

Guía del usuario de Norton Personal Firewall 2000

NORTON™

Personal Firewall 2000 VERSIÓN 2.0



07-30-00411-ES

Guía del usuario de Norton Personal Firewall 2000

El software descrito en la presente guía está sujeto a un acuerdo de licencia y sólo podrá ser utilizado según los términos del mismo.

Aviso de copyright

Copyright © 1995-2000 Symantec Corporation. Todos los derechos reservados.

Norton Personal Firewall 2000

SIN GARANTÍA. La presente documentación se proporciona tal cual es. Symantec Corporation no garantiza la precisión de la información en ella contenida ni se responsabiliza por el uso que de ella pueda hacerse. El uso de la documentación técnica o de la información aquí contenida es responsabilidad del usuario. Esta documentación puede contener inexactitudes técnicas o de otro tipo y erratas tipográficas. Symantec se reserva el derecho de realizar cambios sin previo aviso.

Queda prohibida la reproducción de esta publicación o de parte de ella sin la autorización expresa por escrito de Symantec Corporation, Peter Norton Group, 20330 Stevens Creek Blvd., Suite 200, Cupertino, CA 95014, (EE.UU.).

Marcas comerciales

Symantec, el logotipo de Symantec, Norton, Norton Internet Security, Norton SystemWorks, Emergency Disk, LiveUpdate, Norton AntiVirus, Norton Utilities y Rescue Disk son marcas comerciales de Symantec Corporation.

Windows es una marca registrada de Microsoft Corporation. Iomega es una marca registrada; Zip y Zip Rescue son marcas comerciales de Iomega Corporation. AOL y CompuServe son marcas comerciales registradas de America Online, Inc. Prodigy Internet es una marca comercial de Prodigy. Pentium es una marca comercial registrada de Intel Corporation. Otros nombres de productos mencionados en este manual pueden ser marcas comerciales registradas de sus respectivos propietarios y son reconocidas como tales.

Impreso en Irlanda.

10 9 8 7 6 5 4 3 2 1



NOTA: SYMANTEC LE CONCEDE LA LICENCIA DE USO DEL PROGRAMA Y LOS DATOS INCLUIDOS SÓLO BAJO LA CONDICIÓN DE QUE ACEPTÉ TODOS LOS TÉRMINOS CONTENIDOS EN ESTE CONTRATO DE LICENCIA. SI NO ESTÁ DE ACUERDO CON LOS MISMOS, SYMANTEC NO PUEDE CONCEDERLE LA LICENCIA DE USO, POR LO QUE DEBE DEVOLVER EL PRODUCTO COMPLETO, CON LA PRUEBA DE COMPRA CORRESPONDIENTE, A SU DISTRIBUIDOR EN EL PLAZO DE SESENTA DÍAS DESDE LA FECHA DE COMPRA, SIÉNDOLE RESTITUIDO SU IMPORTE.

LICENCIA Y GARANTÍA

El programa y los datos incluidos con esta licencia (el "Software") son propiedad de Symantec o sus proveedores y está protegido por las leyes de Propiedad Intelectual. Aunque Symantec continúa siendo el propietario del Software, usted adquiere ciertos derechos de uso del Software una vez que acepte el contrato de licencia. Salvo modificaciones contenidas en los apéndices del contrato de licencia que puedan incluirse con el mismo, sus derechos y obligaciones con respecto a este Software son los siguientes:

Usted puede:

- (i) usar una copia del Software en un único ordenador;
- (ii) hacer una copia de seguridad del Software o copiar el Software en el disco duro del ordenador y mantener los originales como copia de seguridad;
- (iii) usar el Software en una red, siempre que disponga de una copia con contrato de licencia del Software para cada ordenador que tenga acceso al Software a través de dicha red;
- (iv) tras notificarlo por escrito a Symantec, cedido el Software de forma permanente a otra persona o entidad, siempre que usted no retenga copias del Software y el cesionario acepte los términos del contrato; y

Usted no puede:

- (i) copiar la documentación que acompaña al Software;
- (ii) otorgar licencias de uso, alquilar o arrendar el Software o parte del mismo;
- (iii) realizar ingeniería inversa, decompilar, desensamblar, modificar, traducir, realizar intento alguno de descubrir el código fuente del Software ni crear productos que se deriven del mismo; o
- (iv) usar una versión anterior o copia del Software una vez que se hayan recibido disquetes que reemplacen a los originales o una versión actualizada que reemplace a la anterior, salvo que haya cedido la versión anterior a la actualizada un cesionario de su elección, y que dicho cesionario se comprometa por escrito que será el único usuario final del producto, y se obligue a los términos de este acuerdo. A no ser que haya cedido en estas condiciones la versión anterior de una versión actualizada, al actualizar el Software deben destruirse todas las copias de la versión anterior.

