido. Haga clic en el botón  para escuchar el sonido seleccionado. (Para reproducir un sonido de Internet Guard Dog, es necesario disponer de una tarjeta de sonido y altavoces.)

Lista los sonidos que Internet Guard Dog puede reproducir al mostrar una alerta de virus. Seleccione **Silencio** si desea desactivar el sonido. Haga clic en el botón  para escuchar el sonido seleccionado. (Para reproducir un sonido de Internet Guard Dog, es necesario disponer de una tarjeta de sonido y altavoces.)

Lista los sonidos que Internet Guard Dog puede reproducir al mostrar una alerta de privacidad. Seleccione **Silencio** si desea desactivar el sonido. Haga clic en el botón  para escuchar el sonido seleccionado. (Para reproducir un sonido de Internet Guard Dog, es necesario disponer de una tarjeta de sonido y altavoces.)

Lista los sonidos que Internet Guard Dog puede reproducir al mostrar una alerta de seguridad. Seleccione **Silencio** si desea desactivar el sonido. Haga clic en el botón  para escuchar el sonido seleccionado. (Para reproducir un sonido de Internet Guard Dog, es necesario disponer de una tarjeta de sonido y altavoces.)

Lista los sonidos que Internet Guard Dog puede reproducir al mostrar una alerta de virus. Seleccione **Silencio** si desea desactivar el sonido. Haga clic en el botón  para escuchar el sonido seleccionado. (Para reproducir un sonido de Internet Guard Dog, es necesario disponer de una tarjeta de sonido y altavoces.)

Lista los sucesos programados. El nombre del suceso aparece en la columna **Nombre**, y la frecuencia, la fecha y la hora de ejecución del suceso aparecen en la columna **Cuándo**. Internet Guard Dog utiliza las columnas **Siguiente ejecución** y **Última ejecución** para mostrar información útil para los sucesos que se ejecutan más de una vez.

Suprime de la lista los sucesos programados seleccionados.

Inicia **Add a Scheduled Event Wizard** para un suceso seleccionado, lo que le permitirá modificar la configuración de dicho suceso.

Agrega un suceso programado mediante **Add a Scheduled Event Wizard**.

Configuración de protección de Bloqueador de cookies

La página Configuración de protección de Bloqueador de cookies contiene las opciones necesarias para que pueda seleccionar si acepta las cookies de los sitios Web que visite. De este modo, podrá disfrutar de las ventajas que ofrecen las cookies de sus sitios Web favoritos y bloquear las cookies procedentes de otros sitios.

También puede utilizar las opciones del cuadro de grupo **Sitios que establecen cookies** para controlar cómo responde Internet Guard Dog cuando un sitio Web envía una cookie al PC por primera vez.

Un sitio de acceso directo es cualquier ubicación de Internet que se visita escribiendo su dirección (también conocida como dirección URL (Universal Resource Locator) o haciendo clic en un hipervínculo que conecta un sitio Web con otro. Si se conecta directamente con un sitio, es probable que ninguna de las cookies que reciba sea de gran utilidad para usted. Los sitios importantes le indicarán si debe aceptar una cookie para poder visualizarlo.

Puede configurar Internet Guard Dog para realizar una de las siguientes acciones al visitar un sitio Web de acceso directo:

- **Aceptar**—Internet Guard Dog permite que entren automáticamente en el PC las cookies procedentes del sitio Web de acceso directo.
- **Rechazar**—Internet Guard Dog agrega el sitio Web a la lista **Rechazado** y, a continuación, bloquea el intercambio de cookies al visitar directamente dicho sitio.
- **Solicitar**—Internet Guard Dog muestra un mensaje de alerta al visitar un sitio de acceso directo y le solicita si **Permitir siempre** o **No aceptar nunca** las cookies procedentes de ese sitio Web.

Permite el intercambio de cookies entre su equipo y cualquier sitio Web al cual se conecte directamente. Un sitio de acceso directo es cualquier ubicación de Internet que se puede visitar escribiendo simplemente su dirección, también conocida como dirección URL (Universal Resource Locator), o haciendo clic en un hipervínculo que conecta un sitio Web con otro.

Bloquea el intercambio de cookies entre su equipo y cualquier sitio Web al cual se conecte directamente. Un sitio de acceso directo es cualquier ubicación de Internet que se puede visitar escribiendo simplemente su dirección, también conocida como dirección URL (Universal Resource Locator), o haciendo clic en un hipervínculo que conecta un sitio Web con otro.

Solicita si hay que bloquear el intercambio de cookies cada vez que visite un sitio Web al que se ha conectado indirectamente. Un sitio de acceso directo es cualquier ubicación de Internet que se puede visitar escribiendo simplemente su dirección, también conocida como dirección URL (Universal Resource Locator), o haciendo clic en un hipervínculo que conecta un sitio Web con otro.

Un sitio Web de acceso indirecto es un sitio al que se conecta sin saberlo. Con frecuencia, al ir directamente a un sitio Web comercial, también conecta indirectamente con otros sitios Web que envían cookies para supervisar sus hábitos de conexión. Por ejemplo, un sitio al que ha accedido directamente puede contener en su página un anuncio procedente de otro sitio Web. El sitio del que procede el anuncio puede enviar una cookie para realizar un seguimiento y saber si visita otros sitios en los que figuren sus anuncios.

Configure Internet Guard Dog para que realice una de las siguientes opciones:

- **Aceptar**—Internet Guard Dog permite que entren automáticamente en el PC las cookies procedentes del sitio Web de acceso indirecto.
- **Rechazar**—Internet Guard Dog agrega el sitio Web a la lista **Rechazado** y, a continuación, bloquea el intercambio de cookies entre su PC y el sitio Web de acceso indirecto.
- **Solicitar**—Internet Guard Dog muestra un mensaje de alerta al visitar un sitio de acceso indirecto y le solicita si **Permitir siempre** o **No aceptar nunca** las cookies procedentes de ese sitio Web.

Permite el intercambio de cookies entre su equipo y cualquier sitio Web al cual se conecte indirectamente. Un sitio de acceso indirecto es cualquier ubicación de Internet al que se conecta sin teclear su dirección Web, también conocida como dirección URL (Universal Resource Locator), o sin hacer clic en un hipervínculo que conecte con ese sitio. Normalmente, se conectará con un sitio de acceso indirecto como resultado de la conexión con un sitio de acceso directo que visualice contenido procedente de un sitio de acceso indirecto.

Bloquea el intercambio de cookies entre su equipo y cualquier sitio Web al cual se conecte indirectamente. Un sitio de acceso indirecto es cualquier ubicación de Internet al que se conecta sin teclear su dirección Web, también conocida como dirección URL (Universal Resource Locator), o sin hacer clic en un hipervínculo que conecte con ese sitio. Normalmente, se conectará con un sitio de acceso indirecto como resultado de la conexión con un sitio de acceso directo que visualice contenido procedente de un sitio de acceso indirecto.

Solicita si hay que bloquear el intercambio de cookies cada vez que visite un sitio Web al que se ha conectado indirectamente. Un sitio de acceso indirecto es cualquier ubicación de Internet al que se conecta sin teclear su dirección Web, también conocida como dirección URL (Universal Resource Locator), o sin hacer clic en un hipervínculo que conecte con ese sitio. Normalmente, se conectará con un sitio de acceso indirecto como resultado de la conexión con un sitio de acceso directo que visualice contenido procedente de un sitio de acceso indirecto.

Muestra los sitios Web que ha visitado y si el equipo está habilitado para intercambiar o rechazar las cookies procedentes de dichos sitios.

A medida que vaya visitando nuevos sitios Web, Internet Guard Dog aceptará cookies en función de lo que haya seleccionado en el cuadro de grupo **Sitios que establecen cookies**. Si selecciona **Aceptar**, Internet Guard Dog permitirá la entrada de cookies. Si selecciona **Solicitar**, Internet Guard Dog mostrará los mensajes de alerta del Bloqueador de cookies. Si, para responder a dicho mensaje, hace clic en **Permitir siempre**, Internet Guard Dog agregará el nombre del sitio a la lista **Permitido**. Los sitios Web que aparecen en esa lista pueden intercambiar cookies con su equipo sin desencadenar una alerta del Bloqueador de cookies. Una vez que Internet Guard Dog ha agregado un sitio a la lista **Permitido**, puede moverlo a la lista **Rechazado** mediante **>>**, o eliminarlo de ambas listas con **Suprimir**.

A medida que va visitando sitios Web, Internet Guard Dog rechaza las cookies en función de lo que haya seleccionado en el cuadro de grupo **Sitios que establecen cookies**. Si selecciona **Rechazar**, Internet Guard Dog impedirá la entrada de cookies. Si selecciona **Solicitar**, Internet Guard Dog mostrará los mensajes de alerta del Bloqueador de cookies. Si, para responder a dicho mensaje, hace clic en **No aceptar nunca**, Internet Guard Dog agregará el nombre del sitio en la lista **Rechazado**. Los sitios Web que aparecen en esta lista son aquéllos que no pueden intercambiar cookies con su equipo. Una vez incluido un sitio en la lista **Rechazado**, puede moverlo a la lista **Permitido** mediante >>, o eliminarlo de ambas listas con **Suprimir**.

Mueve los sitios Web seleccionados de la lista **Permitidos** a la lista **Rechazados**.

Elimina de ambas listas los sitios Web seleccionados. Si visita nuevamente este sitio Web, Bloqueador de cookies le solicitara si acepta o rechaza las cookies en función de las opciones seleccionadas en el cuadro de grupo **Sitios que establecen cookies**.

Mueve los sitios Web seleccionados de la lista **Rechazados** a la lista **Permitidos**.

Internet Guard Dog muestra la información personal especificada en el bloque Privacidad de la Entrevista o especificada directamente en Protector de identidad. De forma predeterminada, Internet Guard Dog le envía un mensaje de alerta cuando esta información está lista para ser enviada a través de Internet. Para modificar las opciones de alerta, seleccione una entrada y haga clic en **Editar**. Para agregar y borrar información desde Protector de identidad, utilice **Suprimir** y **Agregar**.

Muestra la información personal especificada durante el bloque Privacidad de la Entrevista o especificada directamente en Protector de identidad. Para trabajar con esta información, utilice los botones **Suprimir**, **Editar** y **Agregar**.

Suprime de la lista la entrada seleccionada.

Inicie **Add Identity Information Wizard**, y visualizará la información existente relativa a la entrada seleccionada. Modifique la información que desee y, para guardar los cambios realizados, haga clic en el botón **Finalizar** que aparece en la última página del asistente

Inicie **Add Identity Information Wizard**, que le indicará los pasos a seguir para agregar la información personal que se debe proteger.

Internet Guard Dog muestra la información financiera especificada durante el bloque Privacidad de la Entrevista o especificada directamente en Protector de identidad. De forma predeterminada, Internet Guard Dog le envía un mensaje de alerta cuando esta información está lista para ser enviada a través de Internet. Para modificar las opciones de alerta, seleccione una entrada y haga clic en **Editar**. Para agregar y borrar información desde Protector de identidad, utilice **Agregar** y **Suprimir**.

Muestra información financiera especificada durante el bloque Privacidad de la Entrevista o agregada directamente en Protector de identidad. Para trabajar con esta información, utilice los botones **Suprimir**, **Editar** y **Agregar**.

Suprime de la lista la entrada seleccionada.

Inicie **Add Financial Information Wizard**, y visualizará la información existente relativa a la entrada seleccionada. Modifique la información que desee y, para guardar los cambios realizados, haga clic en el botón **Finalizar** que aparece en la última página del asistente

Inicie **Add Financial Information Wizard**, que le indicará los pasos a seguir para agregar la información financiera que se debe proteger.

Seleccione **Solicitar limpiar después de cerrar el navegador Web** si desea controlar el borrado del historial de conexiones y de los archivos basura de Internet. Se le solicitará que confirme el borrado de los archivos:

- Cada vez que cierre el navegador Netscape o Internet Explorer.
- Cuando apague Windows, si utiliza Internet Explorer y existe algún archivo de conexiones.
- Cuando apague Windows, si utiliza Active Desktop de Microsoft.

Seleccione **Limpiar automáticamente después de cerrar el navegador Web** si desea que Limpiador de rastros de Internet borre el historial de conexiones y los archivos basura de Internet. Limpiador de rastros de Internet lo hará:

- Cada vez que cierre el navegador Netscape o Internet Explorer.
- Cuando apague Windows, si utiliza Internet Explorer y existe algún archivo de conexiones.
- Cuando apague Windows, si utiliza Microsoft Active Desktop.

Seleccione **Conservar elementos favoritos** para que Limpiador de rastros de Internet no borre los archivos relativos a los sitios marcados como favoritos (o seleccionados en Favoritos).

Marque la casilla de verificación **Conservar elementos favoritos** para que, después de cerrar el navegador, Limpiador de rastros de Internet no borre los archivos relativos a los sitios marcados como favoritos (o seleccionados como Favoritos). Los elementos marcados como favoritos sirven para conectar ágilmente con los sitios Web importantes o con los sitios que visita con frecuencia, sin tener que escribir su dirección URL. Esta opción estará disponible sólo si ha marcado **Limpiar automáticamente después de cerrar el navegador Web**.

Las entradas que aparecen en este cuadro representan las acciones que los programas de Internet pueden ejecutar y que podrían tener consecuencias nefastas. En función de cómo utilice Internet, decida las acciones sobre las cuales desea que Vigilante le avise y marque la casilla de verificación que correspondan.

Le avisa cuando se inicia la conexión con un sitio conocido por contener controles ActiveX dañinos, programas Java, virus o caballos de Troya.

Le avisa cuando el módem marca en modo silencioso, Algunos programas pueden reunir información confidencial de su equipo y utilizar su módem para enviarla a otro lugar.

Le avisa cuando un programa inicia otro programa sin su autorización. Por ejemplo, un programa hostil podría intentar iniciar el navegador Web.

Le avisa cuando un programa envía fuera a través de Internet cualquier número que parezca un número de tarjeta de crédito. Algunos programas hostiles han sido diseñados para buscar números de tarjeta de crédito y enviarlos a otro sitio.

Lista los programas que tienen su autorización para acceder a Internet sin mostrar un mensaje de alerta. Inicialmente, Internet Guard Dog lo comprueba cada vez que un programa, como el navegador, accede a Internet. Si responde al mensaje de alerta con **Permitir siempre**, Internet Guard Dog agrega el programa a la lista y no le vuelve a avisar con respecto a ese programa. Revise estos programas periódicamente y decida si conservarlos en la lista o suprimirlos.

Suprime de la lista el programa seleccionado. La próxima vez que el programa intente acceder a Internet, Internet Guard Dog mostrará un mensaje de alerta para solicitarle su permiso.

Las entradas que aparecen en este cuadro representan las acciones cuyas consecuencias podrían ser nefastas para los datos del equipo. En función de las necesidades de seguridad que tenga y de cómo utilice Internet, decida las acciones sobre las cuales desea que Guardián de archivos le avise y marque la casilla de verificación correspondiente.

Le avisa cuando un control ActiveX explora los archivos del PC. Los controles ActiveX pueden ejecutar exploraciones inofensivas, como cuando necesita comprobar mediante un control ActiveX los archivos que posee en su PC para actualizar archivos relativos a un sitio Web. No obstante, un control ActiveX puede haber sido creado para comprometer su seguridad; por ejemplo, puede buscar archivos que contengan información financiera privada para enviarla a otra ubicación. Marque esta casilla de verificación para recibir un mensaje de alerta.

Le avisa cuando un programa empieza a dar formato a cualquier unidad de disco duro, incluidas las unidades Jaz y Zip. Dar formato de nuevo a la unidad de disco duro del equipo sin su conocimiento puede tener consecuencias catastróficas. No sólo puede perder datos valiosos, sino que también podría perder una gran cantidad de tiempo tratando de restituir el anterior estado de funcionamiento del equipo. Marque esta casilla de verificación para recibir un mensaje de alerta.

Le avisa cuando un control ActiveX elimina un archivo del PC. Los controles ActiveX pueden tener motivos legítimos para borrar archivos; por ejemplo, pueden borran los archivos temporales creados al descargar archivos desde un sitio Web con controles ActiveX. No obstante, un control ActiveX también puede estar diseñado para eliminar archivos importantes. Marque esta casilla de verificación para recibir un mensaje de alerta.

Le avisa cuando un programa accede a cualquier archivo de contraseña de Windows (archivo .pwl). Las contraseñas tienen una función de seguridad importante, ya que controlan qué personas acceden a los recursos compartidos que dispone en su PC. Marque esta casilla de verificación para recibir un mensaje de alerta.

Muestra la lista de archivos que supervisa Guardián de archivos y los programas que tienen acceso a éstos. Puede agregar o suprimir archivos o programas en estas listas.

Muestra la lista de archivos seleccionados para que los supervise Guardián de archivos. Los archivos se visualizan según el método por el cual se han seleccionado: por nombre de archivo, carpeta o unidad en que están almacenados, grupo de archivo o tipo de archivo. Si marca la casilla de selección **Incluir para codificación de archivos** del cuadro de diálogo **Add Guarded File Wizard**, el archivo aparecerá junto con un icono de una cerradura. Para codificar (o descodificar el archivo), haga clic en el icono de Internet Guard Dog  que se encuentra en la bandeja del sistema y seleccione **Codificar archivos de Guardián de archivos** (o **Descodificar archivos de Guardián de archivos**) en el menú emergente.

Muestra la lista de programas a los que se ha autorizado el acceso al archivo seleccionado. Guardián de archivos muestra un mensaje de alerta y le solicita que confirme su autorización la primera vez que el programa accede a un archivo de la lista de archivos protegidos. Si responde al mensaje de alerta con **Permitir siempre**, Guardián de archivos agrega el programa a la lista **Programas con acceso a este archivo**.

Suprime el archivo o programa seleccionado de las listas **Archivos protegidos** o **Programas con acceso a este archivo**

Inicia Add Guarded File Wizard y le guía paso a paso para agregar archivos a la lista **Archivos protegidos** o para especificar los programas que tendrán acceso a los archivos de la lista. Antes de hacer clic en el botón **Agregar** para que un programa pueda acceder a un archivo, debe seleccionar el archivo que desea proteger.

Muestra la lista de registros almacenados por Administrar contraseñas. Cada registro contiene el nombre del sitio Web y el nombre de usuario y contraseña utilizados para conectarse al sitio.

Elimina el registro seleccionado de la lista de Administrar contraseñas.

Abre el cuadro de diálogo **Introduzca la contraseña para guardar** y muestra la información correspondiente al registro seleccionado.

Abre el cuadro de diálogo **Introduzca la contraseña para guardar,** donde podrá almacenar el nombre del sitio Web y el nombre de usuario y contraseña correspondientes a dicho sitio.

Configuración de protección de Centinela de virus

En la página Configuración de protección de Centinela de virus podrá especificar cómo desea que Internet Guard Dog proteja su PC de la infección de virus. En esta página, puede especificar opciones para que se realice la detección de virus mientras trabaja mediante **Cuándo realizar la comprobación,** así como especificar los tipos de archivos a explorar (en la función Comprobación) mediante **¿Qué desea comprobar?**.

Utilice las opciones que ofrece este cuadro para controlar las acciones que Centinela de virus debe supervisar mientras trabaja en su PC.

Utilice esta opción de trabajo para explorar todos los programas al iniciarlos.

Utilice esta opción de trabajo para explorar todos los archivos adjuntos de correo electrónico al abrirlos.

Utilice esta opción de trabajo para explorar todos los archivos al abrirlos.

Utilice esta opción de trabajo para explorar todos los archivos al moverlos o cambiarles el nombre.

Utilice esta opción de trabajo para explorar todos los disquetes al abrirlos.

Explora DOS e identifica los virus que detecta antes de cargar Windows. El sistema operativo Windows todavía depende de las funciones de un antiguo sistema operativo llamado DOS. Algunos virus, como los virus del sector de arranque, los virus de las tablas de partición y los virus de memoria, pueden infectar los archivos antes de cargar Windows. Aunque estos tipos de virus podrían detectarse en Windows, la mayoría deben eliminarse desde DOS. Por este motivo, debería marcar esta opción si desea contar con una protección antivirus más completa.

Determina la respuesta de Internet Guard Dog cuando detecta un virus en los tipos de programas o archivos especificados en **¿Qué desea comprobar?**.

Puede controlar la acción de Centinela de virus cuando éste detecta un virus en los tipos de programas o archivos especificados en **¿Qué desea comprobar?**. Seleccione la opción de Centinela de virus que le interese:

- **Solicitar**–Podrá decidir lo que hacer caso por caso.
- **Denegar el acceso**–No podrá hacer nada con el archivo, excepto eliminarlo con el explorador de Windows o limpiarlo con la función Comprobación. (Cuando se abre un archivo infectado, el virus se extiende.)
- **Eliminación automática**–Elimina el archivo de su disco duro.
- **Limpieza automática**–Suprime el virus del archivo infectado, y si no puede, Internet Guard Dog le solicita que elimine el archivo.
- **Desconexión del equipo**–Apaga el sistema Windows sin llevar cabo ninguna acción adicional.

Determina los tipos de archivos que explora Internet Guard Dog durante la función Comprobación.

Determina los tipos de archivos que explora Internet Guard Dog durante la función Comprobación. Puede indicar a Internet Guard Dog que explore:

- **Todos los archivos**–Comprueba todos los archivos del equipo. Ésta es la comprobación más completa, y también la que tarda más tiempo en realizarse si cuenta con muchos archivos en el equipo. Con este tipo de comprobación puede detectar virus en archivos que utilizan tipos de archivos que no son estándar.
- **Archivos de programa**–Comprueba todos los archivos que un programa necesita para funcionar correctamente. Se comprueban los archivos con las extensiones de programa más comunes,
como .com, .exe, .bat, .bin, .ovl, .drv, .dll, .sys, .tsk, .vxd y .ocx. Esta opción no detecta virus de macros.
- **Archivos de documento**–Únicamente comprueba los archivos de datos que pueden contener virus, que normalmente son virus de macros. Por ejemplo, se comprueban los archivos de documento de Microsoft Word y Excel y los documentos comprimidos con extensiones .zip, .arc y .lzh. Esta opción no detecta virus de programa.
- **Archivos de programa y documento**–Comprueba los archivos de programa y los archivos de documento. Esta opción encontrará la mayoría de los virus y tarda menos tiempo que la comprobación de todos los archivos.

Sugerencia

Utilice **Editar** para agregar, suprimir o personalizar los tipos de archivos que desea que se comprueben durante la función Comprobación.

Personaliza los tipos de archivos de documento o archivos de programa que comprueba Internet Guard Dog durante la función Comprobación. En la pestaña **Archivos de programa** o en la pestaña **Archivos de documento**, utilice los botones **Agregar** y **Suprimir** para especificar los tipos de archivos y programa en los que realizar la detección de virus.

Para especificar los tipos de archivos que Internet Guard Dog debe comprobar durante la función Comprobación, agréguelos a la pestaña **Archivos de programa** o **Archivos de documento**.

Muestra la lista de archivos de programa que comprueba Centinela de virus durante la función Comprobación.

Muestra la lista de archivos de documento que comprueba Centinela de virus durante la función Comprobación.

Agrega los tipos de archivo que seleccione a la lista **Archivos de programa** o **Archivos de documento**.

Suprime los tipos de archivos que seleccione de la lista **Archivos de programa** o **Archivos de documento**.

Controla los archivos y carpetas que Centinela de virus no comprueba durante cualquier tipo de exploración de virus, excepto para las opciones de trabajo del cuadro **Cuándo realizar la comprobación** de Centinela de virus.

Muestra los archivos y carpetas que Centinela de virus no comprueba durante cualquier tipo de exploración de virus, excepto para las opciones de trabajo del cuadro **Cuándo realizar la comprobación** de Centinela de virus.

Utilice el botón **Agregar archivos** para incluir archivos en la lista **No comprobar…** .

Utilice el botón **Agregar carpetas** para incluir carpetas en la lista **No comprobar…** .

Utilice el botón **Suprimir** para eliminar los archivos o carpetas seleccionados de la lista **No comprobar…** .

Sugerencia

Utilice MAYÚS+CLIC para seleccionar varias entradas de la lista.

Explora DOS e identifica los virus que detecta antes de cargar Windows. El sistema operativo Windows todavía depende de las funciones de un antiguo sistema operativo llamado DOS. Algunos virus, como los virus del sector de arranque, los virus de las tablas de partición y los virus de memoria, pueden infectar los archivos antes de cargar Windows. Aunque estos tipos de virus podrían detectarse en Windows, la mayoría deben eliminarse desde DOS. Por este motivo, debería marcar esta opción si desea contar con una protección antivirus más completa.

Entrevista - Antivirus

Con un poco de suerte, los virus pueden ser sólo una pequeña molestia, pero también pueden destruir datos importantes del PC. Olvídese de estos problemas activando la detección de virus de Internet Guard Dog. Después de la Entrevista, puede determinar exactamente el tipo de archivos que debe comprobar el programa antivirus.

Seleccione las siguientes casillas de verificación para detectar los virus

- **Siempre que se inicie Windows**–Internet Guard Dog detecta automáticamente los archivos de alto riesgo (archivos de documento y archivos de programa) cuando se inicia Windows.
- **Automáticamente, siempre que se registren actividades de archivo o de descarga**–Guard Dog detecta los posibles virus al:

  Ejecutar un programa

  Acceder a archivos de correo electrónico

  Abrir un archivo

  Mover o renombrar

  Leer un disquete

Consulte los siguientes temas si desea obtener más información acerca de cómo configurar la protección antivirus.

Cómo sacar más provecho de la protección antivirus

Acerca de Centinela de virus

Entrevista - Disco de emergencia

Un disco de emergencia es una copia de seguridad válida a la que puede recurrir cuando existe algún problema con los datos protegidos por Internet Guard Dog. El disco contiene una copia de esta información, además de un programa que le permite iniciar el PC en modo DOS. Si no crea ningún disco de emergencia en este momento, puede hacer que Internet Guard Dog le avise para hacerlo más adelante.

Consulte el siguiente tema si desea obtener más información acerca de cómo configurar planificaciones y acerca de los tipos de sucesos que pueden programarse.

Acerca del Planificador

Registro de Internet Guard Dog

Haga clic en Registro para ver las acciones llevadas a cabo por Internet Guard Dog para proteger los datos del PC. Internet Guard Dog realiza un seguimiento de las acciones que lleva a cabo en el PC y muestra esa información en forma de lista. En la pantalla Registro, puede ver la siguiente información:

{button ,PI(`gd.hlp',`Date_Time_column_on_the_Report_page')} Fecha/Hora

{button ,PI(`gd.hlp',`Guard_Dog_Action_column_on_the_Report_page')} Acción de Guard Dog

{button ,PI(`gd.hlp',`Date_Time_column_on_the_Report_page')} Tipo

{button ,PI(`gd.hlp',`User_column_on_the_Report_page')} Usuario

Puede decidir qué hacer con los datos del Registro. Puede:

{button ,PI(`gd.hlp',`Print_button_on_the_Report_page')} Imprimir

{button ,PI(`gd.hlp',`Cancel_button_on_the_Report_page')} Cancelar

{button ,PI(`gd.hlp',`Clear_button_on_the_Report_page')} Borrar

Haga clic en **Cancelar** para cerrar esta pantalla y volver a la pantalla La comprobación ha detectado si no desea comprobar la existencia de actualizaciones.

Haga clic en **Actualizar** para iniciar Oil Change con el fin de comprobar y recuperar las últimas mejoras del programa Internet Guard Dog.

La comprobación ha detectado - Disco de emergencia

Si los datos del PC son víctima de algún siniestro, podrá recuperarlos mediante el disco de emergencia. Este disco contiene los datos importantes protegidos por Internet Guard Dog, así como un programa que le permite iniciar el PC en modo DOS. Puede hacer lo siguiente:

{button ,PI(`gd.hlp',`Create_button_on_the_Emergency_Disk_page')} Create

{button ,PI(`gd.hlp',`Cancel_button_the_Create_an_Emergency_disk_page')} Cancel

La comprobación ha detectado - Actualización del disco de emergencia

La información contenida en el disco de emergencia de Internet Guard Dog puede quedar obsoleta. Tenga siempre a mano los discos y deje que Internet Guard Dog vaya actualizando la información.

{button ,PI(`gd.hlp',`CheckUp_Found_Emergency_Disk_out_of_date_Update_button')} Update

{button ,PI(`gd.hlp',`CheckUp_Found_Emergency_disk_out_of_date_Cancel_button')} Cancel

Haga clic en Cancelar para cerrar esta pantalla y volver a la pantalla La comprobación ha detectado si no desea comprobar la existencia de actualizaciones.

La comprobación ha detectado - Virus

Centinela de virus de Internet Guard Dog ha detectado archivos infectados por un virus. El nombre y la ubicación de cada archivo se mostrarán en la lista que aparece en la parte inferior de la pantalla. Para eliminar la infección de los archivos, seleccione las casillas de verificación que aparecen junto a los nombres y haga clic en **Limpiar**.

{button ,PI(`gd.hlp',`CheckUp_Clean_Viruses_Clean_button')} Limpiar

{button ,PI(`gd.hlp',`CheckUp_Clean_Viruses_Cancel_button')} Cancelar

Centinela de virus Buscar carpeta

Puesto que el proceso de detección de virus puede ser muy largo, puede controlar la cantidad de archivos que comprueba Centinela de virus añadiendo carpetas a la lista **No comprobar los archivos de estas carpetas**.

Para agregar carpetas a la lista No comprobar los archivos de estas carpetas:

- Haga clic en la carpeta y después en **Aceptar**.

Sugerencia

Ello afecta no sólo a las comprobaciones efectuadas en los archivos, sino también a la detección rápida de virus y a la Comprobación. De forma predeterminada, Internet Guard Dog no comprueba los archivos de la Papelera de reciclaje.

Editar lista de detecciones de virus - Archivos de documento

Si ha seleccionado Archivos de documento en el cuadro **Qué comprobar**, podrá **Agregar** o **Suprimir** los tipos de archivos de documento en los que Centinela de virus detectará la existencia de virus.

Para agregar un tipo de documento:

1 En la página Centinela de virus, seleccione **Archivos de documento** en la lista **Qué comprobar** y haga clic en **Editar**.

2 Haga clic en la ficha **Archivos de documento** y haga clic en **Agregar**.

3 En la siguiente pantalla, seleccione los tipos de documentos que desee que sean comprobados por Centinela de virus y haga clic en **Aceptar**.

Para suprimir tipos de documentos:

1 En la página Centinela de virus, seleccione Archivos de documento en la lista **Qué comprobar** y haga clic en **Editar**.

2 Haga clic en la ficha **Archivos de documento**, seleccione un tipo de documento de la lista y haga clic en **Suprimir**.

Editar lista de detecciones de virus

Centinela de virus puede comprobar tipos de documentos y programas específicos basándose en la selección realizada en el cuadro **Qué comprobar** de la página de Configuración de protección de Centinela de virus.

Para agregar un tipo de programa:

1 On the Virus Sentry page, select **Program Files** from the list in the **What to Check** list box, then click **Edit**.
In the **Edit Virus Check List** screen the **Program Files** tab appears by default.

2 Haga clic en **Agregar**.

3 En **Agregar lista de detecciones de virus**, seleccione los tipos de programas y haga clic en **Aceptar**.

Para agregar un tipo de documento:

1 En la página Centinela de virus, seleccione **Archivos de documento** en la lista **Qué comprobar** y haga clic en **Editar**.

2 Haga clic en la ficha **Archivos de documento** para colocarla en primer plano y haga clic en **Agregar**.

3 En **Agregar lista de detecciones de virus**, seleccione los tipos de archivos de documento y haga clic en **Aceptar**.

Para agregar un tipo de archivo personalizado:

1 En la página Centinela de virus, haga clic en **Editar**.

2 Haga clic en **Personalizar**.

3 Escriba la extensión de archivo que desee comprobar y haga clic en **Aceptar**.

Para restablecer los tipos de archivos predeterminados que deben comprobarse:

1 En la página Centinela de virus, haga clic en **Editar**.

2 Haga clic en **Predeterminado**.

Para suprimir un tipo de programa:

1 On the Virus Sentry page, select **Program Files** in the list in the **What to Check** list box then click **Edit**.
In the **Edit Virus Check List** screen the **Program Files** tab appears by default.

2 Haga clic en la ficha **Archivos de programa**, seleccione un tipo de programa de la lista y haga clic en **Suprimir**.

Para suprimir un tipo de documento:

1 En la página Centinela de virus, seleccione **Archivos de documento** en la lista **Qué comprobar** y haga clic en **Editar**.

2 Haga clic en la ficha **Archivos de documento** para colocarla en primer plano, seleccione un tipo de documento de la lista y haga clic en **Suprimir**.

Agregar lista de detecciones de virus

Para agregar tipos de archivo para que Centinela de virus los compruebe:

- Select file types from the list and click **OK** when you are finished to return to the **Edit Virus Check List** screen.

Your entry appears at the bottom of the list in the Program Files tab.

Sugerencia

Para realizar selecciones múltiples de la lista de tipos de archivo, pulse MAYÚSCULAS+CLIC o CONTROL+CLIC.

Agregar una extensión personalizada para la detección de virus

Para agregar extensiones de archivo personalizadas con el fin de que Centinela de virus las compruebe:

- Type a three letter file extension in the box and click **OK** to return to the **Edit Virus Check List** screen.

Your entry appears at the bottom of the list in the Program Files tab.

Nota

Las extensiones de archivo forman parte del nombre de los archivos. Windows utiliza la extensión de archivo para determinar qué tipo de información contiene el archivo. Si se trata de un archivo de documento, Windows utiliza la extensión de archivo para determinar los programas asociados al archivo. De forma predeterminada, Windows no visualiza la extensión de archivo como parte del nombre del archivo en Mi PC o en el Explorador de Windows.

McAfee Emergency Disk - Crear un disco de emergencia, página 1

Internet Guard Dog grabará la información de emergencia (archivos, programas y configuración de Internet Guard Dog) en la unidad que seleccione en esta lista. Algunas cosas a tener en cuenta al seleccionar la unidad son:

Sugerencia

Por norma, deberá seleccionar una unidad multimedia extraíble como, por ejemplo, la unidad de disquete. Si la información de emergencia está almacenada en una unidad de red, es posible que no pueda acceder a esa unidad cuando tenga problemas con su equipo.

McAfee Emergency Disk - Crear un disco de emergencia, página 2

Si ha seleccionado una unidad de disquete en la anterior pantalla del asistente, Internet Guard Dog almacenará la información de emergencia (archivos, programas y configuración de Internet Guard Dog) en tres disquetes de 1/2 pulg con formato. Cuando el primer disco esté lleno, Emergency Disk Wizard mostrará un mensaje pidiéndole que inserte el segundo disco.

Para empezar a crear un disco de emergencia:

- Inserte un disco en la unidad de disquete de su equipo y haga clic en **Siguiente**.

Sugerencia

Puede hacer clic en **Cancelar** para volver a la Entrevista o en **Atrás** para volver a la anterior página del asistente.

McAfee Emergency Disk - Crear un disco de emergencia, página 3

Internet Guard Dog necesitará algunos minutos para copiar la información de emergencia (archivos, programas y configuración de Internet Guard Dog) en la unidad que ha seleccionado. Si Internet Guard Dog está copiando los archivos en disquetes, cuando el primer disco esté lleno recibirá un mensaje indicándole que inserte el segundo disco.

Para continuar cuando Internet Guard Dog haya terminado de copiar la información:

- Haga clic en **Siguiente** para continuar con la siguiente página del asistente.

Para detener Internet Guard Dog mientras está copiando información:

- Click **Cancel**.

When Internet Guard Dog displays a message asking you if you are sure you want to stop, click **Yes** to return to the Interview.

McAfee Emergency Disk - Crear un disco de emergencia, página 4

Internet Guard Dog ha terminado de copiar la información de emergencia.

Para finalizar el procedimiento de creación de un disco de emergencia:

- Haga clic en **Finalizar** para volver a la Entrevista.

Pantalla inicial de Internet Guard Dog

Desde la pantalla inicial puede acceder a las siguientes funciones:

- **Configuración del usuario**

  Haga clic para acceder a la pantalla Configuración del usuario. Podrá agregar, editar y eliminar perfiles de usuario. Asimismo, podrá configurar las opciones de filtrado de Internet de modo que indiquen distintas restricciones, como pueden ser el bloqueo de sitios Web a los cuales no se permite el acceso, la utilización de la lista de palabras para seleccionar y agregar palabras rechazables que los perfiles deben omitir y el bloqueo de elementos adjuntos a mensajes de correo electrónico.

- **VirusScan**

  Haga clic para iniciar McAfee VirusScan. Gracias a sus componentes, podrá configurar distintas tareas de detección de virus de acuerdo con sus preferencias, configurar operaciones de comprobación y visualizar información acerca de virus desde el sitio Web de McAfee.

- **Informes de registro de usuarios**

  Podrá visualizar las medidas que Internet Guard Dog ha tomado, mediante esta función, para proteger su seguridad y privacidad, así como la de otros usuarios con perfil definido en su equipo. Los informes se agrupan en tres categorías: Registros de violación, registros de mantenimiento y registros de actividades.

- **Comprobación de seguridad**

  Cuando ejecute Comprobación, Internet Guard Dog efectuará en el equipo una inspección exhaustiva en busca de posibles problemas de seguridad y privacidad. Cuando encuentra problemas, Internet Guard Dog crea una lista y la muestra en la pantalla La comprobación ha detectado. Puede seleccionar un problema e Internet Guard Dog lo mostrará en una pantalla adicional con una descripción del mismo y una recomendación sobre cómo solucionarlo. Si soluciona un problema y no le gusta el resultado, Internet Guard Dog le permite Deshacer el cambio.

- **Opciones**

  Si desea modificar la configuración relativa a los procesos de comprobación y detección, o bien si desea reiniciar la Entrevista de Internet Guard Dog para introducir algunos cambios, haga clic en Opciones y seleccione la acción correspondiente del menú desplegable. Consulte Utilización de las Opciones de Internet Guard Dog.

- **Ayuda**

  Si desea visualizar el sistema de ayuda de Internet Guard o algún tema específico acerca de la pantalla en la que está trabajando, haga clic en Ayuda y realice la selección correspondiente del menú desplegable. Consulte Acerca del menú Ayuda.

- **McAfee.com**

  Haga clic para acceder al sitio Web de McAfee.

Desde estas ventanas también podrá consultar información relativa a la seguridad en la pantalla inicial:

- **Ventana Violaciones**

  Muestra un informe resumido de la configuración ante cualquier brecha en la protección de su perfil o del de otros usuarios. También muestra el día, la fecha y la hora de conexión y desconexión de un usuario con perfil en un equipo determinado.

- **Ventana Estado de la seguridad**

  Muestra la configuración predeterminada de seguridad establecida para su equipo (es decir, máximo, mínimo o seguridad personalizada).

- **Ventana Comprobación de la seguridad**

  Muestra cualquier novedad respecto a la seguridad (por ejemplo, vencimiento de la detección de virus, actualizaciones de determinadas funciones, creación de discos de recuperación, etc.).

Registro de mantenimiento

La ventana Registro de mantenimiento le permitirá visualizar una lista de las acciones llevadas a cabo por Internet Guard Dog. Se especifican las funciones concretas utilizadas en cada caso.

Desde esta ventana también podrá acceder a otros informes, utilizando los botones que se listan a continuación:

- **Registro de violación**

  Haga clic para visualizar una lista de las actividades realizadas por un usuario con perfil definido que violen la configuración de protección establecida por el Administrador (por ejemplo, intentar enviar el número de una tarjeta de crédito).

- **Registro de actividades**

  Haga clic para visualizar la identidad del usuario con perfil definido que ha utilizado el equipo. También muestra el día, la fecha y la hora de conexión y desconexión del equipo.

Impresión, borrado o guardado de los registros de actividades del usuario

Tras visualizar el Registro de mantenimiento, lleve a cabo alguna de las acciones que se detallan a continuación:

- Haga clic en **Borrar** para eliminar el informe.
- Haga clic en **Imprimir** para imprimir el informe.
- Haga clic en **Guardar** para guardar el informe. Navegue hasta la ubicación en la que desea guardar el informe y haga clic en Guardar.

Sugerencia

- Haga clic en alguno de los títulos de las columnas si desea visualizar las entradas por orden alfabético.
- Si desea conservar entradas de registro durante algunos días, introduzca el número correspondiente en la casilla que se ofrece para este fin.

Registro de violación

La ventana Registro de violación le permitirá visualizar una lista de las actividades realizadas por un usuario con perfil definido que violen la configuración de protección establecida por el Administrador (por ejemplo, intentar enviar el número de una tarjeta de crédito).

Desde esta ventana también podrá acceder a otros informes, utilizando los botones que se listan a continuación:

- **Registro de mantenimiento**

  Haga clic para visualizar una lista de las acciones llevadas a cabo por Internet Guard Dog. Se especifican las funciones concretas utilizadas en cada caso.
- **Registro de actividades**

  Haga clic para visualizar la identidad del usuario con perfil definido que ha utilizado el equipo. También muestra el día, la fecha y la hora de conexión y desconexión del equipo.

Impresión, borrado o guardado de los registros de actividades del usuario

Tras visualizar el Registro de mantenimiento, lleve a cabo alguna de las acciones que se detallan a continuación:

- Haga clic en **Borrar** para eliminar el informe.
- Haga clic en **Imprimir** para imprimir el informe.
- Haga clic en **Guardar** para guardar el informe. Navegue hasta la ubicación en la que desea guardar el informe y haga clic en Guardar.

Sugerencia

- Haga clic en alguno de los títulos de las columnas si desea visualizar las entradas por orden alfabético.
- Si desea conservar entradas de registro durante algunos días, introduzca el número correspondiente en la casilla que se ofrece para este fin.

Registro de actividades

La ventana Registro de actividades le permitirá visualizar la identidad de un usuario con perfil definido que utilizó el equipo. También muestra el día, la fecha y la hora de conexión y desconexión del equipo.

Desde esta ventana también podrá acceder a otros informes, utilizando los botones que se listan a continuación:

- **Registro de mantenimiento**

  Haga clic para visualizar una lista de las acciones llevadas a cabo por Internet Guard Dog. Se especifican las funciones concretas utilizadas en cada caso.

- **Registro de violación**

  Haga clic para visualizar una lista de las actividades realizadas por un usuario con perfil definido que violen la configuración de protección establecida por el Administrador (por ejemplo, intentar enviar el número de una tarjeta de crédito).

Impresión, borrado o guardado de los registros de actividades del usuario

Tras visualizar el Registro de mantenimiento, lleve a cabo alguna de las acciones que se detallan a continuación:

- Haga clic en **Borrar** para eliminar el informe.
- Haga clic en **Imprimir** para imprimir el informe.
- Haga clic en **Guardar** para guardar el informe. Navegue hasta la ubicación en la que desea guardar el informe y haga clic en Guardar.

