MCAFEE

Internet Guard Dog

para Windows 95 y Windows 98

Manual del usuario

CONTRATO DE LICENCIA

AVISO PARA TODOS LOS USUARIOS: LEA DETENIDAMENTE EL SIGUIENTE CONTRATO LEGAL ("CONTRATO"), PARA LA LICENCIA DEL SOFTWARE ESPECIFICADO ("SOFTWARE") DE NETWORK ASSOCIATES, INC. ("McAfee"). AL HACER CLIC EN EL BOTÓN ACEPTAR O AL INSTALAR EL SOFTWARE, EL USUARIO (YA SEA UN INDIVIDUO O UNA ENTIDAD INDIVIDUAL) ACEPTA VINCULARSE POR ESTE ACUERDO Y FORMAR PARTE DEL MISMO. SI NO ESTÁ DE ACUERDO CON TODOS LOS TÉRMINOS DE ESTE CONTRATO, HAGA CLIC EN EL BOTÓN QUE INDICA QUE NO ACEPTA LOS TÉRMINOS DE ESTE CONTRATO Y NO INSTALE EL SOFTWARE. (EN CASO APLICABLE, PUEDE DEVOLVER EL PRODUCTO AL ESTABLECIMIENTO DE COMPRA Y SE LE REEMBOLSARÁ EN SU TOTALIDAD).

1. **Concesión de la Licencia.** Sujeto al pago de las tasas de licencia correspondientes y a los términos y condiciones de este Contrato, McAfee le otorga por el presente documento el derecho no exclusivo e intransferible a utilizar una copia de la versión especificada del Software y de la documentación que le acompaña (la "Documentación"). Se le autoriza a instalar una copia del Software en un equipo, estación de trabajo, asistente digital personal, localizador, "teléfono inteligente" u otro dispositivo electrónico para el que se haya diseñado el Software (conocidos todos ellos como "Dispositivos Cliente"). Si el Software se ha concedido bajo licencia como un conjunto o agrupación de más de un producto especificado del Software, esta licencia será

aplicable a todos los productos especificados del Software, estando sujeta a las restricciones o condiciones de uso especificadas en la lista de precios correspondiente o en el embalaje del producto que se aplique a cualquiera de estos productos del Software individualmente.

a. **Utilización.** El Software se ha concedido bajo licencia como un único producto y no se permite su utilización en más de un Dispositivo Cliente ni por más de un usuario a la vez, exceptuando lo establecido en esta Sección 1. El Software se está "utilizando" en un Dispositivo Cliente cuando está cargado en la memoria temporal (es decir, memoria de acceso aleatorio o RAM) o instalado en la memoria permanente (por ej., en un disco duro, CD-ROM, u otro dispositivo de almacenamiento) de dicho Dispositivo Cliente. Esta licencia le autoriza a realizar una copia del Software con la única finalidad de realizar una copia de seguridad o archivo, siempre que la copia que realice contenga la totalidad de los avisos de propiedad del Software.

b. **Utilización de Servidor.** Puede utilizar este Software en un Dispositivo Cliente como un servidor ("Servidor") en un entorno de varios usuarios o de red ("Modo de Servidor") únicamente si dicha utilización se permite en la lista de precios correspondiente o en el embalaje del producto para el Software. Es necesaria una licencia aparte para cada Dispositivo Cliente o "asiento" que pueda conectarse al Servidor en cualquier momento, sin tener en cuenta si dichos Dispositivos Cliente o asientos bajo licencia están conectados, acceden o utilizan a la vez el Software. La utilización de software o hardware que reduzca el número de Dispositivos Cliente o asientos que acceden directamente o utilizan el Software (por ej., hardware o software de "multiplexing" o de "agrupación") no reduce el número necesario de licencias (es decir, el número de licencias necesario equivale al número de diferentes entradas a la "parte frontal" del software o hardware de multiplexing o agrupación). Si el número de Dispositivos Cliente o asientos que se pueden conectar al Software puede superar el número de licencias obtenidas, debe aplicar un mecanismo razonable para asegurar que su utilización del Software no supere los límites de uso especificados para las licencias que ha obtenido. Esta licencia le autoriza a realizar o descargar una copia de la Documentación para cada Dispositivo Cliente o asiento con licencia, siempre que cada una de estas copias contenga todos los avisos de propiedad de la Documentación.

c. **Licencias de volumen.** Si el Software se ha concedido bajo licencia con los términos de licencia de volumen especificados en la lista de precios correspondiente o en el embalaje del producto para el Software, puede realizar, utilizar e instalar tantas copias adicionales del Software en el número correspondiente de Dispositivos Cliente como autorice la licencia de volumen. Debe aplicar un mecanismo razonable que garantice que el número de Dispositivos Cliente en los que se ha instalado el Software no supere al número de licencias que ha obtenido. Esta licencia le autoriza a realizar o descargar una copia de la Documentación para cada copia adicional autorizada por la licencia de volumen, siempre que cada una de estas copias contenga la totalidad de los avisos de propiedad de la Documentación.

2. **Término.** Este Contrato es efectivo durante una duración ilimitada, a menos que se resuelva antes del tiempo tal como se establece en el presente documento. Este Contrato se resolverá automáticamente en caso de incumplimiento por su parte de alguna de las restricciones u otros requisitos aquí descritos. Una vez resuelto o expirado este Contrato, debe destruir todas las copias del Software y la Documentación. Puede rescindir este Contrato en cualquier momento, destruyendo todas las copias del Software y la Documentación.

3. **Actualizaciones.** Durante el período de tiempo especificado en la lista de precios correspondiente o el embalaje del producto para el Software, tiene derecho a descargar revisiones o actualizaciones del Software, siempre que McAfee las publique a través de su sistema de boletín electrónico, sitio

Web u otros servicios en línea. Durante un período de noventa (90) días a partir de la fecha de compra original del Software, tiene derecho a descargar una (1) revisión o actualización del Software cuando McAfee lo publique a través de su sistema de boletín electrónico, sitio Web u otros servicios en línea. Transcurrido el período de tiempo especificado, deja de tener derecho a recibir las revisiones y actualizaciones sin la compra de una nueva licencia o plan anual de actualización para el Software.

4. **Derechos de propiedad.** El Software está protegido por las leyes de Copyright de los EE.UU. y las disposiciones de los acuerdos internacionales. McAfee y sus proveedores poseen y retienen todos los derechos, títulos e intereses sobre el Software y del Software, incluidos todos derechos de Copyright, de patentes, de secreto comercial, de marcas registradas y otros derechos de propiedad intelectual. La posesión, instalación o utilización del Software por parte del usuario no le transfiere ningún derecho sobre la propiedad intelectual del Software; asimismo, no adquirirá ningún derecho sobre el Software, exceptuando lo establecido de modo explícito en el presente Contrato. Todas las copias del Software y la Documentación realizadas según lo estipulado en el presente Contrato deben contener los mismos avisos de propiedad que aparecen en el Software y en la Documentación.

5. **Restricciones.** Se prohíbe alquilar, otorgar en leasing, prestar o vender el Software. No debe permitir que terceros se beneficien de la utilización o funcionalidad del Software mediante un aprovechamiento por turnos, oficina de servicios u otro acuerdo, exceptuando la utilización especificada en la lista de precios correspondiente o embalaje del producto para el Software. No puede transferir ninguno de los derechos que se le han concedido por este Contrato. No se le permite realizar operaciones de ingeniería inversa, desmontaje o descompilación del Software, salvo hasta donde la restricción anterior se prohiba expresamente por la ley aplicable. No se le permite modificar ni crear obras derivadas basadas en parte del Software o en su totalidad. No se le permite copiar el Software ni la Documentación, salvo en lo que se le permita expresamente en la Sección 1 mencionada anteriormente. No se le permite eliminar los avisos de propiedad ni las etiquetas del Software. McAfee se reserva todos los derechos no establecidos de manera expresa en este documento. McAfee se reserva el derecho a realizar auditorías de forma periódica con un aviso previo por escrito, para verificar el cumplimiento de los términos de este Contrato.

6. **Garantía y limitación de responsabilidad**

   a. **Garantía limitada.** McAfee garantiza que durante un período de sesenta (60) días a contar a partir de la fecha de compra original del producto, el soporte (por ej., disquetes) en el cual reside el Software no presentará ningún defecto de material ni de mano de obra.

   b. **Recursos del cliente.** Toda la responsabilidad de McAfee y sus proveedores y el recurso exclusivo del usuario por cualquier violación de la garantía anterior será, a elección de McAfee, (i) reembolsarle el precio de compra pagado por la licencia, (en caso de haberlo), o (ii) sustituir el soporte defectuoso en el que reside el Software. Debe devolver el soporte defectuoso a McAfee asumiendo usted los gastos con una copia del recibo. Esta garantía limitada se anula si el defecto se debe a accidente, abuso o aplicación incorrecta. Cualquier soporte de repuesto estará bajo garantía durante el período restante de la garantía original. Fuera de los EE.UU., este recurso no estará disponible en la medida en que McAfee está sujeto a las restricciones de las leyes y regulaciones de control de las exportaciones de los EE.UU.

c. **Limitación de responsabilidad de la garantía.** Exceptuando la garantía limitada mencionada anteriormente, EL SOFTWARE SE PROPORCIONA "TAL CUAL". HASTA LA MÁXIMA EXTENSIÓN PERMITIDA POR LA LEY APLICABLE, MCAFEE RENUNCIA A LA RESPONSABILIDAD DE TODAS LAS GARANTÍAS, TANTO IMPLÍCITAS COMO EXPLÍCITAS, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIABILIDAD, IDONEIDAD PARA UN OBJETIVO CONCRETO Y NO VIOLACIÓN CON RESPECTO AL SOFTWARE Y LA DOCUMENTACIÓN QUE LE ACOMPAÑA. EL COMPRADOR ASUME LA RESPONSABILIDAD DE SELECCIONAR EL SOFTWARE PARA CONSEGUIR LOS RESULTADOS DESEADOS, ASÍ COMO DE LA INSTALACIÓN, UTILIZACIÓN Y RESULTADOS OBTENIDOS DEL SOFTWARE. SIN LIMITAR LAS ANTERIORES DISPOSICIONES, MCAFEE NO GARANTIZA QUE EL SOFTWARE ESTÉ LIBRE DE ERRORES O DE INTERRUPCIONES U OTROS FALLOS NI QUE CUMPLIRÁ SUS REQUISITOS. ALGUNOS ESTADOS Y JURISDICCIONES NO PERMITEN LA LIMITACIÓN DE GARANTÍAS IMPLÍCITAS, POR LO QUE LA LIMITACIÓN ANTES MENCIONADA PUEDE NO APLICÁRSELE EN SU CASO. Las disposiciones anteriores serán obligatorias hasta la extensión máxima permitida por la ley aplicable.

7. **Limitación de la responsabilidad.** BAJO NINGUNA CIRCUNSTANCIA Y NINGUNA TEORÍA LEGAL, YA SEA EN ACTO DELICTIVO, CONTRATO U OTRA CIRCUNSTANCIA DIFERENTE, MCAFEE O SUS PROVEEDORES SERÁN RESPONSABLES FRENTE AL USUARIO O A CUALQUIER OTRA PERSONA POR LOS DAÑOS INDIRECTOS, ESPECIALES, FORTUITOS, DERIVADOS O DE CUALQUIER TIPO, INCLUIDOS, SIN LIMITARLOS, LOS DAÑOS POR PÉRDIDA DE CLIENTELA, INTERRUPCIÓN DEL TRABAJO, ERROR O FUNCIONAMIENTO INCORRECTO DEL EQUIPO NI POR NINGÚN OTRO DAÑO O PÉRDIDA. EN NINGÚN CASO SERÁN RESPONSABILIDAD DE MCAFEE LOS DAÑOS EN EXCESO DEL PRECIO DE LA LISTA QUE MCAFEE CARGA POR UNA LICENCIA DE SOFTWARE, AUNQUE MCAFEE HAYA SIDO ADVERTIDO DE LA POSIBILIDAD DE DICHOS DAÑOS. ESTA LIMITACIÓN DE RESPONSABILIDAD NO SE APLICARÁ A LA RESPONSABILIDAD POR MUERTE O DAÑOS PERSONALES HASTA LA EXTENSIÓN QUE LA LEY APLICABLE PROHIBA DICHA LIMITACIÓN. ADEMÁS, ALGUNOS ESTADOS Y JURISDICCIONES NO PERMITEN LA EXCLUSIÓN O LIMITACIÓN DE DAÑOS FORTUITOS O DERIVADOS, DE MODO QUE ESTA LIMITACIÓN Y EXCLUSIÓN PUEDE NO APLICÁRSELE EN SU CASO. Las disposiciones anteriores serán obligatorias hasta la extensión máxima permitida por la ley aplicable.

8. **Gobierno de los EE.UU.** El Software y la Documentación que le acompaña se consideran "software informático comercial" y "documentación de software informático comercial" respectivamente, según la normativa DFAR Sección 227.7202 y FAR Sección 12.212, siempre que sea aplicable. Cualquier utilización, modificación, reproducción, lanzamiento, funcionamiento, visualización o revelación del Software y su Documentación por el Gobierno de los EE.UU. se regirá únicamente por los términos de este Contrato y se prohibirá salvo hasta donde los términos de este Contrato lo permitan expresamente.

9. **Controles de exportación.** No está permitido descargar ni exportar o reexportar el Software ni la Documentación, así como tampoco la tecnología o información básica, (i) a (o a un nacional o residente de) Corea del Norte, Cuba, Irán, Irak, Libia, Sudán, Siria o cualquier otro país al que EE.UU. haya embargado mercancías, ni (ii) a ningún miembro de la lista de Naciones

Designadas Especialmente del Departamento del Tesoro de los Estados Unidos o de la Tabla de Pedidos Denegados del Departamento de Comercio de los Estados Unidos. La descarga o utilización del Software implica que está de acuerdo con lo anteriormente estipulado y que certifica que no se encuentra ni está bajo el control de ninguno de dichos países ni en ninguna de las listas y que no es un nacional ni reside en dichos países.

ADEMÁS, DEBE ESTAR INFORMADO DE LO SIGUIENTE: LA EXPORTACIÓN DEL SOFTWARE PUEDE ESTAR SUJETA AL CUMPLIMIENTO DE LAS NORMAS Y REGULACIONES PROMULGADAS CADA CIERTO TIEMPO POR LA OFICINA DE ADMINISTRACIÓN DE EXPORTACIÓN, DEPARTAMENTO DE COMERCIO DE LOS ESTADOS UNIDOS, QUE RESTRINGEN LA EXPORTACIÓN Y REEXPORTACIÓN DE DETERMINADOS PRODUCTOS Y DATOS TÉCNICOS. SI LA EXPORTACIÓN DEL SOFTWARE ESTÁ CONTROLADA POR ESTAS NORMAS Y REGULACIONES, EL SOFTWARE NO SE EXPORTARÁ NI SE REEXPORTARÁ DIRECTA NI INDIRECTAMENTE, (A) SIN TODAS LAS LICENCIAS DE EXPORTACIÓN O REEXPORTACIÓN Y LAS AUTORIZACIONES DE LOS ESTADOS UNIDOS U OTRAS ENTIDADES GUBERNAMENTALES NECESARIAS SEGÚN LAS LEYES APLICABLES NI(B) EN VIOLACIÓN DE CUALQUIER PROHIBICIÓN APLICABLE CONTRA LA EXPORTACIÓN O REEXPORTACIÓN DE CUALQUIER PARTE DEL SOFTWARE.

ALGUNOS PAÍSES TIENEN RESTRICCIONES PARA LA UTILIZACIÓN DE CODIFICACIÓN DENTRO DE SUS FRONTERAS, O PARA LA IMPORTACIÓN O EXPORTACIÓN DE CODIFICACIÓN, AUNQUE SÓLO SEA PARA USO COMERCIAL O PERSONAL TEMPORAL. DEBE SABER QUE LA IMPLANTACIÓN Y OBLIGATORIEDAD DE ESTAS LEYES NO SIEMPRE ES COHERENTE EN TODOS LOS PAÍSES. AUNQUE LOS SIGUIENTES PAÍSES NO SON UNA LISTA EXHAUSTIVA, PUEDEN EXISTIR RESTRICCIONES EN LA EXPORTACIÓN, IMPORTACIÓN O CODIFICACIÓN POR PARTE DE: COREA DEL SUR, ARABIA SAUDÍ, BÉLGICA, CHINA (INCLUIDO HONG KONG), FRANCIA, INDIA, INDONESIA, ISRAEL, RUSIA Y SINGAPUR. DEBE SABER QUE ES SU RESPONSABILIDAD FINAL EL CUMPLIMIENTO DE TODAS LAS LEYES DE EXPORTACIÓN GUBERNAMENTALES Y OTRAS LEYES APLICABLES Y QUE MCAFEE DEJA DE TENER RESPONSABILIDAD DESPUÉS DE LA VENTA INICIAL DENTRO DEL PAÍS ORIGINAL DE VENTA.

10. **Actividades de alto riesgo.** El Software no es tolerante a fallos y no está diseñado para ser utilizado en entornos peligrosos que requieren un funcionamiento a prueba de fallos, incluidos, aunque sin limitarse a éstos, el funcionamiento de las instalaciones nucleares, navegación aeronáutica o sistemas de comunicaciones, control del tráfico aéreo, sistemas de armamento, máquinas de soporte vital o cualquier otra aplicación en la que el fallo del Software pueda conducir directamente a la muerte, daños personales, daños físicos graves o daños a la propiedad (denominadas en su conjunto "Actividades de alto riesgo"). McAfee renuncia expresamente a la responsabilidad por cualquier garantía implícita o explícita de adecuación para Actividades de Alto Riesgo.