Garantía Limitada:

Symantec no garantiza que el Software vaya a cubrir sus necesidades, que el Software trabaje de forma ininterrumpida o que esté libre de errores.

LA ANTERIOR GARANTÍA ES EXCLUSIVA Y REEMPLAZA CUALQUIER OTRA GARANTÍA EXPLÍCITA O IMPLÍCITA, INCLUYENDO LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, ADECUACIÓN A UN FIN PARTICULAR O NO INFRACCIÓN. ESTA GARANTÍA LE PROPORCIONA DERECHOS LEGALES ESPECÍFICOS. PUEDE TENER OTROS DERECHOS ADICIONALES, QUE PUEDEN VARIAR DE ESTADO A ESTADO.

Inexistencia de Responsabilidad por Daños:

CON INDEPENDENCIA DE QUE CUALQUIER SOLUCIÓN INCLUIDA NO CUMPLA SUS OBJETIVOS BÁSICOS, EN NINGÚN CASO SERÁ SYMANTEC RESPONSABLE DE CUALQUIER DAÑO DIRECTO O INDIRECTO, INCLUYENDO PÉRDIDAS DE BENEFICIOS O DATOS DEBIDA AL USO O IMPOSIBILIDAD DE USO DEL SOFTWARE, INCLUSO EN EL CASO DE QUE SYMANTEC HAYA SIDO INFORMADO DE LA POSIBILIDAD DE TAL DAÑO.

ALGUNOS ESTADOS NO PERMITEN LA LIMITACIÓN O EXCLUSIÓN DE RESPONSABILIDAD POR DAÑOS FORTUITOS O SUS CONSECUENCIAS, POR LO QUE ES POSIBLE QUE EN SU CASO LA LIMITACIÓN O EXCLUSIÓN ANTERIOR NO SEA APLICABLE.

LA RESPONSABILIDAD DE SYMANTEC NO EXCEDERÁ, EN NINGÚN CASO, EL PRECIO DE COMPRA DEL SOFTWARE. La limitación y exclusión de responsabilidades arriba expuesta será aplicable con independencia de si acepta el Software.

Derechos Restringidos del Gobierno de los Estados Unidos de América:

DERECHOS RESTRINGIDOS. El uso, la duplicación o la revelación por el gobierno está sujeto a las restricciones establecidas en el subpárrafo (c) (1) (ii) de la cláusula de los Derechos sobre Datos Técnicos y Software de Ordenadores en DFARS 252.227-7013 o los subpárrafos (c) (1) y (2) de la cláusula de Derechos Restringidos sobre el Software de Ordenadores Comercial en 48 CFR 52.227-19, cuando sea aplicable, Symantec Corporation, 10201 Torre Avenue, Cupertino, CA 95014, EE.UU.

General:

Este Contrato sólo puede ser modificado por un apéndice al contrato de licencia incluido con el mismo o por un documento escrito firmado por usted y Symantec. Si desea realizar cualquier pregunta con respecto a este Contrato o si, por cualquier razón, desea contactar con Symantec, por favor escriba al Servicio de Asistencia y Ventas al Cliente de Symantec, Symantec Europe, PO Box 5689, Blanchardstown, Dublin 15, Irlanda.

C O N T E N I D O

Capítulo 1 Introducción

¿Qué hace Norton Personal Firewall?	7
Norton Privacy	9
Estadísticas y archivos de registro	9
Instalación de Norton Personal Firewall	9
Requisitos de sistema	9
Procedimiento para la instalación	10
Para desplazarse dentro de Norton Personal Firewall	10
Configuración de las opciones de Norton Personal Firewall	11
Actualización de Norton Personal Firewall utilizando LiveUpdate	11
Acerca de su suscripción	11
Uso de la Ayuda para saber más sobre Norton Personal Firewall	12