Sugerencia

- Haga clic en alguno de los títulos de las columnas si desea visualizar las entradas por orden alfabético.
- Si desea conservar entradas de registro durante algunos días, introduzca el número correspondiente en la casilla que se ofrece para este fin.

La comprobación ha detectado

Al finalizar la comprobación de seguridad en un equipo, Internet Guard Dog elabora una lista de los problemas y temas detectados dignos de mención y la muestra en esta ventana. Estos problemas aparecen bajo los títulos de Seguridad y Privacidad en la pantalla La comprobación ha detectado. Cuando selecciona un problema, puede realizar las siguientes acciones:

- **Arreglar**

  Haga clic en **Arreglar** para indicar a Internet Guard Dog la acción que debe realizar para solucionar el problema. Internet Guard Dog muestra una segunda pantalla con información importante sobre el problema y recomendaciones para su resolución.

- **Deshacer arreglar**

  Para identificar un problema solucionado, Internet Guard Dog pone una marca de verificación al lado del problema en la pantalla La comprobación ha detectado. Si no está satisfecho con la solución, puede volver a la configuración anterior. Seleccione el problema en la pantalla La comprobación ha detectado y haga clic en **Deshacer arreglar**.

Estado de la comprobación

Esta ventana muestra qué comprueba exactamente Internet Guard Dog en su equipo.

Para comprobar los aspectos generales de seguridad, puede seleccionar:

- **Comprobación de Actualizaciones de Internet Guard Dog**–McAfee mejora continuamente Internet Guard Dog y coloca estas mejoras, llamadas actualizaciones, en el sitio Web de McAfee. Si selecciona Comprobación de actualizaciones de Internet Guard Dog, el programa iniciará McAfee Software Update Finder desde el navegador con el fin de encontrar actualizaciones de Internet Guard Dog y de nuevos archivos de patrón de virus. Puede utilizar esta función para localizar, recuperar e instalar cualquier actualización disponible.

  Consulte Utilización de las actualizaciones si desea obtener más información.

- **Comprobación de la versión del navegador**–Microsoft y Netscape también mejoran el software de navegador y proporcionan actualizaciones en sus sitios Web. Es preciso que mantenga actualizado el software del navegador para beneficiarse de las funciones adicionales de seguridad que proporcionan los navegadores.

Para salvaguardar su privacidad, puede seleccionar:

- **Comprobación de Protector de identidad**–Internet Guard Dog explora los archivos del equipo para determinar si contienen información personal o financiera introducida en Protector de identidad durante la Entrevista o directamente en la página Protector de identidad de Configuración de protección. Internet Guard Dog le pregunta si desea agregar estos archivos a la lista de archivos controlados por Guardián de archivos.

  Consulte Acerca de Guardián de archivos y Acerca de Protector de identidad si desea obtener más información.

- **Comprobación de Administrador de cookies**–Internet Guard Dog comprueba el equipo para ver si ha quedado alguna cookie después de cerrar el navegador Web.

  Consulte Acerca de Bloqueador de cookies si desea obtener más información.

- **Comprobación de Protector de búsquedas**–Cuando se eliminan archivos y carpetas del disco duro, los datos no desaparecen. Permanecen en el disco y se sobreescriben. Internet Guard Dog identifica estos datos y le da la oportunidad de suprimirlos de forma definitiva.

  Consulte Acerca de Protector de búsquedas si desea información.

- **Comprobación de Limpiador de rastros de Internet**–Internet Guard Dog determina si el navegador ha dejado algún sitio Web en el equipo.

  Consulte Acerca de Limpiador de rastros de Internet si desea obtener más información.

Para crear un entorno informático seguro, puede seleccionar:

- **Vigilante**–Internet Guard Dog determina dos cosas al seleccionar Vigilante:

  1. Which programs on your computer have unrestricted access to the Internet.
  2. Qué nivel de seguridad, en caso de tenerlo instalado, se ha establecido para su navegador (por ejemplo, Microsoft Internet Explorer).

  Consulte Acerca de Vigilante si desea obtener más información.

- **Guardián de archivos**–Internet Guard Dog comprueba los archivos de correo electrónico (Microsoft Outlook, Netscape, Eudora, etcétera) y los archivos financieros (Quicken y MS Money). Si encuentra cualquiera de estos tipos de archivos, Internet Guard Dog determina si los archivos están protegidos por Guardián de archivos. Si no lo están, Internet Guard Dog le solicitará si desea agregarlos a la lista de Archivos protegidos.

  Consulte About File Guardian si desea obtener más información.

- **Comprobación de Contraseña**–Internet Guard Dog determina si hay alguna carpeta compartida del equipo que no tenga una contraseña asignada.

Limpiador de rastros de Internet

Esta ventana le permitirá evitar que otros usuarios puedan ver qué sitios Web ha estado visitando. Limpiador de rastros de Internet limpiará automáticamente todos los rastros que hayan quedado tras su navegación por la Web. Al cerrar el navegador, Internet Guard Dog muestra un mensaje de alerta de Limpiador de rastros de Internet.

Seleccione una de las siguientes opciones en esta ventana:

- **Solicitar Limpiar después de cerrar el navegador Web**

  Elija esta opción si desea que Internet Guard Dog realice esta solicitud siempre que cierre el navegador.

- **Limpiar automáticamente después de cerrar el navegador**

  Elija esta opción si desea que Internet Guard Dog limpie las carpetas de URL, el historial y la caché cada vez que cierre el navegador, sin necesidad de solicitárselo.

Sugerencia

When you select Automatically clean up after closing Web browser, you can ensure that Internet Guard Dog does not delete the URLs to any sites that you have bookmarkedor added to your favorites list by selecting the **Keep bookmarked items** check box.

Desde esta ventana, podrá acceder a otras opciones de privacidad especificadas en el menú desplegable:

- **Protector de identidad**

  Haga clic aquí para visualizar la ventana de la opción de privacidad Protector de identidad.

- **Bloqueador de cookies**

  Haga clic aquí para visualizar la ventana de la opción de privacidad Bloqueador de cookies.

- **Filtro de búsqueda**

  Haga clic aquí para visualizar la ventana de la opción de privacidad Filtro de búsqueda.

Nota: También puede hacer clic en **Seguridad** si desea visualizar las funciones de seguridad de Internet Guard Dog que están disponibles.

Bloqueador de cookies

Esta ventana le permite seleccionar la opción que controlará la utilización de cookies en su equipo. Internet Guard Dog puede:

- Rechazar todas las cookies.
- Permitir la entrada de todas las cookies.
- Mostrar un mensaje de alerta cada vez que se envíe una cookie al navegador. La alerta muestra el nombre de la entidad que intenta enviar la cookie y le permite aceptarla o rechazarla.

Seleccione alguna de las opciones disponibles en esta ventana:

Para sitios de acceso directo:

- **Aceptar** para aceptar siempre las cookies procedentes de los sitios a los que se conecte directamente. A medida que navegue, Bloqueador de cookies agregará estos sitios a la lista **Permitido**.
- **Rechazar** para rechazar siempre las cookies procedentes de los sitios a los que se conecte directamente. A medida que navegue, Bloqueador de cookies agrega estos sitios a la lista **Rechazados**.
- **Solicitar** para seleccionar si aceptar o rechazar una cookie procedente de un sitio de acceso directo en función de cada caso. A medida que navegue, Internet Guard Dog le pide su confirmación cada vez que un sitio de acceso directo intenta enviar una cookie al equipo.

Para sitios de acceso indirecto:

- **Aceptar** para aceptar siempre las cookies procedentes de los sitios a los que se conecte indirectamente. Bloqueador de cookies agrega estos sitios a la lista **Permitidos**.
- **Rechazar** para rechazar siempre las cookies procedentes de los sitios a los que se conecte indirectamente. A medida que navegue, Bloqueador de cookies agrega estos sitios a la lista **Rechazados**.
- **Solicitar** para seleccionar si aceptar o rechazar una cookie procedente de un sitio de acceso indirecto en función de cada caso.

Para suprimir un sitio URL de las listas

Haga clic en un sitio de los que aparecen en el cuadro de texto. A continuación, haga clic en **Suprimir**.

Para aceptar un sitio URL de las listas

Haga clic en un sitio de los que aparecen en el cuadro de texto. A continuación, haga clic en **Aceptar**.

Para rechazar un sitio URL de las listas

Haga clic en un sitio de los que aparecen en el cuadro de texto. A continuación, haga clic en **Rechazar**.

Desde esta ventana, podrá acceder a otras opciones de privacidad especificadas en el menú desplegable:

- **Protector de identidad**

  Haga clic aquí para visualizar la ventana de la opción de privacidad Protector de identidad.
- **Limpiador de rastros de Internet**

  Haga clic aquí para visualizar la ventana de la opción de privacidad Limpiador de rastros de Internet.
- **Filtro de búsqueda**

  Haga clic aquí para visualizar la ventana de la opción de privacidad Filtro de búsqueda.

Nota: También puede hacer clic en **Seguridad** si desea visualizar las funciones de seguridad de Internet Guard Dog que están disponibles.

Administrador de contraseñas

Esta ventana le permitirá guardar en un lugar seguro varios nombres de inicio de sesión y contraseñas para sitios Web. Cuando visite un sitio que requiera dicha información, puede arrastrarla desde Asistente de navegación hasta el formulario que se visualiza en el navegador.

Aparecerán las funciones siguientes:

Para agregar una contraseña

1. Haga clic en Agregar.
2. Escriba la información que desee almacenar en ese registro.
3. Haga clic en Aceptar.

Para editar un registro de contraseña

1. En la lista Administrador de contraseñas, proceda según corresponda:
   - Haga doble clic en el registro que desee editar.
   - Haga clic en el registro que desee editar y, a continuación, haga clic en **Editar**.
2. Modifique la información que desee almacenar en ese registro.
3. Haga clic en **Aceptar**.

Para suprimir una contraseña

1. En la lista del Administrador de contraseñas, haga clic en el registro que le interese para seleccionarlo.
2. A continuación, haga clic en **Suprimir**.

Desde esta ventana, podrá acceder a otras opciones de seguridad especificadas en el menú desplegable:

- **Vigilante**

  Haga clic aquí para visualizar la ventana de la opción de seguridad Vigilante.
- **Guardián de archivos**

  Haga clic aquí para visualizar la opción de seguridad Guardián de archivos.

Nota: También puede hacer clic en **Privacidad** si desea visualizar las funciones de privacidad de Internet Guard Dog que están disponibles.

Sistema de clasificación

Esta ventana muestra el sistema de clasificación utilizado por Internet Guard Dog para bloquear cualquier tipo de contenido peligroso que pueda encontrar al navegar por Internet. Se trata de una opción de filtrado que puede aplicarse para personalizar la configuración de protección de cada uno de los usuarios.

Si desea agregar algún tema a la lista

1. Seleccione una categoría en la ventana de desplazamiento (por ejemplo, Idioma, Desnudos, Sexo, etc.).
2. A continuación, haga clic en Agregar y siga las instrucciones que aparecen en pantalla.
3. Al terminar, haga clic en Aceptar.

Nota: Sólo tienen acceso a esta ventana el Administrador y el Autoadministrador.

Lista de URL

Esta ventana le permitirá bloquear o permitir el acceso de un usuario a sitios Web susceptibles de contener elementos peligrosos.

Nota: Sólo tienen acceso a esta ventana el Administrador y el Autoadministrador.

Para permitir el acceso de un usuario a un sitio Web

1. Seleccione un sitio de los que aparecen en el cuadro de texto.
2. A continuación, haga clic en Permitir.

Para bloquear el acceso de un usuario a un sitio Web

1. Seleccione un sitio de los que aparecen en el cuadro de texto.
2. A continuación, haga clic en Bloquear.

Para suprimir un sitio Web de la lista visualizada.

1. Seleccione un sitio de los que aparecen en el cuadro de texto.
2. A continuación, haga clic en Suprimir.

Para agregar un sitio Web a la lista

1. Introduzca la dirección en el cuadro de texto correspondiente.
2. A continuación, haga clic en Agregar
3. Al terminar, haga clic en Aceptar.

Lista de palabras

Esta ventana mostrará una lista de las palabras que Internet Guard Dog busca para determinar el bloqueo de contenido peligroso que el usuario puede encontrar al navegar por la Web.

Nota: Sólo tienen acceso a esta ventana el Administrador y el Autoadministrador.

Para agregar una palabra a la lista

1. En el cuadro Agregar/Editar, introduzca la palabra en el cuadro de texto correspondiente.
2. Seleccione la categoría en el menú desplegable.
3. Seleccione una categoría y, a continuación, haga clic en Agregar.
4. Al terminar, haga clic en Aceptar.

Planificación

Esta ventana le permitirá establecer el día y la hora en los que un determinado usuario con perfil obtendrá el permiso necesario para acceder a Internet y navegar por ella.

Nota: Sólo tienen acceso a esta ventana el Administrador y el Autoadministrador.

Para indicar el día y la hora

1. Seleccione un día y una hora en el gráfico.
2. A continuación, seleccione Permitir siempre o Bloquear siempre.
3. Al terminar, haga clic en Aceptar.

Funciones de Internet Guard Dog

Casi seguro que, cuando navega por un sitio Web, se pregunta qué tipo de información se transfieren su equipo y los equipos de Internet. Probablemente haya oído decir que estas transferencias se realizan sin problemas; sin embargo, existen virus y caballos de Troya, por ejemplo, que pueden comprometer su privacidad o dañar la integridad de los datos del equipo.

Internet Guard Dog de McAfee está pensado para proteger sus datos y le permite controlar la forma en que utiliza Internet.

Internet Guard Dog le protege de dos formas básicas:

1. Internet Guard Dog comprueba que en el equipo no existan posibles riesgos para la seguridad y la privacidad, y le permite solucionarlos antes de que los datos resulten dañados o se ponga en peligro su privacidad. Algunas de las cosas que comprueba Internet Guard Dog son:
   - Programas que tienen acceso a Internet.
   - Datos confidenciales, como archivos financieros, y los programas que pueden acceder a ellos.
   - Mediante la utilización de McAfee VirusScan, detecta virus que pueden dañar los datos del equipo, obligándole incluso a volver a dar formato al disco duro.

Los controles como ActiveX y los subprogramas Java, que pueden realizar acciones peligrosas en el equipo.

2. Internet Guard Dog, fiel a su nombre (Perro guardián), mantiene la guardia y le alerta de los sucesos dañinos que pueden amenazar su privacidad y su seguridad. Internet Guard Dog activará su sistema de alerta, por ejemplo, cuando se produzca alguno de estos sucesos:
   - Cuando se produzca una intrusión sin garantías procedente de otras fuentes de Internet.
   - Cuando los programas del equipo transfieran datos confidenciales a otros sitios.
   - Cuando detecte sitios Web que envían cookies al equipo mientras utiliza Internet.

   Consulte Conceptos esenciales acerca de la privacidad y la seguridad para obtener más información.

El extenso conjunto de funciones de protección de Internet Guard Dog se puede utilizar directamente o mientras utiliza el equipo:

1. Funciones que puede utilizar directamente

- Comprobación de la seguridad del equipo.
- Limpieza del navegador eliminando todo el historial de conexiones Web.
- Actualización de Internet Guard Dog con la tecnología de protección más reciente de McAfee.
- Ejecución de la Entrevista para cambiar las preferencias de privacidad y seguridad.
- Configuración de una protección por contraseña de Internet Guard Dog.
- Adición de un perfil de usuario y personalización de la configuración de protección individual, incluidas las opciones de Filtro de Internet.

  Nota: Únicamente el Administrador puede agregar y aplicar la configuración de protección para usuarios individuales.

2. Funciones que están en ejecución mientras utiliza el equipo

- Control de los programas de su equipo que pueden conectarse a Internet. Si un programa no autorizado intenta conectarse a Internet, Internet Guard Dog le alerta.
- Protección del correo electrónico y los archivos fundamentales del sistema para que programas no autorizados, como los caballos de Troya, no puedan alterarlos.
- Impedir que terceras personas fisgoneen los archivos del navegador de Internet, amenazando así su privacidad.
- Bloqueo del acceso a los datos personales por parte de programas no autorizados basados en Internet.

El conjunto de funciones incluido en Internet Guard Dog representa la protección mínima que debería tener cualquier usuario de Internet. Dispondrá de las últimas mejoras de Internet Guard Dog introducidas por McAfee mediante la función Actualización.

Para obtener más información acerca de las funciones de seguridad, privacidad y protección por contraseña de Internet Guard Dog, consulte:

- Acerca de Preferencias de Internet Guard Dog
- Acerca de Planificador
- Acerca de Bloqueador de cookies
- Acerca de Protector de identidad
- Acerca de Limpiador de rastros de Internet
- Acerca de Filtro de búsquedas
- Acerca de Vigilante

- Acerca de Administrar contraseñas

Funcionamiento de Internet Guard Dog

McAfee diseñó Internet Guard Dog para poder sacar el máximo partido de las posibilidades de Internet sin necesidad de preocuparse por la privacidad o la seguridad del equipo. Guard Dog tiene como finalidad protegerle del modo más transparente posible, evitando en la medida de lo posible las explicaciones demasiado técnicas.

Guard Dog simplifica las cosas:

- Realizando una Entrevista preliminar

  La primera vez que ejecute Internet Guard Dog, interactuará con el programa respondiendo a algunas preguntas. Internet Guard Dog utiliza las respuestas para determinar la mejor forma de garantizar sus necesidades particulares en cuanto a seguridad y privacidad. Cuando finalice la Entrevista, Internet Guard Dog estará preparado para proteger su equipo. Si tiene que cambiar la configuración de seguridad, podrá volver a ejecutar la Entrevista.

  Consulte Respuesta a las preguntas de la entrevista para obtener más información.

- Controlando sus hábitos informáticos

  A medida que vaya utilizando el programa, Internet Guard Dog le planteará otras preguntas. Internet Guard Dog está aprendiendo sobre su forma de utilizar el equipo e Internet. Tal vez le parezca una molestia tener que responder a estas preguntas, pero después de las primeras sesiones de utilización del equipo ya no serán tan frecuentes. Le rogamos que sea paciente y responda con atención a las preguntas formuladas.

  Si observa repetidamente que Internet Guard Dog le alerta de forma errónea, Internet Guard Dog no estará adecuadamente personalizado. Para solucionar esta situación, puede volver a responder a las preguntas de la Entrevista o cambiar la configuración de Internet Guard Dog directamente en el cuadro de diálogo **Configuración de protección**.

  Consulte Temas generales acerca de la Configuración de protección de Internet Guard Dog para obtener más información.

- Ejecutando Internet Guard Dog en segundo plano

  Parte de Internet Guard Dog se ejecuta discreta y continuamente, en un segundo plano, protegiendo su equipo mientras lo utiliza. El icono de Internet Guard Dog en la bandeja del sistema, situada en el ángulo derecho de la barra de tareas de Windows, le indicará que está en ejecución. Sin embargo, cuando Internet Guard Dog detecta una amenaza para la seguridad, le avisa mostrando un cuadro de diálogo en segundo plano con opciones para controlar la situación.

  Consulte Respuesta a las alertas de Internet Guard Dog para obtener más información.

Conceptos esenciales acerca de la privacidad y la seguridad

El creciente interés suscitado por Internet y la expansión de la comercialización de bienes y servicios en la World Wide Web están convirtiendo el tema de la seguridad en un concepto esencial. Las transacciones comerciales deben protegerse tanto desde el punto de vista del comprador como del vendedor. El problema de llevar a cabo operaciones empresariales por Internet es de fácil definición. Aunque es relativamente fácil configurar un sitio Web para mostrar y vender cosas, no lo es tanto desarrollar mecanismos para garantizar la seguridad de la información que debe transmitirse en ambos sentidos para realizar las transacciones. Además, está la presencia de determinadas personas (llamados '**hackers**') que disponen de medios para controlar las transacciones y extraer datos tan importantes como los números de las tarjetas de crédito y de las cuentas bancarias.

Sin embargo, no hay que darlo todo por perdido. El software de navegador de Microsoft Internet Explorer y Netscape ha incorporado una tecnología de codificación denominada Secure Sockets Layer (SSL). Cuando la utiliza, aparece un icono en el navegador para indicar que la tecnología SSL está activa, lo cual le da la certeza casi absoluta de que su transacción es segura.

Aunque los métodos de codificación suponen un importante avance, subsisten, no obstante, algunos problemas. En primer lugar, no todos los servidores y navegadores admiten la tecnología SSL. El software SSL incrementa el coste de la inversión en servidores, y puede disminuir la velocidad de las transacciones. En segundo lugar, Microsoft y Netscape no han realizado un esfuerzo de cooperación en materia de seguridad, con lo cual, cada una de estas empresas posee su propio navegador y, aunque ninguno es perfecto, cada uno posee sus propias carencias de seguridad. Por ello, puede resultar bastante difícil evaluar los riesgos de seguridad, e incluso puede verse obligado a echar a suertes la elección del navegador. Sin embargo, las empresas son conscientes de los riesgos y los peligros que supone la introducción de medidas de seguridad, y están trabajando para corregir sus problemas.

Las transacciones seguras son sólo una parte del problema. Cuando los servidores Web reciben información, deben ser capaces de mantenerla a salvo. En una red de grandes dimensiones, en la que un servidor Web es sólo uno de los múltiples tipos de servidores, el administrador de redes intenta aislar los servidores Web de otros servidores importantes de la empresa. Sin embargo, algunas aplicaciones Web interactuan con los datos almacenados en otros servidores, con lo cual dejan un resquicio para acceder a datos potencialmente confidenciales. Los "hackers" eligen como blanco a los servidores Web porque la tecnología para garantizar su seguridad está todavía en fase de desarrollo. Existe una tecnología de seguridad llamada “cortafuegos” que permite controlar el acceso no autorizado a los datos confidenciales, pero requiere un mantenimiento correcto, por lo que, incluso en los sistemas con un mantenimiento óptimo, los cortafuegos no logran proteger determinados servicios.

Los usuarios disponen de dos formas para determinar si es posible transmitir información a un sitio Web de forma segura.

- En primer lugar, la mayoría de sitios Web comerciales poseen servidores seguros y le notifican que está utilizando una conexión segura. Si el sitio no es seguro, recibirá una advertencia y tendrá la opción de continuar o no.
- En segundo lugar, la mayoría de navegadores son suficientemente inteligentes para detectar el nivel de seguridad del sitio al que están conectados y, además, son capaces de mostrar esa información.

Cuando utilice Internet, le será de gran ayuda recurrir a todas las medidas de seguridad disponibles. Microsoft y Netscape están desarrollando una importante labor para introducir una serie de soluciones avanzadas y corregir los fallos de seguridad de los productos de Internet existentes. Para beneficiarse de sus últimas innovaciones, puede actualizar su software de navegador ejecutando Internet Guard Dog con frecuencia.

Protección de la información personal privada mientras utiliza Internet

Proteger la integridad de los datos y proteger su privacidad contra la intrusión de programas no autorizados diseñados para recopilar información personal son dos temas importantes a los que debe prestar atención cuando utiliza Internet. Internet Guard Dog proporciona una serie de funciones de privacidad para proteger la información personal confidencial mientras navega por Internet.

Entre estas funciones cabe destacar:

- **Bloqueador de cookies**

  Las cookies mejoran la eficacia de un sitio Web utilizando la información obtenida y almacenada anteriormente en el equipo Por ejemplo, las cookies permiten que su sitio comercial favorito muestre información personalizada cada vez que lo visite, o que un sitio Web protegido por contraseña la recupere para que no tenga que introducirla cada vez que lo visita.

  Puesto que no puede controlar qué seguimiento se está realizando ni quién está recopilando información acerca de usted, las cookies también representan una amenaza para la privacidad. Sin embargo, Bloqueador de cookies de Internet Guard Dog le permite controlar quién envía y recupera las cookies de su equipo. De este modo, podrá disfrutar de las ventajas que ofrecen las cookies de sus sitios Web favoritos y bloquear las cookies procedentes de otros sitios.

- **Protector de identidad**

  Internet Guard Dog le permite especificar cuáles son los datos personales que desea controlar. Puede introducir su nombre, dirección, dirección de correo electrónico, así como los números de la cuenta bancaria y de la tarjeta de crédito. Internet Guard Dog le alertará cuando una aplicación intente enviar a través de Internet la información incluida en Protector de identidad.

- **Limpiador de rastros de Internet**

  Internet Guard Dog realiza un seguimiento de las actividades de navegación. Una vez haya salido de Internet, Limpiador de rastros de Internet suprimirá los archivos del historial de Internet y de la caché del navegador Esta función puede ser muy útil para mantener la privacidad y la seguridad en entornos en los que los usuarios comparten equipos.

- **Filtro de búsquedas**

  Internet Guard Dog controla determinados tipos de actividades mientras navega por Internet. Por ejemplo, puede introducir su dirección de correo electrónico en un sitio. Esta información se registra y correlaciona con cookies, con lo que determinados sitios Web pueden crear bases de datos con información acerca de usted y de sus intereses Es posible que no desee que se recopile esta información. Con Filtro de búsquedas esté activado, la información importante no se moverá de donde está.

Creación de un entorno informático seguro

Proteger la integridad de los datos contra la intrusión por parte de programas no autorizados diseñados para recopilar información personal es uno de los temas más importantes a considerar cuando se utiliza Internet. Internet Guard Dog proporciona una serie de funciones de privacidad destinadas a proteger la información personal y confidencial mientras navega por Internet.

Entre estas funciones cabe destacar:

- **Vigilante**

  Vigilante controla el equipo y lo que en él ocurre mientras navega por Internet. Vigilante actúa como una red de seguridad alertándole cuando se conecta con sitios Web que incluyen contenidos dañinos como controles ActiveX o subprogramas Java. Por otra parte, los programas instalados en el equipo pueden proceder de diversas fuentes, algunas de las cuales pueden no ser completamente fiables. En realidad, es imposible qué va a hacer un programa hasta que se instala y se utiliza. Un programa aparentemente inocente puede haber sido diseñado para buscar determinado tipo de información de su equipo y utilizar Internet para transmitirla a otro equipo.

  Vigilante le alerta cuando un programa no autorizado intenta conectar con Internet o cuando se envía a través de Internet la información protegida por Protector de identidad.

  Consulte Acerca de Vigilante para obtener más información.

- **Guardián de archivos**

  El principal objetivo de Guardián de archivos es proteger los archivos confidenciales o fundamentales del equipo, permitiéndole especificar qué aplicaciones tienen acceso a ellos. Guardián de archivos protege automáticamente los archivos de correo electrónico para que sólo pueda utilizarlos la aplicación de correo. Por otra parte, puede agregar archivos (como, por ejemplo, archivos financieros) a la lista Archivos protegidos, asegurándose con ello de que sólo pueda acceder a ellos la aplicación utilizada para crearlos.

  Otra función importante de Guardián de archivos es la alerta que emite cuando detecta sucesos potencialmente dañinos como, por ejemplo, un control ActiveX explorando la unidad de disco duro o el hecho de que un caballo de Troya vuelva a dar formato al disco duro.

  Para obtener más información, consulte Acerca de Guardián de archivos.

- **Administrar contraseñas**

  ¿Es capaz de recordar la contraseña y el nombre de usuario de todos los sitios Web protegidos que visita? Si los ha anotado en un papel, ¿es capaz de recordar dónde guardó la lista y dispone de un lugar seguro donde guardarla?

  Si deja que Internet Guard Dog administre sus contraseñas, no tendrá que volver a plantearse cuestiones como ésta. Para no tener que escribir el nombre de usuario y la contraseña cada vez que visita un sitio Web controlado por contraseña, puede arrastrar y soltar esta información desde Asistente de navegación hasta los cuadros correspondientes de la pantalla de inicio de sesión.

  Para obtener más información, consulte Acerca de Administrar contraseñas y Acerca de Asistente de navegación.

Protección de datos importantes contra la infección de virus

Los virus se transmiten fácilmente, sobre todo si descarga datos de sitios Web. Mediante la búsqueda constante de virus en los archivos nuevos, Centinela de virus puede reducir en gran medida el riesgo de infección por virus, eliminándolos antes de que puedan causar daños.

Dispone de pleno control sobre Centinela de virus. Puede configurarlo para que se ejecute automáticamente en la página Configuración de protección de Centinela de virus, o personalizar Comprobación para detectar los virus según sus necesidades.

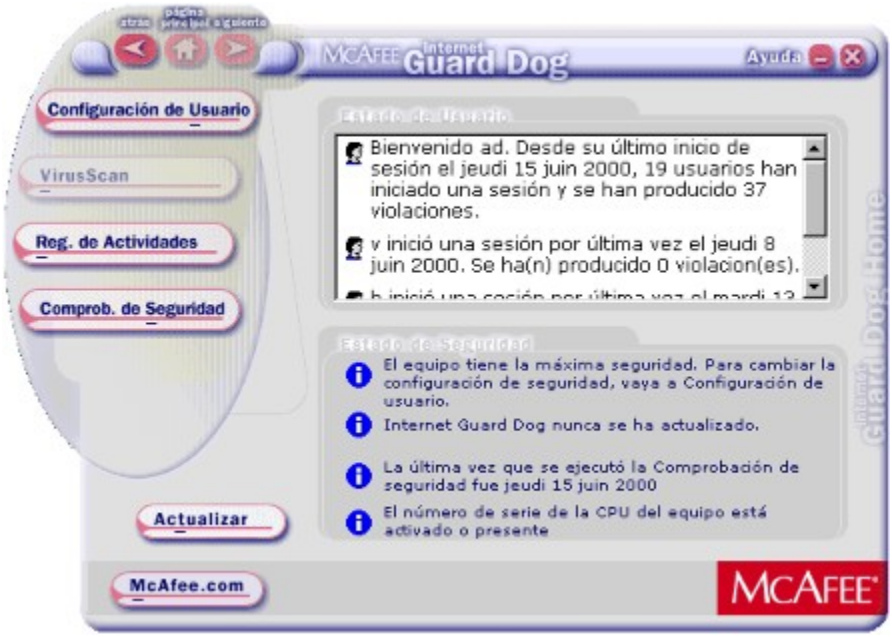
McAfee trabaja constantemente para identificar y encontrar soluciones para los virus. Asimismo, McAfee incluye la información sobre los virus conocidos en un archivo de patrón de virus. A medida que van identificándose nuevos virus, el archivo de patrón se actualiza con la nueva información. Puede cargar el archivo de patrón de virus más reciente utilizando la función Actualización de Internet Guard Dog.

Para obtener más información, consulte:

- Determinación del tipo de Comprobación
- Utilización de la Actualización

Utilización de las funciones de la pantalla inicial de Internet Guard Dog

La pantalla inicial de Internet Guard Dog es la puerta de entrada al mundo de las funciones de protección y seguridad de Internet Guard Dog.



Desde la pantalla inicial puede acceder a las siguientes funciones:

- **Configuración del usuario**

  Haga clic para acceder a la pantalla Configuración del usuario. En esta pantalla puede agregar, editar y borrar el perfil del usuario, así como establecer opciones de filtrado de Internet que especifiquen restricciones como, por ejemplo, bloquear los sitios Web a los que no se permite el acceso; utilizar listas de palabras a seleccionar, añadir palabras para que los perfiles no las encuentren o bloquear los archivos adjuntos de correo electrónico.

- **VirusScan**

  Haga clic para iniciar McAfee VirusScan. Mediante sus componentes, puede establecer tareas de exploración de virus según sus preferencias, configurar operaciones de exploración y visualizar información de virus a través del sitio Web de McAfee.

- **Registros de actividades**

  Mediante esta función, podrá ver las medidas adoptadas por Internet Guard Dog para proteger su seguridad y privacidad, así como la de otros usuarios con perfil definido en su equipo. En la lista se incluye información acerca de violaciones de la seguridad, mantenimiento y actividades.

  Sugerencia

  Para ver las entradas de las columnas Acciones y Tipo de Internet Guard Dog por orden alfabético, haga clic en el título de una de las columnas.

  Para obtener más información, consulte Acerca de los registros de actividades del usuario y Acerca de Asistente de navegación.

- **Actualización**

  McAfee trabaja constantemente para mejorar Internet Guard Dog. La mayoría de estas mejoras, llamadas actualizaciones, están disponibles en el sitio Web de McAfee. La función Actualización utiliza McAfee Software Update Finder y su conexión a Internet para buscar cualquier actualización disponible de los programas VirusScan e Internet Guard Dog de McAfee.

  Para obtener más información, consulte Utilización de la Actualización.

- **Comprobación de seguridad**

  Cuando ejecute Comprobación de seguridad, Internet Guard Dog efectuará en el equipo una inspección exhaustiva en búsqueda de posibles problemas de seguridad y privacidad. Cuando encuentra problemas, Internet Guard Dog crea una lista y la muestra en la pantalla La comprobación ha detectado. Puede seleccionar un problema e Internet Guard Dog lo mostrará en una pantalla adicional con una descripción del mismo y una recomendación sobre cómo solucionarlo. Si

soluciona un problema y no le gusta el resultado, Internet Guard Dog le permite Deshacer el cambio.

Para obtener más información, consulte Utilización de la comprobación y Determinación del tipo de comprobación.

- **Opciones**

  Si desea cambiar la configuración de la comprobación o protección, o bien reiniciar Entrevista de Internet Guard Dog para realizar cambios, haga clic en Opciones y seleccione una opción del menú desplegable. Consulte Utilización de las opciones de Internet Guard Dog.

- **Ayuda**

  Si desea ver el sistema de Ayuda de Internet Guard Dog o visualizar un tema de Ayuda concreto en la pantalla en la que está trabajando, haga clic en Ayuda y seleccione una opción del menú desplegable Consulte Acerca del menú Ayuda.

- **McAfee.com**

  Haga clic aquí para acceder al sitio Web de McAfee.

También puede ver información relacionada con la seguridad en la pantalla inicial a través de estas ventanas:

- **Ventana Estado del usuario**

  Muestra un informe que indica la última vez que se conectó un usuario, incluyendo la fecha y la hora concretas.

- **Ventana Estado de seguridad**

  Muestra la configuración predeterminada de la seguridad del equipo (seguridad máxima, mínima o personalizada).

Utilización de la Comprobación de seguridad

La función Comprobación de seguridad realizará una inspección exhaustiva de posibles problemas de seguridad y privacidad. Internet Guard Dog resume los problemas que se han identificado en esta función y los muestra en la pantalla La comprobación ha detectado.

Asimismo, Internet Guard Dog identifica los temas y acciones relacionados con la seguridad que se han producido recientemente en el equipo para que pueda solucionarlos. Cuando Internet Guard Dog finalice una comprobación de seguridad, puede estar seguro de que continuará manteniendo la privacidad y la seguridad de todos los datos confidenciales del equipo.

Comprobación de seguridad puede utilizarse específicamente para garantizar que:

- Los archivos fundamentales y de correo electrónico están protegidos.
- La información privada se ha suprimido de las carpetas de historial y de caché del navegador.
- La configuración de seguridad es la adecuada.
- Está satisfecho con su gestión reciente de las alertas.
- Nadie más ha cambiado la configuración de seguridad sin que lo sepa.

¿Cómo se realiza una comprobación de seguridad?

Haga clic en **Comprobación de seguridad** en la pantalla inicial de Internet Guard.

Internet Guard Dog mostrará una segunda pantalla con una lista de las comprobaciones y proporcionará información acerca del progreso de cada una de ellas.

Para obtener más información, consulte Comprobaciones de Internet Guard Dog y Respuesta a La comprobación ha detectado.

Utilización de la Actualización

McAfee trabaja constantemente para mejorar Internet Guard Dog. La mayoría de estas mejoras, llamadas actualizaciones, están disponibles en el sitio Web de McAfee. La función Actualización utiliza McAfee Software Update Finder para buscar las actualizaciones del software de Internet Guard Dog disponibles, incluyendo los archivos de patrón de virus actualizados, , las descarga y las instala.

Actualización de Internet Guard Dog

- Haga clic en **Actualización** en la pantalla inicial de Internet Guard Dog. Internet Guard Dog muestra McAfee Software Update Finder a través de un navegador de Web para comprobar si existen actualizaciones. Si hay una actualización disponible, Internet Guard Dog la descarga e instala automáticamente.

Acerca de los registros de actividades

Los registros de actividades del usuario le permiten ver una lista de todas las interacciones existentes entre usted y otros usuarios del equipo con perfil definido, e Internet Guard Dog. Haga clic en Actividades del usuario en la pantalla inicial para que aparezca la ventana Actividades del usuario.

La lista muestra la información disponible sobre:

1. **Violación**

   Visualiza información sobre las actividades realizadas por un usuario con perfil definido que violen la configuración de protección establecida por el Administrador (por ejemplo, intentar enviar el número de una tarjeta de crédito).

2. **Información**

   Visualiza información acerca de las acciones realizas por Internet Guard Dog. Se especifican las funciones concretas utilizadas en cada caso.

3. **Actividad**

   Visualiza información acerca de la identidad del usuario con perfil definido que ha utilizado el equipo. También muestra el día, la fecha y la hora de conexión y desconexión del equipo.

Impresión, borrado o guardado de los registros de actividades del usuario

Tras visualizar la ventana de registro de actividades, realice una de las siguientes acciones:

- Haga clic en **Borrar** para eliminar el informe.
- Haga clic en **Imprimir** para imprimir el informe.
- Haga clic en **Guardar** para guardar el informe. Desplácese hasta la ubicación en la que desea guardar el informe y haga clic en Guardar.

  Sugerencia

  Para visualizar las entradas de las columnas Acciones y Tipo de Internet Guard Dog por orden alfabético, haga clic en el título de una de las columnas.

Utilización de las opciones de Internet Guard Dog

La función Opciones de Internet Guard Dog le permite cambiar la configuración específica para personalizar el modo de funcionamiento del equipo. Tras seleccionar Editar opciones del usuario en la pantalla Configuración del usuario, aparecerá la ventana Opciones del usuario. Seleccione uno de los botones disponibles:

- Filtrado de Internet Haga clic en este botón para seleccionar en el menú desplegable las opciones para configurar el modo en que Internet Guard Dog protege al usuario mientras navega por Internet.

  Para obtener más información, consulte Funcionamiento del filtrado de Internet.
- **Privacidad:** Haga clic en este botón para seleccionar en el menú desplegable las opciones para configurar el modo en que Internet Guard Dog protege su privacidad mientras navega por Internet.

  Para obtener más información, consulte Temas generales acerca de la Configuración de protección de Internet Guard Dog.
- **Seguridad:** Haga clic en este botón para seleccionar en el menú desplegable las opciones para configurar el modo en que Internet Guard Dog protege su seguridad mientras navega por Internet.

  Para obtener más información, consulte Temas generales acerca de las Funciones de seguridad de Internet Guard Dog.
- **Opciones**: Haga clic en este botón para seleccionar en el menú desplegable las opciones para cambiar su contraseña, seleccionar mensajes de alerta o agregar un soporte de idiomas.

Obtención de ayuda

Puede acceder al sistema de ayuda de varias formas . Puede acceder a la Ayuda desde la pantalla inicial de Internet Guard Dog y, si desea más información durante la Entrevista, puede pulsar **F1** para recibir ayuda sobre la página en la que está trabajando. Si está solucionando problemas que Internet Guard Dog ha identificado durante una Comprobación, puede obtener una pantalla de ayuda específica haciendo clic en **Ayuda** y después en **Ayuda sobre esta pantalla**.

¿Cómo se accede al sistema de Ayuda de Internet Guard Dog?

1. Haga clic en **Ayuda** en la barra de menú de la parte superior de la pantalla.
2. Haga clic en **Temas de ayuda** para acceder al sistema de Ayuda, o bien haga clic en **Ayuda sobre esta pantalla** para obtener más información sobre la pantalla en la que está trabajando.
3. Puede acceder al contenido de la Ayuda desde el menú emergente de Internet Guard Dog. Haga clic con el botón derecho del ratón en el icono de Internet Guard Dog y haga clic en **Ayuda**.

Para obtener más información, consulte Acerca del menú Ayuda.

Respuesta a las preguntas de la Entrevista

Siempre que utilice una aplicación de control de la seguridad del equipo, debe valorar el nivel de seguridad que necesita y el impacto que pueda tener sobre el rendimiento del equipo.

Para que no sea difícil tomar una decisión, Internet Guard Dog utiliza la función Entrevista para determinar qué grado de seguridad necesita. Puede utilizar las recomendaciones de Internet Guard Dog como orientación. Si desea más información sobre la página, pulse **F1** en el teclado. Una vez haya terminado de responder a las preguntas de la Entrevista, Internet Guard Dog utilizará sus respuestas para configurarse automáticamente.

¿Cómo se inicia la Entrevista?

La Entrevista se realiza después de finalizar la instalación de Internet Guard Dog en el equipo. Siga las instrucciones que aparecen en la pantalla y escriba la información necesaria para personalizar las funciones de Internet Guard Dog.

Nota: Sólo puede acceder a la función Entrevista de Internet Guard Dog el Administrador. Consulte Administrador de Internet Guard Dog.

¿Cómo se reinicia la Entrevista?

Si desea cambiar la configuración del funcionamiento de Internet Guard Dog, puede reiniciar la Entrevista desde la pantalla inicial.

Haga clic en **Opciones** en la pantalla inicial de Internet Guard Dog y seleccione **Entrevista** en el menú.

Sugerencia

Puede inspeccionar o modificar las opciones que Internet Guard Dog ha seleccionado a través de la función Configuración de protección. Existen dos maneras de iniciar el cuadro de diálogo Configuración de protección:

- Haga clic con el botón derecho del ratón en el icono de Internet Guard Dog en la bandeja del sistema de la barra de tareas de Windows y seleccione **Configuración de protección** en el menú emergente.
- Haga clic en Opciones en la pantalla inicial de Internet Guard Dog y, a continuación, seleccione **Configuración de protección** en el menú.

  Para obtener más información, consulte Temas generales acerca de la Configuración de privacidad de Internet Guard Dog.

Acerca de Planificador

Internet Guard Dog dispone de una serie de elementos que se pueden programar. Puede programar Internet Guard Dog para que ejecute tareas que de larga duración como, por ejemplo, una detección de virus minuciosa mientras no está trabajando en el equipo. Recuerde que el equipo no puede estar apagado durante el suceso programado.

Puede programar las siguientes tareas:

- **Codificación de archivos del equipo**–Codifica los archivos que están en la lista Archivos protegidos del Guardián de archivos.
- **Descodificación de archivos del equipo**–Descodifica los archivos que están en la lista Archivos protegidos de Guardián de archivos.
- **Programar la eliminación de archivos eliminados del PC**–Sobrescribe los datos que quedan después de eliminar permanentemente los archivos de la Papelera de reciclaje.
- **No olvide comprobar actualizaciones de Internet Guard Dog**–Muestra un mensaje recordatorio. Al instalar Internet Guard Dog, este suceso se programará para que tenga lugar cada mes.