11. **Varios.** Este contrato se rige por las leyes de los Estados Unidos y del Estado de California, sin referencia a conflictos de los principios legales. La aplicación de la Convención de las Naciones Unidas sobre Contratos para la Venta Internacional de Mercancías se excluye de manera expresa. Este Contrato expone todos los derechos del usuario del Software y constituye el acuerdo total entre las partes. Este Contrato sustituye a cualquier otro comunicado respecto al Software y su Documentación. El presente Contrato no se puede modificar salvo mediante un apéndice por escrito emitido por un representante de McAfee debidamente autorizado. Ninguna

de las disposiciones anteriores se considerará renunciada, a menos que dicha renuncia se realice por escrito y esté firmada por McAfee o un representante de McAfee debidamente autorizado. Si alguna de las disposiciones de este Contrato se invalidase, el resto del Contrato continuaría siendo válido y estando en vigor. Las partes confirman que es su deseo que este Contrato se haya escrito solamente en Inglés.

12. **Contacto de los clientes con McAfee.** Si tiene preguntas sobre estos términos y condiciones, o desea ponerse en contacto con McAfee por cualquier otra razón, llame al número (408) 988 -3832, envíe un fax al número (408) 970 -9727, o escriba a: McAfee Software, 3965 Freedom Circle, Santa Clara, California 95054. http://www.mcafee.com.

    Las declaraciones efectuadas en el curso de esta venta están sujetas a la ley Year 2000 Information and Readiness Disclosure Act (Public Law 105-271). En caso de disputa, esta ley puede reducir sus derechos legales en relación con la utilización de cualquier declaración sobre la preparación para el Año 2000, a menos que se especifique lo contrario en el contrato o tarifa.

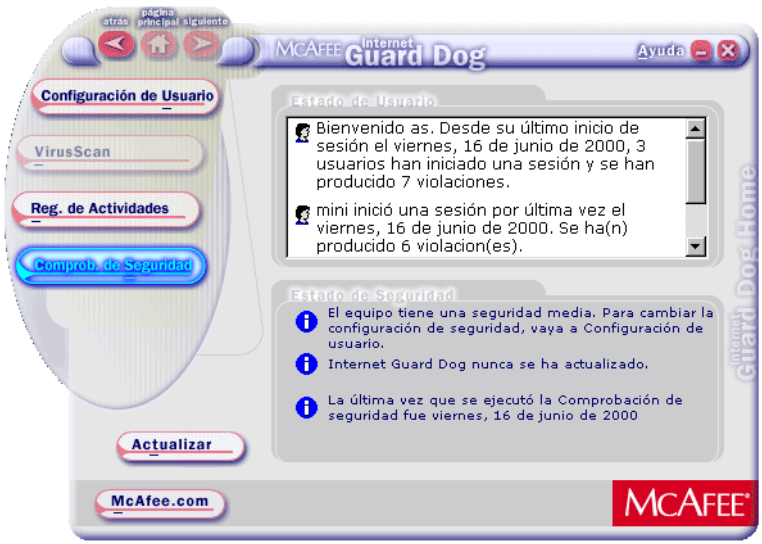
Contenido

Bienvenido a Internet Guard Dog™ 1

Utilización de Internet Guard Dog

En los últimos años, Internet ha pasado de ser una red de comunicaciones utilizada casi exclusivamente por los gobiernos y universidades a transformarse en una valiosa fuente de información utilizada por personas de todas las edades y profesiones. Con una cuenta de Internet, puede enviar correo electrónico (e-mail) a cualquier parte del mundo en tan sólo unos segundos, efectuar investigaciones sin salir de casa, conocer a nuevos amigos en una sala de conversación en línea o hacer compras desde su hogar.
Sin embargo, todas estas comodidades comportan un elemento de riesgo. Al utilizar Internet, la información se transmite de su equipo a otros equipos de Internet—información que puede no desear que posean otros usuarios. A su vez, estos equipos también pueden enviar archivos al suyo que contengan virus. Aunque la mayoría de estos archivos son inocuos, algunos pueden invadir su privacidad o incluso dañar los datos contenidos en la unidad de disco duro del equipo.

Figura 1-1. Pantalla inicial de Internet Guard Dog



Internet Guard Dog de McAfee evalúa los posibles riesgos mediante sus exhaustivas funciones ideadas para proteger la privacidad y seguridad al navegar por Internet.

Gracias a las nuevas funciones, también es posible actuar como administrador y aplicar los valores de protección personalizados no solamente a uno mismo, sino también a otros usuarios del equipo y supervisar fácilmente los posibles riesgos a los que pueden enfrentarse al navegar por Internet.

Funcionamiento de Internet Guard Dog

Internet Guard Dog utiliza las principales funciones que aparecen en la pantalla inicial:

Configuración de usuario

Como administrador, esta función permite configurar los valores de protección para otros usuarios del equipo. Es posible añadir, editar y eliminar un perfil de usuario para, a continuación, personalizar las opciones de privacidad, seguridad y filtrado de Internet que Internet Guard Dog aplicará cuando uno de estos usuarios navegue por la Web utilizando su equipo.

Consulte los siguientes apartados si desea obtener más información:

- “Personalización de la configuración de usuario” en la página 33.
- Capítulo 4, “Funciones de privacidad.”
- Capítulo 5, “Dispositivos de seguridad.”

VirusScan

Ahora, Internet Guard Dog utiliza McAfee VirusScan para resolver los problemas de virus que se encuentran al navegar por Internet. Esta función permite establecer cómo desea que se realice una operación de exploración de virus en el equipo; qué hacer si se detecta un virus y cómo avisarle que se ha detectado un virus. Asimismo, puede indicar a VirusScan que guarde un registro de las acciones que se llevan a cabo en el equipo.

Con las principales funciones de Internet Guard Dog, el usuario tiene el control en todo momento. El usuario decide qué funciones de seguridad y privacidad desea utilizar. Si el usuario cambia de hábitos o tiene otras prioridades, es fácil modificar los valores de protección de Internet Guard Dog para que se adapten a sus propias necesidades y a las de los demás usuarios que utilizan el equipo con frecuencia. Consulte “¿Qué es McAfee VirusScan?” en la página 53.

Registros de actividades

En la pantalla inicial de Internet Guard Dog, haga clic en Registro de actividades para ver una lista de las interacciones que usted y los demás usuarios del equipo han tenido con Internet Guard Dog, incluidas la fecha y la hora de la acción. Esta lista puede imprimirse, guardarse o borrarse. Consulte “Visualización de los registros de actividades” en la página 26.

Comprobación de seguridad

Esta función permite ejecutar una comprobación completa del equipo para detectar problemas de seguridad y privacidad. Una vez que Internet Guard Dog ha realizado la comprobación, muestra los problemas encontrados, proporciona información adicional acerca de los problemas y le guía durante la resolución del problema. Consulte “Cómo realizar una comprobación de seguridad” en la página 28.

Internet Guard Dog y la conexión en línea

Para utilizar todas las funciones de Internet Guard Dog, debe contar con una conexión a Internet a través de una red local o un módem. Algunas redes disponen de una conexión a Internet que puede utilizarse conectándose a la red directamente o a través de una conexión de acceso telefónico. Si no se conecta a través de una red, el equipo debe contar con un módem instalado.

Puede establecer una conexión a Internet a través de un Proveedor de servicios de Internet (ISP) como Earthlink. Un ISP actúa como intermediario entre el usuario e Internet. El equipo se conecta al equipo del ISP (mediante el módem), el cual a su vez se conecta a Internet. Asimismo, también puede conectarse a Internet a través de un servicio en línea como America Online o Compuserve.

Un requisito adicional es que debe disponer de un navegador. Un navegador es software, como Netscape Navigator o Microsoft Internet Explorer (debe tratarse de una versión diseñada para Windows 95 o Windows 98), que permite ver texto y gráficos y descargar archivos de los sitios Web.

Funciones de Internet Guard Dog

En este apartado se describen brevemente otras funciones de Internet Guard Dog que le protegen frente a la mayoría de amenazas más usuales de Internet. Si desea obtener más información secundaria sobre temas de privacidad, seguridad y virus de Internet, consulte el apartado "Seguridad y privacidad en Internet" en la página 59.

NOTA: Únicamente el administrador designado o el usuario con administración propia tienen acceso a estas funciones que les permiten personalizar sus valores de protección y en el caso del administrador, la protección de los demás usuarios del equipo.

Protección frente a las amenazas contra la privacidad

- **Protector de identidad** supervisa la conexión a Internet y le avisa antes de enviar información privada a un sitio de Internet poco seguro. Interrumpe el envío sin su consentimiento, a través de Internet, de su nombre y números de tarjetas de crédito, a otros programas y usuarios que utilizan el equipo (como sus hijos).
- **Bloqueador de cookies** impide que los sitios Web guarden cookies en la unidad de disco duro. Los sitios Web de otros fabricantes utilizan las cookies para hacer un seguimiento de sus hábitos de navegación por la Web. Con la función Bloqueador de cookies, puede elegir su nivel de interacción. (Para obtener más información, consulte el apartado "¿Qué son las cookies y cómo se utilizan?" en la página 70.)
- **Limpiador de rastros de Internet** borra el historial de conexiones de navegación por la Web—archivos almacenados en la memoria caché, lista de sitios URL (*Uniform Resource Locator*, conocidos también como direcciones Web) visitados, archivos de historial—cuando cierra el navegador. Esta función evita que los demás usuarios del equipo puedan realizar un seguimiento de sus operaciones en línea visualizando los archivos y las direcciones URL encontradas al navegar por Internet.
- **Filtro de búsqueda** impide que la información de búsqueda que solicita en un sitio Web pase al siguiente sitio que visite. Sin la función Filtro de búsqueda, el navegador puede transferir la información de búsqueda solicitada de un sitio Web a otro sin su conocimiento.

Protección frente a las amenazas contra la seguridad

- **La función Vigilante** permite controlar los programas que tienen acceso a la conexión a Internet. Los programas del PC pueden estar programados para acceder a Internet sin su consentimiento.
- **Guardián de archivos** impide abrir, renombrar, copiar, mover o eliminar los archivos que contienen datos confidenciales. Programas como ActiveX y Java, pueden explorar el PC para detectar información personal o eliminar archivos sin su permiso.

  Guardián de archivos también limita, mediante la codificación de archivos, el acceso a los archivos protegidos de programas especificados por el usuario. Puede limitar los programas que pueden acceder a los archivos de datos contables personales, datos bancarios en línea o datos fiscales.
- **Administrar contraseñas** guarda las contraseñas y nombres de registro inicio de sesión de sitios Web en una ubicación segura. Cuando visite un sitio que requiere esta información, arrástrelo desde el Asistente de navegación hasta el formulario visualizado en el navegador. Se acabó guardar los nombres de inicio de sesión y contraseñas en una ubicación poco segura como, por ejemplo, una nota pegada al monitor o un archivo de texto en el escritorio de Windows.

Protección frente a las amenazas de virus

Mediante McAfee VirusScan, dispondrá de las siguientes funciones:

- **Comprobar** para iniciar la tarea de exploración predeterminada inmediatamente o configurar una tarea de exploración según sus necesidades.
- **Planificador** para iniciar el Planificador de McAfee VirusScan. Esta utilidad permite configurar y ejecutar operaciones de exploración desatendidas.
- **Información de virus** para mostrar la información de virus a través del sitio Web de McAfee.

Novedades de Internet Guard Dog

La versión 3.0 de Internet Guard Dog incluye estas nuevas funciones.

- **Inclusión de McAfee VirusScan**
  Ahora, McAfee VirusScan se ha incorporado a Internet Guard Dog. Elija entre las opciones disponibles y personalizadas el tipo de protección que desea para su equipo.

- **Inicio de sesión de múltiples usuarios y configuración de usuario**
  Ahora Internet Guard Dog permite que distintos usuarios dispongan de configuraciones de protección diferentes. El usuario principal también puede actuar como administrador personalizando la configuración de los demás usuarios del equipo.

- **Opciones de filtrado de Internet**
  Una vez que un administrador ha añadido perfiles de otros usuarios del equipo, pueden utilizarse las opciones de filtrado de Internet según sitios URL predeterminados, lista de palabras, sistemas de clasificación y hora de acceso a Internet. El administrador también puede introducir listas adicionales o sitios Web si lo desea.

- **Registros de actividades**
  Un administrador puede ver una lista de actividades, registros de mantenimiento y violaciones con sólo hacer clic en un botón. Esta lista contiene información del tipo utilización del equipo o cualquier violación de la configuración de protección que hayan cometido los usuarios (por ejemplo, intentar utilizar un número de tarjeta de crédito). El administrador también puede borrar, imprimir o guardar esta lista.

- **Interfaz de ayuda en línea mejorada**
  La Ayuda en línea se muestra ahora mediante la ventana tripartita Ver Ayuda de Explorer. Al visualizar un tema del archivo Ayuda, ahora el usuario también puede visualizar la tabla de contenido y acceder al índice y a las opciones de búsqueda de texto simultáneamente mientras dicho tema aparece a la derecha de la ventana.

Otras funciones y mejoras

- **Contraseña de Internet Guard Dog**
  Impide ver o modificar la información y la configuración de Internet Guard Dog. También impide que otros usuarios que utilizan el equipo envíen información especificada como privada.
- **Mejora del Guardián de archivos**
  Protege archivos incluso cuando están codificados.
- **Mejora de la administración de cookies**
  Indica si las cookies son directas o indirectas y el dominio del cual proceden.
- **Protección de la identidad personal**
  Permite “Marcar” la información de identidad personal y archivos confidenciales (como registros financieros y números de tarjetas de crédito) de modo que no se envíen jamás a través de Internet sin su consentimiento.
- **Codificar archivos confidenciales**
  Permite añadir un nivel de protección adicional, codificando archivos para impedir su lectura hasta que los descodifique.
- **Mejora del Asistente de navegación**
  Guarde y administre las contraseñas de sitios Web en una ubicación segura y adecuada. El usuario ahora puede restablecer los números.
- **Botón Actualización única**
  Con un solo clic en un botón, el usuario puede actualizar Internet Guard Dog y McAfee VirusScan por medio de la Web.

Documentación acerca de Internet Guard Dog

Este manual proporciona la información básica necesaria para instalar, configurar y utilizar Internet Guard Dog. Se proporciona información más detallada acerca de Internet Guard Dog en los archivos de Ayuda a los que puede acceder mientras se encuentra en distintas ventanas.

Organización de este manual

Este Manual del usuario está diseñado para enseñarle a utilizar Internet Guard Dog con rapidez. Lea los capítulos 1 y 2 para instalar y ejecutar Internet Guard Dog. Sólo es necesario leer los capítulos 3, 4, 5 y 6 si desea obtener más información sobre la personalización de Internet Guard Dog o la utilización de funciones específicas. Lea el capítulo 7 si desea obtener más información acerca de McAfee VirusScan. Si hace poco que utiliza Internet o tan sólo desea tener más información sobre los asuntos de seguridad y privacidad en Internet, lea el Apéndice A.

Tabla 1-1.

Para averiguar	Lea
Qué acciones realiza esta versión de Internet Guard Dog y cómo buscar información sobre Internet Guard Dog.	Capítulo 1, “Bienvenido a Internet Guard Dog™.”
Los requisitos del sistema y cómo instalar Internet Guard Dog.	Capítulo 2, “Instalación de Internet Guard Dog™.”
Cómo utilizar las funciones principales de Internet Guard Dog.	Capítulo 3, “Un paseo rápido por Internet Guard Dog™.”
En qué consisten las funciones Bloqueador de cookies, Protector de identidad, Limpiador de rastros de Internet y Filtro de búsqueda y cómo trabajar con ellas.	Capítulo 4, “Funciones de privacidad.”
En qué consisten las funciones Vigilante, Guardián de archivos y Administrar contraseñas y cómo utilizarlas.	Capítulo 5, “Dispositivos de seguridad.”
En qué consisten las funciones VirusScan y cómo utilizarlas.	Capítulo 6, “McAfee VirusScan.”
Qué problemas de privacidad, seguridad y virus existen en Internet.	Apéndice A, “Seguridad y privacidad en Internet”
Cómo ponerse en contacto con los departamentos de ventas, el servicio al cliente y el soporte de McAfee Software.	Apéndice B, “Soporte del producto”

Utilización de la ayuda de Internet Guard Dog

Para iniciar la ayuda de Internet Guard Dog

1. En la pantalla inicial de Internet Guard Dog, haga clic en Ayuda y seleccione Temas de ayuda. El sistema de Ayuda se muestra mediante la ventana tripartita Ver de Explorer.
2. Puede realizar una búsqueda de un tema de ayuda mediante las fichas Contenido, Índice o Buscar.

   - **Ficha Contenido**

     1. Haga doble clic en un icono de libro para mostrar su tabla de contenido de temas relacionados.
     2. Localice el tema que desea y haga doble clic para abrir el tema de Ayuda.

   - **Ficha Índice**

     1. En el cuadro de texto, escriba las primeras letras de la palabra o frase que desea buscar.
     2. Localice lo que busca y haga doble clic en el tema o un solo clic en el botón Mostrar.

NOTA: Para pasar a la siguiente página de ayuda, haga clic en el botón Siguiente >> del examinador (si está activado). Para volver a la página anterior, haga clic en el botón Anterior << de navegación (si está activado) o haga clic en el botón Atrás.

   - **Ficha Buscar**

     Haga clic en la ficha Buscar para iniciar una búsqueda de texto completo. Si es la primera vez que se realiza una búsqueda de temas mediante la ficha Buscar, aparecerá Find Setup Wizard. Siga las instrucciones que aparecen en pantalla para configurar la opción de búsqueda de texto completo. Una vez finalizada la configuración:

     1. En el cuadro de texto, escriba las primeras letras de la palabra o frase que desea buscar. También puede seleccionar palabras coincidentes para limitar la búsqueda.
     2. Una vez localizado el texto que buscaba en el cuadro de visualización de temas, haga clic encima del mismo.

Para mostrar ayuda para una pantalla

1. En la pantalla inicial de Internet Guard Dog, haga clic en Ayuda.
2. Haga clic en Ayuda para que esta pantalla muestre un tema de ayuda que explica lo que puede hacer o qué puede necesitar saber sobre la pantalla actual de Internet Guard Dog.

Para obtener ayuda para la configuración de un cuadro de diálogo

- Cuando vea el botón  situado en el ángulo superior derecho de un cuadro de diálogo, haga clic en dicho botón y, a continuación, haga clic en la configuración para la que desea obtener la información.