Capítulo 2 Personalización de Norton Personal Firewall

Personalización de las funciones de seguridad	16
Personalización de Norton Personal Firewall	17
Configuración de los niveles de seguridad de Java y de ActiveX	19
Protección de la privacidad	22
Bloqueo de información confidencial	22
Bloqueo de cookies	24
Activación o desactivación de conexiones Web seguras	25

Capítulo 3 Solución de problemas

Preguntas más frecuentes	27
¿Cómo se desactiva Norton Personal Firewall?	27
¿Por qué no puedo enviar información en línea?	28
¿Por qué hay problemas de acceso a ese sitio Web?	29
¿Por qué FTP no funciona en los exploradores antiguos?	31
¿Cómo puede un sitio Web obtener información sobre mi explorador?	31
¿Qué son conexiones de entrada y de salida?	32

Preguntas sobre redes domésticas	32
¿Cómo trabaja el firewall con conexiones de Internet compartidas?	32
¿Cómo trabaja el firewall con archivos e impresoras compartidos?	32
¿Cómo se utiliza Norton Personal Firewall con un servidor proxy?	34
Preguntas sobre firewall	35
¿Por qué no aparece el Asistente de normas de firewall?	35
¿Cómo reviso o cambio las normas de firewall?	36
Si dos normas de firewall tratan del mismo asunto, ¿cuál se ejecuta?	37
¿Para qué sirven las normas de firewall predeterminadas?	38
Si elimino las normas predeterminadas de firewall, ¿puedo recuperarlas?	39
¿Puedo crear configuraciones para determinados sitios Web?	39

Índice

Soluciones de servicio y asistencia de Symantec

Introducción

Existen millones de equipos conectados a Internet y su número aumenta día a día. Cuando su PC realiza una conexión con Internet, se conecta con millones de otros equipos y, a su vez, éstos pueden conectarse al suyo. Una conexión a Internet sin protección puede dejar su PC expuesto a ataques de piratas informáticos, virus, programas de caballos de Troya, sitios Web ofensivos y muchas otras amenazas de la red.

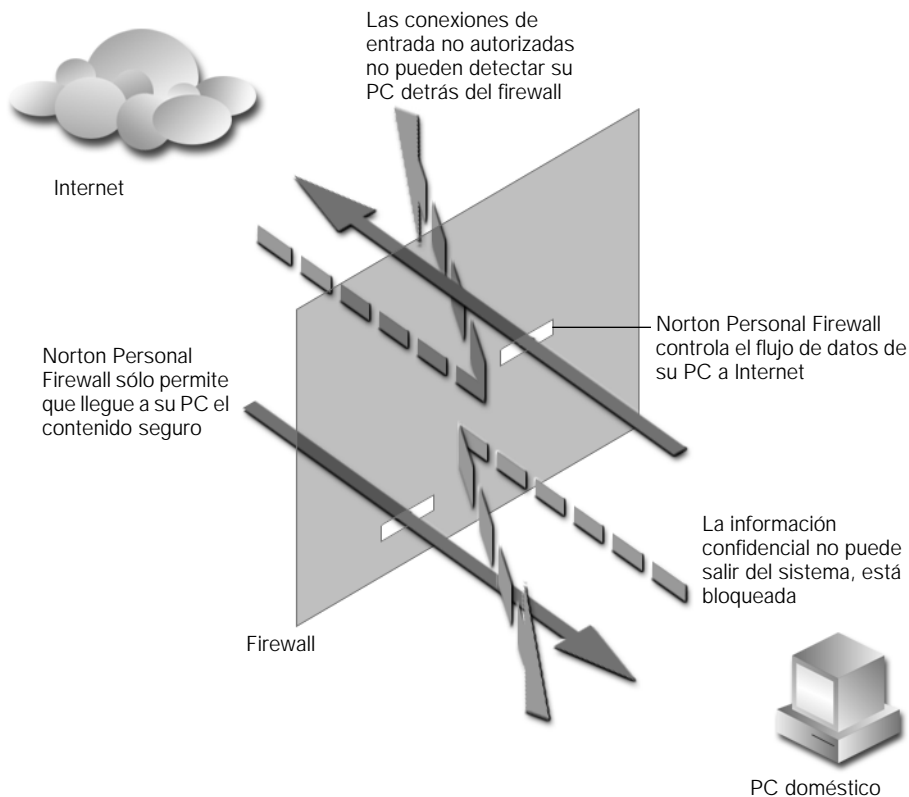
Norton Personal Firewall puede ayudarle a detectar todo lo que ocurre en su PC. Norton Internet Security controla la conexión con Internet para evitarle preocupaciones cuando el equipo está en línea. Le ayuda a proteger su seguridad y su privacidad.