Configuración de Planificador

1. Haga clic en **Opciones** en la página inicial de Internet Guard Dog. A continuación, haga clic en **Configuración de protección**.
2. En la parte izquierda de la pantalla, compruebe que aparece una marca en la casilla de verificación que se encuentra junto a Planificador.
3. Haga clic en **Planificador**.
4. Haga clic en **Agregar**.
5. Seleccione un suceso para programar.
6. En Add Schedule Wizard encontrará los pasos que debe seguir para seleccionar un intervalo, una fecha y una hora para el suceso.
7. Haga clic en **Finalizar** para agregar el suceso a la lista de Planificador.

Para editar un suceso programado

1. Seleccione un suceso de la lista de Planificador.
2. Haga clic en **Editar**. En Add Schedule Wizard encontrará los pasos que debe seguir para efectuar las selecciones correspondientes.

Para suprimir un suceso programado

1. Seleccione un suceso de la lista de Planificador.
   - Para seleccionar sucesos contiguos, haga clic en el primer suceso, pulse la tecla Mayús y haga clic en el último suceso.
   - Para seleccionar sucesos que no son contiguos, haga clic en el primer suceso, pulse la tecla Control y haga clic en los sucesos que desee.
2. Haga clic en **Suprimir.**

Temas generales acerca de la Configuración de protección de Internet Guard Dog

Internet Guard Dog le permite determinar los niveles de privacidad y seguridad aplicables mediante un conjunto de opciones configurables llamado Configuración de protección. Una parte de Internet Guard Dog trabaja constantemente en segundo plano para proteger la privacidad de los datos del equipo en función de la selección realizada. Internet Guard Dog muestra las opciones en una serie de páginas de Configuración de protección que contienen casillas de verificación, cuadros de lista, botones y otros controles que puede utilizar para introducir valores.

Para obtener más información, consulte Utilización de las opciones de Internet Guard Dog y Acceso al menú Opciones de Internet Guard Dog.

Las páginas de Configuración de protección están organizadas en tres categorías:

1. **Preferencias:** La categoría Preferencias contiene dos páginas de Configuración de protección:
   - **Página Preferencias de Configuración de protección**–Las opciones de esta página le permiten controlar el comportamiento general de Internet Guard Dog, como el momento en que se carga, la forma en que le alerta o si es necesaria una contraseña para ejecutar el programa. Si el equipo está equipado con una tarjeta de sonido, Internet Guard Dog puede emitir una alerta sonora.
   - **Página Planificador de Configuración de protección:** Las opciones de esta página le permiten configurar Internet Guard Dog para que realice determinadas tareas que requieren mucho tiempo, como la exploración de virus, en postergándolas hasta el momento que considere más oportuno.

     Para obtener más información, consulte Acerca de Preferencias de Internet Guard Dog y Acerca de Planificador.
2. **Privacidad**–La categoría Privacidad contiene tres páginas de Configuración de protección:
   - **Bloqueador de cookies**–Las opciones de esta página le permiten configurar Internet Guard Dog para que acepte o rechace las cookies cuando navegue por Internet. Puede decidir qué hacer con las cookies procedentes de sitios Web con acceso directo e indirecto. Cuando visite por primera vez un sitio y decida si aceptar o rechazar una cookie, Internet Guard Dog agregará el sitio a la lista de sitios Permitidos o Rechazados. Con ello, cuando vuelva a visitar un sitio, Internet Guard Dog comprobará la lista y aceptará o rechazará la cookie sin molestarle.
   - **Protector de identidad**–Las opciones de esta página le permiten introducir información personal específica para que Internet Guard Dog la proteja. Internet Guard Dog explora los archivos y las carpetas del equipo para determinar si contienen algunos de estos datos personales y financieros. Cuando localiza estos archivos, Internet Guard Dog le pregunta si desea agregar estos archivos a la lista de archivos controlados por Guardián de archivos.
   - **Limpiador de rastros de Internet**–Las opciones de esta página le permiten determinar si desea que Limpiador de rastros de Internet elimine los archivos de Internet automáticamente o si debe preguntárselo cada vez que cierra el navegador.

     Para obtener más información, consulte:

     - Acerca de Bloqueador de cookies
     - Acerca de Protector de identidad
     - Acerca de Limpiador de rastros de Internet
3. **Seguridad**–La categoría Seguridad contiene tres páginas de Configuración de protección:
   - **Vigilante**–Las opciones de esta página le permiten configurar Vigilante para que mantenga la guardia sobre el equipo. Vigilante actúa como una red de seguridad del equipo y le alerta cuando detecta determinadas actividades potencialmente dañinas, como el envío de números de tarjetas de crédito a través de Internet o la conexión con un sitio Web dañino.
   - **Guardián de archivos**–Las opciones de esta página de Configuración de protección le ayudan a configurar Guardián de archivos para que proteja los archivos confidenciales o críticos del equipo. También puede especificar los tipos de alerta que muestra Guardián de archivos cuando se realiza una actividad potencialmente dañina, como el intento por parte de un programa de acceder a un archivo protegido por Guardián de archivos.
   - Guardián de archivos puede proteger automáticamente sus archivos de correo electrónico para que sólo los pueda utilizar la aplicación de correo. Puede agregar otros archivos a la lista Archivos protegidos, como archivos financieros, asegurándose con ello de que sólo tendrá acceso la aplicación que utilizó para crearlos .
   - **Administrar contraseñas**–Para no tener que escribir el nombre de usuario y la contraseña cada vez que visita un sitio Web controlado por contraseña, introduzca sus nombres de usuario y contraseñas en Administrar contraseñas. Cuando visite ese sitio, arrastre esa información desde Asistente de navegación y suéltela en los cuadros correspondientes de la pantalla de inicio de sesión.

     Para obtener más información, consulte:

     - Acerca de Vigilante
     - Acerca de Guardián de archivos
     - Acerca de Administrar contraseñas
     - Acerca de Asistente de navegación

Comprobaciones de Internet Guard Dog

Una vez finalizada la Entrevista, deseará conocer cuáles son los peligros que amenazan a su equipo. Comprobación de seguridad examina la privacidad y los problemas de seguridad del equipo basándose en la información proporcionada durante la Entrevista y le orienta en la resolución de los problemas que encuentra. Si utiliza las opciones recomendadas por Internet Guard Dog en la Entrevista, sólo será necesario que ejecute Comprobación de seguridad después de instalar Internet Guard Dog y, en lo sucesivo, una vez al mes.

Comprobaciones de Internet Guard Dog

- **Comprobación de Actualizaciones de Internet Guard Dog**–McAfee mejora continuamente Internet Guard Dog y coloca estas mejoras–llamadas actualizaciones–en el sitio Web de McAfee. Si selecciona Comprobación de actualizaciones de Internet Guard Dog, Internet Guard Dog iniciará McAfee Software Update Finder a través de un navegador para buscar las actualizaciones de Internet Guard Dog, así como los nuevos archivos de patrón de virus. Puede utilizar esta función para localizar, recuperar e instalar cualquier actualización disponible.

  Para obtener más información, consulte Utilización de la Actualización.

- **Versión del navegador**–Microsoft y Netscape también mejoran el software de navegador y proporcionan actualizaciones en sus sitios Web. Es preciso mantener actualizado el software del navegador para beneficiarse de las funciones de seguridad adicionales que proporcionan los navegadores.

- **Protector de identidad**–Internet Guard Dog explora los archivos del equipo para determinar si contienen de los datos personales o financieros introducidos en Protector de identidad durante la Entrevista o directamente en la página Protector de identidad de Configuración de protección. Internet Guard Dog le preguntará si desea agregar estos archivos a la lista de archivos controlados por Guardián de archivos.

  Para obtener más información, consulte Acerca de Guardián de archivos y Acerca de Protector de identidad.

- **Cookies**–Internet Guard Dog comprueba el equipo para ver si ha quedado alguna cookie después de cerrar el navegador de Web.

  Para obtener más información, consulte Acerca de Bloqueador de cookies.

- **Rastros de Internet**–Internet Guard Dog determina si el navegador ha dejado algún archivo de Internet en el equipo.

  Para obtener más información, consulte Acerca de Limpiador de rastros de Internet.

- **Vigilante**–Internet Guard Dog determina dos cosas cuando se selecciona Vigilante:

  1. Qué programas del equipo tienen acceso no restringido a Internet.
  2. Qué tipo de nivel de seguridad, si lo ha instalado, está establecido en el navegador (p. ej., Microsoft Internet Explorer).

  Para obtener más información, consulte Acerca de Vigilante.

- **Guardián de archivos**–Internet Guard Dog comprueba los archivos de correo electrónico (Microsoft Outlook, Netscape, Eudora, etcétera) y los archivos financieros (Quicken y MS Money). Si encuentra alguno de estos archivos, Internet Guard Dog determina si están protegidos por Guardián de archivos. Si no lo están, Internet Guard Dog le preguntará si desea agregarlos a la lista Archivos protegidos.

  Para obtener más información, consulte Acerca de Guardián de archivos.

  Para obtener más información, consulte:

  - Utilización de Comprobación
  - Cómo se realiza una comprobación

Respuesta a La comprobación ha detectado

Internet Guard Dog compila una lista de los problemas y los temas encontrados durante una comprobación de seguridad. Estos problemas aparecen bajo los títulos Seguridad y Privacidad en la pantalla La comprobación ha detectado. Cuando selecciona un problema, puede realizar las siguientes acciones:

- **Arreglar**–Haga clic aquí para indicar a Internet Guard Dog la acción que debe realizar con el fin de solucionar el problema. Internet Guard Dog muestra una segunda pantalla con información importante sobre el problema y recomendaciones para su resolución.
- **Deshacer arreglar**–Para identificar un problema solucionado, Internet Guard Dog pone una marca de verificación al lado del problema en la pantalla La comprobación ha detectado. Si no está satisfecho con la solución, puede volver a la configuración anterior. Seleccione el problema en la pantalla La comprobación ha detectado y haga clic en **Deshacer arreglar**.

Sugerencia

Si desea obtener más información acerca de un problema, selecciónelo en la pantalla **La comprobación ha detectado** y haga clic en **Arreglar**. Cuando aparezca la pantalla **Arreglar**, haga clic en **Ayuda** y después en **Ayuda sobre esta pantalla**.

Temas generales acerca de las funciones de seguridad de Internet Guard Dog

Una vez finalizada la Entrevista, deseará conocer cuales son los peligros que amenazan a su equipo. Comprobación examina la privacidad, la seguridad y la posible existencia de virus en el equipo, y le orienta en la resolución de los problemas encontrados. Si utiliza las opciones recomendadas por Internet Guard Dog en la Entrevista, sólo tendrá que ejecutar Comprobación después de instalar Internet Guard Dog y, en lo sucesivo, una vez al mes.

Para crear un entorno informático seguro, puede seleccionar:

- **Vigilante**– Vigilante supervisa el equipo constantemente y le alerta cuando detecta determinadas actividades potencialmente dañinas, como el envío de números de tarjetas de crédito a través de Internet o la conexión con un sitio Web dañino.

  Si desea obtener más información acerca de Vigilante, consulte el siguiente tema.

  Acerca de Vigilante

- **Guardián de archivos**–El principal objetivo de Guardián de archivos es proteger los archivos confidenciales, permitiéndole especificar qué aplicaciones tienen acceso a ellos. Guardián de archivos protegerá automáticamente sus archivos de correo electrónico para que sólo pueda utilizarlos la aplicación de correo. Asimismo, podrá agregar otros archivos a la lista Archivos protegidos, como archivos financieros, asegurándose con ello de que sólo la aplicación utilizada para crearlos tenga acceso a ellos. Otra función esencial de Guardián de archivos es controlar la actividad del equipo y alertarle de las actividades potencialmente dañinas, como cuando un programa intenta volver a dar formato al disco duro.

  Si desea obtener más información acerca de Guardián de archivos, consulte el siguiente tema.

  Acerca de Guardián de archivos

- **Administrar contraseñas**– Administrar contraseñas crea un entorno seguro para almacenar las contraseñas y los nombres de usuario que se utilizan para acceder a sitios Web. Si deja que Internet Guard Dog administre las contraseñas, no tendrá que molestarse en recordarlas ni en localizarlas. Para no tener que escribir el nombre de usuario y la contraseña cada vez que visita un sitio Web controlado por contraseña, puede arrastrar y soltar esta información desde Asistente de navegación hasta los cuadros correspondientes de la pantalla de inicio de sesión.

  Consulte los siguientes temas si desea obtener más información acerca de Administrar contraseñas y Asistente de navegación.

  - Acerca de Administrar contraseñas
  - Acerca de Asistente de navegación

Acerca de Asistente de navegación

Asistente de navegación es una forma práctica de obtener un resumen de la actividad de una cookie. Manténgalo abierto mientras navega por sitios Web para controlar las actividades de las cookies.

En el cuadro Estadísticas, puede seleccionar:

- Todos los sitios Web–muestra el número total de cookies de todos los sitios Web que visite.
- Sitio Web local–muestra el número total de cookies del sitio Web al que está conectado actualmente.

En función de la selección que realice en el cuadro Estadísticas, puede obtener la siguiente información:

- **Cookies permitidas**–Muestra el número total de cookies del sitio Web seleccionado en el cuadro Estadísticas.
- **Cookies bloqueadas**–Muestra el número total de cookies bloqueadas procedentes del sitio Web seleccionado en el cuadro Estadísticas.
- **Filtro de búsquedas**–Muestra el número total de veces que Internet Guard Dog ha impedido que la información se enviara a un sitio Web indirecto.
- **Administrar contraseñas**–Para no tener que escribir el nombre de usuario y la contraseña cada vez que visita un sitio Web controlado por contraseña, puede arrastrar y soltar esta información desde Asistente de navegación hasta los cuadros correspondientes de la pantalla de inicio de sesión.

¿Cómo se accede a Asistente de navegación?

En la barra de tareas de Windows, haga clic con el botón derecho del ratón en el icono de Internet Guard Dog  y haga clic en Asistente de navegación en el menú emergente. Haga clic en el icono Cerrar (**x**) de la esquina superior derecha del cuadro de diálogo

¿Cómo se agrega un nombre de usuario y una contraseña a Asistente de navegación?

1. En Asistente de navegación, seleccione **Agregar nueva entrada** en la lista **Sitio Web actual**.
2. En el cuadro **Sitio Web**, escriba el nombre del sitio Web tal y como desea que aparezca en la lista Administrar contraseñas.
3. En el cuadro **ID de usuario**, escriba el nombre con el cual se identifica en el sitio Web. En el sitio Web, podría ser el equivalente al ID de miembro, el Nombre de miembro, al ID de inicio de sesión, el Nombre de acceso, etc.
4. En el cuadro **Contraseña**, introduzca la contraseña que confirma su identidad. (La contraseña aparece como una serie de asteriscos (*), uno por cada carácter de la contraseña.)
5. Haga clic en **Aceptar**.

¿Cómo se accede a las contraseñas almacenadas en Asistente de navegación?

1. En Asistente de navegación, seleccione el nombre del sitio si éste no aparece automáticamente en la lista **Sitio Web actual**.
2. Arrastre el ID de inicio de sesión o la contraseña desde el cuadro Administrar contraseñas hasta el campo correspondiente del formulario de entrada del sitio Web. El texto aparecerá en el campo. (La contraseña aparece como una serie de asteriscos (*), uno por cada carácter de la contraseña.)
3. Conéctese al sitio Web como de costumbre.

Acerca del disco de emergencia

Durante la Entrevista, Internet Guard Dog le pregunta si desea crear un disco de emergencia para guardar los datos protegidos más importantes, así como un programa que le permite iniciar el PC en modo DOS. De esta forma, si se produce un desastre, el disco le permitirá restaurar la configuración de Internet Guard Dog .

Es posible que Internet Guard Dog le avise que debe actualizar los datos del disco de emergencia. Establezca la frecuencia de este aviso en Planificador.

Para obtener más información, consulte Acerca de Planificador y Respuesta a un aviso de disco de emergencia.

Sugerencia

Necesitará tres disquetes para que Internet Guard Dog pueda crear el disco de emergencia.

¿Cómo se crea un disco de emergencia?

1. Haga clic en **Opciones** en la pantalla inicial de Internet Guard Dog y después en Entrevista.
   Utilice la flecha **Siguiente** para localizar la pantalla **Disco de emergencia**.
2. Inserte un disco en la unidad de disquetes y haga clic en **Crear disco de emergencia**.
   El asistente le ayudará durante el proceso.

Acerca del menú emergente

En el caso de que desee trabajar con las funciones de Internet Guard Dog sin iniciar el programa Internet Guard Dog, encontrará algunas de las funciones más utilizadas en un menú emergente de fácil acceso. En el menú emergente puede seleccionar:

- **Ejecutar Internet Guard Dog**–Inicia el programa
- **Asistente de navegación**–Abre Asistente de navegación.
- **Configuración de protección**–Abre el cuadro de diálogo **Configuración de protección,** desde el que puede acceder a las páginas de Configuración de protección asociadas a la configuración de Internet Guard Dog.
- **Ayuda**–Inicia el sistema de Ayuda del programa Internet Guard Dog y muestra su contenido.
- **Codificar archivos de Guardián de archivos**–Codifica los archivos seleccionados para la codificación en la lista Archivos protegidos de Guardián de archivos.
- **Descodificar archivos de Guardián de archivos**–Suprime la codificación de los archivos, permitiendo así leer los datos.
- **Salir**–Cierra el programa Internet Guard Dog y lo suprime de la memoria. Si se selecciona Salir, Internet Guard Dog dejará de proteger su privacidad y la seguridad de los datos del equipo.

¿Cómo se accede al menú emergente?

Haga clic con el botón derecho del ratón en el icono de Internet Guard Dog  en la bandeja del sistema.

Acerca del menú Ayuda

Si tiene dudas acerca del modo de utilizar alguna de las funciones de Internet Guard Dog, utilice el menú Ayuda. Puede seleccionar:

- **Temas de ayuda**

  Proporcionan información o instrucciones detalladas para las tareas de Internet Guard Dog. Para buscar ayuda, utilice las fichas Contenido, Índice o Buscar. Haga clic en uno de los libros de la ficha Contenido para visualizar los temas correspondientes; a continuación, haga clic en el título de uno de los temas para que se muestre el tema de ayuda asociado al título.

  Si selecciona la ficha Buscar, podrá iniciar una búsqueda de texto completo. Cuando selecciona temas por primera vez con la ficha Buscar, aparece Find Setup Wizard. Para configurar la opción de búsqueda de texto completo, siga las instrucciones que aparecen en la pantalla. Una vez finalizada la configuración:

  1. En el cuadro de texto, escriba las primeras letras de la palabra o frase que busca. También puede seleccionar palabras coincidentes para limitar la búsqueda.
  2. Una vez ha localizado lo que buscaba en el cuadro de temas visualizados, haga clic en el tema.

  El sistema de ayuda utiliza botones de navegación estándar de Ayuda de Windows, incluyendo **Temas de ayuda,** para volver de un tema al índice, **Atrás** para volver al tema anterior, **>>** y **<<** para explorar hacia delante o hacia atrás los temas del sistema de Ayuda.

- **Ayuda sobre esta pantalla**

  Le da acceso a un tema de ayuda que contiene información específica para la pantalla que se visualiza. Pulse **ESC** para cerrar el tema.

- **McAfee en la Web**

  Esta selección abre el navegador y le da acceso al sitio Web de McAfee, donde podrá obtener las últimas novedades sobre los productos de McAfee.

- **Internet Guard Dog en la Web**

  Esta selección abre su navegador y le conecta con la página inicial de Internet Guard Dog en el sitio Web de McAfee, donde podrá obtener las últimas novedades de Internet Guard Dog.

- **Preguntas más frecuentes**

  El equipo de soporte técnico de McAfee le ayuda a sacar el máximo provecho de Internet Guard Dog; a tal efecto, ha confeccionado una lista con la respuesta a las preguntas más habituales sobre Internet Guard Dog. Esta selección abre el navegador y le da acceso a la página Preguntas más frecuentes del sitio Web de McAfee.

- **Informar de un problema**

  ¿Ha tenido algún problema con Internet Guard Dog? Esta selección abre el navegador y le da acceso a un formulario de correo electrónico en el que puede introducir sus quejas. Este mensaje se envía al Soporte técnico de McAfee.

- **Acerca de Internet Guard Dog**

  Es posible que, durante su llamada al Soporte técnico de McAfee, el técnico que le atienda le solicite la versión de Internet Guard Dog que tiene instalada. Esta selección abre el navegador y muestra una página con información sobre la versión y el Copyright.

Para indicar a Internet Guard Dog las funciones que debe utilizar, marque o quite la marca de las casillas de verificación que se encuentran a la izquierda del nombre de la función en el panel izquierdo del cuadro de diálogo. Haga clic en el nombre de la función en el panel izquierdo para visualizar sus correspondientes opciones de configuración en la página Configuración de protección del panel de la derecha.

Restaura los valores de todas las opciones de todas las funciones de protección (excepto las de Protector de identidad y Administrar contraseñas) con los valores predeterminados con los que se suministra Internet Guard Dog. Al restaurar los valores predeterminados, Internet Guard Dog no modifica el estado activado o desactivado de las funciones de protección (como Planificador o Bloqueador de cookies).

Cierre el cuadro de diálogo **Configuración de protección** sin guardar los cambios realizados en la configuración.

Guarde los cambios realizados en cualquier página Configuración de protección y cierre el cuadro de diálogo **Configuración de protección**.

Configuración de protección de Preferencias

Para controlar las funciones y acciones básicas de Internet Guard Dog, seleccione las opciones correspondientes en la página Configuración de protección de Preferencias.

Ofrece información acerca de los valores de esta página y acerca de lo que controlan.

Seleccione el modo de funcionamiento de Internet Guard Dog que desea al iniciar Windows.

Muestra la pantalla de bienvenida de CyberMedia mientras Internet Guard Dog se está cargando en la memoria del equipo.

Inicia la parte de supervisión del programa Internet Guard Dog cada vez que se inicia Windows.

Para controlar el acceso a Internet Guard Dog, asigne una contraseña que proteja el programa Internet Guard Dog. Es posible que ya lo haya hecho durante la Entrevista de Internet Guard Dog. En tal caso, puede modificar la contraseña aquí. Si no ha asignado ninguna contraseña, puede hacerlo ahora. Se recomienda asignar una contraseña a Internet Guard Dog, ya que ofrece un grado de protección adicional entre sus datos privados y confidenciales y cualquier persona que pueda utilizar el equipo.

Solicita la contraseña de Internet Guard Dog cada vez que inicie Windows.

Si no ha creado una contraseña o si desea modificar la contraseña existente, haga clic en **Cambiar contraseña**.

Crea una nueva contraseña de Internet Guard Dog o modifica la contraseña existente.

Mientras Internet Guard Dog supervisa su equipo, el programa puede avisarle de situaciones inminentes que puedan dañar los datos. Si tiene instalada una tarjeta de sonido, Internet Guard Dog emite una alerta sonora además de mostrar el cuadro de alerta estándar. Para controlar las alertas sonoras, seleccione las opciones correspondientes en el cuadro de grupo **Efectos de sonido**.

Lista los sonidos que Internet Guard Dog puede reproducir al mostrar una alerta de privacidad. Seleccione **Silencio** si desea desactivar el sonido. Haga clic en el botón  para escuchar el sonido seleccionado. (Para reproducir un sonido de Internet Guard Dog, es necesario disponer de una tarjeta de sonido y altavoces.)

Lista los sonidos que Internet Guard Dog puede reproducir al mostrar una alerta de seguridad. Seleccione **Silencio** si desea desactivar el sonido. Haga clic en el botón  para escuchar el sonido seleccionado. (Para reproducir un sonido de Internet Guard Dog, es necesario disponer de una tarjeta de sonido y altavoces.)

Lista los sonidos que Internet Guard Dog puede reproducir al mostrar una alerta de virus. Seleccione **Silencio** si desea desactivar el sonido. Haga clic en el botón  para escuchar el sonido seleccionado. (Para reproducir un sonido de Internet Guard Dog, es necesario disponer de una tarjeta de sonido y altavoces.)

Lista los sonidos que Internet Guard Dog puede reproducir al mostrar una alerta de privacidad. Seleccione **Silencio** si desea desactivar el sonido. Haga clic en el botón ▶ para escuchar el sonido seleccionado. (Para reproducir un sonido de Internet Guard Dog, es necesario disponer de una tarjeta de sonido y altavoces.)

Lista los sonidos que Internet Guard Dog puede reproducir al mostrar una alerta de seguridad. Seleccione **Silencio** si desea desactivar el sonido. Haga clic en el botón ▶ para escuchar el sonido seleccionado. (Para reproducir un sonido de Internet Guard Dog, es necesario disponer de una tarjeta de sonido y altavoces.)

Lista los sonidos que Internet Guard Dog puede reproducir al mostrar una alerta de virus. Seleccione **Silencio** si desea desactivar el sonido. Haga clic en el botón ▶ para escuchar el sonido seleccionado. (Para reproducir un sonido de Internet Guard Dog, es necesario disponer de una tarjeta de sonido y altavoces.)

Configuración de protección de Planificador

Para programar las acciones que debe ejecutar Internet Guard Dog o visualizar recordatorios, utilice las opciones que aparecen en la página Configuración de protección de Planificador. Puede programar:

- La codificación o descodificación de los archivos de Guardián de archivos.
- La eliminación de los archivos borrados.
- Recordatorios para comprobar si existen actualizaciones del programa Internet Guard Dog o de patrones de virus.

Lista los sucesos programados. El nombre del suceso aparece en la columna **Nombre**; la frecuencia, la fecha y hora de ejecución del suceso aparecen en la columna **Cuándo**. Internet Guard Dog utiliza las columnas **Siguiente ejecución** y **Última ejecución** para mostrar información acerca de los sucesos que se ejecutan más de una vez.

Suprime de la lista los sucesos programados seleccionados.

Inicia Add Scheduled Event wizard para un suceso seleccionado, lo que le permitirá modificar la configuración de dicho suceso.

Agrega un suceso a la programación mediante Add a Scheduled Event Wizard.

Configuración de protección de Bloqueador de cookies

La página Configuración de protección de Bloqueador de cookies contiene las opciones que le permitirán seleccionar si acepta o no las cookies de los sitios Web visitados. De este modo, podrá disfrutar de las ventajas que ofrecen las cookies de los sitios Web favoritos y bloquear las cookies procedentes de otros sitios.

También puede utilizar las opciones del cuadro de grupo **Sitios que establecen cookies** para controlar cómo responde Internet Guard Dog cuando un sitio Web envía una cookie al PC por primera vez.

Un sitio de acceso directo es cualquier ubicación de Internet que se visita tecleando su dirección, también conocida como dirección URL -(Uniform Resource Locator), o haciendo clic en un hipervínculo que conecta un sitio Web con otro. Normalmente, las cookies recibidas de los sitios de acceso directo son útiles . Los sitios importantes le indicarán si debe aceptar una cookie para poder visualizarlo.

Puede configurar Internet Guard Dog para realizar una de las siguientes acciones al visitar un sitio Web de acceso directo:

- **Aceptar**—Internet Guard Dog permite la entrada automática de las cookies procedentes del sitio Web de acceso directo.
- **Rechazar**—Internet Guard Dog agrega el sitio Web a la lista **Rechazado** y, a continuación, bloquea el intercambio de cookies al visitar directamente dicho sitio.
- **Solicitar**—Internet Guard Dog muestra un mensaje de alerta al visitar un sitio de acceso directo y le solicita si desea **Permitir siempre** o **No aceptar nunca las** cookies de este sitio Web.

Permite el intercambio de cookies entre su equipo y cualquier sitio Web al cual se conecte directamente. Un sitio de acceso directo es cualquier ubicación de Internet que se puede visitar tecleando su dirección, también conocida como dirección URL (Uniform Resource Locator), o haciendo clic en un hipervínculo que conecta un sitio Web con otro.

Bloquea el intercambio de cookies entre su equipo y cualquier sitio Web al cual se conecte directamente. Un sitio de acceso directo es cualquier ubicación de Internet que se puede visitar tecleando su dirección, también conocida como dirección URL(Uniform Resource Locator), o haciendo clic en un hipervínculo que conecta un sitio Web con otro.

Solicita si es necesario bloquear el intercambio de cookies cada vez que visite un sitio Web de acceso indirecto. Un sitio de acceso directo es cualquier ubicación de Internet que se puede visitar escribiendo su dirección, también conocida como dirección URL (Uniform Resource Locator), o haciendo clic en un hipervínculo que conecta un sitio Web con otro.

Un sitio Web de acceso indirecto es un sitio al que se conecta sin saberlo. Con frecuencia, al ir directamente a un sitio Web comercial, también conecta indirectamente con otros sitios Web que envían cookies para supervisar sus hábitos de conexión. Por ejemplo, un sitio al que ha accedido directamente puede contener en su página un anuncio procedente de otro sitio Web. El sitio del que procede el anuncio puede enviar una cookie para realizar un seguimiento y saber si visita otros sitios en los que figuren sus anuncios.

Configure Internet Guard Dog para que realice una de las siguientes opciones:

- **Aceptar**–Internet Guard Dog permite la entrada automática en el PC de las cookies procedentes del sitio Web de acceso indirecto.
- **Rechazar**–Internet Guard Dog agrega el sitio Web a la lista **Rechazado** y, a continuación, bloquea el intercambio de cookies entre su PC y el sitio Web con acceso indirecto.
- **Solicitar**–Internet Guard Dog muestra un mensaje de alerta al visitar un sitio de acceso indirecto y le solicita si desea **Permitir siempre** o **No aceptar nunca** cookies procedentes de ese sitio Web.

Permite el intercambio de cookies entre su equipo y cualquier sitio Web al cual se conecte indirectamente. Un sitio de acceso indirecto es cualquier ubicación de Internet al que se conecta sin teclear la dirección Web, también conocida como dirección URL (Uniform Resource Locator), o sin hacer clic en un hipervínculo que conecte con ese sitio. Normalmente, se conectará con un sitio de acceso indirecto como resultado de la conexión con un sitio de acceso directo que visualice contenido procedente de un sitio de acceso indirecto.

Bloquea el intercambio de cookies entre su equipo y cualquier sitio Web al cual se conecte indirectamente. Un sitio de acceso indirecto es cualquier ubicación de Internet al que se conecta sin teclear su dirección Web, también conocida como dirección URL (Uniform Resource Locator), o sin hacer clic en un hipervínculo que conecte con ese sitio. Normalmente, se conectará con un sitio de acceso indirecto como resultado de la conexión con un sitio de acceso directo que visualice contenido procedente de un sitio de acceso indirecto.

Solicita si hay que bloquear el intercambio de cookies cada vez que visite un sitio Web al que se ha conectado indirectamente. Un sitio de acceso indirecto es cualquier ubicación de Internet al que se conecta sin teclear su dirección Web, también conocida como dirección URL (Uniform Resource Locator), o sin hacer clic en un hipervínculo que conecte con ese sitio. Normalmente, se conectará con un sitio de acceso indirecto como resultado de la conexión con un sitio de acceso directo que visualice contenido procedente de un sitio de acceso indirecto.

Muestra los sitios Web que ha visitado y si el equipo está habilitado para intercambiar o rechazar cookies procedentes de dichos sitios.

A medida que vaya visitando nuevos sitios Web, Internet Guard Dog aceptará cookies en función de lo que haya seleccionado en el cuadro de grupo **Sitios que establecen cookies** . Si selecciona **Aceptar**, Internet Guard Dog permitirá la entrada de cookies. Si selecciona **Solicitar**, Internet Guard Dog mostrará los mensajes de alerta de Bloqueador de cookies. Si, para responder a dicho mensaje, hace clic en **Permitir siempre**, Internet Guard Dog agregará el nombre del sitio a la lista **Permitido**. Los sitios Web que aparecen en esa lista pueden intercambiar cookies con su equipo sin desencadenar una alerta de Bloqueador de cookies. Una vez que Internet Guard Dog ha agregado un sitio en la lista **Permitido**, puede moverlo a la lista **Rechazado** mediante **>>**, o eliminarlo de ambas listas con **Suprimir**.

A medida que vaya visitando sitios Web, Internet Guard Dog rechazará las cookies en función de lo que haya seleccionado en el cuadro de grupo **Sitios que establecen cookies** . Si selecciona **Rechazar**, Internet Guard Dog impedirá la entrada de cookies. Si selecciona **Solicitar**, Internet Guard Dog mostrará los mensajes de alerta de Bloqueador de cookies. Si, para responder a dicho mensaje, hace clic en **No aceptar nunca**, Internet Guard Dog agregará el nombre del sitio en la lista **Rechazado**. Esta lista muestra los sitios Web que no pueden intercambiar cookies con su equipo. Una vez incluido un sitio en la lista **Rechazado**, puede moverlo a la lista **Permitido** mediante >>,o eliminarlo de ambas listas con **Suprimir**.

Mueve los sitios Web seleccionados de la lista **Permitidos** a la lista **Rechazados**.

Elimina de ambas listas los sitios Web seleccionados. Si visita nuevamente este sitio Web, Bloqueador de cookies le solicitara si acepta o rechaza las cookies en función de las opciones seleccionadas en el cuadro de grupo **Sitios que establecen cookies**.

Mueve los sitios Web seleccionados de la lista **Rechazados** a la lista **Permitidos**.

Configuración de protección de Protector de identidad

La página Configuración de protección de Protector de identidad se utiliza para especificar la información personal y financiera que desea proteger. Si un programa intenta enviar esta información a través de Internet, Internet Guard Dog le avisará en función de lo que haya seleccionado al agregar dicha información.

Internet Guard Dog muestra la información personal especificada en le bloque Privacidad de la Entrevista o especificada directamente en Protector de identidad. De forma predeterminada, Internet Guard Dog le envía un mensaje de alerta cuando esta información está lista para ser enviada a través de Internet. Para modificar las opciones de alerta, seleccione una entrada y haga clic en **Editar**. Para agregar y borrar información desde Protector de identidad, utilice **Suprimir** y **Agregar**.

Muestra la información personal especificada en el bloque Privacidad de la Entrevista acerca de privacidad o especificada directamente en Protector de identidad. Para trabajar con esta información, utilice los botones **Suprimir**, **Editar** y **Agregar**.

Suprime de la lista la entrada seleccionada.

Inicia **Add Identity Information wizard**, que visualizará la información existente acerca de la entrada seleccionada. Modifique la información que desee y, para guardar los cambios realizados, haga clic en el botón **Finalizar** que aparece en la última página del asistente.

Inicia Add Identity Information wizard, que le indicará los pasos que debe seguir para agregar la información personal que es necesario proteger.

Internet Guard Dog muestra la información financiera especificada durante el bloque Privacidad de la Entrevista o especificada directamente en Protector de identidad. De forma predeterminada, Internet Guard Dog le envía un mensaje de alerta cuando esta información está lista para ser enviada a través de Internet. Para modificar las opciones de alerta, seleccione una entrada y haga clic en **Editar**. Para agregar y borrar información desde Protector de identidad, utilice **Agregar** y **Suprimir**.

Muestra la información financiera especificada en el bloque Privacidad de la Entrevista o agregada directamente en Protector de identidad. Para trabajar con esta información, utilice los botones **Suprimir**, **Editar** y **Agregar**.

Suprime de la lista la entrada seleccionada.

Inicia **Add Financial Information wizard**, que visualizará la información existente relativa a la entrada seleccionada. Modifique la información que desee y, para guardar los cambios realizados, haga clic en el botón **Finalizar** que aparece en la última página del asistente.

Inicia Add Financial Information wizard, que le indicará los pasos que debe seguir para agregar la información financiera que es necesario proteger.

Configuración de protección de Limpiador de rastros de Internet

La página Configuración de protección de Limpiador de rastros de Internet le permite suprimir los archivos del historial de Internet y borrar los archivos de la caché del navegador después de salir del navegador o, en función del navegador que utilice, al cerrar Windows. Internet Guard Dog le permite controlar totalmente lo que suprime Limpiador de rastros de Internet.

Seleccione **Solicitar Limpiar después de cerrar el navegador Web** si desea controlar el historial de conexiones y los archivos basura de Internet borrados. Se le solicitará que confirme el borrado de los archivos:

- Cada vez que cierre el navegador Netscape o Internet Explorer.
- Cuando apague Windows, si utiliza Internet Explorer y existe algún archivo de conexiones.
- Cuando apague Windows, si utiliza Active Desktop de Microsoft.

Seleccione **Limpiar automáticamente después de cerrar el navegador Web** si desea que Limpiador de rastros de Internet borre el historial de conexiones y los archivos basura de Internet. Limpiador de rastros de Internet borrará estos archivos:

- Cada vez que cierre el navegador Netscape o Internet Explorer.
- Cuando apague Windows, si utiliza Internet Explorer y existe algún archivo de conexiones.
- Cuando apague Windows, si utiliza Microsoft Active Desktop.

Seleccione **Conservar elementos favoritos** para que Limpiador de rastros de Internet no borre los archivos relativos a los sitios marcados como favoritos (o seleccionados en Favoritos).

Marque la casilla de verificación **Conservar elementos favoritos** para que, después de cerrar el navegador, Limpiador de rastros de Internet no borre los archivos relativos a los sitios marcados como favoritos (o seleccionados como Favoritos). Los elementos marcados como favoritos sirven para agilizar la conexión a los sitios Web importantes o visitados con más frecuencia sin tener que escribir la dirección URL. Esta opción estará disponible sólo si ha marcado **Limpiar automáticamente después de cerrar el navegador Web**.

Configuración de protección de Filtro de búsquedas

Impide que la información de búsqueda pase de un sitio Web al siguiente sitio Web visitado. Para que funcione el botón Anterior del navegador, la información del sitio Web visitado pasa a formar parte de la información de referencia del sitio que visita a continuación. Parte de esa información de referencia puede contener la información de búsqueda del sitio anterior. Cuando se activa **Filtro de búsquedas**, Internet Guard Dog filtra todos los datos de búsqueda antes de que se incorporen a la información de referencia.

Configuración de protección de Vigilante

Con la página Configuración de protección de Vigilante puede especificar que Vigilante le avise cuando se produzcan determinadas actividades potencialmente dañinas para que pueda decidir cómo proceder al respecto. Vigilante controla el equipo y lo que en él ocurre al utilizar Internet.

Las entradas de este cuadro representan las acciones que los programas de Internet pueden ejecutar y que podrían tener consecuencias nefastas. En función de cómo utilice Internet, decida las acciones sobre las cuales desea que Vigilante le avise y marque la casilla de verificación correspondiente.

Le avisa cuando se inicia la conexión con un sitio que puede contener controles ActiveX dañinos, programas Java, virus o caballos de Troya.

Le avisa cuando el módem marca en modo silencioso, Algunos programas pueden reunir información confidencial de su equipo y utilizar el módem para enviarla a otro lugar.

Le avisa cuando un programa inicia otro programa sin su autorización. Por ejemplo, un programa hostil podría intentar iniciar el navegador Web.

Le avisa cuando un programa envía a través de Internet un número parecido al de una tarjeta de crédito. Algunos programas hostiles han sido diseñados para buscar números de tarjeta de crédito y enviarlos a otro sitio.

Lista los programas con autorización para acceder a Internet sin mostrar un mensaje de alerta. Inicialmente, Internet Guard Dog verifica la autorización cada vez que un programa, como el navegador, accede a Internet. Si responde al mensaje de alerta con **Permitir siempre**, Internet Guard Dog agrega el programa a la lista y no vuelve a enviar nuevos avisos sobre ese programa. Revise estos programas periódicamente y decida si conservarlos en la lista o suprimirlos.

Suprime de la lista el programa seleccionado. La próxima vez que el programa intente acceder a Internet, Internet Guard Dog mostrará un mensaje de alerta para solicitarle su permiso.

Configuración de protección de Guardián de archivos

En la página Configuración de protección de Guardián de archivos, puede especificar los programas que tienen acceso a los archivos importantes o confidenciales con el fin de protegerlos. Por ejemplo, puede proteger sus archivos de correo electrónico para que únicamente pueda utilizarlos el programa de correo . Además, puede configurar Guardián de archivos para que le avise cuando otro programa, como un control ActiveX, lleve a cabo acciones que puedan ser dañinas para los datos de sus archivos.

Las entradas que aparecen en este cuadro representan las acciones con consecuencias potencialmente nefastas para los datos del equipo. En función de sus necesidades de seguridad y de su forma de utilizar Internet, decida qué acciones merecen un aviso de Guardián de archivos y marque la casilla de verificación correspondiente.

Le avisa cuando un control ActiveX explora los archivos del sistema. Les controles ActiveX pueden ejecutar exploraciones inofensivas, como cuando necesita comprobar mediante un control ActiveX los archivos existentes en el PC para actualizar los archivos de un sitio Web. No obstante, un control ActiveX puede haber sido creado para amenazar su seguridad; por ejemplo, puede buscar archivos que contengan información financiera privada para enviarla a otra ubicación. Marque esta casilla de verificación para recibir un mensaje de alerta.

Le avisa cuando un programa empieza a dar formato a cualquier unidad de disco duro, incluidas las unidades Jaz y Zip. Dar formato de nuevo a la unidad de disco duro del equipo sin su conocimiento puede tener consecuencias catastróficas. No sólo puede perder datos valiosos, sino que también podría perder una gran cantidad de tiempo tratando de restituir el anterior estado de funcionamiento del equipo. Marque esta casilla de verificación para recibir un mensaje de alerta.

Le avisa cuando un control ActiveX elimina un archivo del sistema. Los controles ActiveX pueden tener motivos legítimos para borrar archivos; por ejemplo, pueden borrar los archivos temporales creados al descargar archivos desde un sitio Web con controles ActiveX. No obstante, un control ActiveX también puede estar diseñado para eliminar archivos importantes. Marque esta casilla de verificación para recibir un mensaje de alerta.

Le avisa cuando un programa trata de acceder a un archivo de contraseña de Windows (archivo .pwl). Las contraseñas desempeñan una importante función de protección, ya que controlan qué personas acceden a los recursos compartidos que dispone en su PC. Marque esta casilla de verificación para recibir un mensaje de alerta.

Muestra la lista de archivos que supervisa Guardián de archivos y los programas que tienen acceso a éstos. Puede agregar o suprimir archivos o programas en estas listas.