Instalación de Internet Guard Dog™ 2

La mayoría de problemas de instalación se deben a que hay programas en ejecución mientras se intenta instalar nuevo software. Even if the installation appears normal, you won't be able to run the new program. Para evitar este tipo de problemas, antes de instalar Internet Guard Dog, cierre todos los programas, incluidos aquéllos que se ejecutan en segundo plano, como protectores de pantalla o detectores de virus.

Requisitos del sistema

Para utilizar Internet Guard Dog necesita lo siguiente:

- Un IBM PC o PC compatible que ejecute Windows 95 o Windows 98.
- 16 megabytes (MB) de RAM como mínimo.
- 20 MB de espacio libre en el disco duro para instalar Internet Guard Dog y McAfee VirusScan. Para instalar software de Internet opcional que puede estar incluido en la versión de CD, se necesitará más espacio en disco.
- Pantalla de vídeo con 256 colores o superior. Internet Guard Dog requiere una resolución de 800 x 600 píxeles (o superior) y una paleta de 32.000 colores (15 bits) o superior para contar con las condiciones óptimas de funcionamiento. Puede utilizarse con una paleta de 256 colores, pero es posible que se produzcan algunos cambios de color (debido al intercambio de paletas) al pasar de una aplicación a otra.
- Ratón de Microsoft o dispositivo señalador compatible.
- Acceso a Internet, bien a través de una cuenta de conexión con un ISP (Proveedor de servicios de Internet) o con una conexión permanente a través de una red.
- Navegador Web de Windows 95 o Windows 98 (denominado también navegador de 32 bits).

  Algunas funciones de Ayuda—McAfee Software en la Web, Internet Guard Dog en la Web, FAQ e Informe de un problema—requerirán que se conecte al sitio Web de McAfee Software con un navegador Web (software que permite ver documentos y transferir archivos de la World Wide Web). Para utilizar las funciones de soporte en línea, el navegador debe ser Microsoft® Internet Explorer, Netscape Navigator™, o America Online v3.0 (o una versión posterior) para Windows 95 o Windows 98.

NOTA: Los usuarios de America Online necesitan Winsock de 32 bits de AOL para utilizar Internet Guard Dog. Para actualizar un Winsock de 16 bits, póngase en contacto con America Online.

Instalación de Internet Guard Dog

Después de cerrar todos los programas abiertos, estará preparado para instalar Internet Guard Dog en el PC. La instalación debería realizarse sin problemas, sin embargo, si tuviera dificultades, consulte el apartado "Solución de problemas de instalación" en la página 13.

Para instalar Internet Guard Dog

1. Cierre todos los programas abiertos.
2. Introduzca el CD de Internet Guard Dog en la unidad de CD-ROM.
3. En la pantalla Configuración de Internet Guard Dog, haga clic en Instalar Internet Guard Dog.

   NOTA: Si la pantalla de configuración no se inicia automáticamente al cerrar la unidad de CD-ROM, haga clic en Inicio en la barra de tareas de Windows, haga clic en Ejecutar y escriba d:\setup. Si D no es la letra de la unidad de CD-ROM, escriba en su lugar la letra de unidad correcta.

4. Una vez finalizada la instalación, se inicia la función Entrevista de Internet Guard Dog. Siga las instrucciones que aparecen en pantalla y proporcione la información necesaria.

NOTA: El Administrador es el único que puede acceder a la función Entrevista de Internet Guard Dog. Para obtener más información, consulte los apartados "Utilización de la Entrevista de Internet Guard Dog" en la página 17.

Solución de problemas de instalación

Un intento de instalación fallido puede originar problemas de software que son difíciles de localizar. Las causas principales de los errores de instalación son:

- Errores en la unidad de disco duro
- Archivos temporales que entran en conflicto con la instalación
- Intento de instalación mientras hay otro software ejecutándose

Siga el procedimiento indicado a continuación para minimizar los efectos que estos conflictos habituales pueden tener en la instalación.

Paso 1: Limpiar la unidad de disco duro

Ejecute las utilidades de la unidad de disco duro de Windows 95, ScanDisk y Desfragmentador de disco para identificar y resolver los errores del disco duro:

1. Haga clic en Inicio en la barra de tareas de Windows, señale Programas, a continuación Accesorios y, por último, Herramientas del sistema y haga clic en ScanDisk.
2. En la ventana ScanDisk, seleccione Estándar y Reparar errores automáticamente.

NOTA: Ésta es la configuración predeterminada.

---

3. Haga clic en Avanzado. En el cuadro de diálogo Opciones avanzadas, asegúrese de que los siguientes valores están seleccionados:
   - Sólo si se encuentran errores
   - Reemplazar informe
   - Eliminar
   - Liberar
4. Ignore las demás opciones y haga clic en Aceptar. Haga clic en Iniciar. ScanDisk empieza a explorar la unidad para detectar la existencia de errores. Según el tamaño de la unidad de disco duro, ScanDisk puede tardar varios minutos en realizar esta función.
5. Cuando ScanDisk haya finalizado, cierre ScanDisk.

6. Haga clic en Inicio en la barra de tareas de Windows, señale Programas y a continuación Accesorios y, por último, Herramientas del sistema y haga clic en Desfragmentador de disco.
7. Haga clic en Aceptar para iniciar el Desfragmentador de disco. Según la velocidad del equipo y el tamaño de la unidad, este proceso puede tardar varios minutos en finalizar.
8. Cierre el Desfragmentador de disco cuando éste haya terminado de desfragmentar el disco.

Paso 2: Suprimir archivos temporales

Suprima el contenido de la carpeta Temp de Windows:

1. Haga doble clic en el icono Mi PC del escritorio. Se abrirá la ventana Mi PC. Haga doble clic en la unidad C: Ello le permitirá ver el contenido de la unidad de disco duro.
2. Haga doble clic en la carpeta Windows.
3. En dicha carpeta, haga doble clic en la carpeta Temp.
4. En el menú, haga clic en Edición y, a continuación, en Seleccionar todo. Todos los elementos de la carpeta Temp estarán ahora resaltados.
5. Pulse la tecla Supr del teclado para eliminar los archivos. Si Windows le pregunta si desea eliminar los archivos, haga clic en Sí.
6. En la barra de tareas de Windows, haga clic en Inicio y, a continuación, en Apagar el sistema.
7. Haga clic en Reiniciar el equipo y, a continuación, haga clic en Sí en el cuadro de diálogo Salir de Windows para reiniciar el equipo.

Paso 3: Cerrar otro software

Desactive todo el software que se está ejecutando en segundo plano:

1. Mantenga pulsadas las teclas Control y Alt del teclado, y pulse una vez la tecla Supr. Aparece el cuadro de diálogo Cerrar programa.
2. Haga clic en Finalizar tarea para cada elemento de la lista salvo Explorer.
3. Repita los pasos 2 y 3 hasta que haya cerrado todo salvo Explorer.
4. Cuando sólo vea Explorer en el cuadro de diálogo Cerrar programas, haga clic en cancelar.

   Ahora está preparado para instalar el nuevo software.

Instalación de McAfee VirusScan desde el CD de Internet Guard Dog

El CD de Internet Guard Dog contiene una copia de McAfee VirusScan.

Para instalar McAfee VirusScan

1. Introduzca el CD de Internet Guard Dog en la unidad de CD-ROM.
2. En la pantalla Configuración de Internet Guard Dog, haga clic en Instalar McAfee VirusScan.
3. Siga las instrucciones que aparecen en la pantalla.

Un paseo rápido por Internet Guard Dog™ 3

Internet Guard Dog es un programa fácil de usar. En este capítulo se tratan los aspectos principales que deben tenerse en cuenta al utilizar Internet Guard Dog. En primer lugar, el lector debe responder a algunas preguntas mediante la Entrevista para que Internet Guard Dog pueda utilizar sus funciones con eficacia y protegerle de las amenazas de Internet.

Utilización de la Entrevista de Internet Guard Dog

Aunque Internet Guard Dog está configurado para utilizar la configuración de seguridad y privacidad adecuada para la mayoría de usuarios, algunas funciones requieren que el usuario introduzca algunos datos. La Entrevista proporciona un medio sencillo de personalizar la configuración de Internet Guard Dog.

Las pantallas de la entrevista proporcionan datos sobre una función de Internet Guard Dog, le solicitan que introduzca información o preguntan sobre el modo en que desea que Internet Guard Dog responda a determinadas situaciones. (Figura 3-1.)

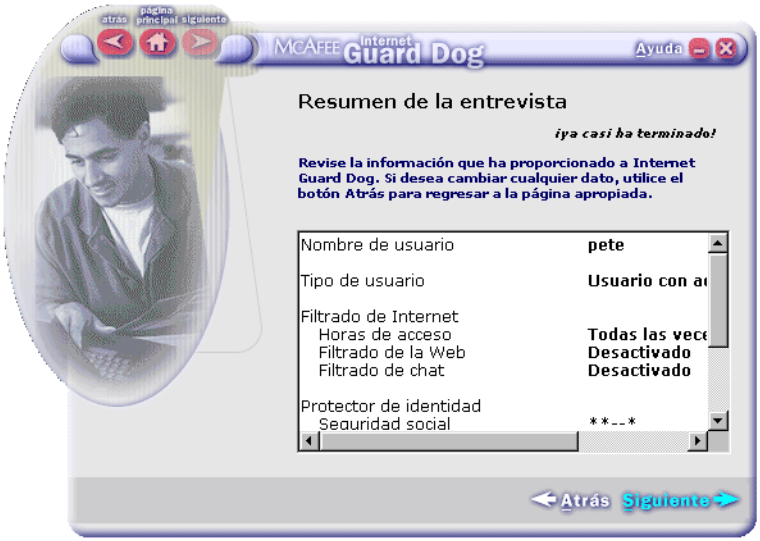


Figura 3-1. Internet Guard Dog Pantalla Entrevista

En todas las pantallas de la entrevista, podrá hacer clic en Atrás para volver a una pantalla anterior o en Siguiente para pasar a la siguiente pantalla. En la última pantalla de la entrevista, haga clic en Finalizar para guardar la configuración que ha seleccionado y cerrar la Entrevista.

¿Qué información me pide que introduzca Internet Guard Dog?

La entrevista de Internet Guard Dog le pide que introduzca la información personal y financiera que desea proteger. Toda la información introducida en Internet Guard Dog se guarda en formato codificado en el disco duro: jamás se envía a McAfee Software.

Es posible que desee reunir sus datos personales antes de iniciar la entrevista. Durante la Entrevista, Internet Guard Dog permite introducir:

- Una contraseña que se utiliza para proteger la información de Internet Guard Dog.
- Información personal y financiera que desea proteger para que no se envíe a través de Internet sin su consentimiento:
    - Nombre
    - Dirección
    - Número de la seguridad social
    - Número de teléfono
    - Dirección de correo electrónico
    - Otros datos financieros tales como los números de cuenta bancaria, cuenta de intermediación, tarjeta de crédito, tarjeta telefónica, etc.
- Las contraseñas y nombres de inicio de sesión de sitios Web que desea guardar en Administrar contraseñas.
- Información acerca de los demás usuarios del equipo. Como administrador podrá crear perfiles de usuarios y establecer la configuración de protección que Internet Guard Dog utilizará cuando el usuario navegue por Internet mediante su equipo. Consulte “Funcionamiento del Administrador de Internet Guard Dog” en la página 19.

Para obtener la protección óptima de Protector de identidad, incluya todos los guiones (por ejemplo, en el número de la seguridad social, cuentas bancarias, cuentas de correduría y tarjetas de débito). Por ejemplo, si introduce 123-45-6789 como número de la seguridad social, Guard Dog lo reconocerá con o sin guiones. Si introduce 123456789, Guard Dog no le avisará si se envía el número con guiones (123-45-6789). En el caso de las tarjetas de crédito no es necesario introducir guiones porque los números se escriben en casillas separadas.

> **NOTA:** Puede ajustar la configuración de las funciones de seguridad, privacidad y antivirus de Internet Guard Dog en Configuración de la protección. Haga clic en **Opciones** de la pantalla inicial de Internet Guard Dog y, a continuación, haga clic en **Configuración de la protección**.

Funcionamiento del Administrador de Internet Guard Dog

Dado que Internet Guard Dog ofrece ahora la capacidad de conexión de múltiples usuarios, esta función permite que un usuario actúe como administrador de la información personal, configuración de protección y configuración de seguridad que se realizan a través de las funciones de Internet Guard Dog. Esta función es especialmente útil, por ejemplo, para filtrar, bloquear o supervisar determinados tipos de información a la que no desea que sus hijos accedan al navegar por Internet.

La creación de una cuenta de Administrador de Internet Guard Dog sólo puede realizarse en la función Entrevista de Internet Guard Dog. Asimismo, únicamente el administrador designado puede acceder a la información y configuración de protección del equipo y modificarlas.

Una vez realizada la configuración, el administrador puede añadir otros usuarios y establecer los niveles de seguridad y protección para cada perfil de usuario.

> **NOTA:** Al añadir perfiles de usuario, el administrador puede designar un usuario como usuario con administración propia.

Consulte la Ayuda en línea de Internet Guard Dog para ver las instrucciones detalladas acerca de cómo establecer una cuenta de administrador.

Usuario con administración propia

Administrador de Internet Guard Dog puede designar otros usuarios como usuarios con administración propia. Esta función puede utilizarse, por ejemplo, en el caso de un usuario adulto que se considera suficientemente responsable para personalizar sus propias configuraciones de privacidad y protección.

Este usuario será el único que pueda acceder a las funciones de Internet Guard Dog y modificar su configuración.

Consulte la Ayuda en línea de Internet Guard Dog para ver las instrucciones detalladas acerca de cómo designar un usuario como usuario con administración propia.

Funcionamiento de la protección mediante contraseñas de Guard Dog

Al iniciar Windows, Internet Guard Dog solicitará que introduzca la contraseña que estableció durante la Entrevista. Si introduce una contraseña incorrecta, Guard Dog mostrará la sugerencia que proporcionó al crear la contraseña.

Sin la contraseña, todavía podrá abrir la pantalla inicial de Guard Dog, pero no podrá modificar la Configuración de comprobación ni la Configuración de la protección. Internet Guard Dog tampoco le permitirá utilizar la información de Administrar contraseñas de Asistente de navegación ni enviar información protegida por Protector de identidad.

ADVERTENCIA: No olvide su contraseña. Si la olvidara, su única opción es volver a instalar Internet Guard Dog y empezar de nuevo. Perderá la anterior configuración de Internet Guard Dog, la información de Administrar contraseñas y no podrá utilizar ninguno de los archivos codificados.

Utilización de la pantalla inicial de Internet Guard Dog

Tras finalizar la entrevista, Internet Guard Dog muestra su pantalla inicial (Figura 3-2).

Figura 3-2. Internet Guard Dog Pantalla inicial

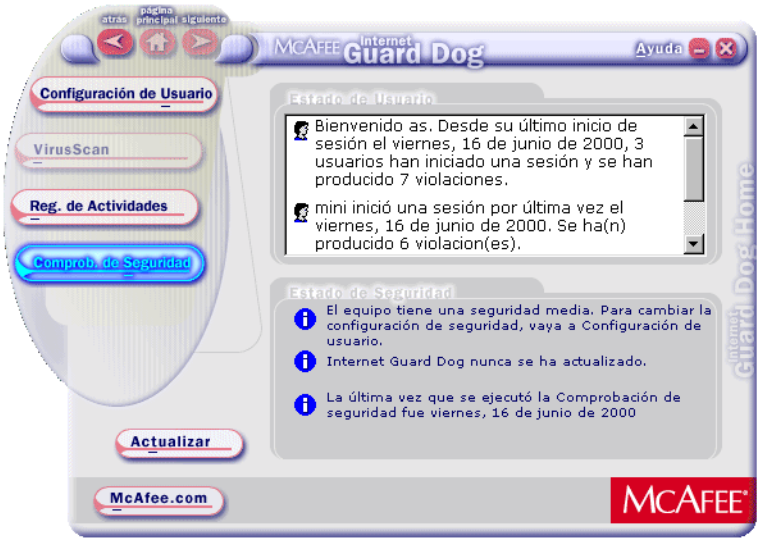


Tabla 3-1. Acciones que se pueden realizar en la pantalla inicial

Para	Haga clic en
Añadir, editar o eliminar un perfil de usuario, establecer el filtrado de Internet y otras opciones.	Configuración de usuario
Realizar o programar una exploración de virus.	VirusScan. Se inicia McAfee VirusScan
Realizar una comprobación de seguridad para detectar problemas de privacidad o seguridad en el equipo.	Comprobación de seguridad
Mostrar registros de actividades del usuario.	Registros de actividades
Mostrar la pantalla inicial de McAfee Software en el navegador de Web.	Ayuda y, a continuación, seleccionar McAfee Software en la Web

Tabla 3-1. Acciones que se pueden realizar en la pantalla inicial

Para	Haga clic en
Mostrar la página Soporte de McAfee Software en el navegador de Web.	Ayuda y, a continuación, seleccionar Internet Guard Dog en la Web
Acceder al sitio Web de McAfee.	McAfee.com
Mostrar la página Soporte de preguntas más frecuentes en el navegador de Web.	Ayuda y, a continuación, Preguntas más frecuentes
Iniciar la actualización de los componentes de Internet Guard Dog y McAfee VirusScan instalados en el equipo.	Actualizar. Se inicia McAfee Software Update Finder
Crear un mensaje de correo electrónico dirigido al sitio Soporte técnico de McAfee Software.	Ayuda y, a continuación, Informar de un problema
Iniciar el archivo de Ayuda de Internet Guard Dog.	Ayuda y, a continuación, seleccionar Temas de ayuda o bien Ayuda de esta pantalla
Mostrar el número de versión de producto de Internet Guard Dog.	Ayuda y, a continuación, Acerca de
Cerrar la pantalla inicial de Internet Guard Dog. (Esto no afecta a la supervisión de Internet Guard Dog, que continúa ejecutándose).	 Botón Cerrar situado en el ángulo superior derecho de la ventana Internet Guard Dog.

NOTA: Si la cuenta de acceso telefónico a Internet no está configurada para marcar automáticamente, conéctese a Internet antes de utilizar cualquiera de los comandos de Ayuda basados en la Web.

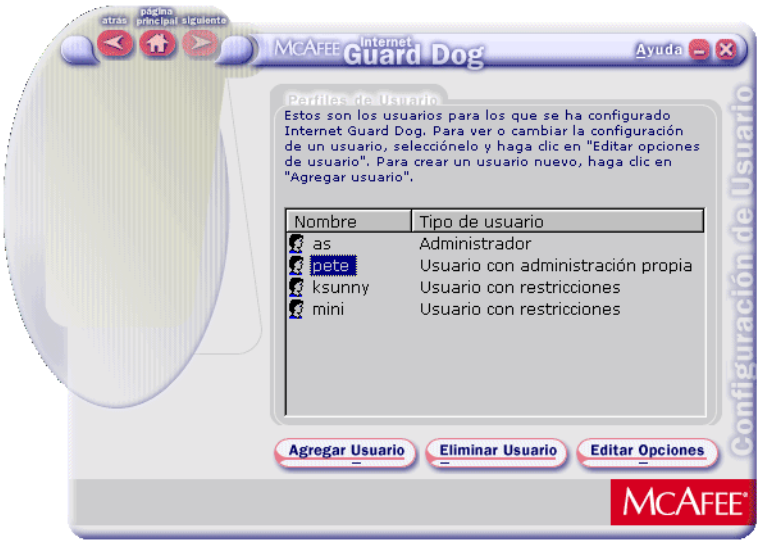
Funcionamiento de Configuración de usuario

El Administrador de Internet Guard Dog puede añadir, editar y eliminar los perfiles de los demás usuarios que navegan por Internet desde el mismo equipo. Además de crear perfiles de usuarios, el Administrador puede personalizar las configuraciones de protección, incluidas las opciones de filtrado de Internet, e incluso puede supervisar los hábitos de navegación por la Web.

Perfil de usuario

Para personalizar la configuración de protección para otro usuario, haga clic en Configuración de usuario en la página inicial de Internet Guard Dog para que aparezca la pantalla Configuración de usuario. En esta pantalla es posible añadir, editar y eliminar un perfil de usuario. Haga clic en uno de los botones disponibles y siga las instrucciones que aparecen en pantalla.

Figura 3-3. Pantalla Configuración de usuario



Consulte la Ayuda en línea de Internet Guard Dog para ver las instrucciones detalladas acerca de cómo añadir, editar o eliminar un perfil de usuario.

Funcionamiento del filtrado de Internet

Una de las nuevas funciones de Internet Guard Dog permite personalizar la configuración de protección de un usuario mediante las opciones de filtrado de Internet. En la pantalla Configuración de usuario, seleccione un usuario; haga clic en Editar opciones de usuario y, a continuación, haga clic en el botón Filtrado de Internet.

Filtro de contenidos

Al iniciar Filtrado de Internet, aparece la pantalla Filtro de contenidos. Esta pantalla permite activar y desactivar rápidamente filtros de Internet Guard Dog.

- **Permitir el acceso a Internet.** Seleccione esta opción si desea que el usuario pueda acceder a Internet en todo momento.
- **Filtrar el acceso a la Web.** Seleccione esta opción si desea limitar el acceso del usuario a Internet.
- **Utilizar Limpiador de búsquedas.** Seleccione esta opción si desea que Internet Guard Dog filtre determinado contenido automáticamente (por ejemplo, ciertas palabras o frases).
- **Activar Bloqueador de anuncios.** Seleccione esta opción si desea que Internet Guard Dog bloquee determinados anuncios que no desea que vea el usuario.
- **Permitir chats.** Seleccione esta opción para permitir que el usuario entre en sesiones de chat en línea.
- **Filtrar chat.** Seleccione esta opción para permitir que el usuario entre en sesiones de chat en línea pero desea filtrar determinado contenido (por ejemplo, ciertas palabras y frases).

Filtrado de Internet

También puede establecer opciones de filtrado de Internet específicas. Haga clic en el botón Filtrado de Internet y seleccione las opciones pertinentes del menú desplegable:

- **Clasificar el contenido.** Esta opción permite controlar el tipo de contenido Web que se permite ver al usuario.
- **Lista de URL.** Esta opción permite controlar los sitios Web que el usuario podrá ver y los que no.
- **Lista de palabras.** Esta opción permite filtrar los sitios Web y los mensajes de chat utilizando palabras y frases.
- **Horas de acceso.** Esta opción permite controlar las horas en las que se permite que el usuario acceda a Internet.

Consulte la Ayuda en línea de Internet Guard Dog para ver las instrucciones detalladas acerca de cómo establecer las opciones de filtrado de Internet.

Figura 3-4. Pantalla Filtrado de Internet (lista de URL)

Funcionamiento de las opciones de privacidad y seguridad

Internet Guard Dog permite determinar los niveles de privacidad y seguridad mediante una serie de opciones configurables cuyo conjunto se conoce como Configuración de la protección. Una parte de Internet Guard Dog siempre está alerta para proteger los datos del equipo y la privacidad en función de las opciones que elija. Internet Guard Dog muestra una serie de páginas de Configuración de la protección que contienen casillas de verificación, cuadros de lista, botones y otros controles que pueden utilizarse para introducir los valores de configuración.

Dispositivos de privacidad	Dispositivos de seguridad
Protector de identidad	Vigilante
Bloqueador de cookies	Guardián de archivos
Limpiador de rastros de Internet	Administrar contraseñas
Filtro de búsqueda	

Para obtener más información, consulte Capítulo 4, “Funciones de privacidad” y Capítulo 5, “Dispositivos de seguridad”.

Internet Guard Dog cuanta con una base de datos de sitios URL, una extensa lista de palabras y un nuevo sistema de clasificación para proteger a los usuarios de las amenazas contra la privacidad y la seguridad en Internet. El Administrador también puede establecer la hora y el día en los que un usuario puede tener acceso a Internet.

Consulte la Ayuda en línea de Internet Guard Dog para ver las instrucciones detalladas acerca de cómo establecer las opciones de filtrado de Internet.

Opciones

El botón Opciones de la pantalla Configuración de usuario permite acceder a los valores de las funciones de Internet Guard Dog y modificarlos como, por ejemplo, la contraseña y los mensajes de alerta sonoros.

Consulte la Ayuda en línea de Internet Guard Dog para ver las instrucciones detalladas acerca de cómo modificar la configuración mediante esta función.

Utilización de McAfee VirusScan

Ahora, Internet Guard Dog utiliza McAfee VirusScan para resolver los problemas de virus que se encuentran al navegar por Internet. Esta función permite establecer cómo desea que se realice una operación de exploración de virus en el equipo; qué hacer si se detecta un virus y cómo avisarle que se ha detectado un virus. Asimismo, puede indicar a VirusScan que guarde un registro de las acciones que se llevan a cabo en el equipo.

Para obtener más información, consulte Capítulo 6, “McAfee VirusScan”.

Visualización de los registros de actividades

Internet Guard Dog proporciona una lista de actividades que el Administrador puede ver mediante la función Registros de actividades. Esta lista se genera basándose en la configuración de privacidad y seguridad del Administrador y de los demás usuarios que ha creado. La información del tipo fechas y horas en las que se conectó un usuario, mantenimiento del PC y violaciones (p. ej., un usuario que intenta utilizar un número de tarjeta de crédito) puede visualizarse con sólo hacer clic en un botón.

El Administrador puede imprimir, guardar o borrar una lista que contenga información del siguiente tipo:

- **Violación**
  Muestra las actividades de un usuario que viola uno de los valores de configuración de protección que ha establecido el Administrador (p. ej., intento de utilizar un número de tarjeta de crédito).
- **Mantenimiento**
  Muestra una lista de acciones que ha realizado Internet Guard Dog incluida la función específica que se utilizó para finalizar la tarea.
- **Actividad**
  Muestra la identidad del usuario que navegó por Internet utilizando ese equipo. También muestra el día, la fecha y la hora en los que el usuario se conecta y desconecta del equipo.

NOTA: Si desea obtener instrucciones detalladas sobre cómo trabajar con los registros de informe, consulte la Ayuda en línea de Internet Guard Dog.

Actualización de Internet Guard Dog y VirusScan

Internet Guard Dog se pone al día de los nuevos virus y amenazas de Internet al actualizar los archivos de programa y los patrones de virus a través de Internet.

NOTA: Si ha adquirido Internet Guard Dog en CD, debe ejecutar la función Actualizar aunque acabe de instalar Internet Guard Dog. En el tiempo transcurrido entre la creación del CD y su instalación, es posible que existan nuevos patrones de virus.

Actualizar el programa de Internet Guard Dog o los archivos de patrones de virus

Los programas McAfee Software incluyen una ubicación central para iniciar los componentes del producto. Para Internet Guard Dog, también es posible iniciar las actualizaciones desde la pantalla inicial. Haga clic en el botón Actualizar de la pantalla inicial. Se iniciará el subprograma de actualización de Internet Guard Dog en busca de actualizaciones disponibles. Si existen actualizaciones disponibles, se mostrará la información pertinente.

Cómo realizar una comprobación de seguridad

Tras finalizar la entrevista, deseará averiguar hasta qué punto existe riesgo en el PC. Comprobación de seguridad examina el PC para detectar cualquier problema de privacidad y seguridad y, a continuación, le proporciona instrucciones para solucionar los problemas que va encontrando. Si utiliza la configuración que Internet Guard Dog sugiere en la entrevista, sólo deberá ejecutar Comprobación de seguridad después de realizar la instalación y, a partir de ahí, una vez al mes aproximadamente. Si reduce el nivel de protección, debe ejecutar Comprobación de seguridad con mayor frecuencia.

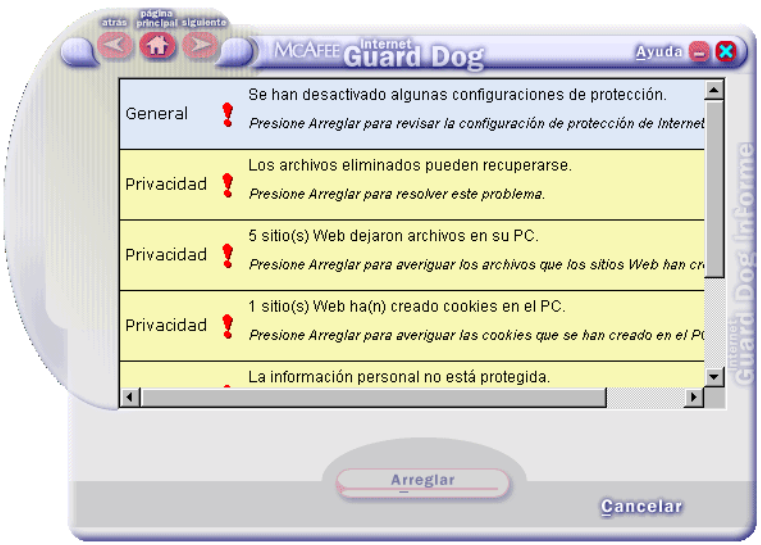
También es posible personalizar la configuración de Comprobación de seguridad.

Para realizar una comprobación de seguridad

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

   Una vez finalizada la comprobación de seguridad, Internet Guard Dog muestra un informe que detalla los problemas detectados. (Figura 3-5 de la página 28)

Figura 3-5. Pantalla Informe de Guard Dog



2. Para ver un problema identificado por Internet Guard Dog, resalte el elemento en cuestión y haga clic en Arreglar.

3. Lea la recomendación de Internet Guard Dog y, a continuación, haga clic en el botón adecuado. Si desea obtener más información, haga clic en Ayuda y, a continuación, en Ayuda de esta pantalla.

   Aparecerá una marca de verificación junto a cada problema que resuelva.

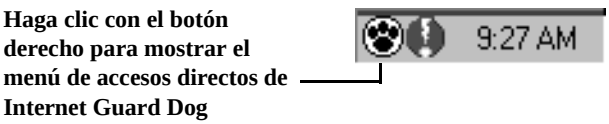
4. Repita los pasos 2 y 3 para cada problema que desee resolver.

5. Una vez haya finalizado, haga clic en el botón Atrás o Inicio para volver a la pantalla inicial de Internet Guard Dog.

Acciones que Internet Guard Dog realiza mientras el PC está funcionando

Mientras el usuario utiliza el PC, Internet Guard Dog busca problemas potenciales de privacidad y seguridad y, si se detecta algún problema, lleva a cabo la acción pertinente. (Internet Guard Dog utiliza la información guardada en Configuración de la protección para determinar qué debe supervisar y cómo debe reaccionar). Puede saber cuándo Internet Guard Dog está funcionando, ya que su icono aparece en la barra de tareas de Windows, tal como se muestra en la Figura 3-6.

Figura 3-6. El icono de Internet Guard Dog en la barra de tareas



> **NOTA:** Si aparece un mensaje de alerta de Internet Guard Dog, consulte el apartado "Respuesta a los mensajes de alerta de Internet Guard Dog" que aparece más adelante en este capítulo.

Utilización del menú de accesos directos de Internet Guard Dog

Aunque no esté ejecutando el programa principal de Internet Guard Dog, sigue teniendo acceso rápido a varias funciones mediante el menú de accesos directos. Haga clic con el botón derecho en el icono de Internet Guard Dog que aparece en la barra de tareas de Windows para mostrar este menú. Realice una de las siguientes acciones:

- Iniciar el programa principal de Internet Guard Dog.
- Mostrar Asistente de navegación, que le permite recuperar las contraseñas de Internet y muestra estadísticas acerca del número de cookies permitidas o bloqueadas, y acerca de la frecuencia de borrado de la información de búsqueda.
- Mostrar la ayuda de Windows para Internet Guard Dog.
- Codificar y descodificar los archivos que protege el Guardián de archivos.
- Cerrar la parte de Internet Guard Dog que supervisa el PC mientras se ejecuta Windows.

Respuesta a los mensajes de alerta de Internet Guard Dog

Internet Guard Dog funciona mientras el usuario trabaja, para proteger la privacidad y seguridad. Cuando Internet Guard Dog detecta un problema potencial, lo resuelve automáticamente o le avisa con un mensaje de alerta basándose en la configuración de Internet Guard Dog.

Los mensajes de alerta le indican el problema potencial que ha activado el mensaje y la recomendación de Internet Guard Dog sobre cómo responder. Si desea obtener más información acerca del problema, haga clic en el botón Signo de interrogación y, a continuación, haga clic en cualquier punto del interior del mensaje de alerta.

Si con el tiempo se da cuenta de que aparecen advertencias de riesgos de seguridad potenciales con demasiada frecuencia, puede ajustar la configuración de los mensajes de alerta en Configuración de la protección. Bloqueador de cookies y Vigilante requieren un período de ajuste para que Internet Guard Dog aprenda a solucionar sus problemas provocando el menor número de interrupciones posible.

SUGERENCIA: Si decide que no desea ver más un mensaje de alerta, utilice el botón Signo de interrogación (?) del mensaje de alerta para averiguar la configuración que debe modificar. La configuración que controla los mensajes de alerta se encuentra en Configuración de la protección del menú Opciones.

Utilización del Asistente de navegación para recuperar o guardar las contraseñas de sitios Web

Confíe en Internet Guard Dog para navegar sin problemas por las complejidades de la Web. Por ejemplo, cuando se conecta a sitios Web que requieren un nombre y contraseña, debe utilizar el Asistente de navegación para:

- Arrastrar su nombre de usuario o contraseña desde Administrar contraseñas y colocarlo en el formulario de inicio de sesión del sitio Web.
- Añadir nueva información de contraseña de un sitio Web.

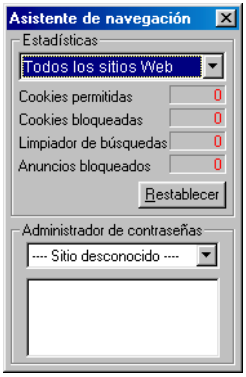
El Asistente de navegación también le informa del número de cookies que el Bloqueador de cookies ha aceptado o rechazado y cuántas veces el Filtro de búsqueda ha bloqueado la información de una búsqueda que ha iniciado desde un sitio Web para que no pasara a otro sitio Web.

SUGERENCIA: El Asistente de navegación aparece permanentemente en la parte superior de cualquier programa abierto en la pantalla. Si el Asistente de navegación se encuentra en una posición poco adecuada, puede cerrarlo y volver a abrirlo según convenga.

Para abrir el Asistente de navegación

1. Haga clic con el botón derecho en el icono de Internet Guard Dog de la barra de tareas de Windows y, a continuación, haga clic en Asistente de navegación. Aparece el siguiente cuadro de diálogo.

Figura 3-7. Asistente de navegación



Para añadir una contraseña y un nombre de usuario nuevos

1. En el Asistente de navegación, seleccione Agregar nueva entrada en la lista desplegable de Administrar contraseñas. Aparecerá el cuadro de diálogo Introducir contraseña para guardar.
2. En el cuadro de texto del sitio Web, introduzca la dirección del sitio Web; en la casilla Nombre de usuario, escriba el nombre con el que se identifica en este sitio Web, que puede corresponder a Nombre de usuario, ID de miembro, Nombre de miembro, ID de inicio de sesión, Nombre de inicio de sesión, etc.
3. En el cuadro de texto Contraseña, introduzca la contraseña que confirma su identidad. (En Administrar contraseñas, Internet Guard Dog muestra un asterisco para cada carácter de la contraseña).
4. Haga clic en Aceptar.

Para recuperar su nombre de usuario y contraseña

1. En Asistente de navegación, seleccione el nombre de sitio si éste no aparece automáticamente en la lista de Sitios Web actuales.
2. Arrastre su nombre de usuario o contraseña desde el cuadro Administrar contraseñas hasta el campo adecuado en el formulario de inicio de sesión del sitio Web.

   El texto aparecerá en el campo. (Si el sitio en el que se registra muestra el texto de la contraseña como una serie de asteriscos (*), Internet Guard Dog mostrará un asterisco para cada carácter de la contraseña).
3. Continúe registrándose al sitio Web como lo haría normalmente.