Muestra la lista de archivos seleccionados para que los supervise Guardián de archivos. Los archivos se visualizan según el método por el cual se han seleccionado: por el nombre de archivo, carpeta o unidad en los que están almacenados, por el grupo de archivo o por el tipo de archivo. Si marca la casilla de verificación **Incluir para codificación de archivos** del cuadro de diálogo **Add Guarded File Wizard**, aparecerá junto al archivo el icono de una cerradura. Para codificar (o descodificar) el archivo, haga clic en el icono de Internet Guard Dog ▶ que se encuentra en la bandeja del sistema y seleccione **Codificar archivos de Guardián de archivos** (o **Descodificar archivos de Guardián de archivos**) en el menú emergente.

Muestra la lista de programas que tienen autorización para acceder al archivo seleccionado. Guardián de archivos muestra un mensaje de alerta y le solicita que confirme su autorización la primera vez que el programa accede a uno de los archivos de la lista de archivos protegidos. Si responde al mensaje de alerta con **Permitir siempre**, Guardián de archivos agrega el programa a la lista **Programas con acceso a este archivo**.

Suprime el archivo o programa seleccionado de las listas **Archivos protegidos** o **Programas con acceso a este archivo**

Inicia Add Guarded File Wizard, que le guiará paso a paso para agregar archivos a la lista **Archivos protegidos** o para especificar los programas que tendrán acceso a los archivos de la lista. Antes de hacer clic en el botón **Agregar** para que un programa pueda acceder a un archivo, debe seleccionar el archivo que desea proteger.

Configuración de protección de Administrar contraseñas

En la página Configuración de protección de Administrar contraseñas puede almacenar de modo seguro las contraseñas de los sitios Web. Algunos sitios Web controlan el acceso solicitándole que especifique un nombre de usuario y una contraseña cada vez que lo visita. Al visitar un sitio protegido por contraseña, abra Asistente de navegación y arrastre y suelte la información de inicio de sesión de Administrar contraseñas en el formulario de conexión del sitio Web.

Muestra la lista de registros almacenados por Administrar contraseñas. Cada registro contiene el nombre del sitio Web y el nombre de usuario y la contraseña utilizados para conectarse al sitio.

Elimina el registro seleccionado de la lista de Administrar contraseñas.

Abre el cuadro de diálogo Introduzca la contraseña para guardar y muestra la información correspondiente al registro seleccionado.

Abre el cuadro de diálogo **Introduzca la contraseña para guardar,** donde podrá almacenar el nombre del sitio Web y el nombre de usuario y la contraseña correspondientes a dicho sitio.

Configuración de protección de Centinela de virus

En la página Configuración de protección de Centinela de virus puede especificar cómo desea que Internet Guard Dog proteja su sistema de la infección de virus. En esta página, puede especificar las opciones necesarias para activar la detección de virus mientras trabaja mediante **Cuándo realizar la comprobación;** asimismo, puede especificar los tipos de archivos que es necesario explorar (en la función Comprobación) mediante **¿Qué desea comprobar?**.

Utilice las opciones de comprobación de este cuadro para controlar las acciones que Centinela de virus debe supervisar mientras trabaja en su PC.

Utilice esta opción para detectar mientras trabaja si existe algún virus en un programa que está iniciando.

Utilice esta opción que explorará mientras trabaja todos los archivos adjuntos de correo electrónico que abre en busca de algún virus.

Utilice esta opción que explorará mientras trabaja los archivos que abre en busca de algún virus.

Utilice esta opción de trabajo que explorará mientras trabaja todos los archivos al moverlos o cambiarles el nombre en busca de algún virus.

Utilice esta opción que explorará mientras trabaja todos los disquetes que abre.

Explora el sistema DOS en busca de virus y los identifica antes de cargar Windows. El sistema operativo Windows todavía depende de las funciones de un antiguo sistema operativo llamado DOS. Algunos virus, como los virus del sector de arranque, los virus de las tablas de partición y los virus de memoria, pueden infectar los archivos antes de cargar Windows. Aunque estos tipos de virus podrían detectarse en Windows, la mayoría deben eliminarse desde DOS. Por este motivo, debería marcar esta opción si desea contar con una protección antivirus más completa.

Determina la respuesta de Internet Guard Dog cuando detecta un virus en los tipos de programa o archivos especificados en ¿Qué desea comprobar?.

Puede controlar la acción de Centinela de virus cuando éste detecta un virus en los tipos de programa o archivos especificados en **¿Qué desea comprobar?**. Seleccione la opción de Centinela de virus que le interese:

- **Solicitar**–Podrá decidir qué hacer caso por caso.
- **Denegar el acceso**–No podrá realizar ninguna acción en el archivo, excepto eliminarlo con el explorador de Windows o limpiarlo con la función Comprobación. (Cuando se abre un archivo infectado, el virus se extiende.)
- **Eliminación automática**–Elimina el archivo de su disco duro.
- **Limpieza automática**–Suprime el virus del archivo infectado, y si no puede, Internet Guard Dog le solicita que elimine el archivo.
- **Desconexión del equipo**–Apaga el sistema Windows sin llevar cabo ninguna acción adicional.

Determina los tipos de archivos que explora Internet Guard Dog durante la función Comprobación.

Determina los tipos de archivos que explora Internet Guard Dog durante la función Comprobación. Puede indicar a Internet Guard Dog que explore:

- **Todos los archivos**–Comprueba todos los archivos del equipo. Ésta es la comprobación más completa, y también la que tarda más tiempo en realizarse si cuenta con muchos archivos en el equipo. Con este tipo de comprobación puede detectar virus en archivos que utilizan tipos de archivos no estándar.
- **Archivos de programa**–Comprueba todos los archivos que un programa necesita para funcionar correctamente. Se comprueban los archivos con las extensiones de programa más comunes,
como .com, .exe, .bat, .bin, .ovl, .drv, .dll, .sys, .tsk, .vxd y .ocx. Esta opción no detecta virus de macros.
- **Archivos de documento**–Únicamente comprueba los archivos de datos que pueden contener virus, que normalmente son virus de macros. Por ejemplo, se comprueban los archivos de documento de Microsoft Word y Excel y los documentos comprimidos con extensiones .zip, .arc y .lzh. Esta opción no detecta los virus de programas.
- **Archivos de programa y documento**–Comprueba los archivos de programa y los archivos de documento. Esta opción tiene la ventaja de que detecta la mayoría de los virus y tarda menos tiempo que la comprobación de todos los archivos.

Sugerencia

Utilice **Editar** para agregar, suprimir o personalizar los tipos de archivos que desea comprobar durante la función Comprobación.

Personaliza los tipos de archivos de documento o archivos de programa que comprueba Internet Guard Dog durante la función Comprobación. En la ficha **Archivos de programa** o en la ficha **Archivos de documento**, utilice los botones **Agregar** y **Suprimir** para especificar los tipos de archivo de programa y de documento en los que deben detectarse virus.

Para especificar los tipos de archivos que Internet Guard Dog debe comprobar durante la función Comprobación, agréguelos a la ficha **Archivos de programa** o **Archivos de documento**.

Muestra la lista de archivos de programa que comprueba Centinela de virus durante la función Comprobación.

Muestra la lista de archivos de documento que comprueba Centinela de virus durante la función Comprobación.

Agrega los tipos de archivo seleccionados a la lista **Archivos de programa** o **Archivos de documento**.

Suprime los tipos de archivos seleccionados de la lista **Archivos de programa** o **Archivos de documento**.

Controla los archivos y carpetas no comprobados por Centinela de virus durante la exploración de virus, excepto para las opciones que se activan mientras trabaja incluidas en el cuadro **Cuándo realizar la comprobación** de Centinela de virus.

Muestra los archivos y carpetas no comprobados por Centinela de virus durante la exploración de virus, excepto para las opciones que se activan mientras trabaja del cuadro **Cuándo realizar la comprobación** de Centinela de virus.

Utilice el botón **Agregar archivos** para incluir archivos en la lista **No comprobar…** .

Utilice el botón **Agregar carpetas** para incluir carpetas en la lista **No comprobar…** .

Utilice el botón **Suprimir** para eliminar los archivos o carpetas seleccionados de la lista **No comprobar…** .

Sugerencia

Utilice MAYÚS+CLIC para realizar varias selecciones en la lista.

Explora DOS en busca de virus y los identifica antes de cargar Windows. El sistema operativo Windows todavía depende de las funciones de un antiguo sistema operativo llamado DOS. Algunos virus, como los virus del sector de arranque, los virus de las tablas de partición y los virus de memoria, pueden infectar los archivos antes de cargar Windows. Aunque estos tipos de virus podrían detectarse en Windows, la mayoría deben eliminarse desde DOS. Por este motivo, debería marcar esta opción si desea contar con una protección antivirus más completa.

Entrevista – **¡Bienvenido a Internet Guard Dog!**

Internet Guard Dog necesita algunos datos personales para proteger su privacidad mientras utiliza el PC. Después de introducir datos personales en las pantallas que aparecen a continuación, podrá estar seguro de que esta información se almacenará en un archivo codificado del disco duro. Internet Guard Dog no divulgará ninguna información personal a terceros y garantiza que la información almacenada no podrá ser utilizada por ningún otro programa.

Utilice los botones **Siguiente** y **Anterior** para navegar por la Entrevista. Si más adelante desea modificar o agregar algunos datos, haga clic en **Opciones** en la pantalla inicial de Internet Guard Dog y seleccione **Entrevista** en el menú desplegable.

Entrevista – **Privacidad**

Internet Guard Dog proporciona una gran variedad de funciones de protección diseñadas para proteger su privacidad, especialmente mientras navega por Internet. Las opciones de las siguientes pantallas están diseñadas para alertarle cuando se produce alguna situación que puede poner en peligro su privacidad.

Entrevista – **Información personal en Protector de identidad**

Internet Guard Dog controla la información introducida en esta pantalla y le alerta cuando alguna persona o algún programa intenta enviar a través de Internet alguno de estos datos. Cuando se ejecuta Comprobación de Internet Guard Dog, se utiliza también la información de Protector de identidad para identificar si existen archivos que contengan esta información; además, es posible proteger dichos archivos con Guardián de archivos.

Utilice la tecla tabulador para desplazarse de un cuadro de diálogo al siguiente y haga clic en **Siguiente** para pasar a la siguiente pantalla de la Entrevista.

Consulte el siguiente tema si desea agregar, suprimir o modificar algún dato una vez finalizada la Entrevista.

Acerca de Protector de identidad

Entrevista – **Información financiera en Protector de identidad**

Si guarda información financiera en el equipo (por ejemplo, si utiliza un programa de contabilidad para administrar su talonario y pagar sus facturas electrónicamente) Internet Guard Dog puede protegerla de los programas que intenten recuperarla y enviarla a otro equipo.

Haga clic en un cuadro, coloque el cursor encima y empiece a escribir.

Para obtener información adicional sobre cómo agregar, suprimir o cambiar los datos después de finalizar la entrevista, consulte Acerca de Protector de identidad.

Entrevista – **Contraseña de Internet Guard Dog**

Guard Dog también supervisa la seguridad interna del sistema. Le recomendamos que asigne una contraseña al programa Guard Dog para que sólo usted pueda acceder a **Configuración de protección**.

Si comparte su PC con otras personas, puede utilizar la contraseña para proteger su información personal y financiera. Si no introduce la contraseña de Guard Dog tras el inicio de Windows, Guard Dog bloquea toda la información protegida por Protector de identidad para que no pueda enviarse a través de Internet.

Si no selecciona ninguna contraseña durante la Entrevista, podrá hacerlo más adelante volviendo a ejecutar la Entrevista o modificando directamente la configuración en la página **Preferencias**.

Consulte los siguientes temas si desea obtener más información acerca de cómo reiniciar la Entrevista para modificar la configuración o cambiar la contraseña directamente en las páginas de Configuración de protección de Preferencias.

- Respuesta a las preguntas de la Entrevista
- Acerca de Preferencias de Internet Guard Dog

Entrevista – Antivirus

Con suerte, los virus limitarse a provocar ciertas molestias, pero también pueden destruir datos importantes. Olvídese de esos problemas activando la detección de virus de Guard Dog. Después de la Entrevista, puede determinar exactamente qué tipos de archivos debe comprobar el programa antivirus.

Seleccione las siguientes casillas de verificación para activar la detección de virus:

- **Siempre que se inicie Windows**–Guard Dog comprueba automáticamente los archivos de alto riesgo (archivos de documento y archivos de programa) cuando se inicia Windows.
- **Automáticamente, siempre que se registren actividades de archivo o de descarga**–Guard Dog detecta los posibles virus al:

  Ejecutar un programa

  Acceder a archivos de correo electrónico

  Abrir un archivo

  Mover o renombrar

  Leer un disquete

Consulte los siguientes temas si desea obtener más información acerca de cómo configurar la protección antivirus.

Cómo sacar más provecho de Protección Antivirus

Acerca de Centinela de virus

Entrevista – **Disco de emergencia**

Un disco de emergencia es una copia de seguridad válida a la que es posible recurrir cuando surge algún problema con los datos protegidos por Internet Guard Dog. Este disco contiene una copia de esta información, además de un programa que le permite iniciar el PC en modo DOS. Si no crea ningún disco de emergencia en este momento, puede hacer que Internet Guard Dog le avise para hacerlo más adelante.

Consulte el siguiente tema si desea obtener más información acerca de cómo configurar programaciones y acerca de los tipos de sucesos que pueden programarse.

Acerca de Planificador

Entrevista – **Resumen**

Puede verificar la información introducida en Internet Guard Dog con facilidad. Si necesita realizar modificaciones, haga clic en la flecha **Atrás** hasta que llegue a la pantalla correcta.

Entrevista - ¡Ya ha terminado!

¡Felicidades! Ha proporcionado a Internet Guard Dog la información necesaria para proteger su privacidad y sus datos confidenciales. Cuando haga clic en **Finalizar,** Internet Guard Dog grabará esta información (llamada configuración) en la unidad de disco duro y reiniciará el PC.

Como indicación de que Internet Guard Dog está trabajando, aparecerá un icono en la barra de tareas situada en la parte inferior de la pantalla. Haga clic con el botón derecho del ratón para que aparezca un menú emergente y seleccione **Salir** para borrar Internet Guard Dog de la memoria.

Recuerde que, si lo hace, Internet Guard Dog dejará de supervisar el PC y de proteger sus datos contra intrusiones no permitidas. Para volver a iniciar Internet Guard Dog, haga doble clic en el icono del escritorio.

Para obtener información acerca de las selecciones del menú emergente, consulte Acerca del menú emergente

Acerca de la privacidad

Cada día son más las personas que visitan la World Wide Web sólo para echar un vistazo (o, utilizando un término popular, para "navegar"), compartir información , descargar datos y realizar compras. Los proveedores de servicios de Internet ofrecen servicios de correo electrónico que hacen que comunicarse con otras personas de todo el mundo sea tan fácil como escribir un mensaje y pulsar un botón para enviarlo a su destino. Evidentemente, este avance en las comunicaciones conlleva importantes ventajas, ya que Internet posee una capacidad de crecimiento casi infinita . Sin embargo, estas ventajas acarrean también algunos inconvenientes.

Los avances en las comunicaciones y en la transmisión de datos permiten la captura, almacenamiento y reutilización a través de Internet gran cantidad de información personal. Cada vez que se conecta a la Word Wide Web, transmite información. Esto ocurre con frecuencia mientras navega. Por ejemplo, si realiza una búsqueda utilizando algunos de los motores de búsqueda disponibles en Internet, sus peticiones de búsqueda no sólo se transmiten al motor de búsqueda, sino también a otros sitios, incluidos los sitios que proporcionan los mensajes publicitarios que aparecen en muchos sitios Web. Por otra parte, a medida que navega de un sitio a otro también transfiere información.

Esta información entre sitios se registra y se correlaciona con cookies, permitiendo a determinados sitios Web construir bases de datos acerca de usted y de sus intereses. Filtro de búsquedas de Internet Guard Dog bloquea el paso de esta información.

La necesidad de poseer un cierto nivel de privacidad es esencial para controlar nuestras vidas y nuestra intimidad. Aunque parece existir una aceptación general de este principio, la forma de proteger la privacidad en la World Wide Web sólo está empezando a explorarse. McAfee ofrece Internet Guard Dog como una solución exhaustiva para los problemas relacionados con la privacidad y la seguridad que plantea el mundo de Internet.

Lea más acerca de la seguridad

Política de privacidad de McAfee

Nuestro compromiso con la protección de la seguridad y la privacidad de los usuarios nos permite garantizarle que McAfee no recopila ningún tipo de información fines propios. Asimismo, le aseguramos que tampoco recopila información personal, como su nombre o su dirección, venderla o distribuirla a otras empresas que pueda utilizarla para crear listas de mailing o promociones publicitarias.

Estos criterios se aplican también a Internet Guard Dog. Protector de identidad se ha diseñado con la intención de controlar quién recibe su información personal. Ello significa que Internet Guard Dog no comunicará a terceros ninguno de los datos personales o financieros que haya introducido en Protector de identidad a sin su permiso expreso.

Acerca de la seguridad

Con el interés creciente que ha suscitado Internet y la ampliación de las transacciones comerciales en la World Wide Web, la seguridad está convirtiéndose en un tema importante. Estas transacciones deben estar protegidas tanto desde el punto de vista del comprador como el vendedor. Los problemas de llevar a cabo operaciones empresariales por Internet son de fácil definición. Aunque es relativamente fácil configurar un sitio Web para mostrar y vender cosas, no lo es tanto desarrollar mecanismos que garanticen la seguridad de la información que debe transmitirse en ambos sentidos para llevar a cabo cualquier tipo de transacción. Además, existen personas (los denominados 'hackers') que disponen de medios para controlar las transacciones y extraer datos tan importantes como los números de las tarjetas de crédito o de las cuentas bancarias.

Sin embargo, no hay que darlo todo por perdido. El software de navegador de Microsoft Internet Explorer y Netscape ha incorporado una tecnología de codificación denominada Secure Sockets Layer (SSL). Cuando la utiliza, aparece un icono en el navegador para indicar que la tecnología SSL está activa, . dándole la certeza casi absoluta de que su transacción es segura.

Aunque los métodos de codificación suponen un gran avance subsisten, no obstante, algunos problemas. En primer lugar, no todos los servidores y navegadores admiten la tecnología SSL. El software SSL incrementa el coste de inversión en servidores y puede disminuir la velocidad de las transacciones. En segundo lugar, Microsoft y Netscape no han realizado un esfuerzo de coordinación en materia de seguridad con lo cual, cada una de estas empresas posee su propio navegador y, aunque ninguno es perfecto, cada uno tiene sus propias carencias de seguridad. Por ello, puede resultar bastante difícil evaluar los fallos de seguridad de cada navegador, e incluso puede verse obligado a echar a suertes la elección del navegador. Sin embargo, las empresas son conscientes de los riesgos y los peligros que supone la introducción de medidas de seguridad y están trabajando para corregir sus problemas.

Las transacciones seguras son sólo una parte del problema. Cuando los servidores Web reciben información, deben ser capaces de mantenerla a salvo. En una red de grandes dimensiones, en la que un servidor Web es sólo uno de los múltiples tipos de servidores, el administrador de redes intenta aislar los servidores Web de otros servidores importantes de la empresa. Sin embargo, algunos programas Web interactuan con datos almacenados en otros servidores, con lo cual dejan un resquicio para acceder a datos potencialmente confidenciales. Los "hackers" eligen a los servidores Web como blanco, porque la tecnología para garantizar su seguridad está todavía en fase de desarrollo. Existe una tecnología de seguridad denominada “cortafuegos” que permite controlar el acceso no autorizado a los datos confidenciales, pero requiere un mantenimiento correcto, por lo que, incluso en los sistemas con un mantenimiento óptimo, los cortafuegos no son suficientes para proteger determinados servicios.

Los usuarios disponen de dos formas de determinar si es posible transmitir información a un sitio Web de forma segura.

En primer lugar, la mayoría de sitios Web comerciales poseen servidores seguros y le notifican que está utilizando una conexión segura. Si el sitio no es seguro, recibirá una advertencia y tendrá la posibilidad de continuar o no. En segundo lugar, la mayoría de navegadores son suficientemente inteligentes para detectar el nivel de seguridad del sitio al que están conectados y, además, son capaces de mostrar esa información.

Siempre es una decisión acertada utilizar todas las medidas de seguridad disponibles, ya que existen personas poco honestas que aprovecharán cualquier descuido. Microsoft y Netscape están desarrollando una importante labor para desarrollar soluciones avanzadas y solucionar los fallos de seguridad de los productos Internet existentes. Para beneficiarse de sus últimas innovaciones, actualice el software de navegador ejecutando Internet Guard Dog con frecuencia.

Acerca de los virus

Cada vez que utiliza el correo electrónico o navega por sitios Web corre el riesgo de infectar los datos del PC con un virus.

Los virus son programas diseñados para afectar el sistema una vez incorporados en un programa en buen estado. Mientras utiliza el programa, el virus se va copiando en otros programas, con lo cual infecta su PC del mismo modo que un virus infecta el cuerpo. La mayoría de los programas de virus se limitan a provocar una serie de molestias, ocupando espacio de disco y haciendo que los programas se comporten de forma extraña. Sin embargo, algunos programas de virus, por ejemplo los virus del sector de arranque y los de las tablas de partición, pueden atacar y dañar gravemente los archivos necesarios para iniciar y cargar el sistema operativo.

McAfee trabaja constantemente para identificar virus y coloca la información acerca de los virus conocidos y sus curas en un archivo de patrón de virus. A medida que se van identificando nuevos virus, se actualiza el archivo de patrón.

Para proteger esos datos es preciso utilizar un buen programa de detección de virus, como el que puede encontrar en Internet Guard Dog. Puede ayudar a Internet Guard Dog a detectar y a limpiar los virus con eficacia utilizando este programa para recuperar la última versión del archivo de patrón de virus.

Entrevista - Bloqueador de cookies

Normalmente, las cookies aumentan la eficacia de los sitios Web utilizando la información obtenida y almacenada en su sistema. Por ejemplo, las cookies permiten que su sitio comercial favorito le muestre información personalizada cada vez que lo visita. Un sitio Web protegido por contraseña puede utilizar una cookie para almacenar la información de contraseña, de modo que no tenga que introducirla cada vez que lo visita. Asimismo, algunos sitios requieren cookies para funcionar correctamente. Normalmente, estos sitios le avisan que debe aceptarlas.

Las cookies también pueden representar una amenaza para su seguridad, ya que no puede controlar el seguimiento que realizan ni quién recopila información sobre usted. Bloqueador de cookies le permite controlar quién puede enviar cookies a su PC. De este modo, podrá disfrutar de las ventajas que ofrecen las cookies de sus sitios Web favoritos y bloquear las cookies procedentes de otros sitios.

1. **Cookies de los sitios Web que visito** son las cookies que provienen de sitios Web que visita directamente escribiendo la dirección Web en su navegador o haciendo clic en un vínculo de una página Web. Seleccione una de las siguientes acciones:

    - **Permitir siempre** para aceptar automáticamente las cookies de sitios a los que se conecta directamente.
    - **Rechazar siempre** para rechazar automáticamente las cookies de sitios a los que se conecta directamente.
    - **Solicitar cada vez** para seleccionar si desea aceptar o rechazar una cookie de un sitio de acceso directo según cada caso. Mientras navega por la Web, Internet Guard Dog le pregunta cada vez que un sitio de acceso directo intenta enviar una cookie a su PC y, después, agrega el sitio a la lista Aceptado o Rechazado en la página Bloqueador de cookies de Configuración de protección.

2. **Cookies de otros sitios Web** son las cookies que provienen de sitios Web a los que se conecta indirectamente, sin escribir la dirección Web en su navegador ni hacer clic en ningún vínculo de una página Web. Normalmente se conecta a estos sitios porque su contenido forma parte de una página Web visitada. Seleccione una de las siguientes acciones:

    - **Permitir siempre** para aceptar automáticamente las cookies de sitios con los que se conecta indirectamente.
    - **Rechazar siempre** para rechazar automáticamente las cookies de sitios con los que conecta indirectamente.
    - **Solicitar cada vez** para seleccionar si desea aceptar o rechazar una cookie de un sitio de acceso indirecto según cada caso. Mientras navega por la Web, Internet Guard Dog le pregunta cada vez que un sitio de acceso indirecto intenta enviar una cookie a su PC y, después, agrega el sitio a la lista Aceptado o Rechazado en la página Bloqueador de cookies de Configuración de protección.

Consulte el siguiente tema en Acerca de Bloqueador de cookies para obtener más información acerca de cómo cambiar la configuración de Bloqueador de cookies después de realizar la Entrevista.

Entrevista – **Limpiador de rastros de Internet**

Mientras navega por Internet, su navegador va almacenando archivos que agilizan la visualización y el regreso a las páginas ya visitadas. Sin embargo, otros usuarios también pueden ver estos archivos, ya sea directamente o a través de Internet, cuando abren el navegador de Web

Limpiador de rastros de Internet protege la privacidad y la seguridad suprimiendo esos archivos del historial de Internet y de la caché del navegador. Una ventaja adicional de suprimir los archivos de Internet acumulados en el disco duro es que libera espacio de disco. Puede seleccionar una de las siguientes opciones:

- **Eliminación automática** elimina los archivos cuando cierra el navegador o, dependiendo del navegador utilizado, al salir de Windows.
- **Solicitar eliminación** le solicita que seleccione los sitios de los que desea eliminar la información de los rastros del navegador.
- **Ninguna** desactiva Limpiador de rastros de Internet.

Para obtener más información acerca de cómo cambiar la configuración de Limpiador de rastros de Internet después de realizar la entrevista, consulte Acerca de Limpiador de rastros de Internet.

Entrevista - Seguridad

Internet Guard Dog ofrece varias funciones de seguridad diseñadas para proteger los datos del PC contra los daños provocados por terceros. Siempre es una decisión acertada utilizar todas las medidas de seguridad disponibles, ya que el mundo está lleno de personas poco honestas que aprovecharán cualquier descuido.

Entrevista – **Filtro de búsquedas**

Mientras navega por Internet, la información acerca de lo que busca en un sitio Web determinado puede transferirse al siguiente sitio con el que se conecte. Por ejemplo, imagine que realiza una búsqueda de "McAfee" mediante un motor de búsqueda disponible en el sitio de su proveedor de servicios de Internet (ISP). Tras hacer clic en Buscar, la dirección que aparecerá en el navegador es
http://www-isp.net/cgi-bin/query?pg=q&dp=val&who=isp&what=web&kl=XX&q=McAfee&search.x=38&search.y=10
El próximo sitio que visite podrá consultar esta información para descubrir su origen y las búsquedas que realizó. Filtro de búsquedas suprimirá toda la información acerca de la dirección del sitio Web antes de conectarse al siguiente sitio. Puede seleccionar una de las siguientes opciones:

- **Sí, activar Filtro de búsquedas** —Activa Filtro de búsquedas en Configuración de protección.
- **No, desactivar Filtro de búsquedas** —Desactiva Filtro de búsquedas en Configuración de protección.

Consulte Acerca de Filtro de búsquedas para obtener más información acerca de cómo activar y desactivar Filtro de búsquedas tras completar la Entrevista.

Entrevista – **Vigilante**

Vigilante controla su PC y todo lo que sucede mientras utiliza Internet. Asimismo, Vigilante actúa como una red de seguridad, alertándole cuando está a punto de conectarse a sitios Web con contenidos dañinos, como controles ActiveX o subprogramas Java. Por otra parte, los programas instalados en su PC pueden provenir de diversas fuentes, algunas de las cuales podrían no ser del todo fiables. En realidad no se puede saber qué va a hacer un programa hasta que se instala y se utiliza. Algunos programas aparentemente inocentes pueden haber sido diseñados para buscar cierta información en el PC y transmitirla a otro equipo a través de Internet.

Puede seleccionar una de las siguientes opciones de Vigilante en esta pantalla de la Entrevista para que le alerte cuando se produzcan actividades potencialmente dañinas, de forma que pueda decidir cómo proceder.

- **Cuando un programa no autorizado intente acceder a Internet**—Le alerta cuando un programa intenta acceder a Internet.
- **Cuando visite sitios Web que puedan contener controles ActiveX y virus hostiles**— Le alerta cuando inicia la conexión con un sitio que puede contener controles ActiveX, virus o caballos de Troya dañinos.
- **Si el módem marca silenciosamente**— Le alerta cuando su módem marca en modo silencioso. Algunos programas pueden recopilar información confidencial del PC y utilizar su módem para enviarla a otra persona.
- **Si se envía un número de tarjeta de crédito por Internet**—Le alerta cuando un programa envía a través de Internet un número parecido al de una tarjeta de crédito. Algunos programas hostiles han sido diseñados para buscar números de tarjeta de crédito y enviarlos a otro sitio.

Consulte Acerca de Vigilante si desea obtener más información acerca de cómo cambiar la configuración de Vigilante después de realizar la entrevista.

Entrevista – **Guardián de archivos**

Guardián de archivos protege los archivos confidenciales o fundamentales del sistema. Además, Guardián de archivos puede proteger automáticamente sus archivos, de modo que sólo puedan utilizarlos los programas incluidos en la lista de Archivos protegidos. Para aumentar la protección, también puede codificar los archivos protegidos por Guardián de archivos. Los archivos codificados no pueden utilizarse hasta que se descodifican. Puede proteger los siguientes tipos de archivos:

Archivos de contraseña

Internet Guard Dog le alerta cuando un programa empieza a acceder a un archivo de contraseña basado en Windows (archivos .pwl). Las contraseñas desempeñan una función importante, ya que controlan quién tiene acceso a los recursos compartidos del PC. Internet Guard Dog supervisará el acceso si selecciona esta casilla de verificación.

Archivos de correo electrónico

Guardián de archivos le permite proteger rápidamente los archivos confidenciales asociados a la mayoría de programas de correo electrónico agregándolos como un grupo a la lista Archivos protegidos.

El grupo Archivos de correo electrónico incluye archivos de:

- Correo electrónico de Internet Explorer 4
- Correo electrónico de Internet Explorer 3
- Correo electrónico de Outlook Express de Internet Explorer 4
- Correo electrónico de Netscape
- Correo electrónico de Communicator
- Correo electrónico de Eudora
- Archivos de correo y contraseña de AOL 3

Archivos financieros

Internet Guard Dog también reconoce los archivos asociados a estos programas financieros y los agrega como un grupo a la lista de Archivos protegidos.

El grupo Archivos financieros incluye archivos de:

- Microsoft Money Financial
- Quicken Financial

Nota

Si decide no proteger los archivos financieros o de correo electrónico en este momento, o si más adelante instala alguno de los programas de correo electrónico o financieros mencionados, podrá protegerlos agregando sus grupos de archivos a la lista Archivos protegidos de Guardián de archivos en Configuración de protección.

Consulte Acerca de Guardián de archivos si desea obtener más información acerca de cómo agregar, suprimir o modificar la información protegida por Guardián de archivos.

Entrevista – **Administrar contraseñas**

¿Es capaz de recordar la contraseña y el nombre de usuario de todos los sitios Web protegidos que visita? Si los tiene anotados en papel, ¿es capaz de acordarse de dónde guardó la lista y dispone de un lugar seguro donde guardarla? Si deja que Internet Guard Dog administre sus contraseñas, no tendrá que volver a plantearse estas preguntas.

En lugar de tener que escribir su nombre de usuario y su contraseña cada vez que visita un sitio Web controlado por contraseña, puede arrastrar y soltar esta información desde Asistente de navegación hasta los cuadros de texto correspondientes de la pantalla de inicio de sesión.

- **Sitio**

  Este nombre se muestra sólo en la lista. Puede introducir la dirección o el nombre del sitio.

- **Nombre de usuario**

  El nombre con el cual se identifica en el sitio Web. También se conoce como nombre de inicio de sesión, ID de usuario, nombre de miembro, etcétera.

- **Contraseña**

  La contraseña con la que verifica su identidad en el sitio Web. Para protegerla, cada carácter aparece como un asterisco en Internet Guard Dog.

Consulte Acerca de Administrar contraseñas si desea obtener más información acerca de cómo agregar contraseñas y nombres de usuario a Administrar contraseñas después de realizar la entrevista.

Asistente de navegación es una forma práctica de resumir la actividad de las cookies. Puede seleccionar:

- **Todos los sitios Web**

  Para recibir el número total de cookies intercambiadas entre el PC y todos los sitios Web visitados desde la última limpieza de cookies del equipo

- **Sitios locales**

  Para recibir el número total de cookies intercambiadas entre el PC y el sitio Web al que está conectado actualmente.

Asistente de navegación le da acceso a las contraseñas y nombres de usuario introducidos en Administrar contraseñas. Para acceder a una contraseña, haga clic en la flecha que aparece junto a la lista desplegable de Administrar contraseñas y seleccione el sitio Web al que se está conectando. La contraseña y el nombre de usuario se mostrarán en el cuadro Administrar contraseñas que aparece en la parte inferior de Asistente de navegación.

Para agregar una nueva contraseña en Administrar contraseñas, haga clic en la flecha y seleccione **Agregar nueva entrada**. Escriba la información en el cuadro de diálogo Introduzca la contraseña para guardar y haga clic en **Aceptar**.

Muestra el número total de cookies enviadas al equipo de acuerdo con la selección realizada en Estadísticas.

Muestra el número total de cookies rechazadas de acuerdo con la selección realizada en Estadísticas.

Muestra el número total de veces que Internet Guard Dog ha impedido que su información se enviara a un sitio Web de acceso indirecto.

Arrastre y suelte su nombre de usuario y su contraseña desde Asistente de navegación hasta los cuadros correspondientes de la pantalla de inicio de sesión cada vez que visite un sitio Web protegido por contraseña.

Pantalla inicial de Internet Guard Dog

La pantalla inicial de Internet Guard Dog es la puerta de entrada a Internet Guard Dog. Dispone de las opciones siguientes:

- Configuración del usuario
- Privacidad y seguridad
- VirusScan
- Informes de registro de usuarios
- Actualizar
- Comprobación
- Opciones
- Ayuda

{button ,PI(`',`mcafee_com')} McAfee.com

Haga clic en **Comprobación** para realizar una inspección exhaustiva con el fin de detectar posibles problemas de seguridad o privacidad. Si encuentra algún problema, Internet Guard Dog elabora una lista de problemas y la muestra en la pantalla La comprobación ha detectado. También puede seleccionar un problema e Internet Guard Dog lo mostrará en una pantalla adicional con una descripción detallada y una recomendación sobre cómo solucionarlo. Si soluciona un problema y no le gusta el resultado, Internet Guard Dog le permite Deshacer el cambio.

Haga clic en **Actualizar** para obtener las últimas mejoras del programa Internet Guard Dog, así como los últimos archivos de patrón de virus. McAfee coloca los nuevos archivos de patrón de virus en su sitio Web cada mes. Internet Guard Dog utiliza McAfee Software Update Finder para detectar y recuperar las actualizaciones disponibles.

Haga clic en **Informes de registro del usuario** para visualizar las medidas adoptadas por Internet Guard Dog para proteger su seguridad y privacidad, así como la de otros usuarios con perfil definido en el equipo. Los informes se agrupan en tres categorías: Registros de violación, Registros de mantenimiento y Registros de actividades.

1. **Registro de violación**

   Haga clic para visualizar una lista de las actividades realizadas por un usuario con perfil definido que violen la Configuración de protección establecida por el Administrador (por ejemplo, intentar enviar el número de una tarjeta de crédito).

2. **Registro de mantenimiento**

   Haga clic para visualizar una lista de las acciones llevadas a cabo por Internet Guard Dog, en la que se especifican las funciones utilizadas para llevar a cabo la tarea.

3. **Registro de actividades**

   Haga clic para visualizar la identidad del usuario con perfil definido que ha utilizado el equipo. También muestra el día, la fecha y la hora de conexión y desconexión del equipo.

Seleccione una de las siguientes Opciones:

Configuración de la comprobación–Le lleva a la pantalla Configuración de la comprobación, en la que podrá especificar lo que Internet Guard Dog debe comprobar al ejecutar una Comprobación.

Configuración de protección–Le lleva al cuadro de diálogo Configuración de protección, que contiene las páginas de Configuración de protección de todas las funciones de Internet Guard Dog. En este cuadro podrá especificar el comportamiento de Internet Guard Dog cuando detecte algún tema que afecte la privacidad, la seguridad o la protección antivirus del PC.

Entrevista–Le guía a lo largo de la Entrevista, en la que puede especificar de forma asistida el comportamiento de Internet Guard Dog cuando detecte algún tema que afecte la privacidad y la seguridad del PC.

Haga clic en Ayuda si desea obtener más información acerca del funcionamiento de Internet Guard Dog. El sistema de Ayuda proporciona información acerca de los parámetros y funciones disponibles en esta pantalla. Entre las selecciones disponibles en el menú Ayuda encontrará:

- **Temas de ayuda**–Le da acceso a todo el sistema de Ayuda de Internet Guard Dog, incluyendo el Contenido, el Índice y Buscar. Haga clic en uno de los libros del Contenido para que se muestren los títulos de los temas incluidos en el libro. Haga clic en el título de uno de los temas para que se muestre el tema de ayuda asociado al título.

  El sistema de ayuda utiliza botones de navegación estándar de Ayuda de Windows, incluyendo **Temas de ayuda** para volver de un tema al índice, **Atrás** para volver al tema anterior, **>>** y **<<** para moverse hacia adelante o hacia atrás por los temas del sistema de Ayuda.
- **Ayuda sobre esta pantalla**–Le da acceso a un tema de ayuda con información específica para la pantalla que está viendo. Pulse **ESC** en el teclado para cerrar el tema.
- **McAfee en la Web**–Esta selección abre el navegador y le conecta con el sitio Web de McAfee, donde podrá obtener las últimas novedades de los productos de McAfee.
- **Internet Guard Dog en la Web**–Abre el navegador y le conecta con la página inicial de Internet Guard Dog en el sitio Web de McAfee, donde podrá obtener las últimas novedades de Internet Guard Dog.
- **Preguntas más frecuentes**–Abre el navegador y le da acceso a la página Preguntas más frecuentes del sitio Web de McAfee.
- **Informar de un problema**–Abre el navegador y le da acceso a un formulario de correo electrónico en el que podrá describir su problema. Es preciso que describa el problema con el máximo detalle. Su mensaje de correo electrónico se enviará al servicio de Soporte técnico de McAfee.
- **Enciclopedia de virus**–Le da acceso a un archivo de Ayuda que contiene información detallada acerca de todos los virus identificados por McAfee. Haga clic en la ficha Índice y seleccione el nombre del virus en la lista alfabética.
- **Acerca de Internet Guard Dog**–Abre el navegador y muestra una página con información sobre la versión y el Copyright.

Registro de Internet Guard Dog

Haga clic en Registro para las acciones llevadas a cabo por Internet Guard Dog con el fin de proteger los datos del PC. Internet Guard Dog realiza un seguimiento de las acciones que lleva a cabo en el PC y muestra esa información en forma de lista. En la pantalla Registro, puede ver la siguiente información:

{button ,PI(`gd.hlp',`Date_Time_column_on_the_Report_page')} Fecha/Hora

{button ,PI(`gd.hlp',`Guard_Dog_Action_column_on_the_Report_page')} Acción de Guard Dog

{button ,PI(`gd.hlp',`Type_column_on_the_Report_page')} Tipo

{button ,PI(`gd.hlp',`User_column_on_the_Report_page')} Usuario

Puede decidir qué hacer con los datos del Registro. Puede:

{button ,PI(`gd.hlp',`Print_button_on_the_Report_page')} Imprimir

{button ,PI(`gd.hlp',`Cancel_button_on_the_Report_page')} Cancelar

{button ,PI(`gd.hlp',`Clear_button_on_the_Report_page')} Borrar

Consulte la columna Fecha/Hora para ver en qué momento Internet Guard Dog ha realizado determinadas acciones.

Consulte columna Acción de Internet Guard Dog para ver qué ha hecho Internet Guard Dog para proteger los datos del PC.

Consulte la columna Tipo para ver qué función de Internet Guard Dog ha realizado la acción.

Consulte la columna Usuario para ver a qué usuario estaba protegiendo Internet Guard Dog cuando realizó la acción.

Cierra la pantalla Registro y vuelve a la pantalla inicial de Internet Guard Dog.

Envía la información de la pantalla Registro a la impresora.

Elimina toda la información de la pantalla Registro.

Configuración de la comprobación

Es posible especificar el tipo de comprobaciones que realizará Internet Guard Dog al supervisar la privacidad y la seguridad de los datos del sistema. Una vez realizadas las selecciones adecuadas, haga clic en **Aplicar** para que Internet Guard Dog las guarde y las utilice la próxima vez que ejecute una Comprobación. Si hace clic en **Cancelar,** se cerrará la pantalla Configuración de la comprobación sin guardar los cambios realizados en los elementos de la lista Comprobación.

- **Comprobación de las actualizaciones de Internet Guard Dog**–Ejecuta una Actualización y crea un recordatorio en Planificador para comprobar que Internet Guard Dog se actualiza de acuerdo con la frecuencia especificada. McAfee coloca las actualizaciones, incluyendo los nuevos archivos de patrón de virus, en su sitio Web. Internet Guard Dog utiliza la tecnología McAfee Software Update Finder para buscar y descargar las actualizaciones disponibles.
- **Comprobación de la versión del navegador**–Verifica que el navegador Internet Explorer o Netscape Navigator está actualizado y, en caso necesario, abre el navegador en la página Web que contiene la última actualización.
- **Comprobación de Protección de identidad**–Busca los archivos agregados a Protector de identidad que contienen información confidencial y le permite agregarlos a la lista Archivos protegidos de Guardián de archivos.
- **Comprobación de cookies**–Determina si han quedado cookies en su PC y le permite eliminarlas.
- **Comprobación del Filtro de búsquedas**–Determina si los archivos que ha eliminado de la Papelera de reciclaje están todavía en el disco duro. Cuando Internet Guard Dog encuentra algún archivo, le pregunta si eliminar permanentemente los datos del disco.
- **Limpiador de rastros de Internet**–Determina si el navegador Web ha dejado archivos de la Web o controles ActiveX en el PC y le permite suprimirlos.
- **Comprobación de Vigilante**–Determina qué programas del PC tienen acceso ilimitado a Internet y le permite modificar los derechos de acceso. Si utiliza Internet Explorer, comprobará también el nivel de seguridad del navegador.
- **Comprobación de Guardián de archivos**–Busca archivos de correo electrónico de Outlook, Netscape, Eudora y otros, así como archivos financieros de Quicken y MS Money, muestra si están protegidos por Guardián de archivos y, si no lo están, le permite protegerlos.
- **Comprobación de la contraseña**–Determina si existen carpetas compartidas en el PC que no estén protegidas por contraseña y le ofrece la posibilidad de agregar contraseñas.

La comprobación ha detectado - Informe de Internet Guard Dog

Internet Guard Dog compila una lista de los problemas y los temas encontrados durante una Comprobación. Estos problemas aparecen bajo los títulos de Seguridad, Privacidad y Antivirus en la pantalla La comprobación ha detectado. Cuando selecciona un problema, puede realizar las siguientes acciones:

{button ,PI(`gd.hlp',`Fix_button_on_the_CheckUp_found_page')} Arreglar

{button ,PI(`gd.hlp',`Close_button_on_the_CheckUp_found_page')} Cerrar

Indique a Internet Guard Dog la acción que debe realizar para solucionar un problema pulsando **Arreglar**. Internet Guard Dog muestra una pantalla con información importante acerca de la resolución del problema.

Haga clic en **Cerrar** para cerrar esta pantalla y volver a la pantalla inicial de Internet Guard Dog una vez haya finalizado la selección de problemas. Si ha dejado problemas por resolver, puede volver a ejecutar la Comprobación. Estos problemas, así como los identificados por Internet Guard Dog, se mostrarán en la pantalla La comprobación ha detectado.

La comprobación ha detectado – Archivos eliminados

Cuando ‘‘elimina’’ archivos y carpetas del PC, en realidad no desaparecen: la información permanece en el disco duro y se sobreescribe cuando falta espacio. Internet Guard Dog detecta los datos que han quedado en el disco duro y le permite suprimirlos de forma permanente.

{button ,PI(`gd.hlp’,`Delete_button_the_ChkUp_found_Delete_page’)} Suprimir

{button ,PI(`gd.hlp’,`Cancel_Button_on_the_Complete_Delete_page’)} Cancelar

Haga clic en **Suprimir** para asegurarse de que los archivos y las carpetas suprimidas se eliminen por completo de la unidad de disco duro.

Haga clic en Cancelar si no desea eliminar los archivos identificados por Internet Guard Dog. Volverá a la pantalla La comprobación ha detectado.

La comprobación ha detectado – Disco de emergencia

Si los datos del PC son víctima de algún siniestro, podrá recuperarlos mediante el disco de emergencia. Este disco contiene los datos importantes protegidos por Internet Guard Dog, así como un programa que le permite iniciar el PC en modo DOS. Puede hacer lo siguiente:

{button ,PI(`gd.hlp',`Create_button_on_the_Emergency_Disk_page')} Crear

{button ,PI(`gd.hlp',`Cancel_button_the_Create_an_Emergency_disk_page')} Cancelar

Haga clic en **Crear** para que Internet Guard Dog guarde los datos protegidos más importantes en disquetes. Internet Guard Dog necesitará tres disquetes para crear el disco de emergencia.

Haga clic en **Cancelar** para volver a la pantalla La comprobación ha detectado si no desea que Internet Guard Dog cree un disco de emergencia. Sin embargo, es aconsejable crear uno como medida de seguridad contra siniestros.

La comprobación ha detectado – Actualización del disco de emergencia

La información contenida en el disco de emergencia de Internet Guard Dog puede quedar obsoleta. Tenga siempre a mano los discos y deje que Internet Guard Dog vaya actualizando la información.

{button ,PI(`gd.hlp',`CheckUp_Found_Emergency_Disk_out_of_date_Update_button')} Actualizar

{button ,PI(`gd.hlp',`CheckUp_Found_Emergency_disk_out_of_date_Cancel_button')} Cancelar

Haga clic en Actualizar para actualizar los datos de los discos de emergencia.

Haga clic en **Cancelar** si no desea que Internet Guard Dog actualice la información de los discos de emergencia.

La comprobación ha detectado – Nivel de seguridad de Internet

El navegador Microsoft Internet Explorer cuenta con una serie de funciones de seguridad que le protegen mientras navega por Internet. Internet Guard Dog las comprueba y le alerta cuando no está configurado el nivel de seguridad máximo. Utilice **Actualizar** para acceder a Internet Explorer y al cuadro de diálogo Nivel de seguridad, en el que puede seleccionar dos tipos de protección:

- Alta–le protege de cualquier contenido dañino.
- Media–le alerta de contenidos potencialmente dañinos y le permite decidir si desea continuar.

Sugerencia

Si elige la opción de seguridad alta, Internet Explorer bloqueará todas las descargas de programas, como ActiveX y subprogramas Java, en el PC.

{button ,PI(`gd.hlp',`Update_button_on_CheckUp_Found_Internet_Security_Level')} Actualizar

{button ,PI(`gd.hlp',`Cancel_button_on_CheckUp_Found_Internet_Security_Level_page')} Cancelar

Haga clic en Actualizar para iniciar Internet Explorer y mostrar el cuadro de diálogo Nivel de seguridad.

Haga clic en Cancelar para que Internet Guard Dog deje las opciones como están y vuelva a la pantalla La comprobación ha detectado.

La comprobación ha detectado - Actualización de Internet Guard Dog

Internet Guard Dog utiliza McAfee Software Update Finder para buscar información acerca de actualizaciones de su software de navegador de Internet.

{button ,PI(`gd.hlp',`Update_available_for_browser_button')} Actualizar

{button ,PI(`gd.hlp',`Cancel_button_for_second_update_available_for_browser')} Cancelar

Haga clic en Actualizar para comprobar y recuperar las últimas mejoras del software a través de McAfee Software Update Finder.

Haga clic en **Cancelar** para cerrar esta pantalla y volver a la pantalla La comprobación ha detectado si no desea comprobar la existencia de actualizaciones.

La comprobación ha detectado – Actualización de navegador disponible

Internet Guard Dog utiliza McAfee Software Update Finder para buscar información acerca de las actualizaciones de su software de navegador.

{button ,PI(`gd.hlp',`Update_button_on_second_update_for_browser')} Actualizar

{button ,PI(`gd.hlp',`Cancel_button_for_second_update_available_for_browser')} Cancelar

Haga clic en Actualizar para comprobar y recuperar las últimas mejoras del software de su navegador.

Haga clic en **Cancelar** para cerrar esta ventana y volver a la ventana La comprobación ha detectado. Si no desea comprobar la existencia de actualizaciones de su navegador.

La comprobación ha detectado - Actualización de Internet Guard Dog disponible

McAfee coloca las innovaciones y mejoras de los productos en su sitio Web. Internet Guard Dog utiliza la tecnología McAfee Software Update Finder para comprobar si han aparecido nuevas actualizaciones del software de Internet Guard Dog, incluyendo nuevos archivos de patrón de virus.

Haga clic en Actualizar para comprobar las últimas mejoras del programa Internet Guard Dog a través de McAfee Software Update Finder.

Haga clic en **Cancelar** para cerrar esta pantalla y volver a la pantalla La comprobación ha detectado si no desea comprobar la existencia de actualizaciones.

La comprobación ha detectado – Archivos privados y financieros

Internet Guard Dog comprueba todos los archivos de la unidad de disco duro para ver si contienen alguno de los datos introducidos en Protector de identidad y muestra una lista de los resultados en esta pantalla. Internet Guard Dog también determina si alguno de estos archivos está protegido por Guardián de archivos y lo selecciona automáticamente. Puede realizar las siguientes acciones:

{button ,PI(`gd.hlp',`Protect_button_on_the_CheckUp_protect_page')} Proteger

{button ,PI(`gd.hlp',`Cancel_button_on_the_Protect_file_page')} Cancelar

Seleccione la casilla de verificación que aparece junto al nombre del archivo y haga clic en **Proteger** para agregar alguno de los archivos de esta lista a los archivos protegidos por Guardián de archivos.

Haga clic en **Cancelar** si no desea agregar ningún archivo a Guardián de archivos. Internet Guard Dog vuelve a la pantalla La comprobación ha detectado sin realizar ningún cambio.

La comprobación ha detectado – Supresión de controles ActiveX

Internet Guard Dog detecta la existencia de controles ActiveX y los muestra en esta lista. Internet Guard Dog considera que los controles firmados por sus creadores son seguros y sólo coloca una marca junto a aquellos controles que no están firmados. Aunque haya descargado controles ActiveX de un sitio que considere seguro, es aconsejable eliminarlos porque otros sitios Web podrían identificarlos y utilizarlos. (Si elimina los controles, la próxima vez que visite el sitio que se los envió tendrá que descargarlos de nuevo). Puede realizar las siguientes acciones:

{button ,PI(`gd.hlp',`Remove_button_on_the_CheckUp_ActiveX_control_page')} Suprimir

{button ,PI(`gd.hlp',`Cancel_button_on_the_CheckUp_ActiveX_control_page')} Cancelar

Seleccione el control y haga clic en Suprimir para eliminar un control ActiveX del disco duro.

Haga clic en **Cancelar** para cerrar la pantalla y volver a la pantalla La comprobación ha detectado si no desea llevar a cabo ninguna acción. Internet Guard Dog no guardará ninguno de los cambios que haya realizado mientras la ventana estaba abierta.

La comprobación ha detectado – Cookies

Internet Guard Dog comprueba el número de cookies que se han almacenado en el PC y selecciona la casilla de verificación que aparece junto a las cookies enviadas por los sitios favoritos. Internet Guard Dog no elimina las cookies de los sitios Web favoritos, ya que considera que la información de la cookie podría ser necesaria para dichos sitios. Puede realizar estas acciones:

{button ,PI(`gd.hlp',`Remove_button_on_the_CheckUp_Cookie_page')} Suprimir

{button ,PI(`gd.hlp',`Cancel_button_on_the_CheckUp_Cookie_page')} Cancelar

Seleccione los sitios cuyas cookies no desee eliminar y haga clic en Suprimir.

Haga clic en **Cancelar** si no desea realizar ninguna acción en esta pantalla. Internet Guard Dog cierra la pantalla y vuelve a la pantalla La comprobación ha detectado.

La comprobación ha detectado – Archivos de rastros de Internet

Con frecuencia, los sitios Web descargan en el PC algunos archivos como, por ejemplo, archivos de imagen, que permiten acelerar la descarga de las páginas. Estos archivos son innecesarios y, además, ocupan espacio en el disco duro. Asimismo, pueden utilizarse para realizar un seguimiento de sus hábitos de navegación por la Web.

Puede realizar las siguientes acciones:

{button ,PI(`gd.hlp',`Remove_button_on_the_Internet_files_CheckUp_page')} Suprimir

{button ,PI(`gd.hlp',`Cancel_button_on_the_CheckUp_Internet_files_page')} Cancelar

Utilice **Suprimir** para eliminar los archivos que ocupan espacio en el disco duro. Internet Guard Dog sólo suprimirá los archivos de los sitios que no se han marcado como favoritos. Puede seleccionar o borrar las casillas de verificación que aparecen junto a los nombres de las cookies que Internet Guard Dog debe suprimir.

Haga clic en Cancelar para volver a la pantalla La comprobación ha detectado si no desea realizar ninguna acción en esta pantalla.

La comprobación ha detectado – Programas con acceso a Internet

Internet Guard Dog supervisa los programas que tienen acceso a Internet y muestra en esta pantalla una lista con sus nombres y ubicaciones en el disco duro. Revise los programas a los que desee otorgar privilegios de acceso a Internet. Puede realizar estas acciones:

{button ,PI(`gd.hlp',`Deny_Access__button_for_Checkup_Internet_access_page')} Denegar el acceso

{button ,PI(`gd.hlp',`Cancel_button_on_the_CheckUp_Internet_access_page')} Cancelar

Seleccione un programa de la lista y haga clic en Denegar el acceso para denegarle el acceso automático a Internet.

Haga clic en Cancelar para volver a la pantalla La comprobación ha detectado si no desea realizar ninguna modificación.

La comprobación ha detectado – Archivos compartidos no protegidos por contraseña

Algunas veces, en los entornos de red, es útil permitir el acceso a la información contenida en algunos archivos a los usuarios de otros equipos. Si su PC utiliza el sistema operativo Windows, puede marcar fácilmente las carpetas como "compartidas" para que otros usuarios puedan utilizarlas. Si comparte carpetas, es conveniente que las proteja mediante contraseñas para que sólo los usuarios que las conozcan puedan acceder a la información.

{button ,PI(`gd.hlp',`CheckUp-_Shared_files_are_password_protected_Set_Pass_Button')} Establecer contraseña

{button ,PI(`gd.hlp',`CheckUp-_Shared_files_password_protected_Cancel_button')} Cancelar

Seleccione el nombre del archivo, la carpeta o la unidad y haga clic en Establecer contraseña si desea añadir protección por contraseña.

Haga clic en **Cancelar** si no desea añadir protección por contraseña a las carpetas compartidas. Internet Guard Dog vuelve a la pantalla La comprobación ha detectado sin realizar ningún cambio.

La comprobación ha detectado – Virus

Centinela de virus de Internet Guard Dog ha detectado archivos infectados por un virus. El nombre y la ubicación de cada archivo se mostrarán en la lista que aparece en la parte inferior de la pantalla. Para eliminar la infección de los archivos, seleccione las casillas de verificación que aparecen junto a los nombres y haga clic en **Limpiar**.

{button ,PI(`gd.hlp',`CheckUp_Clean_Viruses_Clean_button')} Limpiar

{button ,PI(`gd.hlp',`CheckUp_Clean_Viruses_Cancel_button')} Cancelar

Seleccione las casillas de verificación que aparecen junto a los nombres y haga clic en **Limpiar**. Una vez que Internet Guard Dog ha suprimido un virus, el archivo es seguro y puede volver a utilizarse.

Haga clic en **Cancelar** para volver a la pantalla La comprobación ha detectado si no desea que Internet Guard Dog desinfecte los archivos. De todas formas, no abra estos archivos, puesto que el virus podría extenderse a otros archivos del PC.

La comprobación ha detectado – Archivos que contienen información personal y financiera

Internet Guard Dog comprueba todos los archivos del equipo para ver si contienen alguno de los datos introducidos en Protector de identidad y muestra una lista de los resultados en esta pantalla. Internet Guard Dog también determina si alguno de estos archivos está protegido por Guardián de archivos y lo selecciona automáticamente. Puede realizar las siguientes acciones:

{button ,PI(`gd.hlp',`Protect_button_on_the_CheckUp_File_Guardian_Add_file_page')} Proteger

{button ,PI(`gd.hlp',`Cancel_button_on_the_File_Guardian_Add_file_page')} Cancelar

Seleccione la casilla de verificación que aparece junto al nombre del archivo y haga clic en **Proteger** para agregar alguno de los archivos de esta lista a los archivos protegidos por Guardián de archivos.

Haga clic en Cancelar para volver a la pantalla La comprobación ha detectado si no desea que Guardián de archivos proteja estos archivos.

Estado de la comprobación

Internet Guard Dog va a empezar la ejecución de una Comprobación de acuerdo con la información recopilada durante la Entrevista y los valores introducidos en Configuración de la comprobación. A medida que Internet Guard Dog trabaja, va resaltando cada comprobación e indicando la evolución en la barra de estado que aparece en la parte inferior de la pantalla. En el cuadro Más información, que aparece a la derecha, encontrará información adicional acerca de las comprobaciones. Puede hacer clic en **Cancelar** para detener la Comprobación en cualquier momento.

ActiveX

Active X es una tecnología utilizada por los programadores de software para introducir controles en un programa. Un control ActiveX puede agregar algo tan simple y útil como un botón a la interfaz de un programa. La mayoría de estos controles están firmados, por lo cual son inofensivos y no pueden dañar los datos del sistema. Sin embargo, existen personas poco honestas que utilizan la tecnología ActiveX para crear programas que pueden poner en peligro la seguridad de los datos de un equipo. Un ejemplo de esto son los programas que buscan determinados tipos de archivos en el disco duro y envían la información que contienen a terceros.

Alerta

Cuando se producen violaciones de la privacidad o surgen potenciales amenazas para la seguridad, Internet Guard Dog muestra información acerca de los inminentes riesgos en un cuadro de diálogo de alerta. La alerta le informa de lo que está ocurriendo y le ofrece soluciones para resolver la situación. Además, si su equipo tiene instalada una tarjeta de sonido, Internet Guard Dog emite un sonido para indicarle la presencia de una posible amenaza para la seguridad.

Favorito

Un favorito es una forma práctica de conectar con un sitio Web sin tener que escribir la dirección URL completa. Mientras navega por Internet, puede marcar como favoritos aquellos sitios que desee visitar con frecuencia. En la terminología de algunos navegadores, esta operación se denomina agregar un sitio Web a ‘‘Favoritos’’.

Sector de arranque

Para poder escribir información en el disco duro y poder leerla correctamente, el sistema operativo del equipo necesita conocer el tipo de sistema de archivos instalado en la unidad de disco duro, por ejemplo: FAT16, FAT32 o NTFS, así como la organización física de la unidad de disco duro en pistas, caras y sectores. En el sector de arranque de la unidad de disco duro encontrará información sobre este tema y sobre otras cuestiones.

Navegar

Normalmente, las personas que utilizamos Internet con frecuencia visitamos varios sitios Web mientras estamos conectados. La acción de pasar de un sitio Web a otro suele denominarse navegar, actividad que se conoce también con el término ‘‘surfear’’.

Navegador

Los navegadores son programas como, por ejemplo, Netscape Navigator o Microsoft Internet Explorer, que le permiten ver texto y gráficos, y descargar archivos de los sitios Web de Internet.

Asistente de navegación

Asistente de navegación es una práctica herramienta con una doble finalidad. En primer lugar, Asistente de navegación le permite ver un resumen de la actividad de las cookies. Para verlo, sólo tiene que seleccionar uno de los sitios Web que ha visitado en la lista desplegable. En segundo lugar, Asistente de navegación le permite acceder a las contraseñas almacenadas en Administrar contraseñas. Cuando accede a un sitio Web controlado por contraseña, puede arrastrar y soltar un nombre de usuario y una contraseña del Asistente de navegación en el cuadro correspondiente del formulario de inicio de sesión. Para acceder al Asistente de navegación, haga clic con el botón derecho en el icono de Internet Guard Dog situado en la bandeja del sistema y después en **Asistente de navegación** del menú emergente.

Caché

La caché es un espacio reservado de la unidad de disco duro del equipo en el que determinados programas, como los navegadores, almacenan información. El navegador puede almacenar en la caché copias de las páginas Web visitadas con sus correspondientes imágenes de esas páginas, de modo que, la próxima vez que la visite, la página pueda cargarse rápidamente utilizando las copias almacenadas en el disco duro en lugar de descargar las páginas del sitio Web.

Cookie

Una cookie es un mecanismo general que pueden utilizar los sitios Web para almacenar y recuperar información acerca de sus visitantes. El navegador copia las cookies en el equipo mientras los usuarios navegan por Internet. Por lo general, uno no se da cuenta de este proceso; durante una sesión de navegación pueden escribirse y leerse docenas de cookies.

Bloqueador de cookies

Las funciones de protección de Internet Guard Dog contra las cookies se agrupan en la función Bloqueador de cookies. Para acceder a la configuración de Bloqueador de cookies de Guard Dog, haga clic en **Opciones** y, a continuación, en **Configuración de protección**. Seleccione **Bloqueador de cookies** para que se muestre la página **Configuración de protección de Bloqueador de cookies** en el panel derecho del cuadro de diálogo.

Sitios de acceso directo e indirecto

Un sitio de acceso directo es cualquier ubicación de Internet que se puede visitar escribiendo simplemente su dirección, también conocida como dirección URL (Uniform Resource Locator), o haciendo clic en un hipervínculo que conecta un sitio Web con otro. Un sitio de acceso indirecto supervisa otros sitios: aunque no esté directamente conectado a ese sitio, su información personal puede transferirse del sitio de acceso directo al sitio de acceso indirecto.

Nombre de dominio

Así como la mayoría de casas tienen un número para facilitar su localización en una calle determinada, los equipos que forman parte de Internet también se identifican por números. Como las palabras son más fáciles de recordar que las largas cadenas de números, a los equipos también se les asigna un nombre.

Normalmente, para conectarse a un sitio Web se introduce la dirección completa del equipo que alberga ese sitio Web. Una parte de esa dirección completa, conocida habitualmente como Uniform Resource Locator (URL), es el nombre de dominio.

Un nombre de dominio se compone de palabras separadas por puntos que aparecen antes de la extensión de nivel superior de tres letras y el final de la dirección; por ejemplo:

usatoday.com o espn.sportszone.com o yahoo.com

Cuando escribe una dirección, puede introducir el nombre de dominio o el número (si lo conoce). Si introduce el nombre, otro equipo lo convertirá en el número correcto.

DOS

En su nivel más básico, el sistema operativo de un equipo contiene instrucciones que le indican lo que debe hacer. Sin embargo, estas instrucciones incluyen tareas bastante complejas, como el envío de datos a la impresora o el almacenamiento de datos en la unidad de disco duro. Microsoft Windows se ha convertido en el sistema operativo dominante en el mercado informático actual. Aunque en principio los sistemas operativos Windows son independientes, siguen dependiendo de las funciones proporcionadas por el antiguo Sistema Operativo en Disco (Disk Operating System), también denominado DOS. Para trabajar con DOS es preciso estar familiarizado con una gran cantidad de comandos. Cada uno de estos comandos debe escribirse en la línea de comandos para poder ejecutarse.

Algunos virus, como los virus del sector de arranque, los virus de las tablas de partición y los virus de memoria, pueden infectar los archivos antes de cargar Windows.

Codificación

La única forma de mantener un secreto es no contárselo a nadie y no anotarlo en ninguna parte. Si necesita compartir el secreto, puede esconderlo en otro mensaje e indicar a su destinatario la forma de encontrarlo. La codificación informática oculta mensajes haciendo que los datos originales sean ininteligibles. El objetivo es falsear los datos para todos, salvo para su destinatario: no sirve de nada tener acceso a datos codificados.

Los sistemas de codificación más simples utilizan el cambio de letras, que codifica el mensaje cambiando cada letra por n letras más en el alfabeto. Por ejemplo, digamos que A se cambia por B y B por C, etc. Siempre y cuando sepa cómo se han cambiado las letras, el destinatario podrá descodificar el mensaje invirtiendo el proceso. Por supuesto, una forma simple de descifrar este tipo de codificación consistiría en realizar todas las combinaciones posibles de las 28 letras del abecedario hasta reconstruir el mensaje final: por lo tanto, éste no es un método de codificación demasiado sólido.

La codificación informática utiliza una técnica mucho más complicada con el fin de ocultar el mensaje. En lugar de un simple esquema de cambio de letras, el mensaje original se transforma a un algoritmo matemático. El algoritmo utiliza una ‘‘clave’’ secreta para desordenar el mensaje, que será necesaria para volverlo a ordenar. La clave es como la llave de una casa: cuantos más dientes tiene una llave, más difícil es abrir la cerradura. De forma parecida, las codificaciones ‘‘seguras’’ utilizan claves con muchos ‘‘dientes’’(en este caso, bits de datos).

En la Web, se utilizan normalmente dos niveles de codificación. El estándar internacional es la codificación de 40 bits, pero algunos sitios de los EE.UU. utilizan un nivel superior de codificación de 128 bits. El número de bits indica la longitud de la clave utilizada para codificar los datos. Cuanto más larga sea la clave, más sólida y segura será la codificación.

Archivo ejecutable

Un archivo ejecutable es aquél que contiene toda la información necesaria para iniciar y ejecutar un programa en un equipo. Cuando se hace clic en el nombre de un programa en el menú Programas de Windows, en realidad se está activando un acceso directo al archivo ejecutable del programa. A menudo, los programas pequeños tienen todos los archivos comprimidos en un archivo ejecutable. Los programas grandes pueden constar de varios archivos, pero el archivo ejecutable se utilizará siempre para iniciar el programa. Los archivos ejecutables se distinguen por la extensión .exe. Los archivos ejecutables también suelen denominarse archivos de programa o archivos ejecutables de programa.

Extensión de archivo

Algunas aplicaciones como, por ejemplo, los programas de procesamiento de texto, gráficos y hojas de cálculo, permiten crear archivos que se almacenan en el disco duro. Cuando se almacena un archivo, la aplicación solicita que se introduzca un nombre al que añade automáticamente tres letras, denominadas extensión de archivo. Algunas veces la aplicación permite almacenar el archivo con distintas extensiones. Estas tres letras asocian el archivo con la aplicación para que, cuando quiera ver el archivo o editar su contenido, pueda abrirlo con la aplicación utilizada para crearlo.

Guardián de archivos

Guardián de archivos de Internet Guard Dog puede alertarle cuando se produce un suceso potencialmente dañino durante la utilización del equipo como, por ejemplo, la actividad de controles ActiveX. Otra función importante de Guardián de archivos es la lista **Archivos protegidos**. En esta lista pueden agregarse archivos e indicar las aplicaciones que pueden utilizarlos, garantizando de este modo que sólo las aplicaciones utilizadas para crear o editar dichos archivos tengan acceso a sus datos. Si un programa no autorizado intenta acceder a un archivo de la lista **Archivos protegidos**, Guardián de archivos le alertará. Para acceder a la configuración de Guardián de archivos, haga clic en Opciones y, después, en **Configuración de protección**. Haga clic en **Guardián de archivos** para que se muestre la página **Configuración de protección de Guardián de archivos** en el panel derecho del cuadro de diálogo.

Vigilante

Vigilante de Internet Guard Dog controla los programas que tienen acceso a los archivos confidenciales y puede bloquear automáticamente las actividades sospechosas. Para acceder a la configuración de **Vigilante** de Internet Guard Dog, haga clic en **Opciones** y, después, en **Configuración de protección**. Haga clic en **Vigilante** para que se muestre la página **Configuración de protección de Vigilante** en el panel derecho del cuadro de diálogo.

Sitio Web dañino

Un sitio Web dañino es aquél que contiene, por ejemplo, virus, controles ActiveX o subprogramas Java que, cuando se descargan, pueden resultar dañinos para el equipo.

Historial

Mientras utiliza Internet, el software del navegador reúne las direcciones URL (Uniform Resource Locator) de todos los sitios Web que visita y las coloca en un archivo del disco duro. Para su comodidad, la mayoría de navegadores tienen una opción que permite ver estas direcciones URL de forma que pueda conectarse a un sitio Web seleccionando la URL directamente.

HTML

Acrónimo de Hypertext Markup Language, el lenguaje utilizado para componer o crear documentos en la World Wide Web.

HTTP

Acrónimo de Hypertext Transfer Protocol, el sistema subyacente a toda la World Wide Web. El protocolo HTTP especifica los métodos de formato y transmisión de mensajes, así como el tipo de respuesta que deben ofrecer los servidores Web y los navegadores. Cuando se introduce una dirección Web en el navegador, éste envía una petición HTTP al servidor Web del Proveedor de servicios de Internet (ISP), pidiéndole acceso al sitio Web solicitado.

Protector de identidad

Las funciones de protección de identidad de Internet Guard Dog se agrupan en la función Protector de identidad. Durante la conexión a Internet, Internet Guard Dog le alerta cuando un programa intenta enviar la información de Protector de identidad a otra ubicación. Para acceder a la configuración de Protector de identidad de Internet Guard Dog, haga clic en **Opciones** y, después, en **Configuración de protección**. Haga clic en **Protector de identidad** para que se muestre la página **Configuración de protección de Protector de identidad** en el panel derecho del cuadro de diálogo.

Internet

Internet y World Wide Web son términos que utilizamos indistintamente para referirnos al conjunto de equipos que se han interconectado para formar una red que abarca el mundo entero. Técnicamente, Internet es el conjunto de equipos, mientras que la Web es el contenido de estos equipos: documentos, gráficos, archivos, etcétera. Normalmente, el equipo se conecta a Internet a través de un Proveedor de servicios de Internet (ISP).

Proveedor de servicios de Internet (ISP)

Un Proveedor de servicios de Internet (ISP) actúa como intermediario entre el usuario e Internet. El equipo se conecta mediante un módem al equipo del ISP que, a su vez, se conecta a los equipos de Internet.

Dirección IP

Consulte TCP/IP

Java

Java es una herramienta para desarrollar programas que se ejecutan por Internet. Estos pequeños programas, llamados ‘‘subprogramas’’, pueden encontrarse en una página Web. Cuando un navegador habilitado para Java accede a una página Web que contiene subprogramas Java, el navegador descarga y ejecuta esos subprogramas. La mayoría de subprogramas son inofensivos, pero no hay garantías de que todos lo sean y, en consecuencia, los datos del equipo pueden estar a merced de programadores que diseñan subprogramas con fines poco honestos.

Memoria

Mientras utiliza su equipo, los datos usados con frecuencia almacenados de forma permanente en el disco duro, se almacenan temporalmente en un dispositivo de hardware denominado memoria para que no tengan que recuperarse del disco duro cada vez que son necesarios. La utilización del dispositivo de memoria mejora considerablemente la velocidad de funcionamiento del equipo. Si la información contenida en la memoria sufre algún daño, el funcionamiento del equipo no será el adecuado.

Módem

Módem es una palabra construida a partir dos palabras, modulador y desmodulador, que hace referencia a un elemento de hardware informático. El módem convierte los datos digitales de los equipos en formato acústico que puede transmitirse fácilmente por la red telefónica. El módem del equipo receptor vuelve a convertir los datos acústicos al formato digital. Los módems modernos son muy flexibles y pueden transmitir datos en un gran abanico de velocidades. Cuando se establece una conexión, los módems emisor y receptor intercambian señales (este proceso se denomina apretón de manos o "handshaking") para determinar el protocolo de transmisión de la sesión. Si tiene el módem configurado con el sonido activado, oirá los tonos que intercambian los equipos a través de los altavoces integrados en el equipo.

Tabla de partición

El disco duro puede dividirse en secciones denominadas particiones. Por ejemplo, si necesitara ejecutar dos sistemas operativos en un único equipo, podría instalar cada sistema operativo, por ejemplo Windows 3.1 y Windows 95, en su propia partición. La tabla de particiones contiene información acerca del tamaño de cada sección y acerca de su situación en el disco duro.

Administrar contraseñas

Administrar contraseñas le permite almacenar en una ubicación segura diversos nombres y contraseñas de conexión a sitios Web. Cuando visite un sitio que requiera dicha información, puede arrastrarla desde Asistente de navegación hasta el formulario que se visualiza en el navegador. Para acceder a la configuración de Administrar contraseñas de Internet Guard Dog, haga clic en **Opciones** y, después, en **Configuración de protección**. Haga clic en **Administrar contraseñas** para que se muestre la página **Configuración de protección de Administrar contraseñas** de Internet Guard Dog en el panel derecho del cuadro de diálogo.

Alerta de privacidad

Internet Guard Dog muestra un cuadro de diálogo de alerta de privacidad cuando intercepta una posible intromisión en la privacidad de su PC.

Planificador

Una función muy útil de Internet Guard Dog es Planificador, que le permite configurar Internet Guard Dog para realizar determinadas tareas que requieren mucho tiempo en momentos en los que no se utiliza el equipo. Para acceder a la configuración de Planificador de Internet Guard Dog, haga clic en **Opciones** y después en **Configuración de protección**. Haga clic en **Planificador** para que se muestre la página de **Configuración de protección de Planificador** de Internet Guard Dog en el panel derecho del cuadro de diálogo.

Motor de búsqueda

Es un sitio Web diseñado para buscar información en Internet. Los motores de búsqueda constan de tres componentes básicos:

1 Un formulario en el que se introduce la consulta. Por ejemplo, si deseara buscar cómo se fabrica el queso de cabra, podría introducir la frase “producción de queso de cabra”.

2 Una base de datos que contiene un índice de contenidos Web. Cuando se introduce una consulta, el motor de búsqueda examina su base de datos y devuelve las URL de los sitios Web que considera adecuados.

3 Un “Webot”, un método automatizado para examinar el contenido de los sitios Web. Puesto que la Web cambia constantemente, los motores de búsqueda deben actualizar permanentemente sus bases de datos. El Webot añade sus descubrimientos a la base de datos del motor de búsqueda.

Filtro de búsquedas

El navegador Web puede enviar la información de búsqueda a sitios Web sin su consentimiento. Filtro de búsquedas de Internet Guard Dog puede advertirle antes de que esto suceda. Para acceder a la configuración de Filtro de búsquedas de Internet Guard Dog, haga clic en **Opciones** y, después, en **Configuración de protección**. Haga clic en **Filtro de búsquedas** para que se muestre la página **Configuración de protección de Filtro de búsquedas** de Internet Guard Dog en el panel derecho del cuadro de diálogo.

Alerta de seguridad

Internet Guard Dog muestra un cuadro de diálogo de alerta de seguridad cuando intercepta una posible intromisión en la seguridad del equipo.

Spam

El correo electrónico y las publicaciones en Usenets que nadie desea. Otra forma de ‘‘spamming’’ son los ataques maliciosos en Internet, que consisten en asaltar un servidor Web con millones de peticiones falsas. Igual que el correo basura normal, el spam es, a menudo, publicidad. El spam no sólo es una molestia; también malgasta muchos recursos de Internet. Algunos servicios en línea, como America Online, han empezado a elaborar políticas para impedir que el spam llegue a sus suscriptores.

TCP/IP

Internet se basa en un sistema llamado TCP/IP (Protocolo de control de la transmisión/Protocolo de Internet). El protocolo TCP hace posible que los equipos compartan datos, troceándolos primero en pequeños segmentos denominados paquetes. Además de datos, cada paquete contiene la dirección del equipo emisor del paquete y la dirección del destinatario al que va dirigido. La parte TCP del sistema es la responsable del direccionamiento de los datos y su división en paquetes. El protocolo IP, la segunda parte del sistema, es responsable de dirigir los paquetes del equipo emisor al equipo receptor. Unos equipos especiales denominados "routers" o encaminadores leen la dirección de cada paquete y encuentran la forma de dirigirlos al destino correspondiente.

¿Por qué es necesario realizar este proceso de separación de los datos en paquetes? La respuesta está en los orígenes de TCP/IP, que , al igual que la propia Internet, es un producto de la Guerra fría. Desarrollado inicialmente por el Departamento de defensa de los EE.UU, Internet fue diseñada para garantizar la seguridad de las comunicaciones incluso a pesar de los múltiples fallos que podrían producirse en las redes de comunicaciones durante una guerra nuclear. TCP/IP resuelve el problema de los fallos de la red considerando que en la red siempre existe una pequeña cantidad de ruido, por ejemplo, errores aleatorios en los datos o colapsos más graves del sistema. Si ha alguna vez ha tratado de hablar en una habitación con mucho ruido sabrá que es importante repetir las cosas y eso es exactamente lo que hace TCP/IP. Al trocear los datos en paquetes, Internet puede buscar rutas alternativas cuando una de las rutas no es accesible. Cuando un paquete no consigue llegar o llega dañado, el equipo receptor vuelve a solicitarlo hasta que llega correctamente.

Cuando se envía un mensaje de correo electrónico, por ejemplo, éste se trocea en varios paquetes. Dependiendo del ruido que haya en la red, cada paquete podría necesitar ser dirigido por una ruta diferente para conseguir llegar hasta su destino. Además, los problemas de red también pueden retrasar la llegada de algunos paquetes, con lo cual algunas veces éstos llegan desordenados. Para compensarlo, se examinan todos los paquetes a medida que llegan para comprobar que están en buen estado. Cuando se han recibido todos los paquetes, TCP los vuelve a colocar en su orden inicial. Por supuesto, todo esto se produce rápidamente y de forma automática, con lo cual nunca verá como se realiza el proceso.

Caballo de Troya

Un caballo de Troya es un programa que parece inofensivo hasta que se descarga e instala en el equipo. Entonces actúa como un virus.

Uniform Resource Locator (URL)

URL (Uniform Resource Locator) es el término que se aplica a la dirección de un sitio Web. El nombre de dominio forma parte de la dirección.

La dirección URL de McAfee, por ejemplo, es:

http://www.McAfee.com

http–Es el método utilizado para codificar y transmitir datos entre los equipos de Internet.

www–Es la abreviatura de World Wide Web.

McAfee.com–Es el nombre de dominio de McAfee.

Virus

Un virus es un programa diseñado con el fin de afectar al equipo incorporándose al código de un programa estándar. Mientras utiliza el programa, el virus va copiándose e incorporándose a otros programas, con lo cual infecta el equipo del mismo modo que un virus infecta el cuerpo. La mayoría de los programas de virus son molestos porque ocupan espacio de disco y pueden hacer que los programas se comporten de forma extraña. Sin embargo, algunos programas de virus pueden infectar y dañar gravemente los archivos que el equipo necesita para iniciar y cargar el sistema operativo.

McAfee trabaja incesantemente para identificar y hallar antídotos a los virus. Asimismo, McAfee incluye la información sobre los virus conocidos en los **archivos de patrón de virus**. A medida que van identificándose nuevos virus, el archivo de patrón se actualiza con la nueva información. Puede cargar el archivo de patrón de virus más reciente utilizando la función Actualización de Internet Guard Dog.

Alerta de virus

Internet Guard Dog muestra un cuadro de diálogo de alerta de virus cuando detecta un posible virus en su PC.

Centinela de virus

Si utiliza Internet a menudo y descarga datos de varias fuentes, corre el riesgo de descargar también algún virus. Internet Guard Dog proporciona una protección antivirus completa para los archivos y programas del equipo y puede alertarle cuando se detecta algún virus. Para acceder a la configuración de Centinela de virus de Internet Guard Dog, haga clic en **Opciones** y, después, en **Configuración de protección**. Haga clic en **Centinela de virus** para que se muestre la página de **Configuración de protección de Centinela de virus** de Internet Guard Dog en el panel derecho del cuadro de diálogo.

Sitio Web

Internet y World Wide Web son términos utilizados indistintamente para hacer referencia al conjunto de equipos interconectados que forman una red de alcance global. Técnicamente, Internet es el conjunto de equipos propiedad, por ejemplo, de instituciones educativas, empresas o el gobierno de los EE.UU. Los propietarios venden espacio de sus equipos a todo aquél que lo desee y se lo pueda permitir. Este espacio y su contenido (por ejemplo, los documentos y gráficos almacenados) se convierten en un sitio Web capaz de subdividirse todavía más. La forma más usual de conectarse a un sitio Web consiste en introducir la dirección URL en el programa de navegación.

Limpiador de rastros de Internet

Limpiador de rastros de Internet de Internet Guard Dog puede suprimir automáticamente los archivos Web que el navegador Web ha dejado en el disco duro. Para acceder a la configuración de Limpiador de rastros de Internet de Internet Guard Dog, haga clic en **Opciones** y, después, en **Configuración de protección**. Haga clic en **Limpiador de rastros de Internet** para que se muestre la página **Configuración de protección de Limpiador de rastros de Internet** de Internet Guard Dog en el panel derecho del cuadro de diálogo.

World Wide Web

Internet y World Wide Web son términos utilizados indistintamente para hacer referencia al conjunto de equipos interconectados para formar una red de alcance global. Técnicamente, Internet es el conjunto de equipos propiedad, por ejemplo, de instituciones educativas, empresas o el gobierno de los EE.UU. Los propietarios venden espacio de sus equipos a todo aquél que lo desee y se lo pueda permitir. Este espacio y su contenido (por ejemplo, los documentos y gráficos almacenados) se convierten en un sitio Web capaz de subdividirse todavía más. La forma más habitual de conectarse a un sitio Web consiste en introducir la dirección URL en el programa de navegación.

URL (Uniform Resource Locator) es el término que se aplica a la dirección de un sitio Web. El nombre de dominio forma parte de la dirección.

La dirección URL de McAfee, por ejemplo, es:

http://www.McAfee.com

http–Es el método utilizado para codificar y transmitir datos entre los equipos de Internet.

www–Es la abreviatura de World Wide Web.

McAfee.com–Es el nombre del dominio de McAfee.

Utilización del glosario de Internet Guard Dog

El glosario de Internet Guard Dog incluye definiciones de algunos de los términos más habituales en el sistema de Ayuda de Internet Guard Dog.

Para ver una lista de las definiciones:

1 Haga clic en Índice.

2 Haga clic en la lista y desplácese hacia arriba y hacia abajo.

3 Si busca una palabra concreta, escriba las primeras letras en el cuadro. El Índice busca automáticamente la palabra que más se parece a la que ha escrito.

Alerta de seguridad de Vigilante - El programa inicia otro programa

Si marca la casilla de verificación **Que un programa intente iniciar otro programa** de la página Configuración de protección de Vigilante, recibirá un mensaje de alerta cuando Vigilante detecte que un programa con autorización de acceso a Internet intenta acceder o ejecutar otro programa en el equipo. Puede utilizar las opciones del cuadro de diálogo de la alerta para autorizar o impedir el acceso.

¿Por qué supone un riesgo?

Algunos programas, sobre todo los programas desconocidos con acceso a Internet, pueden representar una amenaza para la seguridad porque son capaces de enviar datos privados a ubicaciones no deseadas.

¿Qué hacer?

La siguiente información le servirá para tomar una decisión:

- **Permitir siempre**–Seleccione esta opción si ha ejecutado conscientemente el programa con acceso a Internet y desea que, en el futuro, pueda ejecutar el otro programa sin recibir un mensaje de alerta.
- **Sólo esta vez**–Seleccione esta opción si rara vez utiliza esta aplicación. Por otra parte, si no está seguro de si esta aplicación debería poder iniciar el programa en cuestión, haga clic en **Sólo esta vez** y prosiga con cuidado.
- **Esta vez no**–Seleccione esta opción si no ha ejecutado conscientemente esta aplicación y no la reconoce. En cuanto pueda, deberá localizar la aplicación en el equipo y decidir si realmente desea conservarla.

Alerta de seguridad de Vigilante – El navegador se ha conectado a un sitio dañino

Si en la página Configuración de protección de Vigilante marca la casilla de verificación **Ir a sitios dañinos**, recibirá un mensaje de alerta cuando Vigilante detecte la conexión a un sitio Web conocido por su contenido dañino activo como, por ejemplo, controles ActiveX, subprogramas Java hostiles o virus.

¿Por qué supone un riesgo?

No es aconsejable conectarse a sitios que puedan contener controles dañinos, virus o caballos de Troya. El hecho de tener un control ActiveX o subprograma Java en el equipo representa un riesgo para su seguridad, ya que dichos programas, acerca de los cuales no sabe nada, pueden llevar a cabo acciones no deseadas. Por su parte, los virus y los caballos de Troya pueden ser dañinos para los archivos del PC.

¿Qué hacer?

Cierre el navegador inmediatamente para evitar que el contenido del sitio Web dañino se descargue en el equipo. Cuanto más tiempo pase conectado a dicho sitio Web, más posibilidades existen de que se produzcan daños en el PC.

- **Continuar**–Seleccione esta opción únicamente si no le preocupa el posible contenido dañino del sitio Web.

Alerta de seguridad de Vigilante- El programa intenta conectarse a Internet

Cada vez que el programa intente acceder a Internet, Internet Guard Dog le enviará un mensaje de alerta. Puede utilizar las opciones del cuadro de diálogo de la alerta para controlar los programas que tienen acceso a Internet.

¿Por qué supone un riesgo?