Utilización de la codificación de archivos

La codificación de archivos convierte un archivo en un código “secreto” que hace que el archivo no pueda leerse. Antes de utilizar el archivo, debe descodificarlo o *descifrarlo*. La codificación de archivos de Internet Guard Dog está pensada para que pueda codificar o descodificar fácilmente todos los archivos que designe para su codificación en Guardián de archivos.

NOTA: Antes de codificar un archivo, debe añadirlo a la lista de Archivos protegidos de Guardián de archivos. Para obtener instrucciones detalladas sobre cómo añadir un archivo a la lista de Archivos protegidos, consulte la Ayuda de Internet Guard Dog.

Para codificar o descodificar archivos

- Haga clic con el botón derecho en el icono de Internet Guard Dog que aparece en la barra de tareas de Windows y, a continuación, haga clic en Codificar archivos de Guardián de archivos o Descodificar archivos de Guardián de archivos.

Funciones de privacidad 4

Las funciones de privacidad de Internet Guard Dog protegen la información personal y de navegación que no desea que se divulgue al navegar por Internet.

Acciones que realiza el Bloqueador de cookies

Las cookies son pequeños archivos que el navegador de Web guarda en el PC a petición de un servidor Web. Cada vez que ve una página Web del servidor Web, el navegador devuelve la cookie al servidor. Estas cookies pueden actuar a modo de etiqueta, lo que permite al servidor Web realizar un seguimiento de las páginas que visita y de la frecuencia con la que vuelve a consultarlas. Algunos sitios Web, como Microsoft Expedia™, utilizan las cookies para guardar la contraseña y las preferencias del usuario, de modo que éste pueda conectarse automáticamente al sitio Web. Para obtener una descripción más detallada de las cookies, consulte el apartado "¿Qué son las cookies y cómo se utilizan?" en la página 70.

El Bloqueador de cookies de Internet Guard Dog ofrece tres opciones para controlar la utilización de las cookies en el equipo. Internet Guard Dog puede realizar las siguientes acciones:

- Rechazar todas las cookies.
- Aceptar todas las cookies.
- Mostrar un mensaje de alerta cada vez que se envía una cookie al navegador. La alerta muestra el nombre de la entidad que intenta establecer la cookie y le proporciona la opción de aceptarla o no.

  Al configurar Bloqueador de cookies en la Configuración de la protección, el usuario puede seleccionar una opción para *sitios de acceso directo* y otra para *sitios de acceso indirecto*. Los sitios de acceso directo son aquéllos a los que se accede deliberadamente. Por ejemplo: escribiendo la dirección URL en la barra de localización del navegador de Web, haciendo clic en un vínculo de una página Web o seleccionando una opción de la lista de sitios favoritos. Los sitios de acceso indirecto son aquéllos a los que el usuario accede debido a que el sitio al que se está conectando directamente muestra el contenido de otro sitio como parte de su propio contenido. Por ejemplo, si fuese directamente a Cool_site.com, podría mostrar un anuncio de Ads-r-us.com (el sitio de acceso indirecto) en un marco separado de la página Cool_site.

Si durante la Entrevista ha aceptado la recomendación de Internet Guard Dog sobre cómo responder a las cookies, el Bloqueador de cookies actuará de la siguiente manera:

- Permitirá automáticamente que se acepten las cookies de los sitios de acceso directo.
- Mostrará un mensaje de alerta cuando un sitio de acceso indirecto intente establecer una cookie.

Respuesta a un mensaje de alerta del Bloqueador de cookies

Si durante la Entrevista ha indicado a Internet Guard Dog que le avise de todas las acciones, mostrará el mensaje de alerta del Bloqueador de cookies la primera vez que un sitio Web intente establecer una cookie.

Para responder al mensaje de alerta, puede hacerlo de las siguientes maneras:

Tabla 4-1.

Si elige	Internet Guard Dog
Aceptar siempre	Acepta la cookie y añade el sitio Web a la lista Permitidas. La próxima vez que consulte dicho sitio, todas las cookies que procedan del mismo se aceptarán automáticamente.
No aceptar nunca	Rechaza la cookie y añade el sitio a la lista Rechazadas. La próxima vez que consulte dicho sitio, todas las cookies que procedan del mismo se rechazarán automáticamente. (En algunos casos, la cookie puede guardarse en el disco duro local, pero la privacidad sigue protegida dado que la cookie nunca vuelve a enviarse a la página que la solicita).

Cada vez que consulta un sitio que aparece en la lista Permitidas o Rechazadas, Internet Guard Dog añade a la lista las cookies aceptadas o rechazadas. Puede ver los totales de un sitio Web en el Asistente de navegación.

Si cambia de opinión acerca de un sitio, puede suprimirlo de la lista Permitidas o Rechazadas en la configuración del Bloqueador de cookies. La próxima vez que visite ese sitio, será como si estuviese consultándolo por primera vez. Si desea suprimir las cookies de un sitio Web que anteriormente las aceptaba, ejecute una Comprobación de seguridad y suprima las cookies de dicho sitio.

SUGERENCIA: Puede ejecutar Comprobación de seguridad de modo que sólo busque cookies. En la pantalla Inicio de Internet Guard Dog: haga clic en el menú Opciones, seleccione Configuración de comprobación y deseleccione todas las opciones excepto Comprobación de cookies. Cuando haya terminado Comprobación, no olvide volver a cambiar la configuración.

¿Por qué debo cambiar la configuración de Bloqueador de cookies?

Si desea obtener un buen nivel de protección de la privacidad sin necesidad de ver ningún mensaje de alerta del Bloqueador de cookies, utilice la configuración recomendada: aceptar siempre cookies de los sitios que consulta directamente y decidir según cada caso concreto si va a aceptar cookies procedentes de sitios que no ha visitado directamente. También puede cambiar la configuración en circunstancias especiales (consulte la tabla 5-2).

Tabla 4-2.

Si	Utilice esta opción
Desea obtener la menor cantidad de cookies y la mayor garantía de privacidad.	Rechazar sitios de acceso directo y sitios de acceso indirecto. Si un sitio requiere que acepte una cookie, puede modificar su configuración temporalmente en Solicitar.
Desea saber siempre cuándo se envían las cookies.	Solicitar en caso de sitios de acceso directo y sitios de acceso indirecto. Prepárese para responder a numerosos mensajes de alerta. Después de responder al mensaje de alerta del Bloqueador de cookies, no aparecerán más mensajes de alerta para ese sitio.
Las cookies no le preocupan en absoluto.	Desactive el Bloqueador de cookies o modifique la configuración de los sitios de acceso directo en Aceptar. Debe elegir el segundo método si desea conservar la totalidad de las cookies añadidas al PC, que podrá ver en el Asistente de navegación.

Acciones que realiza Protector de identidad

Es fácil olvidar que al enviar información a través de Internet, no se transmite directamente de su equipo al equipo que guarda la información de la página Web, sino que la información puede pasar por muchos equipos antes de alcanzar su destino final.

El Protector de identidad puede impedir que el software de su equipo envíe la información personal a través de Internet a un sitio poco seguro. Aunque cuando un sitio Web utiliza una conexión segura no hay de qué preocuparse, tenga en cuenta que muchos de ellos sólo utilizan una conexión segura cuando realizan transacciones con tarjetas de crédito. (Para obtener más información, consulte el apartado “Privacidad en la Web” en la página 62.)

Si su equipo lo utiliza más de una persona, asegúrese de crear una contraseña de Internet Guard Dog. Si la persona que utiliza el equipo no introduce dicha contraseña, Internet Guard Dog sustituye automáticamente la información personal protegida que se envía a un sitio poco seguro por el texto “xxxx”. Por ejemplo, si su hijo intenta adquirir el CD más reciente sin introducir la contraseña de Internet Guard Dog, éste sustituye su número de tarjeta de crédito por “xxxx xxxx xxxx xxxx”.

Protector de identidad ofrece tres respuestas posibles cuando una aplicación intenta enviar información a un sitio poco seguro a través de Internet:

- Permitir el envío de información.
- Bloquear el envío de información.
- Mostrar un mensaje de alerta cuando una aplicación intenta enviar información a un sitio poco seguro a través de Internet. Ésta es la respuesta que configura Internet Guard Dog cuando el usuario añade información para su protección en la Entrevista de Internet Guard Dog.

Respuesta a un mensaje de alerta del Protector de identidad

Durante la Entrevista, Internet Guard Dog le ha pedido que introduzca la información personal y financiera que desea proteger. Internet Guard Dog muestra el mensaje de alerta del Protector de identidad la primera vez que una aplicación intenta enviar esta información a un sitio poco seguro.

Para responder al mensaje de alerta, puede hacerlo de las siguientes maneras:

Tabla 4-3.

Si elige	Internet Guard Dog
Sólo esta vez	Permite que la información se envíe sólo esta vez.
Esta vez no	Impide que la información se envíe esta vez.

¿Por qué debo cambiar la configuración del Protector de identidad?

En las siguientes circunstancias, es posible que desee cambiar la configuración:

Tabla 4-4.

Si	Utilice esta opción
Es la única persona que utiliza el PC y no desea recibir un mensaje de alerta cada vez que se conecta.	Escriba toda la información que desea impedir que se envíe y seleccione Permitir siempre. Cree una contraseña de Internet Guard Dog. Si la contraseña de Internet Guard Dog no se ha introducido al iniciar Windows, un usuario no autorizado del PC no podrá ver ni enviar la información personal.

Tabla 4-4.

Si	Utilice esta opción
Más de una persona utiliza su PC.	Introduzca toda la información que desea impedir que se envíe y seleccione Permitir siempre o Preguntar antes de bloquear. Para la información que siempre desea impedir que se envíe, seleccione Bloquear siempre. Cree una contraseña de Internet Guard Dog. Si la contraseña de Internet Guard Dog no se ha introducido al iniciar Windows, se bloqueará el envío de toda la información que se introduzca en Protector de identidad.
Desea recibir una advertencia siempre que se envíe esta información.	Introduzca toda la información cuyo envío desea impedir y seleccione Preguntar antes de bloquear.

NOTA: Desde el momento en que Internet Guard Dog le solicite la contraseña y el usuario la introduzca, ésta seguirá estando en vigor hasta que reinicie Windows. Si ha introducido la contraseña y desea bloquear el envío de información personal por parte de otras personas, reinicie Windows antes de permitir que alguien utilice el PC.

Acciones que realiza el Limpiador de rastros de Internet

A medida que navega por Internet, el navegador guarda la información que hace que su experiencia de navegación sea más satisfactoria. Utiliza la información como se indica a continuación:

Tabla 4-5.

El navegador utiliza	Para
Archivos almacenados en la memoria caché	Agilizar la visualización de elementos de la página Web como, por ejemplo, los gráficos.
Sitios URL visitados	Mostrar una lista de sitios Web que ha visitado sirviéndose de direcciones Web.
Historial	Mostrar una lista de sitios Web que ha visitado sirviéndose de nombres de sitios Web.

Los archivos que permanecen en el PC están al alcance de otras personas y, según la configuración del navegador, pueden ocupar muchos megabytes de espacio en disco.

Si ha aceptado la recomendación de Internet Guard Dog durante la entrevista, Internet Guard Dog muestra el mensaje de alerta del Limpiador de rastros de Internet al cerrar el navegador.

Respuesta al mensaje de alerta del Limpiador de rastros de Internet

Para responder al mensaje de alerta dispone de las siguientes opciones.

Tabla 4-6.

Si elige	Internet Guard Dog
Limpiar	Elimina todos los archivos almacenados en la memoria caché, así como la información del historial y del URL asociada al sitio Web (Dominio) seleccionado. Seleccione el sitio que desee limpiar, marcando la casilla de verificación que se encuentra junto al nombre del mismo.
No limpiar	Cierra el mensaje de alerta y continúa cerrando el navegador.

Internet Guard Dog selecciona de manera predeterminada los sitios que no están marcados como favoritos (es decir, parte de la lista de sitios favoritos) puesto que es menos probable que vuelva a consultarlos. Si no vuelve a un sitio, los archivos almacenados en la memoria caché para el mismo no se volverán a utilizar nunca; tan sólo ocupan espacio en disco hasta que el navegador los elimina definitivamente.

Si más adelante desea eliminar los archivos que ha dejado atrás, ejecute Comprobación de seguridad de Internet Guard Dog.

¿Por qué debo cambiar la configuración de Limpiador de rastros de Internet?

En las siguientes circunstancias, es posible que desee cambiar la configuración:

Tabla 4-7.

Si	Utilice esta opción
Desea ver exactamente los archivos que se están eliminando.	Preguntar si deseo limpiar siempre que salga del navegador de Web.
Desea eliminar todo rastro de la navegación.	Limpiar automáticamente siempre que salga del navegador Web. (Quite la marca de la casilla de verificación para “Conservar los elementos marcados como favoritos”.)
Desea suprimir archivos sólo para sitios Web que no ha marcado como favoritos ni ha añadido a la lista de favoritos.	Limpiar automáticamente siempre que salga del navegador Web. Conservar elementos favoritos.

Acciones que realiza el Filtro de búsqueda

Cuando realiza una búsqueda en el navegador de Web, la información de la búsqueda se muestra en el cuadro de dirección del navegador de Web. Cuando consulta otro sitio, el navegador retiene la información de búsqueda que el próximo sitio Web que visite podrá extraer sin que se percate de ello. El Filtro de búsqueda bloquea esta información e impide que pase al siguiente sitio.

Si ha seleccionado Filtro de búsqueda en Configuración de seguridad, Internet Guard Dog suprime automáticamente la información de búsqueda antes de que visite otro sitio Web. Internet Guard Dog no muestra ningún mensaje de alerta para esta función, pero puede ver el número de veces que el Filtro de búsqueda bloquea esta información en Asistente de navegación.

Dispositivos de seguridad 5

Los dispositivos de seguridad de Internet Guard Dog garantizan la protección de la conexión a Internet y protegen los archivos del equipo de miradas curiosas y programas destructivos.

Acciones que realiza la función Vigilante

La función Vigilante permite controlar qué programas del PC tienen acceso a la conexión a Internet. El Vigilante también le avisa de la existencia de cualquiera de las siguientes acciones potencialmente dañinas:

- El navegador se dirige hacia un sitio dañino: es decir, un sitio conocido por contener archivos infectados por virus, caballos de Troya, controles ActiveX destructivos o maliciosos u otros asuntos de seguridad.
- Un programa utiliza silenciosamente el módem para conectarse a otro equipo.
- Un programa inicia otro programa.
- Un programa envía a través de Internet un número que sigue un patrón similar a las tarjetas de crédito habituales.

Respuesta a los mensajes de alerta del Vigilante

Internet Guard Dog puede presentar cinco mensajes de alerta diferentes relacionados con la función Vigilante. Si está utilizando la configuración predeterminada sugerida por la Entrevista, verá los mensajes relacionados con el acceso a Internet, sitios dañinos, programas que inician otro programa, así como programas que envían números similares a las tarjetas de crédito.

Mensaje de alerta sobre el acceso a Internet

Cada vez que inicia un programa que intenta utilizar su conexión a Internet, Internet Guard Dog comprueba si éste se encuentra en la lista de programas a los que se les permite acceder a Internet. Si no se encuentra en la lista, Internet Guard Dog muestra un mensaje de alerta que le indica que el programa está intentando conectarse a Internet y le pregunta cómo debe manejarlo.

Puesto que Internet Guard Dog muestra una alerta la primera vez que inicia un programa de Internet, puede que desee iniciar cada uno de los programas conectados a Internet para descartar dichas alertas en un momento concreto.

Para responder al mensaje de alerta sobre el acceso a Internet, puede hacerlo de las siguientes maneras:

Tabla 5-1.

Si elige	Internet Guard Dog
Sólo esta vez	Permite al programa acceder a Internet sólo esta vez y le avisa la próxima vez que éste intente acceder a Internet.
Permitir siempre	Permite al programa acceder a Internet en cualquier momento. En Configuración de protección de Vigilante, el programa se añade a la lista de programas a los que se les permite acceder automáticamente a Internet. Si más adelante decide que no desea que este programa utilice su conexión a Internet, seleccione su nombre y haga clic en Suprimir.
Esta vez no	Impide que el programa acceda a Internet. Esta opción sigue estando en vigor hasta la próxima vez que reinicie Windows o, para usuarios de Internet Explorer 4, hasta que cierre el navegador. Utilice esta opción si desea que Internet Guard Dog le avise la próxima vez que el programa intente acceder a Internet.

Mensaje de alerta sobre un sitio dañino

Antes de que pueda conectarse a un sitio dañino, Internet Guard Dog mostrará el mensaje de alerta, “Su navegador está consultando *Nombre de sitio*, un sitio Web que puede dañar el equipo o los datos”.

Debe cerrar inmediatamente el navegador para finalizar la conexión del navegador a dicho sitio. Cuanto más rápido cierre el navegador, menos tiempo tendrá el sitio para transferir datos dañinos al equipo.

Si desea ver el sitio Web de todos modos, haga clic en Continuar.

Mensaje sobre el inicio de otro programa por parte del programa

Cuando un programa inicia otro programa, Internet Guard Dog comprueba que el usuario haya autorizado esta acción. Si no ha autorizado que ese programa siempre abra el otro programa, Internet Guard Dog mostrará un mensaje de alerta.

Para responder al mensaje de alerta, puede hacerlo de las siguientes maneras:

Tabla 5-2.

Si elige	Internet Guard Dog actúa de esta forma
Permitir siempre	Permite que el programa inicie el otro programa.
Esta vez no	Impide sólo esta vez que el programa inicie el otro programa.
Sólo esta vez	Permite sólo esta vez que el programa inicie el otro programa.

Mensaje de envío de un número de tarjeta de crédito

Cuando un programa envía un número similar al de una tarjeta de crédito a través de Internet, se muestra un mensaje de alerta.

Para responder al mensaje de alerta, puede hacerlo de las siguientes maneras:

Tabla 5-3.

Si elige	Internet Guard Dog
Esta vez no	Impide que el programa envíe el número en esta ocasión.
Sólo esta vez	Permite que el programa envíe el número sólo esta vez.

¿Por qué debo cambiar la configuración de Vigilante?