Debe familiarizarse con los programas fiables de su equipo que necesitan acceso a Internet para desempeñar su trabajo. Algunos programas de este tipo son el navegador de Internet o los programas financieros que utiliza para pagar facturas de manera electrónica. Cuando un programa desconocido intente conectarse a Internet, deberá observarlo atentamente: tal vez esté intentando enviar datos confidenciales a sitios donde no desea enviarlos.

¿Qué hacer?

La siguiente información le ayudará tomar una decisión:

- **Permitir siempre**–La primera vez que utilice un nuevo programa de Internet que Internet Guard Dog no haya visto antes, aparecerá un mensaje de alerta. Seleccione **Permitir siempre** si va a utilizar este programa con frecuencia. Si selecciona esta opción, Internet Guard Dog agregará el nombre del programa a la lista de programas con permiso para utilizar la conexión a Internet de la página Configuración de protección del Vigilante. Si cambia de idea, podrá suprimir el programa de la lista cuando lo desee.
- **No esta vez**– Si no ha iniciado a propósito este programa o no lo reconoce, deberá seleccionar esta opción. Tome nota del nombre del programa y, en cuanto pueda, búsquelo y decida si desea conservarlo.

  Si no ha iniciado conscientemente el programa pero lo reconoce, seleccione **No esta vez** hasta que descubra por qué se ha iniciado.
- **Sólo esta vez**–Si está probando un nuevo programa pero no le convence plenamente, seleccione esta opción, que le permitirá evaluar el rendimiento del programa antes de autorizar de forma permanente su acceso a Internet.

¿Qué hacer si cambia de idea?

Si autoriza el acceso a Internet de un programa y, posteriormente, cambia de idea, deberá:

- Salir de la aplicación.
- Eliminar el programa de la lista de programas con permiso para utilizar la conexión a Internet de la página Configuración de protección de Vigilante.

Alerta de seguridad de Vigilante – Número de tarjeta de crédito enviado a un sitio no seguro

Si en la página Configuración de protección de Vigilante marca la casilla de verificación **Se envíe algún número de tarjeta de crédito**, recibirá un mensaje de alerta cuando Vigilante detecte que un programa está enviando un número que puede corresponder al de una tarjeta de crédito a través de una conexión a Internet no segura. (Protector de identidad le ofrece protección añadida para las tarjetas de crédito, vigilando en especial los números de tarjeta de crédito que se especifican directamente en Configuración de protección de la página Protector de identidad.)

La mayoría de las empresas que realizan negocios por Internet ofrecen conexiones seguras a su servidor para poder llevar a cabo transacciones comerciales sin riesgos. Si envía un número de tarjeta de crédito a un sitio seguro, puede tener la certeza de que ningún desaprensivo podrá conseguirlo. Puesto que un sitio seguro puede tener sus propios problemas de conexión, en la mayoría de sitios encontrará la opción de utilizar medios de transmisión de datos seguros o no seguros.

Para obtener más información, consulte Conceptos esenciales acerca de la privacidad y la seguridad.

¿Por qué supone un riesgo?

Si envía datos a través de una conexión no segura, siempre existe la posibilidad de que alguien pueda interceptar los datos y utilizarlos para sus propios fines.

¿Qué hacer?

- **No esta vez**–Seleccione esta opción si desea evitar por esta vez que se envíe el número de su tarjeta de crédito a través de una conexión no segura.
- **Sólo esta vez**–Seleccione esta opción si desea aceptar el riesgo por esta vez.

Alerta de seguridad de Guardián de archivos – **Intento de dar formato al disco duro**

¡Advertencia!

Si no desea dar formato al disco, apague ahora mismo el equipo mediante el interruptor de alimentación.

Guardián de archivos es la autoridad protectora de su equipo. Es posible que algunos programas instalados en el sistema provengan de fuentes muy poco fiables. En realidad, es imposible saber qué va a hacer un programa hasta que se instala y se utiliza. Lo que a simple vista parece un programa inocente puede haber sido creado para destruir datos, como es el caso de los programas denominados "caballos de Troya", que pueden dar formato al disco duro. Guardián de archivos le protege de tales amenazas.

¿Por qué supone un riesgo?

El hecho de volver a dar formato a un disco duro no es una tarea que pueda a la ligera, ya que se elimina todo lo que contiene la unidad (sistema operativo, datos y aplicaciones) y la deja a cero. Si un programa ejecuta esta tarea inesperadamente sin su permiso, corre el riesgo de perder todo lo que tenga en el disco duro.

¿Qué hacer?

Apague el equipo AHORA MISMO mediante el interruptor de alimentación si no sabe por qué se está volviendo a dar formato al disco duro. Haga clic en **Ignorar** si usted (o el programa que esté utilizando) ha iniciado a propósito la operación de dar formato.

Alerta de seguridad de Guardián de archivos –Acceso del programa a un archivo

Después de agregar un archivo a la lista **Archivos protegidos** de la página Configuración de protección de Guardián de archivos, recibirá un mensaje de alerta si una aplicación no autorizada intenta acceder a dicho archivo. Puede utilizar las opciones que aparecen en el cuadro de diálogo de la alerta para determinar si la aplicación puede acceder al archivo. Puede seleccionar:

- **Permitir siempre**–La aplicación podrá acceder al archivo.
- **No esta vez**–La aplicación no podrá acceder al archivo esta vez.

¿Qué hacer?

La siguiente información le ayudará para tomar una decisión:

- Si ejecuta a propósito una aplicación que normalmente utiliza el archivo, haga clic en **Permitir siempre** y, si es necesario, reinicie la aplicación. Es una elección adecuada si intenta abrir a propósito un archivo protegido desde una aplicación y piensa hacerlo más veces.
- Si no ha ejecutado a propósito la aplicación y no la reconoce, haga clic en **No esta vez** en el cuadro de diálogo de la alerta. En cuanto pueda, deberá localizar dicha aplicación en su equipo y decidir si realmente desea conservarla.

Alerta de privacidad de Bloqueador de cookies – Envío de una cookie desde un sitio Web de acceso directo

En términos generales, un sitio de acceso directo es un sitio con el que se conecta escribiendo la URL o haciendo clic en un vínculo del navegador. Mientras navega por Internet, los sitios Web y el navegador van intercambiando cookies. Las cookies permiten que los sitios Web sean más eficaces utilizando la información que previamente han obtenido y almacenado en el equipo. Por ejemplo, las cookies permiten que su sitio comercial favorito muestre información personalizada cada vez que lo visite, o dejan que un sitio Web protegido por contraseña recupere la suya para que no tenga que introducirla cada vez que lo visita. En función de lo que haya seleccionado en la página Configuración de protección de Bloqueador de cookies, Internet Guard Dog le enviará un mensaje de alerta cuando un sitio Web al que se ha conectado directamente intente intercambiar cookies con el equipo.

¿Por qué supone un riesgo?

Las cookies representan una amenaza para su seguridad porque no puede qué seguimiento realizan I ni quién recibe información acerca de usted.

¿Qué hacer?

- **Permitir siempre**–Seleccione esta opción si el sitio al que se ha conectado necesita las cookies para funcionar correctamente, o si visita el sitio con frecuencia y es de confianza. Internet Guard Dog agrega el sitio a la lista Permitido de la página Configuración de protección de Bloqueador de cookies. La próxima vez que visite ese sitio, Internet Guard Dog aceptará sus cookies automáticamente.
- **No aceptar nunca**–Seleccione esta opción si no visita con mucha frecuencia el sitio, o si no desea que este sitio le reconozca. Internet Guard Dog agrega el sitio a la lista Rechazado de la página Configuración de protección de Bloqueador de cookies. Lo peor que puede ocurrir es que no pueda visualizar las páginas de ese sitio hasta que lo suprima de la lista Rechazados.

¿Qué hacer si cambia de idea?

Si cambia de idea acerca de un sitio, puede pasar el sitio de la lista **Permitidos** a la lista **Rechazados,** y viceversa, desde la página Configuración de protección de Bloqueador de cookies. Si desea empezar de nuevo, suprima el sitio de la lista en la que se encuentre y, la próxima vez que lo visite y trate de enviarle una cookie, Internet Guard Dog emitirá un mensaje de alerta. En esta página también dispone de opciones que le permiten controlar el comportamiento de Bloqueador de cookies en función de los sitios de acceso directo o indirecto.

Alerta de privacidad de Bloqueador de cookies – Envío de una cookie desde un sitio Web con acceso indirecto

En términos generales, un sitio de acceso indirecto es un sitio con el que se conecta sin escribir la dirección URL o sin hacer clic en un vínculo del navegador. Por ejemplo, si se conecta a un sitio que muestra información en cuadros, la información de un cuadro puede proceder de otro sitio Web. (Según el navegador, es posible que pueda ver las direcciones de otros sitios Web colocando el cursor sobre el cuadro y mirando la información que aparece en la barra de estado.)

Mientras navega por Internet, los sitios Web y el navegador van intercambiando cookies. Las cookies permiten que los sitios Web sean más eficaces utilizando la información que previamente han obtenido y almacenado en el equipo. Por ejemplo, las cookies permiten que su sitio comercial favorito muestre información personalizada cada vez que lo visite, o dejan que un sitio Web protegido por contraseña recupere la suya para que no tenga que introducirla cada vez que lo visita. En función de lo que haya seleccionado en la página Configuración de protección de Bloqueador de cookies, Internet Guard Dog emitirá un mensaje de alerta cuando un sitio Web al que se ha conectado indirectamente intente intercambiar cookies con el equipo.

¿Por qué supone un riesgo?

Puede que no sepa que ha contactado con un sitio Web de acceso indirecto. Como Las cookies representan una amenaza para su privacidad porque no puede controlar qué seguimiento realizan ni quién recibe información acerca de usted.

¿Qué hacer?

- **No aceptar nunca**–Seleccione esta opción si no visita con mucha frecuencia este sitio, o si no desea que dicho sitio le reconozca. Internet Guard Dog agrega el sitio a la lista Rechazado de la página Configuración de protección de Bloqueador de cookies. Si el sitio necesita las cookies, lo peor que puede ocurrir es que no pueda visualizar las páginas de ese sitio hasta que lo suprima de la lista Rechazados.
- **Permitir siempre**–Seleccione esta opción si el sitio necesita las cookies para funcionar correctamente, o si visita el sitio con frecuencia y es de confianza.

¿Qué hacer si cambia de idea?

Si cambia de idea acerca de un sitio, puede pasar el sitio de la lista Permitidos a la lista Rechazados**,** y viceversa, desde la página Configuración de protección de Bloqueador de cookies. Si desea empezar de nuevo, suprima el sitio de la lista en la que se encuentre; la próxima vez que lo visite y trate de enviarle una cookie, Internet Guard Dog le hará llegar un mensaje de alerta. En esta página también dispone de opciones que le permiten controlar el comportamiento de Bloqueador de cookies en función de los sitios de acceso directo o indirecto.

Alerta de Guardián de archivos – ActiveX explorando archivos

Si marca la casilla de verificación **ActiveX examine mi unidad** en la página Configuración de protección de Guardián de archivos, recibirá un mensaje de alerta cuando Guardián de archivos detecte que un control ActiveX explora los archivos de su disco duro.

¿Por qué supone un riesgo?

Un sitio Web puede descargar controles ActiveX en el equipo sin su conocimiento. Como los controles pueden ejecutarse en el equipo como si fueran programas instalados por usted, pueden hacer cosas que no desee, como reunir datos personales y enviarlos a otros equipos. Sin embargo, existen razones legítimas para permitir que un control ActiveX lea sus archivos. Por ejemplo, si visita un sitio Web de detección de virus, el control tendrá que leer todos los archivos para detectar si contienen algún virus. De todas formas, si un sitio explora sus archivos sin advertírselo, desconfíe inmediatamente.

¿Qué hacer?

- **Sólo esta vez**–Seleccione esta opción únicamente si confía en el control y se da cuenta de que no está explorando el disco con intención de dañar sus datos.
- **No esta vez**–Seleccione esta opción si sospecha que el control intenta dañar el contenido del disco.

Alerta de seguridad de Guardián de archivos – ActiveX borrando archivos

Si en la página Configuración de protección de Guardián de archivos marca la casilla de verificación **ActiveX elimine archivos de mi unidad**, recibirá un mensaje de alerta cuando Guardián de archivos detecte que un control ActiveX borra archivos de su disco duro.

¿Por qué supone un riesgo?

Un sitio Web puede descargar controles ActiveX en el equipo sin su conocimiento. Como los controles pueden ejecutarse en el equipo como si fueran programas instalados por usted, pueden hacer cosas que usted no desee, como borrar archivos. Sin embargo, existen razones legítimas para permitir que un control ActiveX borre archivos. Por ejemplo, si visita con regularidad un sitio y éste le comunica que debe actualizar el software que utiliza para ofrecerle un mejor servicio, tendrá que borrar los archivos anticuados.

¿Qué hacer?

- **Sólo esta vez**–Seleccione esta opción únicamente si confía en el control y sabe que no está borrando archivos con intención de dañar sus datos.
- **No esta vez**–Seleccione esta opción si sospecha que el control intenta dañar el contenido del disco.

Alerta de privacidad de Limpiador de rastros de Internet

Limpiador de rastros de Internet le envía mensajes de alerta en función de lo que seleccione en la página Configuración de protección de Limpiador de rastros de Internet. Por lo tanto, si en la página Configuración de protección de Limpiador de rastros de Internet selecciona **Solicitar limpiar después de cerrar el navegador Web**, aparecerá un cuadro de diálogo de alerta cada vez que cierre el navegador de Web. (Si utiliza Microsoft Active Desktop, únicamente aparecerá este cuadro de diálogo cuando salga de Windows, ya que Internet Explorer no se apaga por completo hasta que apague Windows.)

Para obtener más información, consulte Acerca de Limpiador de rastros de Internet.

¿Por qué supone un riesgo?

Mientras navega por Internet, las URL visitadas se almacenan en el equipo junto con las imágenes y páginas que los sitios Web utilizan para acelerar la descarga de contenido. Si otras personas también utilizan el equipo, podrá proteger su privacidad borrando el registro de sus conexiones. Internet Guard Dog elimina archivos de los sitios Web seleccionados de las siguientes carpetas:

- Caché–Los sitios Web almacenan páginas e imágenes en la carpeta de la caché y, cuando visita de nuevo el sitio, las utilizan para agilizar el proceso de descarga.
- URL–El navegador almacena en esta carpeta la URL que ha visitado y muestra las URL visitadas más recientemente.
- Historial–Las URL también se almacenan aquí. El navegador suprime las entradas de esta carpeta periódicamente.

Nota

Los nombres de las carpetas pueden variar en función del navegador que utilice.

¿Qué hacer?

Internet Guard Dog selecciona automáticamente los sitios que no se han marcado como favoritos o que no se han agregado a la lista de sitios favoritos. Como la mayoría de personas marcan como favoritos los sitios que vuelven a visitar, Internet Guard Dog presupone que seguramente desea conservar la información de conexión relativa a dichos sitios.

- **Limpiar**–Seleccione esta opción si desea suprimir los rastros de sus conexiones a Internet con relación a los sitios seleccionados. El hecho de suprimir estos archivos no perjudica el funcionamiento del equipo. Es una decisión suya y sólo afecta a la cantidad de espacio disponible de su disco duro en función de si conserva o no estos archivos.
- **No limpiar**–Hay personas a las que les gusta conservar los historiales por si desean volver a un sitio Web interesante que han olvidado marcar como favorito o agregarlo a la lista de favoritos del navegador.

Sugerencia

Para ordenar los sitios que aparecen en la lista, haga clic en el encabezado de una columna. Para seleccionar sitios contiguos, haga clic en el primer sitio que desee seleccionar, pulse la tecla Mayús y haga clic en el último sitio que desee seleccionar. Para seleccionar sitios no contiguos, pulse la tecla Control y haga clic en los sitios que desee seleccionar. Si marca o quita la marca de la casilla de verificación de cualquier sitio seleccionado, Internet Guard Dog hace coincidir el estado de la casilla de verificación para todos los sitios seleccionados.

Alerta de seguridad de Guardián de archivos – Acceso a un archivo de contraseñas de Windows

Si marca la casilla de verificación **Se acceda a los archivos de contraseña** en la página Configuración de protección de Guardián de archivos, Internet Guard Dog le enviará un mensaje de alerta si un programa intenta acceder a un archivo de contraseñas de Windows (.PWL).

¿Por qué supone un riesgo?

Los archivos de contraseñas de Windows almacenan las contraseñas de Windows, permitiéndole conectarse automáticamente a los recursos protegidos por contraseña (como, por ejemplo, una unidad de red) sin tener que escribir cada vez la contraseña. Si un programa desconocido intenta acceder a este archivo, pueden peligrar los datos que contiene.

¿Qué hacer?

- **Sólo esta vez**–Seleccione esta opción si reconoce y confía en el programa. Si no reconoce el programa pero le permite el acceso, vigile bien los recursos protegidos por contraseña por si se produce en ellos alguna actividad sospechosa.
- **No esta vez**–Seleccione esta opción si el programa le es extraño o si sospecha de él por cualquier motivo.

Alerta de privacidad de Protector de identidad – Envío de información personal o financiera

En Protector de identidad se especifica la información considerada importante. Cuando Internet Guard Dog detecte que su navegador va a enviar total o parcialmente esta información a un sitio Web, Internet Guard Dog le enviará un mensaje de alerta.

¿Por qué supone un riesgo?

Existen muchas empresas que se dedican a reunir información sobre nombres, direcciones y direcciones de correo electrónico para venderla a otras empresas. Dicha información va a parar principalmente a las listas de mailing, que son las que envían mensajes de correo electrónico no deseados. No obstante, no puede permitir que su información personal caiga en manos equivocadas. Por ejemplo, imagine que alguien utiliza su dirección de correo electrónico para enviar chistes obscenos a una lista de mailing o que utilizan su información financiera para intentar acceder a sus cuentas bancarias, de crédito o de seguridad.

¿Qué hacer?

- **Sólo esta vez**–Seleccione esta opción si confía en el sitio al que su navegador envía la información. Si el sitio utiliza una conexión segura, nadie podrá interceptar esta información.
- **No esta vez**–Seleccione esta opción si no confía en el sitio. También puede bloquear esta información si no se envía a través de una conexión segura.

Para obtener más información, consulte Conceptos esenciales acerca de la privacidad y la seguridad.

Alerta de virus – **Virus detectados**

Centinela de virus de Internet Guard Dog comprueba los archivos en función de lo que haya seleccionado en la página Configuración de protección de Centinela de virus. Internet Guard Dog le envía un mensaje de alerta cuando detecta que un virus ha infectado uno de los tipos de archivos que ha especificado.

¿Por qué supone un riesgo?

La mayoría de virus son programas molestos que se incorporan a otros programas, ocupando espacio de disco y haciendo que los programas se comporten de una manera extraña. No obstante, hay virus altamente hostiles que pueden dañar seriamente los archivos que el equipo necesita para funcionar correctamente. Cualquier virus puede ser un riesgo para los datos del disco duro.

¿Qué hacer?

- **Limpiar**–Seleccione esta opción si desea que Centinela de virus suprima el virus del archivo. Si el virus ha dañado el archivo de manera irreversible, Centinela de virus le permitirá borrar el archivo.
- **No limpiar**–Seleccione esta opción si desea que Internet Guard Dog no emprenda ninguna acción. No abra el archivo; de lo contrario, correrá el riesgo de extender el virus.

Alerta de seguridad de Vigilante – Marcado silencioso del módem

Si en la página Configuración de protección de Vigilante marca la casilla de verificación **Mi módem realice un marcado silencioso**, Internet Guard Dog le enviará un mensaje de alerta cuando detecte que su módem está marcando sin sonido.

¿Por qué supone un riesgo?

Porque en su equipo, sin usted saberlo, puede haber un programa que realice llamadas de larga distancia o que, incluso, llame a otro equipo para transmitirle datos.

¿Qué hacer?

- **No esta vez**–Seleccione esta opción si no sabe por qué su módem está marcando.
- **Sólo esta vez**–Seleccione esta opción si conoce el destino de la llamada; por ejemplo, si está llamando a su proveedor de servicios de Internet para realizar una conexión a Internet.

Alerta de Planificador de Internet Guard Dog – Notificación de actualización

Internet Guard Dog tiene configurado un suceso en la página Configuración de protección de Planificador para que no olvide comprobar las actualizaciones de Internet Guard Dog. Cada mes tiene a su disposición un nuevo archivo de patrón de virus, que actualiza la protección antivirus de Internet Guard Dog. También tiene a su disposición una actualización del programa Internet Guard Dog.

¿Qué hacer?

- **Actualizar**–Seleccione esta opción para recuperar Internet Guard Dog e instalar la actualización. Mantenga Internet Guard Dog al día con los patrones de virus, correcciones y mejoras más recientes para asegurarse de que su PC cuenta con la mejor protección posible.
- **Ignorar**–Seleccione esta opción si esta vez no desea actualizar Internet Guard Dog.

Sugerencia

Internet Guard Dog utiliza McAfee Software Update Finder para localizar y descargar actualizaciones desde el sitio Web de McAfee.

Alerta de Planificador de Internet Guard Dog – **Creación o actualización del disco de emergencia**

Programe un suceso en la página Configuración de protección de Planificador para acordarse de crear un disco de emergencia o para actualizar la información de un conjunto de discos ya existente creado anteriormente.

¿Qué hacer?

- **Crear**–Puesto que es imposible predecir el momento en que su equipo será víctima de un desastre, deberá crear o actualizar el disco de emergencia para garantizar el máximo grado de protección.
- **Ignorar**–Haga clic en esta opción para rechazar la alerta sin efectuar ninguna acción.

Acerca de las Preferencias de Internet Guard Dog

Para controlar las funciones y acciones básicas de Internet Guard Dog, seleccione las opciones correspondientes en la página Configuración de protección de Preferencias.

En el cuadro de grupo **Al inicio**, puede seleccionar:

- **Cargar Internet Guard Dog**–Internet Guard Dog empieza a supervisar el equipo en busca de posibles problemas cuando se inicia Windows. Es importante cargar Internet Guard Dog en ese momento, ya que algunos virus pueden atacar los archivos que el equipo necesita para iniciar el sistema operativo Windows, e Internet Guard Dog puede avisarle de ello.
- **Mostrar pantalla de bienvenida**–Se visualiza durante unos breves instantes el logotipo de Internet Guard Dog.
- **Utilizar contraseña**–Protege la configuración del equipo contra modificaciones no autorizadas mediante la asignación de una contraseña para el programa Internet Guard Dog. Tendrá que indicar la contraseña cada vez que inicie el equipo.

En el cuadro de grupo **Efectos de sonido**, puede seleccionar:

- **Efectos de sonido**–Determina el sonido que reproduce Internet Guard Dog al mostrar un mensaje de alerta de privacidad, seguridad o virus.

Haga clic en el botón Altavoz para escuchar el sonido seleccionado.

Configuración de Preferencias de Internet Guard Dog

1. Haga clic en **Opciones** en la pantalla inicial de Internet Guard Dog A continuación, haga clic en **Configuración de protección**. En la parte izquierda de la pantalla, compruebe que aparece una marca en la casilla de verificación que se encuentra junto a Preferencias.
2. Marque las siguientes casillas de verificación:
   - **Cargar Internet Guard Dog**
   - **Mostrar pantalla de bienvenida**
   - **Utilizar contraseña/Cambiar contraseña**–Durante la función Entrevista pudo seleccionar una contraseña para Internet Guard Dog. Si lo hizo, puede hacer clic en **Cambiar contraseña** para seleccionar otra contraseña. Si no asignó ninguna contraseña, seleccione **Utilizar contraseña** y el botón **Establecer contraseña**
3. Si el sistema está equipado con una tarjeta de sonido, también puede seleccionar un sonido diferente para cada tipo de alerta.
   - **Alerta de privacidad**
   - **Alerta de seguridad**
4. Haga clic en la flecha que se encuentra junto al cuadro de lista y seleccione una de las siguientes alertas:
   - **Silencio**
   - **Ladrido**
   - **Doble ladrido**
   - **Aullido**
5. Haga clic en **Aceptar** para que Internet Guard Dog guarde la selección efectuada.

Sugerencia

Para escuchar el sonido seleccionado, haga clic en el botón Altavoz en el cuadro de lista correspondiente.

Consulte Respuesta a las alertas de Internet Guard Dog para obtener más información.

Acerca de Bloqueador de cookies

Las cookies son pequeños archivos que el navegador de Web almacena en el sistema a petición de un servidor de Web. Cada vez que visualiza una página Web desde ese servidor de Web, el navegador devuelve la cookie al servidor. Las cookies actúan como etiquetas que permiten al servidor de Web efectuar un seguimiento de las páginas que visualiza y la frecuencia con que vuelve a visitarlas. Si desea una descripción más detallada de las cookies.

Bloqueador de cookies de Internet Guard Dog le ofrece tres opciones para controlar la utilización de las cookies en el equipo. Internet Guard Dog puede:

- Bloquear la entrada de todas las cookies.
- Permitir la entrada de todas las cookies.
- Borrar todas las cookies.

Al configurar Bloqueador de cookies en Configuración de protección, puede seleccionar una opción para los sitios de acceso directo y otra para los de acceso indirecto. Los sitios de acceso directo son aquellos a los que se conecta deliberadamente escribiendo la dirección URL, haciendo clic en el vínculo de una página Web o seleccionándolo en la lista de sitios marcados como favoritos o de sus sitios favoritos. Los sitios de acceso indirecto son aquéllos a los que accede a través de vínculos de un sitio al que se ha conectado. Por ejemplo, un anuncio visualizado en un cuadro separado de la página puede proceder de un sitio diferente.

Configuración de Bloqueador de cookies

1 Marque la opción correspondiente para **Sitios de acceso directo**:

- **Aceptar** para aceptar siempre las cookies procedentes de los sitios a los que se conecte directamente. A medida que navegue, Bloqueador de cookies agregará estos sitios a la lista **Permitidos**.
- **Rechazar** para rechazar siempre las cookies procedentes de los sitios a los que se conecte directamente. A medida que navegue, Bloqueador de cookies agregará estos sitios a la lista **Rechazados**.
- **Solicitar** para seleccionar si aceptar o rechazar una cookie procedente de un sitio de acceso directo en función de cada caso. A medida que navegue, Internet Guard Dog le pide su confirmación cada vez que un sitio de acceso directo intenta enviar una cookie al equipo.

2 Marque la opción que corresponda para **Sitios de acceso indirecto**:

- **Aceptar** para aceptar siempre las cookies procedentes de los sitios a los que se conecte indirectamente. Bloqueador de cookies agrega estos sitios a la lista **Permitidos**.
- **Rechazar** para rechazar siempre las cookies procedentes de los sitios a los que se conecte indirectamente. A medida que navegue, Bloqueador de cookies agrega estos sitios a la lista **Rechazados**.
- **Solicitar** para seleccionar si aceptar o rechazar una cookie procedente de un sitio de acceso indirecto en función de cada caso.

1. Para permitir, bloquear o borrar cookies de los sitios Web:
   - Seleccione una opción de la Web visualizada en el cuadro de texto; a continuación, haga clic en Permitir, Bloquear o Suprimir.
   - Al terminar, haga clic en Aplicar.

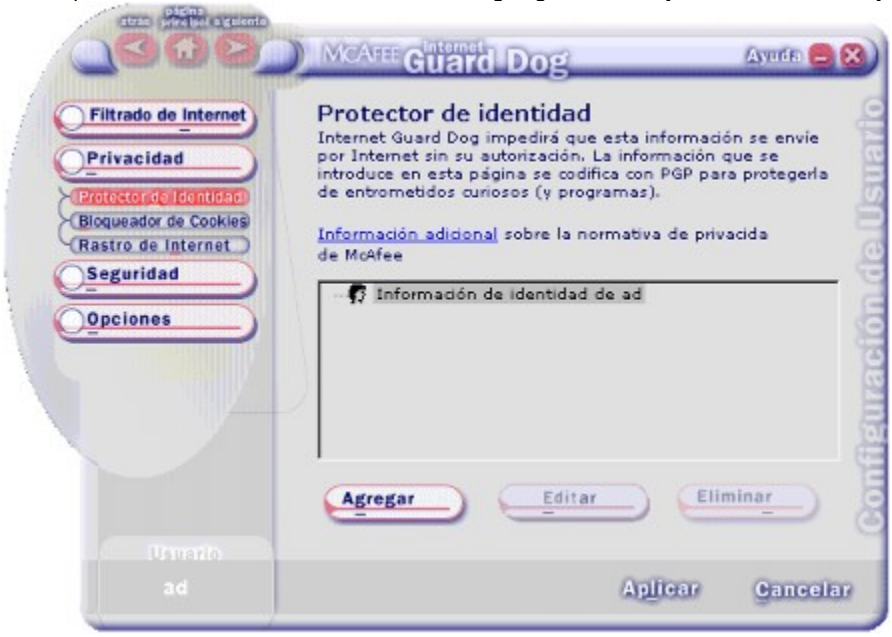
Respuesta a una alerta de Bloqueador de cookies

Acerca de Protector de identidad

Es fácil olvidar que la información que envía a través de Internet no va directamente de su equipo al equipo que almacena la información de la página Web. En realidad, la información puede pasar a través de varios equipos antes de llegar a su destino final. Protector de identidad puede evitar que una aplicación envíe cualquier dato personal que especifique a través de Internet.

Aunque no tiene que preocuparse cuando se conecta a un sitio mediante una conexión segura, tenga en cuenta que hay muchos sitios Web que utilizan una conexión segura únicamente cuando realizan transacciones con tarjetas de crédito. Internet Guard Dog le avisará cuando se vaya a enviar información financiera a un sitio no seguro mostrando un mensaje de alerta y permitiéndole elegir entre aceptar el envío de la información o bloquear su salida.

Además, si más de una persona utiliza su equipo, compruebe que ha creado una contraseña de Internet Guard Dog. Si la persona que utiliza el equipo no escribe la contraseña de Internet Guard Dog, Vigilante sustituye automáticamente por letras x la información personal protegida que se va a enviar a un sitio Web no seguro. Por ejemplo, si su hijo intenta comprar el último CD sin especificar la contraseña de Internet Guard Dog, Vigilante sustituye el número de su tarjeta de crédito por letras x.



Configuración de Protector de identidad

- Haga clic en **Agregar** para visualizar el asistente que le ayudará a especificar más información personal en Protector de identidad.
- Seleccione un elemento de la información personal y haga clic en **Editar** para visualizar un asistente que le ayudará a modificar dicho elemento.
- Seleccione un elemento de la información personal y haga clic en **Suprimir** para borrar el elemento de Protector de identidad.

Consulte Respuesta a las alertas de Protector de identidad para obtener más información.

Acerca de Limpiador de rastros de Internet

A medida que navega por Internet, el navegador almacena información para que las conexiones resulten más satisfactorias. Utiliza la información del siguiente modo:

- Archivos de la caché–Almacena archivos en el equipo para agilizar la visualización de los elementos de la página Web, como los gráficos.
- Direcciones URL visitadas–Le permite volver a los sitios Web visitados durante la sesión de conexión sin tener que escribir nuevamente las direcciones.
- Historial–Las direcciones URL visitadas se almacenan durante un determinado periodo de tiempo que se especifica mediante las opciones del navegador.

Cualquiera que utilice su equipo puede ver estos archivos; además , en función de la configuración del navegador, pueden ocupar gran cantidad de megabytes de espacio de disco. Si aceptó la recomendación de Internet Guard Dog durante la función Entrevista, Limpiador de rastros de Internet borrará automáticamente los rastros de sus conexiones Web. Al cerrar el navegador, Internet Guard Dog muestra un mensaje de alerta de Limpiador de rastros de Internet.

Configuración de Limpiador de rastros de Internet

- **Solicitar Limpiar después de cerrar el navegador Web**–Marque esta opción si desea que Internet Guard Dog solicite una confirmación cada vez que cierre el navegador.
- **Limpiar automáticamente después de cerrar el navegador Web**–Marque esta opción si desea que Internet Guard Dog borre las carpetas de la caché, el historial y las direcciones URL cada vez que cierre el navegador sin solicitarle su conformación.
- **No emprender ninguna acción.** Elija esta opción si no desea que Internet Guard Dog limpie la caché, el historial y las direcciones URL cada vez que cierre el navegador, sin antes preguntarle.

Sugerencia

Si marca la opción Limpiar automáticamente después de cerrar el navegador Web, puede hacer que Internet Guard Dog no borre las direcciones URL de ninguno de los sitios marcados como favoritos o agregados a su lista de favoritos, marcando la casilla de verificación **Conservar elementos favoritos**.

Para obtener más información, consulte Respuesta a las alertas de Limpiador de rastros de Internet.

Acerca de Filtro de búsquedas

Filtro de búsquedas impide que la información facilitada a un sitio Web pase a otro sitio. Sin Filtro de búsquedas, el navegador retiene dicha información, que puede ser extraído por el siguiente sitio que visite.

Si ha seleccionado Filtro de búsquedas en Configuración de protección, Internet Guard Dog suprimirá automáticamente la información de búsqueda antes de pasar a otro sitio Web. Internet Guard Dog no mostrará ningún mensaje de alerta para indicar esta función.

Configuración de Filtro de búsquedas

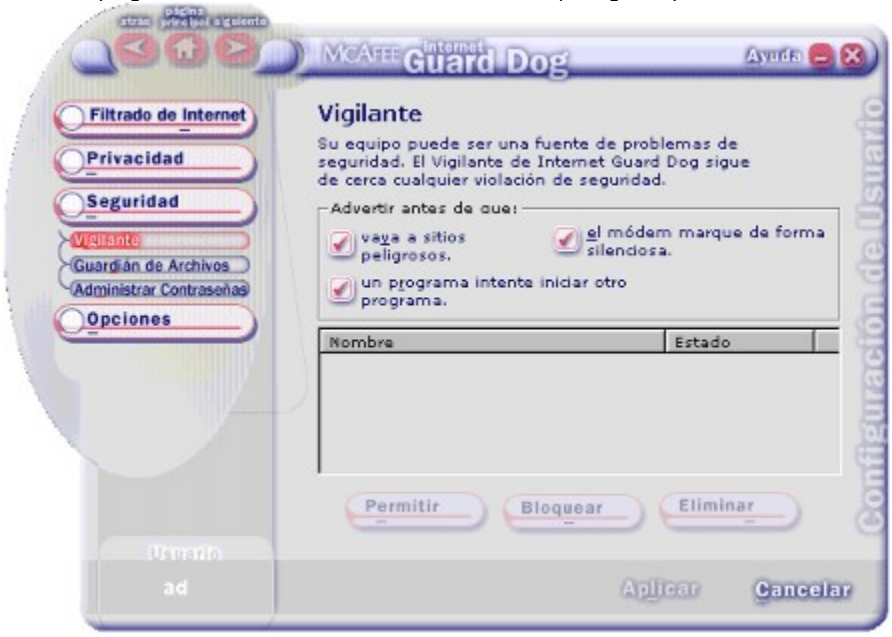
1 Haga clic en **Opciones** en la pantalla inicial de Internet Guard Dog y haga clic en **Configuración de protección**.

2 Asegúrese de que la casilla de verificación correspondiente a Filtro de búsquedas en el panel izquierdo está marcada. No hay ninguna configuración asociada para Filtro de búsquedas. Sólo puede estar activado o desactivado.

Acerca de Vigilante

Vigilante le permite controlar los programas que tienen acceso a su conexión de Internet. Vigilante también puede avisarle de alguna de estas acciones potencialmente dañinas:

- El navegador se dirige a un sitio dañino—un sitio conocido por contener archivos infectados (p. ej., caballos de Troya, controles ActiveX molestos o destructivos, u otras cuestiones de seguridad).
- Un programa utiliza de manera silenciosa el módem para conectarse a otro equipo.
- Un programa inicia otro programa.
- Un programa envía a través de Internet un número que sigue el patrón de un número de tarjeta de crédito común.



Configuración de Vigilante

1. Haga clic en la casilla de verificación de las advertencias que desee recibir. Vigilante le avisará cuando:
   - Esté a punto de conectarse a un sitio Web dañino. Un sitio dañino es un sitio que contiene archivos dañinos como, por ejemplo, controles ActiveX y subprogramas Java.
   - El módem de su equipo marque en modo silencioso. Podría tratar de efectuar una llamada de larga distancia.
   - Una programa intente iniciar otro programa. Algún programa podría estar intentando conectarse a Internet.
   - Se envíe el número de una tarjeta de crédito. Debe asegurarse que usted es la única persona que envía números de tarjeta de crédito a través de Internet.
2. Seguramente, algunos programas tendrán acceso permanente a Internet; Internet Guard Dog los agregará a la lista que se encuentra en el cuadro de diálogo Vigilante. Si cambia de opinión en cuanto al acceso, seleccione uno de los programas de la lista y haga clic en **Suprimir**.

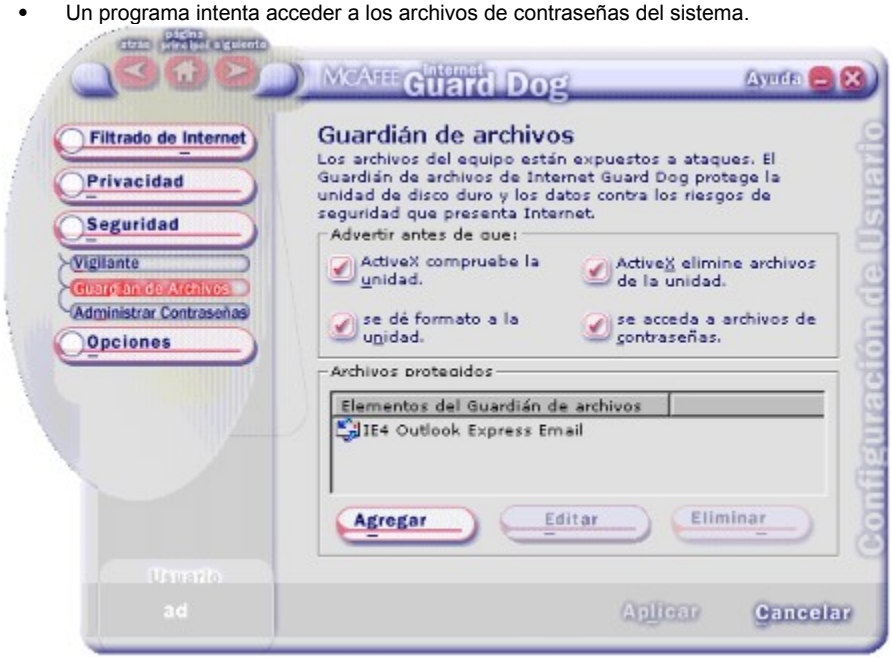
Para obtener más información, consulte:

- Respuesta a una alerta de sitio dañino
- Respuesta a una alerta de marcado silencioso del módem
- Respuesta a una alerta de inicio de programa
- Respuesta a una alerta de información de tarjeta de crédito

Acerca de Guardián de archivos

Guardián de archivos protege los archivos de datos confidenciales contra apertura, renombrado, copia, movimiento o borrado. Internet Guard Dog también le avisa si un programa intenta efectuar una de las siguientes actividades potencialmente dañinas:

- Un programa intenta dar formato a la unidad de disco duro–Cuando se inicia un comando de formateado, Internet Guard Dog no sabe si usted ha solicitado a su equipo que dé formato a un disquete, o si un control ActiveX ha iniciado el formateado de la unidad de disco duro. Como sabe, esta actividad es legítima cuando es usted quien inicia el comando de formateado o si sabe que un programa de los que está utilizando necesita dar formato a un disco.
- Un control ActiveX intenta borrar archivos de la unidad de disco duro–Existen motivos legítimos para permitir que un control ActiveX borre archivos. Por ejemplo, si un control instala software especial en su equipo para que pueda interactuar con el sitio Web, el control podría tener que borrar algunos archivos temporales. No obstante, si un sitio no le avisa y empieza a borrar archivos, Internet Guard Dog le deja ver el archivo que está borrando y le permite evaluar la fiabilidad del sitio en cuestión.
- Un control ActiveX intenta explorar archivos de la unidad de disco duro–Existen motivos legítimos para permitir que un control ActiveX lea, o explore, todos sus archivos. Por ejemplo, puede ir a un sitio Web que utilice un control ActiveX para detectar virus en el equipo. No obstante, si un sitio no le avisa y empieza a explorar sus archivos, Internet Guard Dog le da la oportunidad de evaluar la fiabilidad del sitio en cuestión.
- Un programa intenta acceder a los archivos de contraseñas del sistema.



Configuración de Guardián de archivos

1. Haga clic en la casilla de verificación de las advertencias que desea recibir. Guardián de archivos le avisará cuando:
   - Un control ActiveX explore la unidad.
   - Se esté dando formato a la unidad.
   - Un control ActiveX elimine archivos de la unidad.
   - Se esté dando formato a la unidad.

Indique a Guardián de archivos los archivos que desea vigilar en la unidad de disco duro y los programas que pueden utilizarse para abrirlos. Internet Guard Dog agrega o suprime programas en la lista Archivos protegidos. Si una persona no autorizada intenta acceder a un archivo protegido, Internet Guard Dog muestra un mensaje de alerta para que pueda decidir si permite el acceso al archivo del programa en cuestión. Si no ha ejecutado personalmente el programa no autorizado, debería investigar de inmediato el programa para determinar su origen.

Para agregar archivos y programas a la lista Archivos protegidos

Haga clic en **Agregar** para iniciar el asistente que le ayudará a agregar archivos y programas a la lista Archivos protegidos.

Codificación es otra función de protección de Guardián de archivos. La codificación garantiza que ningún otro programa pueda leer los datos de los archivos protegidos.

Para codificar o descodificar archivos de la lista Archivos protegidos

A medida que avance por Add Guarded Files Wizard, tendrá la oportunidad de codificar un archivo. Si selecciona esta opción, aparecerá el icono de una cerradura junto al nombre del archivo. Para codificar o descodificar todos los archivos marcados en la lista Archivos protegidos, haga clic con el botón derecho del ratón en el icono de Internet Guard Dog que se encuentra en la bandeja del sistema y seleccione **Codificar archivos de Guardián de archivos** o **Decodificar archivos**

de Guardián de archivos.

Para suprimir archivos y programas de la lista Archivos protegidos

Seleccione un archivo en la lista Archivos protegidos y haga clic en **Suprimir**.

Para obtener más información, consulte:

- Respuesta a una alerta de actividad ActiveX
- Respuesta a una alerta de formateado de disco
- Respuesta a una alerta de archivo protegido por contraseña
- Respuesta a una alerta de inicio de programa

Acerca de Administrar contraseñas

Administrar contraseñas le permite almacenar en una ubicación segura diversos nombres y contraseñas de conexión a sitios Web. Cuando visite un sitio que requiera dicha información, puede arrastrarla desde Asistente de navegación hasta el formulario que se visualiza en el navegador.