La configuración de Vigilante sugerida por la Entrevista mostrará el menor número de mensajes de alerta. Si sabe que está utilizando una versión de navegador más antigua o simplemente desea obtener un mayor nivel de seguridad, es posible que desee cambiar la configuración en las siguientes circunstancias:

Tabla 5-4.

Si	Utilice esta opción
• Desea que se le avise cuando el sitio al que se está dirigiendo es conocido por causar daños, por ejemplo, contiene archivos infectados por virus, caballos de Troya, controles ActiveX destructivos o maliciosos u otros asuntos de seguridad. (Para mantener actualizada y vigente la lista de Internet Guard Dog de sitios dañinos, utilice Actualizar mensualmente).	Vaya a sitios dañinos.
• Desea que se le avise cuando un programa está utilizando su módem para marcar.	El módem marque de forma silenciosa
• Desea que se le avise cuando un programa inicia otro programa. Muchos programas más modernos le avisarán antes de hacerlo, pero los programas más antiguos pueden no hacerlo. Por ejemplo, Internet Explorer 4 utiliza “programas de ayuda” para mostrar documentos.	Un programa intente iniciar otro programa.
• Desea que se le avise antes de que cualquier número similar a un número de tarjeta de crédito se envíe a través de Internet. Para proteger números específicos, consulte “Acciones que realiza Protector de identidad” en la página 38.	Se transmita un número de tarjeta de crédito.
• Desea ver una lista de programas a los que ha permitido el acceso automático a Internet. (Al hacer clic en Aceptar siempre en el mensaje de alerta sobre acceso a Internet, se añade un programa a la lista). Si cambia de opinión, puede suprimir un programa de la lista. La próxima vez que el programa intente acceder a Internet, recibirá una advertencia.	Siempre se permite a estos programas el acceso a Internet.

Acciones que realiza la función Guardián de archivos

El Guardián de archivos puede proteger archivos que contienen datos confidenciales, para evitar que se puedan abrir, cambiar de nombre, copiar, mover o eliminar. Para una mayor protección, puede incluso codificar los archivos protegidos mediante el Guardián de archivos. Internet Guard Dog también le puede avisar si un programa intenta realizar alguna de las siguientes actividades potencialmente dañinas:

- Un programa intenta volver a dar formato a la unidad de disco duro.
- Un control ActiveX intenta eliminar archivos de la unidad de disco duro.
- Un control ActiveX intenta explorar archivos de la unidad de disco duro.
- Un programa intenta acceder a los archivos de contraseñas del sistema.

Cuando Internet Guard Dog muestra un mensaje de alerta, puede decidir si se va a permitir que el programa continúe funcionando o no.

Respuesta a los mensajes de alerta de Guardián de archivos

Internet Guard Dog puede mostrar cinco mensajes de alerta diferentes relacionados con el Guardián de archivos. Si está utilizando la configuración predeterminada sugerida por la Entrevista, sólo verá: los mensajes sobre archivo protegido, exploración de ActiveX, eliminación de ActiveX y formato de unidad.

Mensaje de alerta sobre archivo protegido

Debe indicar a Guardián de archivos qué archivos desea proteger de la unidad de disco duro y qué programas se pueden utilizar para abrir los archivos. Si una aplicación no autorizada intenta acceder a un archivo protegido, Internet Guard Dog muestra un mensaje de alerta que le indica qué aplicación está intentando abrir qué archivo.

Puede decidir entonces si desea proporcionar acceso al archivo al programa en cuestión. Si no ha sido usted el responsable de ejecutar el programa no autorizado, debe investigar inmediatamente el programa para determinar su origen.

Tabla 5-5.

Si elige	Internet Guard Dog
Permitir siempre	Permite al programa abrir el archivo y añade el programa a la lista de programas a los que se autoriza a acceder al archivo sin otras advertencias.
Esta vez no	Detiene la apertura del archivo por parte del programa y le avisa la próxima vez que el programa intenta abrir el archivo.

Mensaje de alerta sobre exploración de ActiveX

Existen razones legítimas para permitir que un control ActiveX lea o *explore* todos los archivos. Por ejemplo, puede ir hasta un sitio de la Web que utilice un control ActiveX para buscar virus en el equipo. Sin embargo, si un sitio empieza a explorar los archivos sin avisarle, Internet Guard Dog le da la oportunidad de decidir si confía en el sitio.

Cuando Internet Guard Dog detecta un control ActiveX que explora los archivos del equipo, muestra un mensaje de alerta que le indica qué control ActiveX está explorando la unidad de disco duro.

Para responder al mensaje de alerta, puede hacerlo de las siguientes maneras:

Tabla 5-6.

Si elige	Internet Guard Dog
Esta vez no	Detiene la ejecución del control ActiveX en esta ocasión. Si cambia de opinión, vuelva a cargar la página del navegador y haga clic en **Sólo esta vez** la próxima vez que Internet Guard Dog muestre su mensaje de exploración de ActiveX.
Sólo esta vez	Permite que el control ActiveX explore la unidad sólo esta vez.

Mensaje de alerta sobre la eliminación de ActiveX

Existen razones legítimas para permitir que un control ActiveX elimine archivos. Por ejemplo, si un control instala software especial en el equipo para permitirle interactuar con su sitio Web, el control puede necesitar eliminar archivos que ha creado para su uso temporal. Sin embargo, si un sitio no le avisa y empieza a eliminar archivos, Internet Guard Dog le da la oportunidad de ver qué archivo se está eliminando y pensar sobre cuánto confía en el sitio.

Cuando Internet Guard Dog detecta un control ActiveX que está eliminando archivos del equipo, muestra un mensaje de alerta que le indica el nombre del control.

Para responder al mensaje de alerta, puede hacerlo de las siguientes maneras:

Tabla 5-7.

Si elige	Internet Guard Dog
Esta vez no	Detiene la ejecución del control ActiveX en esta ocasión. Si cambia de opinión, vuelva a cargar la página en el navegador y haga clic en **Permitir esta vez** la próxima vez que Internet Guard Dog muestre su mensaje de eliminación de ActiveX.
Sólo esta vez	Permite que el control ActiveX elimine archivos sólo esta vez.

Mensaje de alerta sobre formato de unidad

Al iniciar un comando de formato, Internet Guard Dog no sabe si ha indicado al equipo que dé formato a un disco Zip o si un control ActiveX ha empezado a dar formato a la unidad de disco duro. Sabrá que esta actividad es legítima al iniciar el comando de formato, o si sabe que un programa que está utilizando necesita dar formato a una unidad de disco duro (o un disco Zip o Jaz).

Cuando Internet Guard Dog detecta un comando de formato, muestra un mensaje de alerta que le indica qué programa ha iniciado el comando de formato.

Si no sabe por qué se está dando formato al disco, anote el nombre del programa en el mensaje de alerta y después apague el PC con el interruptor de alimentación. Si el nombre del programa contiene las letras OCX, se trata de un control ActiveX. No reinicie el navegador hasta haber ejecutado una Comprobación de Internet Guard Dog y haber eliminado del equipo el control ActiveX bajo sospecha.

Haga clic en **Continuar** si desea que el programa dé formato al disco.

¿Por qué debo cambiar la configuración del Guardián de archivos?

En las siguientes circunstancias, es posible que desee cambiar la configuración:

Tabla 5-8.

Si	Utilice esta opción
• Desea que se le avise cuando un control ActiveX examine los archivos del equipo. Esto puede suceder de forma legítima si el control tiene que buscar un archivo para su uso. Si éste asunto le preocupa, compruebe el sitio que le ha enviado el control.	ActiveX compruebe mi unidad
• Desea que se le avise cuando un control ActiveX elimina un archivo. Esto puede ocurrir de forma legítima si el control está eliminando archivos más antiguos o temporales que utiliza. Si éste asunto le preocupa, compruebe el sitio que le ha enviado el control.	ActiveX elimine archivos de la unidad
• Desea que se le avise cuando un programa intenta dar formato a alguna de sus unidades. Aparece un mensaje de alerta cuando da formato a un disquete, otro soporte extraíble o disco duro. Puede desactivar esta opción temporalmente si va a dar formato a muchos discos y no desea ver ningún mensaje.	Se dé formato a la unidad
• Desea que se le avise cuando un programa acceda a los archivos de contraseñas de Windows (es decir, cualquier archivo con la extensión .pwl que se encuentre en el directorio de Windows). Las funciones de Windows protegidas mediante contraseña utilizan estos archivos de contraseñas.	Se acceda a archivos de contraseñas
• Desea que se impida que un programa abra uno o varios archivos. Para obtener una mayor protección, puede hacer que Internet Guard Dog incluya el archivo al codificar los archivos. Puede proteger archivos individuales, archivos de una carpeta específica, archivos del mismo tipo, archivos de la misma unidad.	Archivos protegidos

NOTA: Para obtener instrucciones detalladas sobre cómo añadir, editar o eliminar archivos de la lista de Archivos protegidos, permitiendo que un programa acceda a un archivo protegido, o codificando o descodificando archivos, consulte la Ayuda de Internet Guard Dog.

Acciones que realiza la función Administrar contraseñas

La función Administrar contraseñas le permite almacenar diversos nombres de inicio de sesión de sitios Web en una ubicación segura. Cuando consulta un sitio Web que requiere esta información, puede arrastrarlo desde el Asistente de navegación hasta el formulario visualizado en el navegador.

En Configuración de protección, puede:

- Ver la lista de nombres de inicio de sesión y contraseñas almacenadas.
- Añadir un registro.
- Editar un registro.
- Suprimir un registro.

También puede añadir un registro en Asistente de navegación. Para obtener más información, consulte los apartados "Utilización del Asistente de navegación para recuperar o guardar las contraseñas de sitios Web," en el capítulo 3.

Para añadir un registro de contraseñas

1. En la pantalla Inicio de Internet Guard Dog, haga clic en el menú Opciones y, a continuación, seleccione Configuración de protección.
2. Haga clic en Administrar contraseñas. (Si la casilla de verificación que se encuentra junto a Administrar contraseñas no está seleccionada, no podrá añadir, editar ni suprimir registros).
3. Haga clic en Agregar.
4. Escriba la información que desea almacenar en el registro.
5. Haga clic en Aceptar.

Para editar un registro de contraseñas

1. En la lista Administrar contraseñas, realice una de las siguientes acciones:
   - Haga doble clic en el registro que desea editar.
   - Haga clic en el registro que desea editar y, a continuación en **Editar**.
2. Cambie la información que desea almacenar en el registro.
3. Haga clic en Aceptar.

Para suprimir un registro de contraseñas

- En la lista Administrar contraseñas, haga clic en un registro para seleccionarlo y, a continuación, haga clic en Suprimir.

McAfee VirusScan 6

¿Qué es McAfee VirusScan?

El nombre VirusScan se aplica tanto al conjunto de componentes del programa antivirus de escritorio que se describe en este capítulo como a un determinado componente de ese conjunto: SCAN32.EXE, o la exploración VirusScan "por solicitud". "Por solicitud" significa que como usuario controla el inicio y la finalización de una operación de exploración de VirusScan, los objetivos que examina, las acciones que lleva a cabo cuando detecta un virus o cualquier otro aspecto relacionado con el funcionamiento del programa. En cambio, otros componentes de VirusScan operan automáticamente o según lo que programa el usuario. Inicialmente, VirusScan sólo proporcionaba funciones de exploración por solicitud, sin embargo, desde que se integró en el programa ofrece también un conjunto de funciones antivirus que proporcionan la máxima protección frente a las infecciones de virus y ataques de software perjudicial.

El componente VirusScan por solicitud opera en dos modos: La interfaz VirusScan "Classic" se instala rápidamente, con un mínimo de opciones de configuración, pero con toda la potencia del motor de exploración antivirus VirusScan; el modo VirusScan "Advanced" aumenta la flexibilidad de las opciones de configuración del programa, incluida la capacidad de ejecutar más de una operación de exploración de forma concurrente.

Inicio de VirusScan

VirusScan se una suministra con única operación de exploración predeterminada preconfigurada y lista para ejecutarse. Puede iniciar dicha operación de exploración para detectar virus en la unidad C: inmediatamente o configurar sus propias operaciones de exploración de forma personalizada. VirusScan Advanced también se suministra con una sola operación preconfigurada de exploración de todos los discos duros locales.

Existen dos formas de iniciar VirusScan:

- Haga clic en **VirusScan** en la pantalla Inicio de Internet Guard Dog, o bien
- haga clic en **Inicio** en la barra de tareas de Windows, **Programas** y **McAfee VirusScan**. A continuación, seleccione **McAfee VirusScan Central** en la lista en la que aparece.

Si desea utilizar la ventana de VirusScan Classic:

- Después de iniciar VirusScan en la pantalla Inicio de Internet Guard Dog, haga clic en **Classic VirusScan**, o bien
- haga clic en **Inicio** en la barra de tareas de Windowsy seleccione **Ejecutar** en el menú que aparece. Escriba SCAN32.EXE en el cuadro de diálogo Ejecutar y haga clic en **Aceptar**.

Todos estos métodos inician VirusScan.

Ventana de VirusScan Central

Después de iniciar VirusScan desde la pantalla Inicio de Internet Guard Dog, aparece la ventana de VirusScan Central. Dispone de las siguientes funciones:

- Haga clic en **Comprobar** para iniciar la tarea de exploración predeterminada inmediatamente o configurar una tarea de exploración según sus necesidades (consulte Configuración de VirusScan).
- Haga clic en **Planificador** para iniciar el Planificador de McAfee VirusScan. Esta utilidad permite configurar y ejecutar operaciones de exploración desatendidas.
- Haga clic en **Cuarentena** para mostrar una lista de campos en cuarentena. La función Cuarentena permite aislar un archivo infectado para evitar que el virus se propague.
- Haga clic en **Actualizar** para buscar versiones actualizadas de VirusScan y archivos DAT.

Ventana de VirusScan Classic

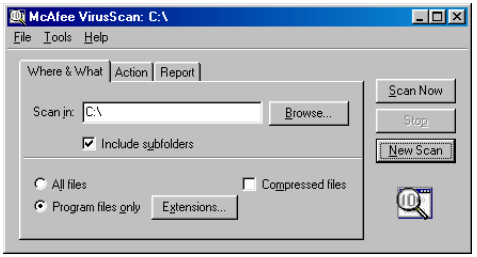


Figura 6-1. Ventana de VirusScan Classic

Una vez iniciada la ventana de VirusScan Classic, haga clic en el botón **Explorar ahora** a la derecha de la ventana para iniciar la tarea de exploración predeterminada, o bien configure una tarea de exploración personalizada haciendo clic en las fichas que aparecen en la parte superior de la ventana y seleccionando las opciones correspondientes en cada página de propiedad.

Los menús que aparecen en la parte superior de la ventana VirusScan permiten modificar algunos aspectos del funcionamiento del programa. Puede:

- **Guardar o restaurar la configuración predeterminada.**
- **Guardar una nueva configuración.**
- **Abrir el registro de actividades de VirusScan.**

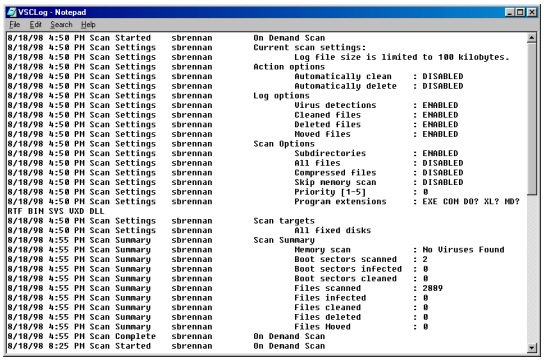


Figure 6-2. Registro de actividades de VirusScan

- **Salir de VirusScan.**
- **Cambiar los modos de VirusScan.**
- **Activar la protección mediante contraseña.**
- **Iniciar el Planificador de VirusScan.**
- **Abrir el archivo de ayuda en línea.**

NOTA: Consulte la Ayuda en línea de McAfee VirusScan para obtener más información e instrucciones detalladas acerca de cómo utilizar las funciones de la ventana de Classic.

Configuración de VirusScan

Para llevar a cabo una operación de exploración, VirusScan necesita saber qué desea explorar, qué debe hacer si detecta un virus y cómo debe notificarle que ha detectado un virus. También puede indicar a VirusScan que lleve a cabo un registro de sus acciones. Una serie de páginas de propiedad controla las opciones de cada tarea.

Opciones por tarea

- **Selección de opciones de ubicación y objetivo**

  Inicialmente, VirusScan asume que desea explorar la unidad C: y todas las subcarpetas, así como explorar únicamente los archivos susceptibles de infecciones de virus.

  Para modificar estas opciones, siga los criterios que se describen a continuación:

  - Seleccione el volumen o la carpeta del sistema o de la red que desea que VirusScan explore.

    Haga clic en ⊞ para ampliar la lista de un elemento que aparece en el cuadro de diálogo. Haga clic en ⊟ para contraer un elemento. Puede seleccionar discos duros, carpetas o archivos como objetivos de exploración, tanto si residen en el sistema o en otros equipos de la red. No es posible seleccionar Mi PC, Entorno de red ni múltiples volúmenes como objetivos de exploración en VirusScan Classic, sino que para seleccionar estos elementos es necesario estar en modo VirusScan Advanced.

  - Especifique los tipos de archivo que desea que examine VirusScan. De forma predeterminada, VirusScan busca virus en los archivos con las extensiones .EXE, .COM, .DO?, .XL?, .MD?, .VXD, .SYS, .BIN, .RTF, .OBD y .DLL. Los archivos con las extensiones .DO?, .XL?, .RTF, .MD? y .OBD son archivos de Microsoft Office, y todos son susceptibles de albergar infecciones de virus de macro. El signo de interrogación ? es un comodín que permite a VirusScan explorar tanto archivos de plantilla como de documento.

- **Selección de opciones de acción**

  Cuando VirusScan detecta un virus, puede reaccionar preguntando qué debe hacer con el archivo infectado, o bien realizando automáticamente una acción que el usuario ha determinado con anterioridad.
  Puede especificar las opciones de respuesta que desea que efectúe VirusScan al detectar un virus, o las acciones que desea que lleve a cabo por su cuenta. Dichas opciones de respuesta incluyen:

  - **Solicitar acciones al usuario.** Elija esta respuesta si sabe que estará presente cuando VirusScan explore el disco, ya que VirusScan mostrará un mensaje de alerta cuando detecte un virus y le ofrecerá las diferentes opciones de respuesta disponibles.

  - **Mover archivos infectados automáticamente.** Elija esta respuesta para que VirusScan mueva los archivos infectados a un directorio de cuarentena al detectarlos. De forma predeterminada, VirusScan mueve los archivos a una carpeta denominada INFECTED que crea en la raíz de la unidad en la que ha detectado el virus. Por ejemplo, si VirusScan ha detectado un archivo infectado en T:\MIS DOCUMENTOS y ha especificado INFECTED en el directorio de cuarentena, VirusScan copiará el archivo en T:\INFECTED.

    Introduzca otro nombre en la casilla de texto o haga clic en **Navegar** para localizar una carpeta adecuada del disco duro.

  - **Limpiar archivos infectados automáticamente.** Elija esta respuesta para indicar a VirusScan que suprima el código de virus en los archivos infectados al detectarlo. Si VirusScan no consigue suprimir el virus, anotará el incidente en su archivo de registro.

  - **Eliminar archivos infectados automáticamente.** Utilice esta opción si desea que VirusScan elimine los archivos infectados tan pronto como los detecta. Asegúrese de activar la función de respuesta para contar con un registro de los archivos que elimina VirusScan. Para restaurar los archivos eliminados deberá utilizar las copias de seguridad. Si VirusScan no consigue eliminar un archivo infectado, anotará el incidente en su archivo de registro.

  - **Continuar la exploración.** Utilice esta opción si desea trabajar en modo desatendido mientras VirusScan efectúa la exploración para detectar virus. Si también activa la función de respuesta de VirusScan, el programa registrará los nombres de los virus que detecte y los nombres de los archivos infectados para que pueda eliminarlos cuando desee.

- **Selección de opciones de informe**

  De forma predeterminada, VirusScan emite un aviso sonoro cuando detecta un virus. Utilice la página Informar para activar o desactivar este aviso o para añadir un mensaje de alerta en el cuadro de texto Virus detectado que aparece cuando VirusScan detecta un archivo infectado. Este mensaje de alerta puede contener información muy variada, desde un simple aviso hasta las instrucciones acerca de cómo informar de un incidente al administrador de red.

  En esta misma página se determina el tamaño y la ubicación del archivo de registro de VirusScan. De forma predeterminada, el programa enumera los valores actuales y resume las acciones que lleva a cabo durante las operaciones de exploración en un archivo de registro llamado VSCLOG.TXT. Puede indicar que VirusScan escriba el registro en este archivo o utilizar un editor de textos para crear un archivo de texto para que lo utilice VirusScan. De esta forma, podrá abrir e imprimir el archivo de registro desde VirusScan o desde el editor de texto para su posterior revisión.

- **Selección de opciones de alerta y registro**

  Puede seleccionar los métodos de tipos de alerta que desea que utilice VirusScan al detectar un virus.

  - **Mostrar un mensaje personalizado.** Seleccione la casilla de verificación **Mostrar mensaje** y escriba el mensaje que desea que aparezca en la casilla de texto. Puede introducir un mensaje de hasta 225 caracteres de longitud.

    NOTA: Para que VirusScan muestre este mensaje, seleccione **Solicitar acciones al usuario** como opción de respuesta de acción.

  - **Aviso sonoro.** Seleccione la casilla de verificación **Aviso sonoro**.

  También puede seleccionar la opción Registrar en archivo. De forma predeterminada, VirusScan escribe la información de registro en el archivo VSCLOG.TXT del directorio del programa VirusScan. Introduzca otro nombre y otra vía de acceso en la casilla de texto o haga clic en **Navegar** para localizar un archivo adecuado en el disco duro o en la red.

Seguridad y privacidad en Internet A

En este capítulo se proporciona alguna información básica que le ayudará a tener una visión global de las amenazas contra la seguridad y privacidad en Internet. Asimismo, se tratan las estrategias de la utilización de Guard Dog para protegerle a usted y a su equipo.

Las redes e Internet

Una red informática vincula equipos individuales entre sí, de modo que puedan compartir datos y recursos. Para conectarse en red, los equipos necesitan algún medio de conexión, que puede ser un módem o una tarjeta de interfaz de red (algunos equipos tienen tarjetas de interfaz de red integradas). El módem o la tarjeta es responsable del envío y recepción de datos a través de la red. Las redes se denominan a menudo *redes de área local* (LAN), debido a que vinculan los equipos en una única ubicación, por ejemplo, una oficina o edificio. En una pequeña oficina, los equipos se pueden vincular directamente conectándolos entre sí con un cable. Esta red sencilla se conoce como conexión en red *de igual a igual*, en la que todos los equipos son equivalentes. Windows tiene posibilidades de conexión en red de igual a igual integradas en el sistema operativo. El mayor tráfico de las redes más amplias requiere los servicios de un equipo especial, llamado *servidor*. Los servidores ayudan a operar a las redes de mayor tamaño, averiguando cómo se deben encaminar los mensajes al destinatario correcto.

Internet es una enorme red informática, que conecta entre sí a equipos de todo el mundo y les permite trabajar conjuntamente y compartir información. Cuando se conecta a Internet, su equipo pasa a formar parte de una red informática mundial.

TCP/IP es el subsistema

Internet se basa en un sistema denominado Protocolo de Control de Transmisión / Protocolo de Internet (TCP / IP). TCP permite a los equipos compartir datos, dividiéndolos antes en pequeños segmentos llamados paquetes. Además de los datos, cada paquete contiene la dirección de la máquina que lo envía, así como la dirección del destinatario deseado. La parte TCP del sistema es la responsable del direccionamiento de los datos y de su división en paquetes. IP, la segunda parte del sistema, es la responsable del encaminamiento de los paquetes del equipo remitente al equipo destinatario. Equipos especiales llamados encaminadores leen la dirección de cada paquete y averiguan cómo encaminarlo al destino correcto.

¿Por qué utilizar paquetes?

¿Por qué es necesario dividir los datos en paquetes? La respuesta se encuentra en los orígenes de TCP / IP. Al igual que Internet, es un producto de la Guerra Fría. Fue el Departamento de Defensa de los EE.UU. donde se creó originariamente Internet. Estaba diseñada para garantizar comunicaciones seguras, incluso con múltiples fallos anticipados de la red de comunicaciones en el caso de una guerra nuclear. TCP / IP resuelve el problema de los fallos de red asumiendo que siempre se produce cierta cantidad de interferencias en la red, ya sea por errores aleatorios de datos o por bloqueos más graves del sistema. Si ha intentado hablar en una sala ruidosa, sabe que a menudo es necesario repetir las frases—y para esto está diseñado exactamente TCP / IP. Al dividir los datos en paquetes, se permite a Internet buscar rutas alternativas si una de ellas es inaccesible. Si un paquete no puede alcanzar su destino o llega dañado, el equipo receptor tan sólo tiene que solicitarlo de nuevo hasta que llegue de manera satisfactoria.

Cuando envía, por ejemplo, un mensaje de correo electrónico, éste se divide en varios paquetes. Según lo ruidosa que sea la red, cada paquete puede necesitar encaminarse a través de una ruta exclusiva, a fin de encontrar la forma de llegar a su destino. Además, los problemas de la red pueden originar el retraso de algunos paquetes, de modo que lleguen desordenados. Para compensarlo, TCP examina cada paquete a medida que llega, para verificar que su estado es satisfactorio. Una vez se reciben todos los paquetes, TCP los vuelve a colocar en su orden original. Por supuesto, todo esto ocurre con rapidez y automáticamente, de modo que el usuario nunca verá la ejecución del proceso.

Internet y la Web… ¿cuál es la diferencia?

Antes de la Web, Internet se basaba principalmente en caracteres y comandos, es decir, debía escribirse la dirección de Internet exacta del lugar al que deseaba ir en la línea de comandos. En 1989, Tim Berners-Lee, de European Particle Physics Laboratory, propuso un nuevo modo de compartir información a través de Internet. La característica esencial de la visión de Berner-Lee de la Web consiste en que vincula documentos entre sí. Al hacer clic en un vínculo en una página Web, el usuario se conecta automáticamente a otro sitio Web. Esta función vinculante, junto con el aumento de las capacidades gráficas de los equipos que se encuentran en los hogares, ha transformado Internet en un lugar lleno de gráficos, completado con vídeo, sonido e imágenes. Al vincular información en un paquete de aspecto gráfico, la Web ha hecho que Internet resulte más atractiva para el cliente típico.

Internet es una red de equipos vinculados que utiliza TCP / IP como su principal sistema de mensajería. La World Wide Web (WWW, o para abreviar, tan sólo la “Web”) actúa como equipo host en Internet, y es una colección de documentos en expansión que emplea un esquema de codificación especial denominado HTML (Hypertext Markup Language).

❑ **NOTA:** HTML es un conjunto de comandos diseñados para ser interpretados por navegadores de Web. Un documento HTML consta de contenido (texto, gráficos, vídeo, etc.) y una serie de comandos que indican a un navegador de Web cómo mostrar el contenido.

Privacidad y seguridad en la Web

Antes de la aparición de la Web, la seguridad en Internet generalmente sólo suponía un problema para los administradores del sistema, que intentaban mantener alejados de sus sistemas a los piratas informáticos. Con la llegada de la Web, la popularidad de Internet aumentó vertiginosamente. Prácticamente de la noche a la mañana, la gente empezó a realizar todo tipo de actividades potencialmente confidenciales a través de Internet, incluidas: transacciones bancarias y bursátiles; envío de datos personales a sitios Web; búsquedas en la Web y compra de libros y ropa. De modo que, aunque la Web es responsable de hacer más accesible Internet, también abre nuevas posibilidades para los robos de datos, las invasiones de privacidad y el fraude.

¿Por qué me afecta la privacidad en Internet?

Considere las diversas transacciones confidenciales que realizamos a diario. A modo de ejemplo, piense en una sencilla transacción por cajero automático: damos por hecho que siempre que utilizamos nuestras tarjetas en un cajero automático se dan las siguientes condiciones:

- **Privacidad:** Sólo usted y el destinatario elegido pueden acceder a la información de la transacción. El PIN (o número de identificación personal) que utiliza para acceder a su cuenta bancaria proporciona un elevado nivel de privacidad—siempre que no comparta su PIN con otras personas ni deje su tarjeta en cualquier lugar, el balance de su cuenta bancaria estará a salvo de miradas curiosas.
- **Integridad:** Durante la transacción, nada puede intervenir ni modificar la información. Cuando sacamos veinte dólares de nuestra cuenta corriente, esperamos lógicamente que el cajero automático no añada un cero adicional.
- **Confianza:** Puede confiar en que el destinatario es quien afirma ser; el destinatario puede confiar en que usted es quien dice ser.

Las empresas como bancos y compañías de seguros están obligadas por ley a atenerse a los estatutos federales que rigen la inviolabilidad de la información de las transacciones. El problema de Internet es que todavía no han evolucionado mecanismos institucionales bien establecidos, que garanticen la inviolabilidad de su información.

Privacidad en la Web

¿Quién está pinchando la red?

Los piratas informáticos son unos individuos a los que les encanta acceder ilegalmente a los equipos con el objetivo de acceder, robar y en ocasiones dañar los datos. La mayoría de piratas informáticos son inofensivos, violan un sistema de seguridad porque les supone un reto emocionante. Pero algunos piratas informáticos creen que si hay organizaciones o personas que no les importan, no está mal entrar en sus equipos y hacer estragos en éstos. Otros piensan que el robo en línea de dinero y de recursos es legítimo, siempre que esté destinado a dar soporte a más pirateo.

“Snooping” y “sniffing”

Desde sus comienzos, Internet ha sido (y va a seguir siendo durante mucho tiempo) una red abierta. La apertura significa que la información de Internet viaja sin ninguna seguridad especial: cualquier individuo que pueda supervisar el tráfico de la red puede interceptarlo. Este tipo de supervisión se conoce como “sniffing” y es fácil de realizar utilizando “sniffers”. Se trata de programas (o aparatos de hardware) diseñados para supervisar los datos que viajan a través de una red. Originariamente, estos programas se diseñaron para ayudar a los administradores de la red a resolver los problemas de conectividad. Desgraciadamente, la misma herramienta se puede utilizar también para robar información. Los “sniffers” son insistentes y difíciles de detectar.

Esta práctica a menudo comienza cuando un pirata informático rompe la seguridad de un ISP (Proveedor de servicios de Internet) local. Un pirata informático no necesita tener acceso físico a los locales del ISP—a veces, basta con una línea telefónica (aunque también es posible pinchar el equipo con el acceso físico a los cables de red). Cuando un pirata informático pone en peligro el sistema de un ISP, el tráfico de red que viaja a través de dicho ISP deja de ser seguro.

Servidores Web y cortafuegos

Las transacciones seguras sólo constituyen una parte del problema. Cuando el servidor Web de un ISP recibe información, el ISP debe poder garantizar la seguridad de la información. A los piratas les gusta atacar la seguridad de los servidores Web, debido a que ésta sigue siendo muy precaria. En consecuencia, los administradores de la Web asumen que un servidor Web puede ser atacado e intentan mantenerlos apartados de otros equipos con misiones cruciales. Sin embargo, algunas aplicaciones Web deben interactuar con bases de datos corporativas, que constituyen una puerta abierta para los piratas avispados. Una forma de tecnología de seguridad denominada "cortafuegos" puede cerrar la puerta, pero los cortafuegos a menudo se mantienen débilmente, e incluso en el mejor entorno, no pueden garantizar la protección de determinados servicios.

¿Qué puedo hacer para mantener a salvo mi material?

Con los "sniffers", un pirata informático puede interceptar números de tarjetas de crédito y otra información privada, capturando transmisiones de datos y utilizando después algoritmos de correspondencia de patrones para filtrar la información importante. La información interceptada sobre las tarjetas de crédito puede venderse a criminales, con la intención de cometer fraude.

Para evitar este problema, los navegadores Web incorporan tecnología de codificación que encubre la información y dificulta su acceso. La codificación es la técnica base que utilizan los navegadores de Web para garantizar la seguridad de la información.

La codificación estándar actual se denomina "Secure Sockets Layer" (SSL), a la que Microsoft y Netscape dan soporte y tienen incorporada en sus navegadores. Un icono del navegador cambia para indicar que SSL está activo. Al realizar una transacción con SSL activo, puede estar tranquilo porque la transacción es segura.

Al visitar un sitio protegido mediante SSL, las versiones más recientes de Netscape Communicator y Microsoft Internet Explorer utilizan un indicador visual que le indica que el sitio es seguro. Si desea obtener más información, consulte *¿Cómo puedo saber si un sitio Web es seguro?*

❑ **NOTA**: La Comprobación de Guard Dog le permite saber si el navegador de Web está actualizado. Las versiones de navegador más recientes suelen ofrece un mayor grado de seguridad.

¿Cómo puedo saber si un sitio Web es seguro?

En la actualidad, muchos sitios utilizan SSL para realizar actividades comerciales seguras en la Web. Además de la seguridad del servidor Web, la mayoría de los navegadores de Internet habituales proporcionan información sobre el nivel de seguridad del sitio al que está conectado actualmente. Por ejemplo, Netscape Communicator muestra un icono con un candado en el ángulo inferior izquierdo de la ventana del navegador. Si dicho icono está roto, indica que el sitio no es seguro. Si no está roto, indica que el sitio es seguro. Además, si el símbolo del candado tiene un fondo dorado, el sitio utiliza una potente codificación de 128 bits.

Las versiones recientes de los navegadores Microsoft Internet Explorer y America Online muestran también información sobre seguridad. Para obtener más información sobre el modo en que el navegador indica el nivel de seguridad de los sitios, consulte la ayuda en línea de los navegadores, o bien la documentación impresa.

¿Si SSL es tan excepcional, cuál es el problema?

SSL tiene algunos problemas. Uno de ellos consiste en que no todo el mundo dispone de un servidor o navegador habilitado para SSL. Algunos administradores de Web no quieren utilizar SSL porque tiene un coste adicional y porque puede reducir la velocidad de las transacciones del servidor. Otro problema más grave que afecta a SSL es la forma en que está implementado. Resulta que algunos programadores hacen suposiciones erróneas sobre SSL, lo que significa que algunas versiones de navegador más antiguas son menos seguras. La buena noticia es que Microsoft y Netscape coordinan ahora sus esfuerzos de seguridad, lo que significa un estándar universal más seguro para la seguridad de la Web.

¿Qué me dice de la Autentificación?

La Autentificación es un método para garantizar que ambas partes de una transacción de Internet son lo que dicen ser. Por ejemplo, si recibe información del banco sobre el balance de su cuenta, deseará estar seguro de que está tratando con el banco y no con alguna entidad no autorizada. Además, el banco desea estar seguro de que le está proporcionando la información a usted, y no a una persona que simplemente conoce el número de su cuenta bancaria.

La Autentificación suele entrañar la introducción de un ID de usuario y contraseña. A fin de evitar la interceptación de ID y contraseñas, la autentificación utiliza la codificación para desvirtuar esta información antes de transmitirla.

❑ **NOTA:** Los Certificados son tecnologías Microsoft diseñadas para garantizar la identidad de una persona y la seguridad de los sitios Web. Los Certificados personales verifican que el usuario es quien dice ser. Los certificados de sitios Web verifican que un sitio Web es seguro y es lo que pretende ser (de modo que los sitios Web no puedan falsear su identidad). Al abrir un sitio Web que tiene un certificado, Internet Explorer comprueba si el certificado es correcto. Si no lo es, Internet Explorer le avisa. Los Certificados son estupendos, en teoría. El problema reside en que sólo establecen un estándar de seguridad—Los sitios Web pueden elegir libremente si van a utilizar certificados o no.