En Configuración de protección, puede:

- Agregar un registro de contraseña.
- Editar un registro de contraseña.
- Suprimir un registro de contraseña.

Utilización de Administrar contraseñas para agregar un registro de contraseña

1 Haga clic en Seguridad desde la ventana Configuración del usuario.

2 Haga clic en **Administrar contraseñas**.

3 Haga clic en **Agregar**.

4 Escriba la información que desee almacenar en ese registro.

5 Haga clic en **Aceptar**.

Para editar un registro de contraseña

1 Haga clic en el registro que desee editar y, a continuación, haga clic en **Editar**.

2 Modifique la información que desee almacenar en ese registro.

3 Haga clic en **Aceptar**.

Utilización de Administrar contraseñas para suprimir un registro de contraseña

Seleccione un registro y haga clic en **Suprimir**.

Nota: También puede agregar un registro a Asistente de navegación.

Consulte Acerca de Asistente de navegación para obtener más información.

Acerca de Centinela de virus

Puede utilizar Centinela de virus para controlar los tipos de archivos que deberá explorar la función Comprobación, así como activar la función de detección de virus mientras trabaja.

Control de los archivos a explorar durante la función Comprobación

1 En la pantalla inicial de Internet Guard Dog, haga clic en **Opciones** y seleccione **Configuración de protección**.

2 Compruebe que la casilla de verificación correspondiente a **Centinela de virus** del panel de la izquierda está marcada y, a continuación, haga clic en Centinela de virus. A la derecha aparecerá la página Configuración de protección de Centinela de virus.

3 En el cuadro **¿Qué desea comprobar?**, haga clic en la flecha que aparece junto a la lista desplegable y seleccione una de las siguientes opciones:

- **Todos los archivos**–Comprueba todos los archivos del equipo. Ésta es la comprobación más completa, y también la que tarda más tiempo en realizarse si cuenta con muchos archivos en el equipo. Con este tipo de comprobación puede detectar virus en archivos que utilizan tipos de archivos que no son estándar.
- **Archivos de programa**–Comprueba todos los archivos que un programa necesita para funcionar correctamente. Se comprueban los archivos con las extensiones de programa más comunes, como .com, .exe, .bat, .bin, .ovl, .drv, .dll, .sys, .tsk, .vxd y .ocx. Esta opción no detecta virus de macros.
- **Archivos de documento**–Únicamente comprueba los archivos de datos que pueden contener virus, que normalmente son virus de macros. Por ejemplo, se comprueban los archivos de documento de Microsoft Word y Excel y los documentos comprimidos con extensiones .zip, .arc y .lzh. Esta opción no detecta virus de programa.
- **Archivos de programa y documento**–Comprueba los archivos de programa y los archivos de documento. Esta opción tiene la ventaja de que es capaz de detectar la mayoría de virus y tarda menos tiempo que la comprobación de todos los archivos.

1. Haga clic en **Editar** en el cuadro **¿Qué desea comprobar?**. Internet Guard Dog muestra un asistente para que le ayude a seleccionar los tipos de archivo que desee comprobar.

Activación de la función de detección durante el trabajo

1. En la pantalla inicial de Internet Guard Dog, haga clic en **Opciones** y, a continuación, en **Configuración de protección**.
2. Compruebe que la casilla de verificación correspondiente a **Centinela de virus** del panel de la derecha está marcada y, a continuación, haga clic en Centinela de virus. A la derecha aparecerá la página Configuración de protección de Centinela de virus.
3. Marque o quite la marca de las casillas de verificación que aparecen junto a las siguientes opciones del cuadro **Cuándo realizar la comprobación**:
   - **Ejecutar el programa**–Detecta los posibles virus en un programa antes de ejecutarlo en el equipo.
   - **Acceso de correo electrónico**–Comprueba los mensajes de correo electrónico antes de abrirlos.
   - **Apertura de archivos**–Realiza una comprobación cada vez que abre un archivo en el equipo.
   - **Mover o renombrar**–Detecta posibles virus cada vez que mueve o renombra un archivo.
   - **Lectura de la unidad de disquetes**–Detecta posibles virus cada vez que lee información de un disquete.
   - **Inicio de DOS**–Detecta posibles virus de sector de arranque o de tabla de particiones durante el proceso de inicio de DOS que sólo se pueden limpiar desde DOS. (Se trata de una opción previa a su sesión de trabajo.)

Para excluir archivos y carpetas de la detección de virus durante la función Comprobación

Haga clic en **Agregar archivos** o **Agregar carpetas** al cuadro **No comprobar estos archivos ni estas carpetas** y seleccione las opciones que desee.

Sugerencia

Internet Guard Dog utiliza como referencia la lista **No comprobar estos archivos ni estas carpetas** durante la función Comprobación y durante cualquier detección de virus programada, pero no utiliza esta lista cuando comprueba los archivos en función de lo seleccionado en el cuadro **Cuándo realizar la comprobación**.

Para suprimir archivos y carpetas de la lista de exclusión

Haga clic en una entrada del cuadro **No comprobar estos archivos ni estas carpetas** y, a continuación, haga clic en **Suprimir**.

Consulte Respuesta a las alertas de Centinela de virus para obtener más información.

Respuesta a las alertas de Internet Guard Dog

En función de la selección efectuada en Configuración de protección, Internet Guard Dog supervisa el equipo y le alerta cuando ocurren determinadas cosas que podrían consecuencias dañinas para el equipo. La alerta le facilita información sobre las causas de la alerta y le ofrece opciones para tratar la situación.

Durante las primeras sesiones de trabajo después de instalar Internet Guard Dog, estas alertas podrían ser frecuentes. No obstante, sea paciente y responda cuidadosamente las preguntas que le formule Internet Guard Dog.

Para obtener más información, consulte:

- Respuesta a una alerta de inicio de programa
- Respuesta a una alerta de sitio dañino
- Respuesta a una alerta de acceso a Internet
- Respuesta a una alerta de información de tarjeta de crédito
- Respuesta a una alerta de formateado de disco
- Respuesta a una alerta de marcado silencioso del módem
- Respuesta a una alerta de Bloqueador de cookies
- Respuesta a una alerta de actividad ActiveX
- Respuesta a un control ActiveX que borra archivos
- Respuesta a una alerta de Limpiador de rastros de Internet
- Respuesta a una alerta de archivo protegido por contraseña
- Respuesta a una alerta de información personal
- Respuesta a una alerta de notificación de actualización

Obtención del máximo grado de protección antivirus

El equipo puede ser objeto de un ataque de virus cuando, por ejemplo, accede a un disquete infectado, abre un archivo adjunto de correo electrónico o descarga un programa infectado con virus desde Internet. Con una protección antivirus potente, como la que le ofrece Internet Guard Dog, mantendrá su PC a salvo de los virus. Internet Guard Dog le ofrece diversas maneras de detectar y eliminar los virus. Inicialmente, durante la función Entrevista puede configurar la detección de virus mediante la selección de:

- **Siempre que se inicie Windows**–Internet Guard Dog comprueba automáticamente los archivos de alto riesgo (archivos de documento y archivos de programa) cuando se inicia Windows.
- **Automáticamente, siempre que se registren actividades de archivo o de descarga**–Guard Dog detecta los posibles virus al:
- Ejecutar un programa
    - Acceder a archivos de correo electrónico
    - Abrir un archivo
    - Mover o renombrar
    - Leer un disquete

Después de la Entrevista también puede:

- **Comprobar los archivos de programa y de documento mediante la función Comprobación**– Después de instalar Internet Guard Dog, ejecute la función Comprobación para que la función antivirus explore minuciosamente los archivos de programa y los archivos de documento de las unidades locales para detectar posibles virus. Después de ejecutar una exploración completa por primera vez, es posible que desee modificar la configuración de la función Comprobación de virus .

Para obtener más información, consulte Detección de virus durante la función Comprobación.

- **Programar diferentes detecciones de virus**–Detectar los posibles virus puede ser un proceso bastante largo si tiene muchos datos en el PC. Puede configurar un suceso programado para un momento del día en que no utilice el equipo.

Para obtener más información, consulte Programación de sucesos para la detección de virus.

- **Comprobar una carpeta específica**–Es posible que desee comprobar únicamente los archivos de una carpeta.

Para obtener más información, consulte Comprobación de los archivos de una carpeta.

- **Comprobación mientras se trabaja mediante las opciones de Configuración de protección de Centinela de virus**– Dispone de diversas opciones en Configuración de protección de Centinela de virus con las que puede efectuar la detección de virus mientras está utilizando el PC.

Para obtener más información, consulte Selección de opciones en Centinela de virus.

Detección de virus durante la función Comprobación

Si utiliza shareware o recibe archivos procedentes de fuentes poco fiables, la detección de virus resulta indispensable para defender su equipo del ataque de virus. La opción Detección de virus le permite especificar los elementos que se van a comprobar mediante la función Comprobación.

Configuración de la protección antivirus durante la función Comprobación

Consiste en un proceso de dos pasos:

Primer paso–Seleccione las unidades y carpetas que se deben comprobar

1 En la pantalla inicial de Internet Guard Dog, haga clic en **Opciones** y seleccione **Configuración de Comprobación**.

2 Para comprobar todas las carpetas de todas las unidades, marque la casilla de verificación **Mi PC**. Aparecerá una marca en todas las unidades y carpetas de la lista.

3 Para seleccionar unidades y carpetas una por una, quite la marca de la casilla de verificación de **Mi PC** y, a continuación, marque las casillas de las unidades y carpetas que desee comprobar. Por ejemplo, si marca la casilla de verificación correspondiente a la unidad *c:*, aparecerá una marca en todas las carpetas que se encuentren en *c:* Quite la marca de las casillas de verificación de las carpetas en las que no desee que Internet Guard Dog detecte la existencia de virus.

Segundo paso–Seleccione lo que se debe comprobar

1 En la pantalla inicial de Internet Guard Dog, haga clic en **Opciones** y seleccione **Configuración de protección**.

2 En el panel izquierdo del cuadro de diálogo **Configuración de protección**, compruebe que aparece una marca en la casilla de verificación correspondiente a **Centinela de virus** y, a continuación, seleccione **Centinela de virus**. A la derecha aparecerá la página Configuración de protección de Centinela de virus.

3 En el cuadro de grupo **¿Qué desea comprobar?** seleccione una de las siguientes opciones de las listas desplegables:

- **Todos los archivos**–Comprueba todos los tipos de archivos de las carpetas seleccionadas en el primer paso.
- **Archivos de programa**–Comprueba únicamente los archivos de programa de las carpetas seleccionadas en el primer paso.
- **Archivos de documento**–Comprueba únicamente los archivos de documento de las carpetas seleccionadas en el primer paso.
- **Archivos de programa y documento**–Comprueba los archivos de programa y los archivos de documento de las carpetas seleccionadas en el primer paso.

1 Haga clic en **Editar** en el cuadro **¿Qué desea comprobar?**. Internet Guard Dog muestra un asistente para que le ayude a seleccionar los tipos de archivo de documento y los tipos de archivos de programa a comprobar.

Sugerencia

Si tiene alguna pregunta respecto al funcionamiento del asistente, haga clic en **Ayuda** en cualquier pantalla del asistente o pulse la tecla **F1** del teclado. Internet Guard Dog muestra información creada específicamente para la página del asistente que aparece en pantalla.

Cuando haya utilizado algunas veces la función Comprobación, tal vez desee excluir archivos y carpetas de la detección de virus, por ejemplo, cuando tenga que realizar una comprobación de un gran grupo de archivos y sepa que algunos de estos archivos del grupo no están infectados. Puede agregarlos a **No comprobar estos archivos ni estas carpetas** en Centinela de virus.

Paso opcional–Especifique lo que NO debe comprobarse durante la función Comprobación.

1. En la pantalla inicial de Internet Guard Dog, haga clic en **Opciones** y seleccione **Configuración de protección**.
2. En el panel izquierdo del cuadro de diálogo **Configuración de protección**, compruebe que aparece una marca en la casilla de verificación correspondiente a **Centinela de virus** y, a continuación, seleccione **Centinela de virus**. A la derecha aparecerá la página Configuración de protección de Centinela de virus.
3. En **No comprobar estos archivos ni estas carpetas**, proceda del siguiente modo para seleccionar lo que desea excluir :
   - Utilice **Agregar archivos** para abrir el cuadro de diálogo **Agregar archivo**, y navegue hasta un archivo determinado.
   - Utilice **Agregar carpetas** para abrir el cuadro de diálogo **Examinar**, y navegue hasta la carpeta.

Programación de sucesos para la detección de virus

Si desea explorar el PC para detectar virus sin tener que ejecutar Comprobación, Internet Guard Dog le permite configurar una detección de virus programada. Programar un suceso para la comprobación puede resultar especialmente útil cuando existen muchos datos en el PC. Seleccione lo que desea comprobar y el tipo de comprobación que desea realizar, y configure un suceso programado para que la comprobación tenga lugar cuando no esté utilizando el PC. Como valor predeterminado, Internet Guard Dog tiene configuradas dos detecciones de virus programadas: para los archivos de alto riesgo (archivos de programa y archivos documento) cada vez que se inicie Windows, y para todos los archivos, cada mes.

Modificación de la protección antivirus para las detecciones de virus programadas

Consiste en un proceso de dos pasos:

Primer paso–Seleccione las unidades y carpetas que se deben comprobar

1. En la pantalla principal de Internet Guard Dog, haga clic en **Opciones** y seleccione **Configuración de Comprobación**.
2. Para seleccionar unidades y carpetas una por una, quite la marca de la casilla de verificación de **Mi PC** y, a continuación, marque las casillas de las unidades y carpetas que desee. Por ejemplo, si marca la casilla de verificación correspondiente a la unidad *c:*, aparecerá una marca en todas las carpetas que se encuentren debajo de *c:* Quite la marca de las casillas de verificación de las carpetas en las que no desee que Internet Guard Dog compruebe la existencia de virus.

Segundo paso–Seleccione lo que se debe comprobar y configure un suceso programado

***Nota*:** Una de las ventajas de utilizar Scheduler Wizard es que no tiene que seleccionar **¿Qué desea comprobar?** en la página Configuración de protección de Centinela de virus.

1. En la pantalla principal de Internet Guard Dog, haga clic en **Opciones** y seleccione **Configuración de protección**.
2. En el panel izquierdo del cuadro de diálogo **Configuración de protección**, compruebe que aparece una marca en la casilla de verificación correspondiente a **Planificador** y, a continuación, seleccione **Planificador**. A la derecha aparecerá la página Configuración de protección de Planificador.
3. Haga clic en la entrada de la lista que desee programar. Puede seleccionar:
   - **Programar una detección de virus de todos los archivos** de las unidades y las carpetas seleccionadas en el primer paso.
   - **Programar una detección de virus en los archivos de alto riesgo** (archivos de programa y documento) de las unidades y las carpetas seleccionadas en el primer paso.
   - **Programar una detección de virus en los archivos modificados** de las unidades y las carpetas seleccionadas en el primer paso. Este tipo de comprobación mira la fecha de la última exploración y la compara con la fecha del archivo. Si la fecha del archivo es más reciente que la fecha de la última exploración, Internet Guard Dog comprueba si existen virus en el archivo.

1. Haga clic en **Siguiente** y siga las instrucciones del asistente para programar un suceso.

Sugerencia

Si tiene alguna pregunta respecto al funcionamiento del asistente, haga clic en **Ayuda** en cualquier pantalla del asistente o pulse la tecla **F1** del teclado. Internet Guard Dog muestra información creada específicamente para la página del asistente que aparece en pantalla.

Cuando haya utilizado algunas veces Scheduler Wizard, tal vez deseará excluir ciertos archivos y carpetas de la detección de virus; por ejemplo, puede excluir una serie de archivos de un gran grupo de archivos cuando sabe a ciencia cierta que no contienen ningún virus. Puede agregarlos a **No comprobar estos archivos ni estas carpetas** en la página Configuración de protección de Centinela de virus.

Paso opcional–Especifique lo que NO hay que comprobar durante la detección de virus programada

1 En la pantalla inicial de Internet Guard Dog, haga clic en **Opciones** y seleccione **Configuración de protección**.

2 En el panel izquierdo del cuadro de diálogo **Configuración de protección**, compruebe que aparece una marca en la casilla de verificación correspondiente a **Centinela de virus** y, a continuación, seleccione **Centinela de virus**. A la derecha aparecerá la página Configuración de protección de Centinela de virus.

3 En **No comprobar estos archivos ni estas carpetas**, proceda del siguiente modo para seleccionar lo que desea excluir:
   - Haga clic en **Agregar archivos** para abrir el cuadro de diálogo **Agregar archivo**, y navegue hasta un archivo determinado.
   - Haga clic en **Agregar carpetas** para abrir el cuadro de diálogo **Examinar**, y navegue hasta la carpeta.

Comprobación de los archivos de una carpeta

Tal vez necesite comprobar únicamente los archivos de una carpeta, por ejemplo, cuando acaba de descargar contenido de un sitio Web que no había visitado anteriormente.

Proceda del siguiente modo:

1. Abra Mi PC o el explorador de Windows.
2. Navegue hasta la carpeta en cuestión y haga clic con el botón derecho del ratón para seleccionarla.
3. Seleccione **Detección de virus** en el menú emergente.

Selección de las opciones de funcionamiento mientras trabaja de Centinela de virus

La opción **Cuándo realizar la comprobación** de la página Configuración de protección de Centinela de virus le permite configurar la protección antivirus de Internet Guard Dog para que proteja a su equipo contra los virus mientras esté trabajando en el PC. Estas funciones de comprobación complementan la función Detección de virus de Comprobación y las opciones de comprobación de Planificador. Las opciones de **Cuándo realizar la comprobación** que se activan mientras trabaja pueden combinarse con la función Comprobación y con Planificador para completar el entorno de protección ofrecido por la función antivirus de Internet Guard Dog.

Modificación de la protección antivirus mientras trabaja

Consiste en un proceso de dos pasos:

Primer paso–Seleccione cuándo se debe efectuar la comprobación mientras usted trabaja

1. En la pantalla inicial de Internet Guard Dog, haga clic en **Opciones** y seleccione **Configuración de protección**.
2. En el panel izquierdo del cuadro de diálogo **Configuración de protección**, compruebe que aparece una marca en la casilla de verificación correspondiente a **Centinela de virus** y, a continuación, seleccione **Centinela de virus**. A la derecha aparecerá la página Configuración de protección de Centinela de virus.
3. En el cuadro de grupo **Cuándo realizar la comprobación**, marque o quite la marca de las siguiente casillas de verificación:
   - **Ejecutar programa**–Detecta posibles virus cuando se inicia un programa en el PC.
   - **Acceso a archivos de correo electrónico**–Detecta posibles virus al abrir archivos adjuntos de correo electrónico.
   - **Abrir archivos**–Detecta posibles virus al abrir un archivo.
   - **Mover o renombrar**–Detecta posibles virus al mover o renombrar un archivo.
   - **Lectura de la unidad de disquetes**–Seleccione esta opción para explorar un disquete al abrirlo.
   - **Inicio de DOS**– Detecta posibles virus en DOS y los identifica ANTES de cargar Windows cada vez que inicia el PC. El sistema operativo Windows todavía depende de las funciones de un antiguo sistema operativo llamado DOS. Algunos virus, como los virus del sector de arranque, los virus de las tablas de partición y los virus de memoria, pueden infectar los archivos antes de cargar Windows. Aunque estos tipos de virus podrían detectarse en Windows, la mayoría deben eliminarse desde DOS. Por este motivo, debería marcar esta opción si desea contar con una protección antivirus más completa.

Nota

No puede excluir archivos o programas si los agrega a la lista **No comprobar estos archivos ni estas carpetas** de la página Configuración de protección de Centinela de virus desde la función **Cuándo realizar la comprobación**.

Segundo paso–Seleccione cómo responder si se detecta un virus mientras usted está trabajando

En la **página Configuración de protección de Centinela de virus**, seleccione una de las siguientes opciones que aparecen en la lista desplegable del cuadro **Si se encuentra un virus**:

- **Limpieza automática**–Suprime el virus del archivo infectado, y si no puede suprimirlo, Guard Dog le indica que lo elimine.
- **Eliminación automática**–Elimina el archivo del disco duro.
- **Denegar el acceso**–No podrá hacer nada con el archivo, excepto eliminarlo con el explorador de Windows o limpiarlo con Comprobación. (Cuando se abre un archivo infectado, el virus se extiende.)
- **Solicitar**–Podrá decidir lo que hacer caso por caso.

***Nota*:** La selección realizada en **Si se encuentra un virus** será valida para todas las selecciones realizada en el cuadro **¿Qué desea comprobar?**, excepto para Inicio de DOS.

Add Guarded File Wizard, página 3

Al agregar elementos a la lista Archivos protegidos, esta pantalla muestra el archivo, la carpeta, el grupo de archivos o la unidad que ha agregado. Cuando concede acceso a un archivo protegido, esta pantalla muestra el archivo o la carpeta en cuestión, así como el programa al que ha concedido los privilegios de acceso. Finalmente, incluye también la ruta de acceso completa de los archivos, las carpetas y los programas.

Para cambiar esta información:

- Haga clic en **Atrás** para volver a la pantalla adecuada del asistente. Haga clic en **Finalizar** para volver a la página de Configuración de protección de Guardián de archivos.

Add Guarded File Wizard, página 2

Para agregar un archivo a la lista Archivos protegidos:

1. Escriba la ruta de acceso del archivo en el cuadro de texto. Por ejemplo, si desea agregar Hojadecálculo.xls en la carpeta proyectos de la unidad C en la lista Archivos protegidos, escribirá

   c:\proyectos\hojadecálculo.xls

   Si no desea escribir, haga clic en **Examinar** para localizar el archivo. La ruta de acceso completa aparecerá automáticamente en el cuadro de texto.
2. Para seleccionar un archivo con el fin de codificarlo, seleccione la casilla de verificación **Incluir para codificación de archivos**. Aparecerá un candado junto al nombre del archivo en la lista Archivos protegidos.
3. Haga clic en **Siguiente** para visualizar una pantalla en la que se mostrará una lista de los archivos que han sido agregados.
4. Para cambiar la información contenida en esta pantalla, haga clic en **Atrás** y realice los cambios necesarios en las pantallas correspondientes. Haga clic en **Finalizar** para volver a la página de Configuración de protección de Guardián de archivos.

Sugerencia

Para codificar o descodificar un archivo de la lista Archivos protegidos, haga clic con el botón derecho en el icono de Internet Guard Dog situado en la bandeja del sistema y seleccione **Codificar archivos de Guardián de archivos** o **Descodificar archivos de Guardián de archivos**.

Add Guarded Folder Wizard, página 2

Para agregar una carpeta a la lista Archivos protegidos:

1. Escriba la ruta de acceso de la carpeta en el cuadro de texto. Por ejemplo, si desea agregar todos los archivos de la carpeta Proyectos a la lista Archivos protegidos, escribirá:

   c:\proyectos

   Si no desea escribir, haga clic en **Examinar** para localizar la carpeta. La ruta de acceso completa aparecerá automáticamente en el cuadro de texto.
2. Si quiere codificar todos los archivos de la carpeta para que no puedan leerse los datos que contiene, seleccione la casilla de verificación **Incluir para codificación de archivos**.
3. Haga clic en **Siguiente** para visualizar una pantalla en la que se mostrará una lista de las carpetas que han sido agregadas.
4. Para cambiar la información que aparece en esta pantalla, haga clic en **Atrás** y realice los cambios necesarios en las pantallas correspondientes. Haga clic en **Finalizar** para volver a la página de Configuración de protección de Guardián de archivos.

Add Guarded File Groups Wizard, página 2

Internet Guard Dog reconoce archivos asociados a programas de correo electrónico y financieros. Para evitar tener que agregar los archivos asociados a estos programas uno a uno, Internet Guard Dog trata estos archivos como un grupo que puede agregarse a la lista Archivos protegidos.

El grupo Archivos de correo electrónico incluye:

- Correo electrónico de Internet Explorer 4
- Correo electrónico de Internet Explorer 3
- Correo electrónico de Outlook Express de Internet Explorer 4
- Correo electrónico de Netscape
- Correo electrónico de Communicator
- Correo electrónico de Eudora
- Archivos de correo y contraseña de AOL 3

El grupo Archivos financieros incluye:

- Microsoft Money Financial
- Quicken Financial

Para agregar un grupo de archivos a la lista Archivos protegidos:

1. Seleccione **Grupo de archivos** en la lista y haga clic en **Siguiente** para visualizar una pantalla con una lista de los grupos que han sido agregados.
2. Para cambiar la información que aparece en esta pantalla, haga clic en **Atrás** y realice los cambios necesarios en las pantallas correspondientes.
3. Haga clic en **Finalizar** para volver a la página de Configuración de protección de Guardián de archivos.

Nota

Puede agregar estos grupos de archivos a la parte Entrevista del programa Internet Guard Dog.

Consulte el siguiente tema si desea obtener más información sobre cómo reiniciar la Entrevista.

Respuesta a las preguntas de la Entrevista

Add Guarded File Types Wizard, página 2

Para agregar tipos de archivos a la lista Archivos protegidos:

1. Seleccione los tipos de archivos de la lista y haga clic en **Siguiente** para visualizar una pantalla que muestre una lista con los tipos de archivos agregados.
2. Para cambiar la información de esta pantalla, haga clic en **Atrás** y realice los cambios necesarios en las pantallas correspondientes. Haga clic en **Finalizar** para volver a la página de Configuración de protección de Guardián de archivos.

Sugerencia

Para realizar selecciones múltiples de la lista de tipos de archivos, pulse MAYÚSCULAS+CLIC o CONTROL+CLIC.

Add Guarded Files Wizard - Unidad, página 2

Para agregar unidades en la lista Archivos protegidos:

1. Seleccione la unidad en la lista y haga clic en **Siguiente** para visualizar una pantalla con una lista de las unidades que han sido agregadas.
2. Para cambiar la información de esta pantalla, haga clic en **Atrás** y realice los cambios necesarios en las pantallas correspondientes. Haga clic en **Finalizar** para volver a la página de Configuración de protección de Guardián de archivos.

Sugerencia

Para realizar selecciones múltiples de la lista de unidades, pulse MAYÚSCULAS+CLIC o CONTROL+CLIC.

Add Guarded File Wizard - Otorgar acceso a programa, página 2

Para conceder a un programa acceso a la selección que ha realizado en la pantalla anterior:

1. Escriba la ruta de acceso del archivo ejecutable del programa en el cuadro de texto. Por ejemplo, seguramente le resultará útil que Microsoft Internet Explorer pueda acceder a los archivos de correo electrónico de Internet protegidos por Guardián de archivos. Puede escribir:

   c:\Archivos de programa\Internet Explorer\Iexplorer.exe

   Para evitar tener que escribir, haga clic en **Examinar** con el fin de localizar el ejecutable del programa. La ruta de acceso completa aparecerá automáticamente en el cuadro de texto.
2. Haga clic en **Siguiente** para visualizar una pantalla con una lista de los programas a los que ha concedido privilegios de acceso.
3. Para cambiar la información de esta pantalla, haga clic en **Atrás** y realice los cambios necesarios en las pantallas correspondientes. Haga clic en **Finalizar** para volver a la página de Configuración de protección de Guardián de archivos.

Add Guarded File Wizard, página 1

En esta pantalla, puede agregar archivos o grupos de archivos para que Guardián de archivos los proteja; también puede especificar qué programas tienen acceso a los archivos protegidos.

Para agregar archivos a la lista Archivos protegidos:

1. Haga clic en **Agregar nuevos elementos**.
2. Haga clic en la flecha junto al cuadro de lista desplegable para seleccionarlos elementos que desea agregar:
   - **Archivos**–Agregar archivos individuales. Por ejemplo, agregar Hojadecálculo.xls a la lista de Archivos protegidos. Puede indicarle a Guardián de archivos que codifique los archivos para que no puedan leerse los datos que contienen.
   - **Carpetas**–Agregar carpetas individuales. Por ejemplo, agregar Mis documentos a la lista Archivos protegidos.
   - **Grupos de archivos**–Agregar grupos de archivos. Es posible que no tenga grupos de archivos en su equipo.
   - **Tipos de archivos**–Agregar extensiones de archivos a la lista de Archivos protegidos. Por ejemplo, si selecciona la extensión de archivo .doc, Guardián de archivos agregará todos los archivos con la extensión .doc a la lista Archivos protegidos y los protegerá.
   - **Unidades**–Agregar unidades a la lista Archivos protegidos. Por ejemplo, agregue c:\ a la lista Archivos protegidos para que Internet Guard Dog proteja todos los archivos y carpetas de la unidad c.

Después de asignar archivos, carpetas y unidades a la lista Archivos protegidos, puede seleccionar qué programas tendrán acceso a estos archivos y carpetas, o esperar hasta que alguno acceda al archivo. Internet Guard Dog mostrará un mensaje de alerta a partir del cual podrá autorizar a un programa el acceso a un archivo protegido.

Para asignar privilegios de acceso a los archivos, las carpetas y las unidades de la lista Archivos protegidos:

1. Haga clic en **Autorizar el acceso del programa a**.
2. Haga clic en la flecha junto al cuadro de lista desplegable para visualizar una lista de los archivos, las carpetas y las unidades que han sido agregadas a la lista Archivos protegidos y seleccione una entrada.
3. En el siguiente cuadro de Add Guarded File Wizard, utilice **Examinar** para encontrar el archivo ejecutable asociado al programa. Por ejemplo, si desea que Microsoft Word tenga acceso a todos los archivos con la extensión .doc, busque la carpeta que contiene Winword.exe.

Add Financial Information Wizard, página 1

Internet Guard Dog supervisará la información financiera incluida en Protector de identidad. Cuando un programa intente enviar esta información a través de Internet, Internet Guard Dog le alertará basándose en las opciones seleccionadas en las siguientes pantallas del asistente.

Para agregar información financiera a Protector de identidad:

1. Haga clic en la flecha junto al cuadro de lista desplegable **Tipo** y seleccione uno de los siguientes elementos:
   - **VISA**–Selecciónelo para introducir un número de tarjeta de crédito Visa en Protector de identidad.
   - **Master Card**–Selecciónelo para introducir un número de tarjeta Master Card en Protector de identidad.
   - **Discover**–Selecciónelo para introducir un número de tarjeta Discover en Protector de identidad.
   - **AMEX**–Selecciónelo para introducir un número de tarjeta American Express en Protector de identidad.
   - **Cuenta bancaria**–Selecciónelo para introducir un número de cuenta bancaria en Protector de identidad.
   - **Intermediación**–Selecciónelo para introducir un número de cuenta de intermediación en Protector de identidad.
   - **Tarjeta telefónica**–Selecciónelo para introducir un número de tarjeta telefónica en Protector de identidad.
   - **Otra**–Selecciónelo para introducir cualquier otro tipo de información financiera en Protector de identidad.
2. Haga clic en **Siguiente** para visualizar la siguiente pantalla del asistente.

Add Financial Information Wizard- VISA página 2

Para agregar un número de tarjeta de crédito VISA a Protector de identidad:

1. Escriba una palabra o frase que le sirva para identificar la tarjeta en el cuadro **Descripción**.
2. Escriba el número de la tarjeta de crédito Visa en los cuadros **Número de tarjeta Visa**. El cursor salta automáticamente de un cuadro al siguiente.
3. Seleccione una de las siguientes acciones de Internet Guard Dog:
   - **Permitir siempre**–Seleccione esta opción si no desea que Internet Guard Dog le avise cuando esta información financiera sea enviada a través de Internet.
   - **Bloquear siempre**–Seleccione esta opción si no desea que esta información financiera sea enviada a través de Internet.
   - **Preguntar antes de bloquear**–Seleccione esta opción si desea decidir qué hacer en cada caso. Internet Guard Dog emitirá un mensaje de alerta cuando detecte que esta información financiera va a ser enviada a través de Internet.

Add Financial Information Wizard - Master Card, página 2

Para agregar un número de tarjeta de crédito Master Card a Protector de identidad:

1. Escriba una palabra o frase que le sirva para identificar la tarjeta en el cuadro **Descripción**.
2. Escriba el número de la tarjeta de crédito Master Card en los cuadros **Número de tarjeta Master Card**. El cursor salta automáticamente de un cuadro al siguiente.
3. Seleccione una de las siguientes acciones de Internet Guard Dog:
   - **Permitir siempre**–Seleccione esta opción si no desea que Internet Guard Dog le avise cuando esta información financiera sea enviada a través de Internet.
   - **Bloquear siempre**–Seleccione esta opción si no desea que esta información financiera sea enviada a través de Internet.
   - **Preguntar antes de bloquear**–Seleccione esta opción si desea decidir qué hacer en cada caso. Internet Guard Dog emitirá un mensaje de alerta cuando detecte que esta información financiera va a ser enviada a través de Internet.

Add Financial Information Wizard- Tarjeta Discover, página 2

Para agregar un número de tarjeta de crédito Discover a Protector de identidad:

1. Escriba una palabra o frase que le sirva para identificar la tarjeta en el cuadro **Descripción**.
2. Escriba el número de la tarjeta de crédito Master Card en los cuadros **Número de tarjeta Discover**. El cursor salta automáticamente de un cuadro al siguiente.
3. Seleccione una de las siguientes acciones de Internet Guard Dog:
   - **Permitir siempre**–Seleccione esta opción si no desea que Internet Guard Dog le avise cuando esta información financiera sea enviada a través de Internet.
   - **Bloquear siempre**–Seleccione esta opción si no desea que esta información financiera sea enviada a través de Internet.
   - **Preguntar antes de bloquear**–Seleccione esta opción si desea decidir qué hacer en cada caso. Internet Guard Dog emitirá un mensaje de alerta cuando detecte que esta información financiera va a ser enviada a través de Internet.

Add Financial Information Wizard - American Express, página 2

Para agregar un número de tarjeta de crédito American Express:

1. Escriba una palabra o frase que le sirva para identificar la tarjeta en el cuadro **Descripción**.
2. Escriba el número de la tarjeta de crédito American Express en los cuadros **Número de tarjeta American Express**.
3. Seleccione una de las siguientes acciones de Internet Guard Dog:
   - **Permitir siempre**–Seleccione esta opción si no desea que Internet Guard Dog le avise cuando esta información financiera sea enviada a través de Internet.
   - **Bloquear siempre**–Seleccione esta opción si no desea que esta información financiera sea enviada a través de Internet.
   - **Preguntar antes de bloquear**–Seleccione esta opción si desea decidir qué hacer en cada caso. Internet Guard Dog emitirá un mensaje de alerta cuando detecte que esta información financiera va a ser enviada a través de Internet.

Add Financial Information Wizard - Cuenta bancaria, página 2

Para agregar un número de cuenta bancaria:

1. Escriba una palabra o frase que le sirva para identificar la cuenta en el cuadro **Descripción**.
2. Escriba el número de una cuenta bancaria en los cuadros **Número de cuenta bancaria**.
   Deberá hacer clic en los cuadros para desplazar el cursor de uno a otro.
3. Seleccione una de las siguientes acciones de Internet Guard Dog:
   - **Permitir siempre**–Seleccione esta opción si no desea que Internet Guard Dog le avise cuando esta información financiera sea enviada a través de Internet.
   - **Bloquear siempre**–Seleccione esta opción si no desea que esta información financiera sea enviada a través de Internet.
   - **Preguntar antes de bloquear**–Seleccione esta opción si desea decidir qué hacer en cada caso. Internet Guard Dog emitirá un mensaje de alerta cuando detecte que esta información financiera va a ser enviada a través de Internet.

Add Financial Information Wizard - Intermediación, página 2

Para agregar un número de intermediación:

1. Escriba una palabra o frase que le sirva para identificar la cuenta de intermediación en el cuadro **Descripción**.
2. Escriba el número de una cuenta de intermediación en los cuadros **Número de cuenta de intermediación**.
3. Seleccione una de las siguientes acciones de Internet Guard Dog:
   - **Permitir siempre**–Seleccione esta opción si no desea que Internet Guard Dog le avise cuando esta información financiera sea enviada a través de Internet.
   - **Bloquear siempre**–Seleccione esta opción si no desea que esta información financiera sea enviada a través de Internet.
   - **Preguntar antes de bloquear**–Seleccione esta opción si desea decidir qué hacer en cada caso. Internet Guard Dog emitirá un mensaje de alerta cuando detecte que esta información financiera va a ser enviada a través de Internet.

Add Financial Information Wizard - Tarjeta telefónica, página 2

Para agregar un número de tarjeta telefónica:

1. Escriba una palabra o frase que le sirva para identificar la tarjeta en el cuadro **Descripción**.
2. Escriba el número de la tarjeta telefónica en los cuadros **Número de tarjeta telefónica**.
   El cursor pasa automáticamente de un cuadro al siguiente.
3. Seleccione una de las siguientes acciones de Internet Guard Dog:
   - **Permitir siempre**–Seleccione esta opción si no desea que Internet Guard Dog le avise cuando esta información financiera sea enviada a través de Internet.
   - **Bloquear siempre**–Seleccione esta opción si no desea que esta información financiera sea enviada a través de Internet.
   - **Preguntar antes de bloquear**–Seleccione esta opción si desea decidir qué hacer en cada caso. Internet Guard Dog emitirá un mensaje de alerta cuando detecte que esta información financiera va a ser enviada a través de Internet.

Add Financial Information Wizard - Otro tipo de información, página 2

Para agregar otros números financieros importantes:

1. Escriba una palabra o frase que le sirva para identificar el número en el cuadro **Descripción**.
2. Escriba cualquier otro número importante en el cuadro **Número**.
3. Seleccione una de las siguientes acciones de Internet Guard Dog:
   - **Permitir siempre**–Seleccione esta opción si no desea que Internet Guard Dog le avise cuando esta información financiera sea enviada a través de Internet.
   - **Bloquear siempre**–Seleccione esta opción si no desea que esta información financiera sea enviada a través de Internet.
   - **Preguntar antes de bloquear**–Seleccione esta opción si desea decidir qué hacer en cada caso. Internet Guard Dog emitirá un mensaje de alerta cuando detecte que esta información financiera va a ser enviada a través de Internet.

Financial Information Wizard - Página Información de tarjeta de crédito, (no utilizar)

Para agregar un número de tarjeta de crédito a Protector de identidad:

1. Escriba el número de la tarjeta de crédito en los cuadros **Número de tarjeta de crédito**. Utilice la tecla tabulador para saltar de un cuadro al siguiente.
2. Introduzca una palabra o frase que le sirva para identificar la tarjeta.
3. Seleccione una de las siguientes acciones de Internet Guard Dog:
   - **Permitir siempre**–Seleccione esta opción si no desea que Internet Guard Dog le avise cuando esta información financiera sea enviada a través de Internet.
   - **Bloquear siempre**–Seleccione esta opción si no desea que esta información financiera sea enviada a través de Internet.
   - **Preguntar antes de bloquear**–Seleccione esta opción si desea decidir qué hacer en cada caso. Internet Guard Dog emitirá un mensaje de alerta cuando detecte que esta información financiera va a ser enviada a través de Internet.

Financial Information Wizard, página 3

La información introducida en las pantallas de Financial Information Wizard aparece en este cuadro.

Para cambiar esta información:

- Haga clic en **Atrás** para volver a la página adecuada del asistente. Haga clic en **Finalizar** para volver a la página de Configuración de protección de Protector de identidad.

Financial Information Wizard - Página Tipos (no utilizar)

Para agregar información financiera a Protector de identidad:

1. Haga clic en la flecha junto al cuadro de lista desplegable **Tipo** y seleccione el tipo de información financiera en la lista.

   Internet Guard Dog mostrará la página del asistente correspondiente a la elección que ha realizado en el cuadro de lista desplegable Tipo.
   Por ejemplo, si seleccionó Master Card, Internet Guard Dog mostrará una página en la que podrá introducir su número de tarjeta Master Card. Si seleccionó Tarjeta telefónica, aparecerá una página en la que podrá introducir un número de tarjeta telefónica.
2. Seleccione una de las siguientes acciones de Internet Guard Dog:
   - **Permitir siempre**–Seleccione esta opción si no desea que Internet Guard Dog le avise cuando esta información financiera sea enviada a través de Internet.
   - **Bloquear siempre**–Seleccione esta opción si no desea que esta información financiera sea enviada a través de Internet.
   - **Preguntar antes de bloquear**–Seleccione esta opción si desea decidir qué hacer en cada caso. Internet Guard Dog emitirá un mensaje de alerta cuando detecte que esta información financiera va a ser enviada a través de Internet.

Add Identity Information Wizard - página Dirección

Para agregar una dirección a Protector de identidad:

1. Complete la pantalla introduciendo en los siguientes cuadros la información correspondiente al nombre introducido en la pantalla de nombre Identity Protection Wizard:
   - **Calle**–Escriba el nombre y el número de la calle en este cuadro.
   - **Ciudad**–Escriba el nombre de la ciudad en este cuadro.
   - **Estado**–Escriba el estado o provincia/código postal en este cuadro.
   - **C.P.**–Escriba el código postal en este cuadro.
   - **País**–Escriba el nombre del país en este cuadro.
2. Haga clic en **Siguiente** para visualizar la pantalla **Más información**.

Add Identity Information Wizard - página Más información

Para agregar más información a Protector de identidad:

1. Haga clic en uno de los siguientes cuadros e introduzca la información correspondiente al nombre que ha introducido en la pantalla de nombre del Asistente de Protección de identidad:
   - **Número de seguridad social**
   - **Número de teléfono**
   - **Dirección de correo electrónico**
2. Seleccione una de las siguientes acciones:
   - **Permitir siempre**–Internet Guard Dog permite que la información introducida en esta página sea enviada a través de Internet.
   - **Bloquear siempre**–Internet Guard Dog bloquea todos los intentos de enviar esta información a través de Internet.
   - **Preguntar antes de bloquear**–Internet Guard Dog emitirá un mensaje de alerta cuando detecte que esta información va a ser enviada a través de Internet. El mensaje de alerta contiene opciones que le permiten decidir cómo continuar.

Nota

Si es necesario utilizar una contraseña de Internet Guard Dog, deberá introducirla antes de poder enviar la información protegida por Protector de identidad.

Add Identity Information Wizard - página Nombre

Internet Guard Dog necesita saber a quién tiene que proteger. Seguramente ha indicado su nombre durante la entrevista, y es posible que ahora desee editar algunos datos o agregar el nombre de otra persona. Internet Guard Dog puede proteger la información de todas las personas que utilizan el equipo al mismo tiempo que la suya.