Funcionamiento de la codificación

La única manera de mantener un secreto es no contárselo a nadie y no anotarlo en ningún sitio. Si necesita compartir el secreto, puede ocultarlo dentro de otro mensaje, e indicar al destinatario deseado cómo puede encontrarlo. La codificación del equipo oculta los mensajes haciendo que los datos originales sean ininteligibles. El objetivo consiste en distorsionar los datos para que no puedan leerse. En este caso, los propios datos no sirven de nada si accede a ellos un destinatario no autorizado.

Los sistemas de codificación más sencillos utilizan el desplazamiento de letras, en el que un mensaje se codifica desplazando las letras *n* del alfabeto. Por ejemplo, digamos que la letra A se cambia por la B, la B por la C, etc. Mientras el destinatario sepa cómo ha desplazado las letras, puede describir con facilidad el mensaje invirtiendo el proceso. Por supuesto, una forma sencilla de romper este tipo de codificación sería simplemente probar las 26 combinaciones posibles de letras, hasta recuperar el mensaje final—no es un método de codificación muy sólido.

La codificación informática utiliza una técnica para ocultar el mensaje mucho más complicada. En lugar de un simple esquema de desplazamiento de letras, el mensaje original se transforma mediante un algoritmo matemático. El algoritmo utiliza una “clave” secreta para desvirtuar el mensaje y la clave es necesaria para volver a transformarlo en el original. La clave es similar a la llave de una casa: Cuantos más dientes tenga una llave, más difícil resultará abrir el candado. De modo similar, la codificación “sólida” utiliza llaves con muchos “dientes”—en este caso, bits de datos.

Se suelen utilizar dos niveles de codificación. El estándar internacional es la codificación de 40 bits, pero algunos sitios de los EE.UU. utilizan un nivel de codificación superior, 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.

En la Web, el navegador trabaja con sitios Web seguros para establecer y administrar la codificación que garantice la seguridad de la información. Si las opciones de seguridad de su navegador incluyen Secure Sockets Layer (SSL), que garantiza la privacidad de la transmisión de datos, debe activar esta opción para facilitar una transmisión de datos segura.

❑ **NOTA:** La Comprobación de Guard Dog comprueba automáticamente el nivel de seguridad del navegador y le indica si es necesario cambiarlo.

Seguridad en la Web

Uno de los desarrollos más interesantes de la Web es la evolución de programas ejecutables y transferibles. Java y ActiveX son dos herramientas que ayudan a los programadores a crear programas que pueden “vivir” en el interior de páginas Web, y utilizan el navegador de Web para ejecutarse automáticamente a través de Internet. Java permite que las páginas Web alojen pequeños programas denominados subprogramas (“applets”). Cuando los navegadores habilitados para Java acceden a una página Web que contiene Java, transfieren y ejecutan automáticamente los subprogramas que encuentran en la página. Se trata de un desarrollo fascinante, puesto que posibilita la transferencia y ejecución de programas a través de la Web. Las previsiones apuntan a la creación de completos programas, dirigidos por la Web, escritos totalmente en Java. ActiveX es una tecnología similar, desarrollada por Microsoft.

Java contiene un sistema de seguridad interno que maneja los riesgos de seguridad. ActiveX utiliza un modelo diferente, basado en la autentificación de certificados. Los certificados contienen información sobre quién ha desarrollado el código ActiveX. La idea en este caso es que si se sabe quién ha desarrollado el código, puede ejecutarse libremente. Ambos esquemas de seguridad ofrecen un nivel de seguridad elevado, pero ninguno puede prometer aún que el contenido ejecutable sea seguro al cien por cien.

Subprogramas perjudiciales

Una posible amenaza contra la seguridad es la existencia de un programa Java o Active X malicioso que ataca al equipo a través de la Web. Un subprograma perjudicial puede, por ejemplo, desbaratar la seguridad de Java, al burlar su modelo de seguridad, y destruir los datos del disco duro, o bien apropiarse de información confidencial de la unidad de disco duro. Los navegadores más recientes han hecho un buen trabajo para resolver estos problemas. Siempre que esté utilizando la versión más reciente de navegador, estará protegido. Hasta la fecha, no ha habido noticias legítimas de que Java o ActiveX hayan perjudicado a nadie. Sin embargo, no existe garantía de que no vaya a producirse un ataque en el futuro.

¿Puedo impedir que los programas accedan a Internet?

Puede utilizar Guard Dog para especificar las aplicaciones a las que se permite el acceso a Internet desde su equipo. Obviamente, el navegador de Internet predeterminado es una de estas aplicaciones.

Si la función Vigilante de Guard Dog se ejecuta en segundo plano mientras el usuario trabaja en Internet, cada vez que la aplicación intente acceder a Internet, aparecerá un cuadro de diálogo preguntándole si desea permitir el acceso una sola vez, siempre o nunca.

Virus informáticos y la Web

Un virus informático es un pequeño programa informático que se reproduce automáticamente y se extiende de un equipo a otro. Los virus pueden infectar a programas, la unidad de disco duro e incluso algunos archivos de documento que emplean macros. Los virus no infectan a los archivos de datos, pero pueden crear problemas que le impiden acceder a los datos. Los virus no son accidentes—siempre los crean programadores informáticos.

Los virus de PC se asemejan a los virus biológicos en lo siguiente:

- Se extienden de un host a otro—el “host,” en este caso, es su PC.
- Se reproducen con mucha facilidad.
- Pueden causar estragos en un host infectado.

Los virus biológicos han demostrado ser tenaces: el éxito de la medicina moderna en su lucha contra las infecciones víricas ha sido hasta ahora limitado. Afortunadamente, los virus de PC difieren de los biológicos en que, una vez identificados, son más fáciles de combatir.

¿Son realmente tan peligrosos los virus?

Tenga en cuenta que sus posibilidades de contraer un virus de PC son escasas, y sus posibilidades de contraer un virus realmente peligroso aún más. Los virus más alarmantes son programas maliciosos que dañan o eliminan intencionadamente los datos del PC. Los virus más benignos pueden simplemente mostrar un mensaje en el monitor o crear un sonido extraño, y después desaparecer. Pero incluso los virus más benignos ocupan espacio en disco, y muchos permanecen en memoria, lo que puede originar un comportamiento errático o el bloqueo del PC.

Tipos de virus

Existen tres tipos de virus principales:

- **Virus de archivo o de programa:** Un virus de programa está unido a un programa específico del PC. Puesto que muchos PC tienen en común determinados archivos (por ejemplo, **command.com** del programa DOS, o el comando "**dir**"), dichos archivos se convierten en destinos tentadores para los programadores de virus. Los virus de programa permanecen inactivos hasta que se ejecuta el programa asociado.
- **Virus de arranque (o virus de Registro de Arranque Principal):** El sector de arranque de un disco es una ubicación física en el disco que contiene información sobre éste y los archivos que contiene. Todos los discos y unidades tienen un sector de arranque, aunque no sean todos "ejecutables". Un virus de arranque infecta el sector de arranque de las unidades de disquetes y de disco duro y se activa cuando el usuario accede o un disco infectado o arranca desde el mismo.
- **Virus en macros:** Los virus en macros se encuentran en archivos de documento, como archivos de Microsoft Word o Excel. Estos archivos pueden contener macros que automatizan el trabajo—pero las macros también pueden grabarse, dañando el PC. Los virus en macros se activan al abrir un archivo de documento infectado.

Hay un último aspecto a mencionar sobre los "virus" trampa, que no son virus en el sentido estricto del término. Un virus trampa reproduce una broma, extendiendo una información errónea (si es bien intencionada) de que si transfiere un determinado archivo, o si recibe un mensaje de correo electrónico con un determinado asunto, su PC se infectará con un virus. Los mensajes de correo electrónico son siempre seguros; se trata de sencillos archivos de texto y no pueden contener virus. Los datos adjuntos a mensajes de correo electrónico (archivos que el emisor adjunta a un mensaje; se transfieren al PC al recuperar el mensaje) sí pueden contener virus. (Si el acceso a archivos de correo electrónico se activa en Centinela de virus, Guard Dog explora automáticamente los datos adjuntos al correo electrónico antes de abrirlos).

¿Cómo se puede infectar el PC con un virus?

Un aspecto importante a recordar es que los virus *sólo* se extienden al ejecutar una aplicación infectada (o abrir un archivo de documento infectado, en el caso de los virus en macros). Un virus no puede viajar a través de la línea telefónica e infectar el PC por su cuenta. Para infectar el PC con un virus, es necesario que el usuario transfiera o copie una aplicación infectada y después la ejecute.

Es decir, la única manera de evitar por completo la infección de virus es no hacer nada—no utilice Internet; jamás transfiera un archivo; no acepte jamás un disquete de otra persona; no comparta jamás archivos de Word o Excel. Por supuesto, este remedio draconiano tipo “Robinson Crusoe” no es realista en el entorno informático actual, en el que compartir los datos es imprescindible y el acceso a Internet es una actividad diaria.

❑ **NOTA:** Internet Guard Dog se suministra con McAfee VirusScan que es fácil de utilizar. Explora automáticamente el PC para detectar signos de infección por virus, e investiga los archivos bajo sospecha antes de que puedan infectar el PC.

Los virus se expanden cuando se comparten disquetes infectados entre varios PC y cuando se transfieren y ejecutan archivos infectados desde servicios en línea, boletines electrónicos o Internet. Otra ruta potencial (pero remota) para la transmisión de virus se produce al acceder a páginas Web que utilizan la tecnología Active X de Microsoft o Java de Sun. Las páginas Web que utilizan ActiveX, por ejemplo, pueden transferir automáticamente programas al PC que programas podrían estar infectados con un virus. Aunque no se conoce ningún caso en el que ActiveX y Java hayan difundido virus, sigue existiendo una posibilidad — muy remota—de que el PC adquiera un virus de esta forma.

Un virus puede ocultarse en el próximo archivo que transfiera, o en un disquete prestado —incluso en disquetes comprados en una tienda. La transferencia de shareware también es una fuente de infección.

❑ **NOTA:** Aunque Java y ActiveX no son, estrictamente hablando, virus (es decir, no se pueden extender ni reproducir), sí pueden dañar el PC. Guard Dog’s default settings allow it to monitor all Java and ActiveX activity on your PC, and warn you before something potentially dangerous occurs.

Preguntas más frecuentes sobre la privacidad en Internet

¿Qué información recogen los sitios Web sobre mí?

Los sitios Web recogen información sobre usted de dos maneras principalmente.

- En primer lugar, puede proporcionar usted mismo la información al registrar el software o responder a cuestionarios de Internet.
- En segundo lugar, cuando pide que se le permita acceder a la versión electrónica de un periódico, o utiliza una "tarjeta de compra" para adquirir productos en la Web, una cookie, descrita en el apartado "¿Qué son las cookies y cómo se utilizan?" en la página 70, podría grabarse en su equipo, donde se almacena información, como su contraseña e ID de usuario para el periódico o los artículos que ha comprado con su calidad y precio.

¿Qué información obtienen las compañías cuando registro productos en línea?

Las compañías sólo obtienen la información que introduce en el formulario de registro cuando se registra electrónicamente. No obtienen ninguna información sobre su sistema informático, su utilización del equipo u otra información guardada, a menos que la proporcione como parte del registro.

Esta información se utiliza para la investigación de estudios de mercado de la empresa y para enviarle información sobre nuevos lanzamientos, otros productos, etc. La información se podría vender a otras empresas, a modo de listas de correo de suscriptores de revista o empresas con un sistema de pedido por correo que a su vez la pueden vender a terceros.

Algunas compañías le permiten especificar que no desea recibir mensajes de correo ni que se venda su nombre y dirección a otras compañías. Si la compañía no proporciona esta opción, puede introducir información falsa para evitar que le envíen mensajes de correo, tanto postales como electrónicos.

¿Qué son las cookies y cómo se utilizan?

Una cookie es un pequeño archivo que contiene datos. Los datos de la cookie varían en función de su objetivo. Después de la solicitud de un sitio Web, el navegador de Web guarda las cookies en el equipo. Generalmente, las cookies contienen tan sólo información que mejora su experiencia en la Web. Por ejemplo, al utilizar un sitio Web para comprar equipo informático, puede añadir elementos a una "cesta de la compra". La información sobre los elementos que añade a la cesta de la compra se guarda en una cookie en el equipo, puesto que el navegador de Internet no puede retener información en

una página de Internet cuando pasa a otra página de Internet. La cookie guarda información sobre sus compras y permite al sitio crear un formulario de pedidos final para usted.

Otro ejemplo es la cookie que una tienda Web guarda en su equipo, conservando su nombre de usuario y contraseña, de modo que no tenga que introducir esta información cada vez que se conecta al sitio.

Algunas tiendas utilizan la información de las cookies para registrar el número de veces que se conecta al sitio, qué páginas utiliza y si ha seleccionado algunos de los títulos de anuncios. Los sitios con reputación proporcionan información sobre privacidad para indicarle cómo se utiliza la información reunida.

Los ejemplos anteriores de cookies son muy útiles para el usuario, por lo menos hasta cierto punto. Sin embargo, otros sitios pueden transferir cookies sólo para recoger información sobre su utilización de Internet. Estas cookies no tienen ninguna utilidad para usted.

Puede utilizar la función Bloqueador de cookies de Guard Dog para controlar qué cookies se transfieren al equipo. Para obtener más información, consulte el apartado “Acciones que realiza el Bloqueador de cookies” en la página 35.

Fuentes de información sobre la privacidad y seguridad en Internet

Información sobre trampas en Internet

United States Department of Energy—Computer Incident Advisory Capability

Enumera y describe trampas, virus y diversa información de seguridad.

http://ciac.llnl.gov/

Más información sobre virus informáticos

International Computer Security Association Anti-Virus Lab

http://www.ncsa.com/virus/

Describe virus, alertas de virus y trampas.

Página de virus de Yahoo!

La página de virus de Yahoo! contiene vínculos para empresas de software antivirus, grupos de noticias sobre virus Usenet y vínculos para la información específica de virus.

Preguntas más frecuentes sobre virus de Usenet

Contiene un compendio bien organizado de información sobre virus, recogida a partir de grupos de noticias sobre virus de Usenet.

http://www.cis.ohio-state.edu/hypertext/faq/bngusenet/comp/virus/top.html

Más información sobre seguridad

Dos buenos puntos de partida para obtener información sobre seguridad en la Web son la ayuda en línea para Netscape Communicator y Microsoft Internet Explorer.

Sitio de National Institute of Health's Computer Security Information

Vínculos interesantes a muchos sitios de información sobre seguridad.

http://www.alw.nih.gov/Security/security.html

Sitio de Seguridad de Microsoft

Documentos y descripciones de los esfuerzos de seguridad de Microsoft

http://www.microsoft.com/security/

Más información sobre privacidad

Electronic Freedom Foundation

http://www.eff.org/pub/Privacy/

Internet Privacy Coalition

http://www.privacy.org/ipc/

Soporte del producto B

ANTES DE PONERSE EN CONTACTO con McAfee Software para obtener soporte técnico, sitúese cerca del equipo en el que se ha instalado McAfee Guard Dog y verifique la siguiente información:

- ¿Ha enviado la tarjeta de registro del producto?
- Versión de Internet Guard Dog
- Número de cliente, en caso de que esté registrado
- Nombre del modelo de disco duro (interno o externo)
- Versión del software del sistema
- Capacidad de memoria (RAM)
- Tarjetas, placas o monitores adicionales
- Nombre y versión del software en conflicto
- Mensaje de error EXACTO que aparece en pantalla
- ¿Qué pasos llevo a cabo antes de recibir el mensaje de error?
- Una descripción detallada del problema

Cómo ponerse en contacto con McAfee

Servicio de atención al cliente

Para realizar pedidos de productos u obtener información acerca de los mismos, póngase en contacto con el departamento de Servicio de atención al cliente de McAfee llamando al número de teléfono (901) 11 67 32 o escribiendo a la siguiente dirección:

McAfee Software
3965 Freedom Circle
Santa Clara, CA 95054
EE.UU.

También puede realizar pedidos de productos en línea en la dirección http: / / store.mcafee.com

Si desea ayuda adicional o desea realizar preguntas específicas, escriba a la dirección de correo electrónico correspondiente:

- Para preguntas generales acerca de realizar pedidos de software: mcafeestore@beyond.com
- Para obtener ayuda a la hora de descargar software: mcafeedownloadhelp@beyond.com
- Para averiguar el estado de un pedido existente: mcafeeorderstatus@beyond.com

Para obtener información acerca de una promoción: mcafeepromotions@beyond.com

Soporte técnico

Soporte a través de la Web

McAfee es famoso por el buen trato que profesa a sus clientes. Hemos seguido esta tradición al convertir nuestro sitio en la World Wide Web (http://www.mcafee.com) en un valioso recurso para ofrecer respuestas a temas de soporte técnico.

Le aconsejamos que visite este sitio Web para consultar las respuestas a las preguntas más frecuentes, las actualizaciones del software de McAfee y para obtener acceso a la información de virus y novedades de McAfee.

Saque el máximo partido de McAfee Product KnowledgeCenter, su centro de soporte en línea gratuito del producto, las 24 horas del día, 7 días a la semana (http://support.mcafee.com/tech_supp/pkc.asp).

Foros de soporte y teléfonos de contacto

Si no encuentra lo que necesita o no dispone de acceso a la Web, utilice uno de nuestros servicios automatizados.

Tabla B-1.

World Wide Web	www.mcafee.com
CompuServe	GO MCAFEE
America Online	palabra clave MCAFEE
Microsoft Network	mcafee

Si los servicios automatizados no poseen las respuestas que necesita, póngase en contacto con McAfee llamando a los siguientes números de teléfono de lunes a viernes, de 9 de la mañana a 6 de la tarde hora del Pacífico para obtener el soporte gratuito de 30 días y el soporte por minuto y por incidente de 24 horas, 7 días a la semana.

Tabla B-2.

Soporte telefónico gratuito de 30 días	972-308-9960
Soporte telefónico por minuto	1-900-225-5624
Soporte telefónico por incidente (35 dólares americanos)	1-800-950-1165

Formación de McAfee

Si desea obtener información acerca de la planificación de la formación in situ de un producto McAfee, llame al (800) 338-8754.

Limitación de responsabilidad: Los horarios y números de teléfono están sujetos a cambios sin previo aviso.

Indice

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W

NA-354-0010-SP-2