Para agregar un nombre a Protector de identidad:

1. Introduzca el nombre en los cuadros correspondientes. Puede utilizar la tecla tabulador para desplazarse de un cuadro al siguiente.
   - **Nombre**–Escriba el nombre.
   - **Inicial del segundo nombre**–Escriba la inicial del segundo nombre.
   - **Apellido**–Escriba el apellido.
2. Haga clic en **Siguiente** para visualizar la página **Dirección**.

Nota

Deberá rellenar como mínimo uno de los cuadros de esta pantalla para poder continuar. No es necesario que rellene el resto de los cuadros del asistente.

Add Identity Information Wizard - página final

Internet Guard Dog reúne toda la información que ha introducido anteriormente en las pantallas del asistente y la visualiza en esta página para que pueda comprobarla. En caso de que alguno de los datos no sea correcto, haga clic en **Atrás** para volver a la pantalla correspondiente del asistente y realizar los cambios necesarios. Haga clic en **Finalizar** para volver a la página Configuración de protección de Protector de identidad.

Introducir contraseña para guardar página Wizard

Para introducir una nueva contraseña y un nuevo nombre de usuario en Administrar contraseñas:

Escriba la información en los siguientes cuadros. Utilice la tecla tabulador para desplazarse de un cuadro al siguiente.

- **Sitio Web**–Introduzca la URL del sitio Web con el que está conectando.
- **Nombre de usuario**–Introduzca el nombre de usuario que utiliza cada vez que se conecta con el sitio.
- **Contraseña**–Introduzca la contraseña que ha seleccionado para este sitio.

Sugerencia

La información que introduzca en este asistente será accesible desde Asistente de navegación. Para ahorrar tiempo y evitar los errores al escribir, puede arrastrar el nombre de usuario y la contraseña desde Asistente de navegación hasta los cuadros correspondientes del formulario de conexión a los sitios Web.

Para visualizarlo, haga clic con el botón derecho en el icono de Internet Guard Dog en la bandeja del sistema y seleccione **Asistente de navegación** en el menú desplegable.

Introducir contraseña para guardar página Editar

Para agregar una contraseña y un ID de usuario a Administrar contraseñas:

Haga clic en el cuadro que contiene la información que desea cambiar. Utilice la tecla tabulador para desplazarse de un cuadro al siguiente.

- **Sitio Web**–Introduzca la URL del sitio Web con el que está conectando.
- **Nombre de usuario**–Introduzca el nombre de usuario que utiliza cada vez que se conecta con el sitio.
- **Contraseña**–Introduzca la contraseña que ha seleccionado para este sitio.

Sugerencia

La información que introduzca en este asistente será accesible desde Asistente de navegación. Para ahorrar tiempo y evitar los errores al escribir, puede arrastrar el nombre de usuario y la contraseña desde Asistente de navegación hasta los cuadros correspondientes del formulario de conexión a los sitios Web.

Para visualizarlo, haga clic con el botón derecho en el icono de Internet Guard Dog en la bandeja del sistema y seleccione **Asistente de navegación** en el menú desplegable.

Add Scheduled Event Wizard - página Frecuencia

Para programar un suceso seleccionado:

Haga clic en una de las siguientes opciones:

- **Una vez**–En la siguiente pantalla del asistente, utilice las flechas para seleccionar la **Hora** y la **Fecha** en las que Internet Guard Dog deberá realizar el suceso seleccionado.
- **Cada hora**–En la siguiente pantalla del asistente, utilice las flechas que aparecen junto a **Y** para seleccionar la hora en la que Internet Guard Dog deberá realizar el suceso seleccionado. Por ejemplo, si selecciona 15, Internet Guard Dog realizará el suceso seleccionado a las 12:15, 1:15, y así sucesivamente.
- **Mensual**–En la siguiente pantalla del asistente, utilice las flechas junto al cuadro **Hora** para seleccionar el día del mes en el que Internet Guard Dog deberá realizar el suceso seleccionado. Por ejemplo, si selecciona 5, Internet Guard Dog realizará el suceso seleccionado el quinto día de cada mes.
- **Diario**–En la siguiente pantalla del asistente, utilice las flechas junto al cuadro **Hora** para seleccionar la hora del día y, a continuación, seleccione las casillas de verificación de los días de la semana en los que Internet Guard Dog deberá realizar el suceso seleccionado.
- **Semanal**–En la siguiente pantalla del asistente, utilice las flechas junto al cuadro **Hora** para seleccionar la hora del día y, a continuación, utilice la flecha del cuadro de lista **Cada** para seleccionar el día de la semana en el que Internet Guard Dog deberá realizar el suceso seleccionado.
- **Inactivo**–En la siguiente pantalla del asistente, utilice las flechas para seleccionar la **Hora** y la **Fecha** en las que Internet Guard Dog deberá realizar el suceso seleccionado. Esta es una opción adecuada si acostumbra a dejar el equipo encendido durante la noche. Puede programar un suceso que necesite mucho tiempo, como una comprobación completa de virus, para un momento en el que nadie esté utilizando el equipo.
- **Inicio**–Internet Guard Dog realizará la tarea programada cuando inicie el equipo.

Add Scheduled Event Wizard - página Una vez

Utilice las flechas para seleccionar la **Hora** y la **Fecha** en las que Internet Guard Dog deberá realizar el suceso seleccionado sólo una vez.

Add Scheduled Event Wizard - página Cada hora

Utilice las flechas que aparecen junto a **Y** para seleccionar la hora en la que Internet Guard Dog deberá realizar el suceso seleccionado. Por ejemplo, si selecciona 15, Internet Guard Dog realizará el suceso seleccionado a las 12:15, 1:15, y así sucesivamente.

Add Scheduled Event Wizard - página Cada mes

Utilice las flechas junto al cuadro **Hora** para seleccionar el día del mes en el que Internet Guard Dog deberá realizar el suceso seleccionado. Por ejemplo, si selecciona 5, Internet Guard Dog realizará el suceso seleccionado el quinto día de cada mes.

Add Scheduled Event Wizard - página Cada día

En la siguiente pantalla del asistente, utilice las flechas junto al cuadro **Hora** para seleccionar la hora del día y, a continuación, seleccione las casillas de verificación de los días de la semana en los que Internet Guard Dog deberá realizar el suceso seleccionado. Por ejemplo, si selecciona 1:15 a.m. y lunes y viernes, Internet Guard Dog realizará el suceso seleccionado a las 1:15 a.m. los lunes y los viernes.

Add Scheduled Event Wizard - página Cada semana

Utilice las flechas junto al cuadro **Hora** para seleccionar la hora del día y, a continuación, utilice la flecha del cuadro de lista **Cada** para seleccionar el día de la semana en el que Internet Guard Dog deberá realizar el suceso seleccionado. Por ejemplo, si selecciona 1:15 a.m. y lunes, Internet Guard Dog realizará el suceso seleccionado los lunes a las 1:15 a.m.

Add Scheduled Event Wizard - página Libre

Utilice las flechas para seleccionar la **Hora** y la **Fecha** en las que Internet Guard Dog deberá realizar el suceso seleccionado. Esta es una opción adecuada si acostumbra a dejar el equipo encendido durante la noche. Puede programar un suceso que necesite mucho tiempo, como una comprobación completa de virus, para un momento en el que nadie esté utilizando el equipo.

Add Scheduled Event Wizard - página final

Internet Guard Dog reúne toda la información que ha introducido sobre el suceso seleccionado y la visualiza en esta página. Si desea realizar algún cambio, haga clic en **Atrás** para volver a la pantalla correspondiente del asistente.

Add Scheduled Event Wizard, página 1

Para programar un suceso:

Haga clic en uno de los siguientes sucesos de la lista y, a continuación, en **Siguiente:**

- **Programar una detección de virus en todos los archivos**–Detecta la existencia de virus en todos los archivos de las unidades locales, incluyendo las unidades de disquete, los CD-ROM y las unidades multimedia extraíbles.
- **Programar una detección de virus en los archivos de alto riesgo**–Detecta la existencia de virus en los archivos de programa y de documentos de todas las unidades locales, incluyendo las unidades de disquete, los CD-ROM y las unidades multimedia extraíbles. Este suceso viene ya programado para que se produzca cuando se inicia Windows.
- **Programar una detección de virus en los archivos modificados** –Realiza una detección de virus sólo en los archivos que han sido creados o modificados después de la fecha y la hora de la última detección de virus. (Comprobará todos los archivos que no hayan sido comprobados anteriormente.)
- **Programar codificación de los archivos de Guardián de archivos**–Codifica los archivos incluidos en la lista Archivos protegidos de Guardián de archivos.
- **Programar descodificación de los archivos de Guardián de archivos**–Descodifica los archivos codificados incluidos en la lista Archivos protegidos de Guardián de archivos.
- **Programar la eliminación de los archivos eliminados de mi PC**– Sobreescribe los datos que quedan cuando se eliminan los archivos de forma permanente de la Papelera de reciclaje.
- **No olvide comprobar actualizaciones de Internet Guard Dog**–Cuando instale Internet Guard Dog, este suceso ya estará programado para producirse cada mes.

Internet Guard Dog muestra páginas adicionales del asistente que le permiten seleccionar una fecha y una hora para el suceso seleccionado.

Centinela de virus Buscar carpeta

Puesto que el proceso de detección de virus puede ser muy largo, puede controlar la cantidad de archivos que comprueba Centinela de virus añadiendo carpetas en la lista **No comprobar los archivos de estas carpetas**.

Para agregar carpetas a la lista No comprobar los archivos de estas carpetas:

- Haga clic en la carpeta y después en **Aceptar**.

Sugerencia

Ello afecta no sólo a las comprobaciones efectuadas en los archivos, sino también a la detección rápida de virus y a la Comprobación. De forma predeterminada, Internet Guard Dog no comprueba los archivos de la Papelera de reciclaje.

Editar lista de detecciones de virus - Archivos de documento

Si ha seleccionado Archivos de documento en el cuadro **Qué comprobar**, podrá **Agregar** o **Suprimir** los tipos de archivos de documento en los que Centinela de virus detectará la existencia de virus.

Para agregar un tipo de documento:

1. En la página Centinela de virus, seleccione **Archivos de documento** en la lista **Qué comprobar** y haga clic en **Editar**.
2. Haga clic en la ficha **Archivos de documento** y haga clic en **Agregar**.
3. En la siguiente pantalla, seleccione los tipos de documentos que desee que sean comprobados por Centinela de virus y haga clic en **Aceptar**.

Para suprimir tipos de documentos:

1. En la página Centinela de virus, seleccione Archivos de documento en la lista **Qué comprobar** y haga clic en **Editar**.
2. Haga clic en la ficha **Archivos de documento**, seleccione un tipo de documento de la lista y haga clic en **Suprimir**.

Editar lista de detecciones de virus

Centinela de virus puede comprobar tipos de documentos y programas específicos basándose en la selección realizada en el cuadro **Qué comprobar** de la página Configuración de protección de Centinela de virus.

Para agregar un tipo de programa:

1. En la página Centinela de virus, seleccione **Archivos de programa** en la lista **Qué comprobar** y haga clic en **Editar**.
   En la pantalla **Editar lista de detecciones de virus**, aparecerá de forma predeterminada la ficha **Archivos de programa**.
2. Haga clic en **Agregar**.
3. En **Agregar lista de detecciones de virus**, seleccione los tipos de programas y haga clic en **Aceptar**.

Para agregar un tipo de documento:

1. En la página Centinela de virus, seleccione **Archivos de documento** en la lista **Qué comprobar** y haga clic en **Editar**.
2. Haga clic en la ficha **Archivos de documento** para colocarla en primer plano y haga clic en **Agregar**.
3. En **Agregar lista de detecciones de virus**, seleccione los tipos de archivos de documento y haga clic en **Aceptar**.

Para agregar un tipo de archivo personalizado:

1. En la página Centinela de virus, haga clic en **Editar**.
2. Haga clic en **Personalizar**.
3. Escriba la extensión de archivo que desee comprobar y haga clic en **Aceptar**.

Para restablecer los tipos de archivos predeterminados que deben comprobarse:

1. En la página Centinela de virus, haga clic en **Editar**.
2. Haga clic en **Predeterminado**.

Para suprimir un tipo de programa:

1. En la página Centinela de virus, seleccione **Archivos de programa** en la lista **Qué comprobar** y haga clic en **Editar**.
   En la pantalla **Editar lista de detecciones de virus**, aparecerá de forma predeterminada la ficha **Archivos de programa**.
2. Haga clic en la ficha **Archivos de programa**, seleccione un tipo de programa de la lista y haga clic en **Suprimir**.

Para suprimir un tipo de documento:

1. En la página Centinela de virus, seleccione **Archivos de documento** en la lista **Qué comprobar** y haga clic en **Editar**.
2. Haga clic en la ficha **Archivos de documento** para colocarla en primer plano, seleccione un tipo de documento de la lista y haga clic en **Suprimir**.

Cambiar la contraseña de Internet Guard Dog

Puede hacer que cualquier persona que utilice el programa tenga que introducir una contraseña. Si ha introducido una contraseña durante la Entrevista, puede cambiarla mediante este asistente.

Para crear una contraseña de Internet Guard Dog

1. En el cuadro de diálogo **Introduzca la contraseña de Internet Guard Dog**, introduzca la contraseña que desee utilizar en el cuadro **Nueva contraseña**.
2. Introduzca la misma contraseña en el cuadro **Confirme la nueva contraseña**.
3. Introduzca una palabra que Internet Guard Dog pueda utilizar para recordarle la contraseña en el cuadro **Introduzca una palabra** y haga clic en **Aceptar**.

Para cambiar la contraseña de Internet Guard Dog:

1. En el cuadro de diálogo **Cambio de contraseña de Internet Guard Dog**, introduzca la contraseña que esté utilizando para acceder a Internet Guard Dog en el cuadro **Anterior contraseña**.
   Puede utilizar la tecla tabulador para desplazarse de un cuadro al siguiente.
2. Introduzca la misma contraseña en el cuadro **Nueva contraseña**.
3. Introduzca la misma contraseña en el cuadro **Confirme la nueva contraseña**.
4. Introduzca una palabra que le ayude a recordar la contraseña en el caso de que se le olvide y haga clic en **Aceptar**.
   La contraseña tendrá efecto desde el momento en que sea creada.

Agregar lista de detecciones de virus

Para agregar tipos de archivo con el fin de que Centinela de virus los compruebe:

- Seleccione los tipos de archivo en la lista y cuando haya terminado, haga clic en **Aceptar** para volver a la pantalla **Editar lista de detecciones de virus**.

Su entrada aparecerá al final de la lista en la ficha Archivos de programa.

Sugerencia

Para realizar selecciones múltiples de la lista de tipos de archivo, pulse MAYÚSCULAS+CLIC o CONTROL+CLIC.

Agregar una extensión personalizada para la detección de virus

Para agregar extensiones de archivo personalizadas con el fin de que Centinela de virus las compruebe:

- Escriba una extensión de archivo de tres letras en el cuadro y haga clic en **Aceptar** para volver a la pantalla **Editar lista de detecciones de virus**.

Su entrada aparecerá al final de la lista en la ficha Archivos de programa.

Nota

Las extensiones de archivo forman parte del nombre de los archivos. Windows utiliza la extensión de archivo para determinar qué tipo de información contiene el archivo. Si se trata de un archivo de documento, Windows utilizará la extensión de archivo para determinar los programas asociados al archivo. Windows no muestra de manera predeterminada la extensión de archivo como parte del nombre de archivo en Mi PC ni en el explorador de Windows.

Disco de emergencia de McAfee - Crear un disco de emergencia, página 1

Internet Guard Dog grabará la información de emergencia (archivos, programas y configuración de Internet Guard Dog) en la unidad que seleccione en esta lista. Cuando seleccione la unidad, deberá tener en cuenta una serie de cosas:

Sugerencia

Por norma, deberá seleccionar una unidad multimedia extraíble como, por ejemplo, la unidad de disquete. Si la información de emergencia está almacenada en una unidad de red, es posible que no pueda acceder a esa unidad cuando tenga problemas con su equipo.

Disco de emergencia de McAfee - Crear un disco de emergencia, página 2

Si ha seleccionado una unidad de disquete en la anterior pantalla del asistente, Internet Guard Dog almacenará la información de emergencia (archivos, programas y configuración de Internet Guard Dog) en tres disquetes de 1/2 pulg. con formato. Cuando el primer disco esté lleno, Emergency Disk Wizard mostrará un mensaje pidiéndole que inserte el segundo disco.

Para empezar a crear un disco de emergencia:

- Inserte un disco en la unidad de disquetes de su equipo y haga clic en **Siguiente**.

Sugerencia

Puede hacer clic en **Cancelar** para volver a la Entrevista o en **Atrás** para volver a la anterior página del asistente.

Disco de emergencia de McAfee - Crear un disco de emergencia, página 3

Internet Guard Dog necesitará algunos minutos para copiar la información de emergencia (archivos, programas y configuración de Internet Guard Dog) en la unidad que ha seleccionado. Si Internet Guard Dog está copiando los archivos en disquetes, cuando el primer disco esté lleno recibirá un mensaje indicándole que inserte el segundo disco.

Para continuar cuando Internet Guard Dog haya terminado de copiar la información:

- Haga clic en **Siguiente** para continuar con la siguiente página del asistente.

Para detener Internet Guard Dog mientras está copiando información:

- Haga clic en **Cancelar**.

Cuando Internet Guard Dog muestre un mensaje preguntándole si está seguro de querer detener el proceso, haga clic en **Sí** para volver a la Entrevista.

Disco de emergencia de McAfee - Crear un disco de emergencia, página 4

Internet Guard Dog ha terminado de copiar la información de emergencia.

Para finalizar el procedimiento de creación de un disco de emergencia:

- Haga clic en **Finalizar** para volver a la Entrevista.

Haga clic en **McAfee.com** para acceder al sitio Web de McAfee.
Nota: Antes de acceder al sitio, verifique que está correctamente conectado a Internet.

Funcionamiento de la configuración del usuario

Internet Guard Dog ofrece capacidades de conexión para varios usuarios. Un usuario designado como Administrador puede agregar, editar y eliminar perfiles de otros usuarios que navegan por Internet desde el mismo equipo. Consulte Administrador de Internet Guard Dog. Después de añadir perfiles a los usuarios, el Administrador puede personalizar su configuración de protección individual, incluidas las opciones de filtrado de Internet, pudiendo incluso supervisar sus hábitos de navegación.

En la pantalla inicial de Internet Guard Dog, haga clic en Configuración del usuario. Una vez visualizada la pantalla, aparecerá una lista de perfiles de usuario en el lado derecho de la ventana.

Para editar un perfil de usuario

1. Resalte el nombre del usuario en la lista mostrada en el cuadro de texto.
2. A continuación, haga clic en Editar opciones de usuario. En las pantallas sucesivas, escriba los cambios que desea aplicar.
3. Haga clic en Aplicar.

Para eliminar un perfil de usuario

1. Resalte el nombre del usuario en la lista mostrada en el cuadro de texto.
2. Una vez resaltado el nombre del usuario, haga clic en Eliminar usuario.
3. Haga clic en Aplicar.

Para crear un nuevo usuario

1. Haga clic en Agregar usuario.
2. En las pantallas siguientes, escriba la información correspondiente (p. ej. el nombre de inicio de sesión, la contraseña, las horas de Internet, etc.).
3. Haga clic en Aplicar.

   Nota: Mientras edita o agrega un perfil de usuario, también puede establecer opciones de filtrado de Internet como configuración de protección adicional para el usuario. Haga clic en Opción de filtro de Internet.

Sugerencia

Durante la entrevista, el Administrador también puede agregar perfiles de usuario y opciones de filtrado personalizadas; consulte Adición de un perfil de usuario mediante la Entrevista.

Utilización de McAfee VirusScan

Internet Guard Dog utiliza actualmente McAfee VirusScan para resolver los problemas relacionados con los virus de Internet. Esta función le permite establecer el modo de realizar una operación de detección de virus en el equipo; saber qué debe hacer en caso de detectar un virus y cómo debe avisarle una vez se detecta el virus. También puede utilizar VirusScan para conservar un registro de las acciones realizadas en el equipo.

Dispone de las siguientes funciones:

- **Scan** para iniciar inmediatamente la tarea de exploración predeterminada, o para configurar una tarea de exploración adaptada a sus necesidades.
- **Planificador** para iniciar el Planificador de McAfee VirusScan. Esta utilidad le permite configurar y ejecutar operaciones de exploración automáticas.
- **Virus info** para visualizar información de virus a través del sitio Web de McAfee.

Funcionamiento de las opciones de filtrado de Internet

Después de que el Administrador haya agregado o editado un perfil de usuario, se pueden aplicar las opciones de filtrado de Internet para personalizar todavía más la configuración de protección de usuarios individuales.

Para establecer las opciones de filtrado:

1. Haga clic en Configuración del usuario en la pantalla inicial de Internet Guard Dog.
2. Resalte un usuario con perfil asignado en la pantalla Configuración del usuario y, a continuación, haga clic en Editar opciones de usuario.
3. En la siguiente pantalla, haga clic en Filtrado de Internet y, en el menú desplegable, seleccione la opción de filtrado que desea utilizar (p. ej., Configurar Internet, Clasificar el contenido, Sitios Web, Filtro del contenido, Bloqueador de anuncios y Horarios de Internet).
4. Después de seleccionar qué opción desea utilizar, aparecerá la ventana correspondiente. Seleccione la restricción disponible que desea aplicar.
5. Haga clic en Aplicar.

Internet Guard Dog ha creado una base de datos de sitios Web y filtros de contenidos, así como una clasificación del contenido, con del fin de utilizarla para proteger la privacidad y la seguridad de los usuarios de Internet. Pero, al igual que el Administrador, usted también puede editar o agregar palabras y sitios Web a la lista .

Para obtener más información, consulte:

- Configurar Internet
- Clasificar el contenido
- Sitios Web
- Filtro del contenido
- Bloqueador de anuncios
- Horarios de Internet

Configurar Internet

Esta pantalla le permite activar o desactivar rápidamente los filtros de Internet Guard Dog.

Seleccione una de las siguientes opciones visualizadas:

- **Permitir el acceso a Internet**. Seleccione esta opción para permitir que el usuario acceda a Internet en cualquier momento.
- **Filtrar el acceso a Internet**. Seleccione esta opción para restringir el acceso del usuario a Internet.
- **Utilizar limpiador de búsquedas**. Seleccione esta opción para filtrar automáticamente determinado contenido (p. ej., palabras y frases).
- **Activar Bloqueador de anuncios**. Seleccione esta opción para bloquear determinados anuncios que no desea que vea el usuario.
- **Permitir Chat**. Seleccione esta opción para permitir que el usuario se conecte a salas de "chat".
- **Filtrar Chat**. Seleccione esta opción para permitir que el usuario se conecte a salas de chat, pero desea filtrar determinado contenido (p. ej. palabras y frases).

Clasificar el contenido

Esta pantalla le permite controlar qué tipo de contenido de Internet se permite ver al usuario.

Si desea ver o cambiar Clasificar el contenido:

1. Para ver la clasificación del contenido, seleccione Clasificar el contenido en el menú desplegable de opciones de Filtrado de Internet.
2. La siguiente pantalla muestra los diferentes sistemas de clasificación utilizados (p. ej., Drogas, Juegos, Desnudos, etc.).
3. Si desea cambiar la definición de la clasificación, haga clic en una Clasificación de la ventana de desplazamiento. A continuación, haga clic y arrastre la barra de deslizamiento para cambiar la definición. A medida que desliza la barra, aparece la definición correspondiente en el cuadro de diálogo de la parte inferior de la pantalla.
4. Repita el paso anterior para cambiar la configuración.
5. Haga clic en Aplicar.

Sitios Web

Esta pantalla le permite controlar los sitios Web a los que se permite o se prohibe el acceso al usuario.

Si desea agregar sitios Web

1. En la pantalla Sitios Web, escriba la dirección del sitio Web y haga clic en Permitir. Si la dirección ya se encuentra en la base de datos de Internet Guard Dog, el sistema le indicará , ‘‘Sitio ya introducido’’. De lo contrario, la dirección se añadirá a la lista y el sistema emitirá el mensaje ‘‘Gracias’’.
2. Repita el paso anterior para agregar otra dirección.
3. Haga clic en Aplicar.

Si desea bloquear sitios Web

1. Seleccione un sitio Web del cuadro de texto.
2. Haga clic en Bloquear.
3. Repita el paso anterior para bloquear otro sitio Web.
4. Al terminar, haga clic en Aplicar.

Filtro del contenido

Esta pantalla le permite filtrar los sitios Web y mensajes chat que no desea que vea el usuario.

Si desea ver, agregar o editar un filtro de contenido

1. En la ventana Filtro del contenido se muestran una serie de listas de contenido.
   - Si desea agregar una palabra, haga clic en la categoría de contenido correspondiente y, a continuación, en Agregar.
   - Si desea editarla, seleccione una categoría y haga clic en Editar.
2. Repita los pasos anteriores para agregar palabras o cambiar la clasificación correspondiente.
3. Haga clic en Aplicar.

Bloqueador de anuncios

Esta pantalla le permite configurar Internet Guard Dog para filtrar anuncios de páginas Web que no desea que vea el usuario.

- Para agregar una subserie bloqueada, haga clic en Agregar y siga las instrucciones de la pantalla.
- Para editar una subserie bloqueada existente, selecciónela en el cuadro de texto y haga clic en Editar. Siga las instrucciones de la pantalla.
- Para suprimir una subserie bloqueada, selecciónela en el texto y haga clic en Suprimir. Al terminar, haga clic en Aplicar.

Horarios de Internet

Esta pantalla le permite controlar los horarios en que se permite al usuario el acceso a Internet.

Si desea seleccionar las horas en que un usuario puede acceder a Internet:

1. En la ventana Horarios de Internet, aparece un gráfico con los días y las horas de una semana. En este gráfico puede permitir o bloquear el acceso de un usuario a Internet.
2. Seleccione la hora y el día correspondiente para un usuario con perfil asignado.
3. A continuación, haga clic en Permitir para que el usuario pueda acceder a Internet o en Prohibir para que no pueda acceder a Internet, según los días y las horas seleccionados en el gráfico.
4. Haga clic en Aplicar.

Novedades de Internet Guard Dog

La versión 3.0 de Internet Guard Dog proporciona más y mejores funciones, que le permiten realizar las tareas sin problema alguno. Se han incluido componentes adicionales con el fin de mejorar el grado de privacidad y seguridad mientras navega por Internet. La principal interfaz se ha rediseñado, para que pueda navegar a través de las diferentes utilidades con el simple clic de un botón.

Funciones nuevas

- **McAfee VirusScan**

  Internet Guard Dog utiliza actualmente McAfee VirusScan, que detecta el 100% de los virus que pueden encontrarse en disquetes, descargas de Internet, documentos adjuntos al correo electrónico, intranets, archivos compartidos, CD-ROM y servicios en línea (incluso en el interior de los tipos de archivo comprimidos más conocidos).

- **Configuración del usuario e inicio de sesión para varios usuarios**

  Internet Guard Dog permite actualmente que varios usuarios dispongan de diferentes configuraciones de protección. El usuario principal puede actuar como Administrador para crear perfiles para otros usuarios del mismo equipo y personalizar su configuración de protección.

- **Filtrado de Internet**

  Después de que un Administrador haya añadido perfiles de otros usuarios del mismo equipo, también dispondrá de las opciones de filtrado de Internet que aumentan la protección frente a las diferentes amenazas de Internet (p. ej., lista de palabras, sitios URL, etc.).

- **Actividad del usuario**

  Internet Guard Dog es capaz de generar diversos informes para el Administrador, que le permiten ver su actividad o la de otros usuarios con perfil asignado creados por él en función de sus preferencias de configuración de la privacidad y la seguridad. De esta forma, podrá ver cualquier informe de actividad (por ejemplo, la fecha y la hora en que se conectó y desconectó un usuario), mantenimiento y violación (por ejemplo, un usuario que intenta transferir un número de tarjeta de crédito) con un simple clic del botón.

- **Mejora de la interfaz de Ayuda en línea**

  La nueva versión de Internet Guard Dog presenta la Ayuda en línea en una ventana de Ayuda de visualización de Explorer que consta de tres paneles. Mientras se visualiza un tema del archivo de Ayuda, el usuario puede ver también la tabla de contenidos y acceder simultáneamente al índice y a las opciones de búsqueda de texto mientras el tema aparece en el lado derecho de la ventana.

Haga clic para acceder a la ventana **Configuración del usuario**. Puede agregar, editar y borrar el perfil del usuario, así como configurar opciones de filtrado de Internet que indiquen diversas restricciones, tales como el bloqueo de sitios Web a los que no permite acceder; la utilización de una lista de palabras para seleccionar o agregar palabras a las que los perfiles no deben tener acceso y el bloqueo de archivos adjuntos de correo electrónico.

Haga clic para acceder a las funciones de **Privacidad y Seguridad** de Internet Guard Dog.

- **Pantalla Privacidad**

  En esta pantalla puede establecer las siguientes funciones de privacidad de Internet Guard Dog:

  - **Protector de identidad,** para avisarle antes de que se envíe información confidencial a través de Internet.
  - **Bloqueador de cookies,** para impedir que los sitios Web almacenen cookies en su disco duro.
  - **Limpiador de rastros de Internet,** para eliminar los rastros de la navegación por Internet, tales como direcciones URL y archivos de historial generados al navegar por Internet.

- **Pantalla Seguridad**

  En esta pantalla puede establecer las siguientes funciones de seguridad de Internet Guard Dog:

  - **Vigilante,** para controlar que los programas del equipo no acceden a Internet sin su conocimiento.
  - **Guardián de archivos,** para impedir que los archivos confidenciales sean abiertos, renombrados o movidos sin su consentimiento.
  - **Administrar contraseñas** le permite almacenar en una ubicación segura diversos nombres y contraseñas de conexión a sitios Web.

Haga clic para iniciar McAfee VirusScan. Gracias a sus componentes, podrá establecer tareas de detección de virus basándose en sus preferencias; configurar operaciones de exploración; y visualizar información acerca de los virus a través del sitio Web de McAfee.

Administrador de Internet Guard Dog

Puesto que Internet Guard Dog ofrece ahora capacidades de conexión para varios usuarios, esta función permite a un usuario actuar como administrador de las configuraciones de seguridad, protección e información personal introducidas en el equipo a través de las funciones de Internet Guard Dog. Esta función resulta especialmente útil si, por ejemplo, desea filtrar o bloquear determinado tipo de información a la que no desea que sus hijos puedan acceder a través de Internet.

La creación de una cuenta de Administrador sólo puede realizarse a través de la función Entrevista de Internet Guard Dog. Únicamente el Administrador puede cambiar la información privada y la configuración del equipo. Tras finalizar esta configuración, el Administrador puede agregar otros usuarios y establecer niveles de protección y seguridad para cada perfil de usuario.

Nota: El Administrador también puede designar a otro usuario como Autoadministrador (consulte Autoadministrador) o simplemente agregar perfiles de otros usuarios (consulte Adición de un perfil de usuario mediante la Entrevista).

Para crear una cuenta de Administrador:

1. En la pantalla Administrador de Internet Guard Dog visualizada mediante la Entrevista, escriba el nombre del Administrador en el cuadro de texto correspondiente.
2. A continuación, escriba una contraseña. Únicamente mediante esta contraseña será posible cambiar toda la información privada y la configuración del equipo.

   Nota: No olvide su contraseña. Si la ha olvidado, no tendrá más remedio que reinstalar Internet Guard Dog y volver a empezar. Perderá la configuración de Internet Guard Dog anterior, la información de Administrar contraseñas, y no podrá utilizar ninguno de los archivos codificados.
3. Haga clic en Siguiente y pase a las siguientes pantallas de la Entrevista. Asegúrese de escribir la información adecuada cuando se le indique.
4. Haga clic en Finalizar.

Autoadministrador

El Administrador puede designar a otro usuario como Autoadministrador. Es posible que desee utilizar esta función si, por ejemplo, uno de los usuarios con perfil asignado es un adulto y tiene la suficiente confianza en él para responsabilizarle de establecer o modificar el modo en que las funciones de Internet Guard Dog deben protegerle al navegar por Internet.

Este usuario puede acceder a las funciones de Internet Guard Dog y modificar su propia configuración de seguridad y protección, pero no la de otros usuarios.

Para crear un Autoadministrador:

1. En la pantalla Agregar usuario de Internet Guard Dog visualizada mediante la Entrevista, escriba el nombre del usuario en el cuadro de texto correspondiente.
2. A continuación, escriba una contraseña.

   Nota: Asegúrese de que ni usted ni el usuario olvidan la contraseña asignada. Si la olvidan, no tendrán más remedio que reinstalar Internet Guard Dog y volver a empezar. Perderán la configuración de Internet Guard Dog anterior, la información Administrar contraseñas, y no podrán utilizar ninguno de los archivos codificados.
3. En la pantalla Autoadministración, seleccione Sí, deseo que este usuario pueda administrar su propia cuenta.
4. Haga clic en Siguiente y pase a las siguientes pantallas de la Entrevista. Asegúrese de escribir la información adecuada cuando se le indique.
5. Haga clic en Finalizar.

Adición de un perfil de usuario mediante la Entrevista

Como Administrador de Internet Guard Dog, puede agregar perfiles y personalizar la configuración de protección de otros usuarios del mismo equipo mediante la Entrevista.

Para agregar perfiles de usuario y personalizar su configuración de protección:

1. Inicie la Entrevista de Internet Guard Dog
2. En la pantalla Agregar usuario de Internet Guard Dog, escriba el nombre del usuario en el cuadro de texto adecuado; a continuación, asigne y escriba una contraseña en el cuadro de texto correspondiente. Si desea designar a este usuario como Autoadministrador, marque la casilla de verificación correspondiente. Consulte Autoadministrador.
3. En la pantalla Nivel de seguridad de Internet Guard Dog, asigne un nivel de seguridad para este usuario (es decir, Máximo, Mínimo o Personalizado).

   Nota: Internet Guard Dog tiene una configuración de protección predeterminada para los niveles de seguridad máximo o mínimo. Si desea ver lo que se activa al seleccionar cualquiera de estos niveles de seguridad, haga clic en **Mostrar qué se activa al elegir la seguridad máx o mín**.
4. En la pantalla Acceso a Internet, puede seleccionar bloquear, permitir o personalizar el total acceso del usuario a Internet.
5. Si selecciona el acceso a Internet Personalizado, aparece la pantalla Bloquear y Filtrar, en la que puede indicar qué tipo de funciones y materiales relacionados con Internet deben bloquearse o filtrarse cuando este usuario navega por Internet. Seleccione una de las opciones disponibles (p. ej., filtrar chat, bloquear correo electrónico, bloquear anuncios, etc.).
6. Si ha seleccionado utilizar las opciones de filtrado, aparecerá la pantalla Métodos de filtro, en la que podrá seleccionar otros métodos de filtro disponibles (es decir, Utilizar lista de palabras censurables, Utilizar lista de URL censurables o Utilizar sistema de clasificación).

   Nota: Como Administrador, también se le permite agregar opciones de cualquiera de los listados predeterminados (p. ej., palabras, sitios URL, etc.), pero sólo puede hacerlo mientras se encuentra en la ventana Opciones de filtro de Internet de la pantalla inicial, y no durante la Entrevista. Consulte Funcionamiento de las opciones de filtrado de Internet.
7. Si desea agregar otro perfil de usuario, haga clic en el botón Atrás de la pantalla visualizada para retroceder a la pantalla Agregar usuario de Internet Guard Dog. También puede ir directamente a la ventana Configuración del usuario a través de la pantalla principal de Internet Guard Dog para agregar usuarios. Consulte Funcionamiento de la Configuración del usuario.

Pantalla de configuración del usuario

La pantalla Internet Guard Dog – Configuración del usuario le permite agregar, eliminar o editar perfiles de usuario, así como aplicar opciones de privacidad, seguridad y filtrado de Internet para usuarios individuales, con el fin de protegerlos mientras navegan por Internet.

Nota: Únicamente el Administrador puede configurar cualquiera de estas opciones.

Aparecerán las siguientes funciones:

- **Agregar usuario**

  Permite agregar un perfil de usuario (es decir, nombre de inicio de sesión, contraseña, etc.). Consulte Funcionamiento de la Configuración del usuario.

- **Eliminar usuario**

  Permite eliminar un perfil de usuario.

- **Editar opciones de usuario**

  Permite cambiar el perfil de usuario. Tras seleccionar esta función, las siguientes pantallas muestran las opciones de privacidad, seguridad, filtrado de Internet, etc., a las que puede aplicar los cambios que desea realizar.

  - **Privacidad**

    Permite aplicar o modificar la configuración de protección para un usuario concreto a través de cualquiera de las opciones de privacidad disponibles. Consulte Temas generales acerca de la configuración de protección de Internet Guard Dog.

    - **Pantallas Privacidad**

      En cualquiera de estas pantallas puede establecer las siguientes funciones de privacidad de Internet Guard Dog:

      - **Protector de identidad,** para avisarle antes de que se envíe información confidencial a través de Internet.
      - **Bloqueador de cookies,** para impedir que los sitios Web almacenen cookies en el disco duro del equipo.
      - **Limpiador de rastros de Internet,** para eliminar los rastros de navegación por Internet, tales como direcciones URL y archivos de historial generados al navegar por Internet.

  - **Seguridad**

    Permite aplicar o modificar la configuración de protección de un usuario concreto a través de cualquiera de las opciones de seguridad disponibles. Consulte Temas generales acerca de la configuración de protección de Internet Guard Dog

    - **Pantallas Seguridad**

      En cualquiera de estas pantallas puede establecer las siguientes funciones de seguridad de Internet Guard Dog:

      - **Vigilante,** para controlar el acceso a Internet de los programas del equipo sin su conocimiento.
      - **Guardián de archivos,** para impedir que los archivos confidenciales se abran, renombren o muevan sin su consentimiento.

        - **Administrar contraseñas,** para almacenar en una ubicación segura diversos nombres y contraseñas de conexión a sitios Web.
    - **Filtro de Internet**

      Haga clic para aplicar las opciones de filtrado de Internet para un usuario concreto. Consulte Funcionamiento de las opciones de filtro de Internet.
    - **Opciones**

      Si desea cambiar su contraseña o la configuración de las alertas, o bien instalar otros paquetes de idiomas que Internet Guard Dog puede utilizar para filtrar sitios Web, haga clic en Opciones y seleccione una opción del menú desplegable. Consulte Utilización de las opciones de Internet Guard Dog.
- **Ayuda**

  Si desea ver el sistema de Ayuda de Internet Guard Dog o visualizar un tema de Ayuda específico en la pantalla en la que está trabajando, haga clic en Ayuda y seleccione una opción del menú desplegable. Consulte Acerca del menú Ayuda.

Administrador

Internet Guard Dog permite a un usuario actuar como Administrador de la configuración de la seguridad, protección e información personal introducida en el equipo. Esta función resulta especialmente útil si, por ejemplo, desea filtrar o bloquear determinado tipo de información a la que no desea que sus hijos puedan acceder a través de Internet.

La creación de una cuenta de Administrador sólo puede realizarse a través de la función Entrevista de Internet Guard Dog. Únicamente el Administrador puede cambiar la información privada y la configuración del equipo. Tras finalizar esta configuración, el Administrador puede agregar otros usuarios y establecer niveles de protección y seguridad para cada perfil de usuario.

Configurar usuario

Puede configurar Internet Guard Dog para un usuario específico o crear un perfil de usuario desde esta pantalla.

- Si desea cambiar la configuración de un usuario existente, haga clic en el nombre de usuario tal como aparece en el cuadro de texto Usuario de Internet Guard Dog y después haga clic en Siguiente. Siga las instrucciones de las sucesivas pantallas. Escriba los cambios correspondientes.
- Si desea crear otro perfil de usuario, haga clic en el botón Crear. Siga las instrucciones de las sucesivas pantallas. Escriba los cambios correspondientes.

Crear nuevo usuario

Tras hacer clic en Agregar usuario en la pantalla Configuración del usuario, esta ventana le permite introducir información acerca del nuevo usuario.

1. Escriba el nombre del usuario en el cuadro de texto Nombre del nuevo usuario
2. Escriba la nueva contraseña del usuario en el cuadro de texto Contraseña.
3. Verifique la contraseña volviéndola a introducir en el cuadro de texto Verificar contraseña.
4. A continuación, en el cuadro de texto Sugerencia de contraseña, proporcione una descripción que Internet Guard Dog mostrará en caso de que usted o el usuario olviden la contraseña.
5. Haga clic en Siguiente y siga las instrucciones de las sucesivas pantallas. Escriba la información correspondiente según sea necesario.

Soporte de idiomas

Esta pantalla le permite añadir Paquetes de idiomas que mejoran la capacidad de Internet Guard Dog para filtrar el contenido en otros idiomas.

- Para agregar un paquete de idiomas, haga clic y siga las instrucciones de la pantalla.
- Para suprimir un paquete de idiomas existente, selecciónelo en el cuadro de texto y haga clic en Suprimir.
- Al terminar, haga clic en Aplicar.

Configurar alertas

Esta pantalla le permite seleccionar el sonido de alerta que Internet Guard Dog va a utilizar cuando detecte amenazas contra la privacidad o la seguridad.

1. En el cuadro de texto Sonidos de alerta, seleccione los sonidos de alerta disponibles en el menú desplegable. Haga clic en el icono de sonido si desea oír una prueba del sonido de alerta seleccionado. También puede hacer clic en Examinar para localizar un archivo de sonido que desea utilizar.
2. Si desea desactivar el sonido de alerta, haga clic en Activar sonido.
3. Al terminar, haga clic en Aplicar.

Consulte también Respuesta a las alertas de Internet Guard Dog.

Modificación de la contraseña

Esta pantalla le permite modificar la contraseña que ha establecido previamente.

1. Escriba la nueva contraseña en el cuadro de texto proporcionado.
2. Verifique la contraseña volviendo a introducirla en el cuadro de texto Reescriba.
3. Escriba una descripción de su contraseña en el cuadro de texto Sugerencia. Internet Guard Dog mostrará esta sugerencia cuando olvide su contraseña.
4. Al terminar, haga clic en Aplicar.

Consulte también, Acerca de Administrar contraseñas.

Nivel de seguridad

Esta pantalla le permite seleccionar el nivel de seguridad que más se ajusta a sus hábitos informáticos.

- **Seguridad máxima** le protege de cualquier contenido dañino.
- **Seguridad mínima** le protege de contenido potencialmente dañino y le permite decidir si desea continuar.
- **Seguridad personalizada** le permite personalizar el nivel de seguridad de un usuario.
- **Copiar la configuración de seguridad de** le permite copiar y aplicar un nivel de seguridad de un usuario a otro usuario.

Haga clic en Ver configuración de seguridad para visualizar la configuración de seguridad.