¿Qué hace Norton Personal Firewall?

Norton Personal Firewall incluye Norton Personal Firewall y Norton Privacy Control. Juntas, controlan la conexión con Internet para evitarle preocupaciones cuando el equipo está conectado. Norton Personal Firewall protege su seguridad y Norton Privacy Control protege sus datos personales.

Norton Personal Firewall proporciona una barrera denominada *firewall* (servidor de seguridad) entre el equipo e Internet. Los programas firewall son filtros que bloquean o autorizan conexiones y transmisiones de datos en Internet. Dado que filtran conexiones e información, los firewalls le protegen de aquellos contenidos de Internet que puedan ser perniciosos.

Norton Personal Firewall utiliza normas para permitir o bloquear automáticamente las conexiones. Usted puede modificar estas reglas, permitiendo o impidiendo que determinados programas accedan a Internet.



De forma automática, Norton Personal Firewall filtra la mayor parte del contenido y determina cuál es la mejor forma de proteger muchas de las aplicaciones más conocidas. Cuando una aplicación no reconocida por Norton Personal Firewall intenta comunicarse a través de Internet, Norton Personal Firewall le avisa, y el Asistente de normas de firewall le ayuda a crear una norma nueva.

Los controles ActiveX y los subprogramas Java son programas que se ejecutan dentro del explorador. Aunque muchos de ellos son útiles, hay algunos nocivos. Norton Personal Firewall impide que los controles ActiveX y los subprogramas Java se ejecuten sin conocimiento del usuario, permitiéndole especificar sitios en los cuales estos programas están permitidos.

Norton Privacy

Es probable que no desee que datos confidenciales tales como números de tarjetas de crédito, el teléfono de su casa, etc., se envíen no cifrados por Internet. Norton Privacy evita que información confidencial se introduzca en sitios Web no seguros.

Los "cookies" son unos archivos de pequeño tamaño almacenados en su sistema que los sitios Web utilizan para realizar un seguimiento de sus visitas. Norton Personal Firewall puede bloquear cookies y otros datos que el explorador envía normalmente a sitios Web, tales como direcciones de correo electrónico o el último sitio visitado.

Estadísticas y archivos de registro

Norton Personal Firewall recoge datos estadísticos completos sobre su actividad. También puede registrar todas las actividades en Internet y tareas realizadas por Norton Personal Firewall que desee. Es muy fácil ver tanto las estadísticas como los archivos de registro.

Instalación de Norton Personal Firewall

Requisitos de sistema

Para poder utilizar Norton Personal Firewall, su PC debe cumplir los siguientes requisitos mínimos de sistema:

- Procesador de clase Pentium 133 MHz o más rápido
- Windows 95, Windows 98, Windows 98 SE, Windows NT 4.0 Workstation Sp3, Windows 2000 Professional
- 24 MB de memoria RAM (32 MB para Windows NT y Windows 2000), aunque se recomienda memoria adicional
- 10 MB de espacio libre en el disco
- Unidad de CD-ROM
- Soporte de Internet de Microsoft Windows
- Microsoft Internet Explorer 4.0, Netscape Navigator 4.0 o un explorador posterior

Procedimiento para la instalación

Siga estos pasos para instalar Norton Personal Firewall.

Para instalar:

- 1 Inicie Windows (si aún no está en funcionamiento).
- 2 Introduzca el CD de Norton Personal Firewall en la unidad de CD-ROM.
- 3 En la pantalla de bienvenida, haga clic en Instalar Norton Personal Firewall y siga las instrucciones que aparezcan en la pantalla.

Si no aparece la pantalla de bienvenida:

- 1 Haga doble clic en el icono Mi PC.
- 2 Haga doble clic en el icono de la unidad de CD-ROM.
- 3 Haga doble clic en el archivo Cdstart.exe.

Para desplazarse dentro de Norton Personal Firewall

Para iniciar Norton Personal Firewall, haga doble clic en el icono Norton Personal Firewall situado en la zona de notificación de la barra de tareas de Windows. También puede hacer clic en el botón Inicio, seleccionar Programas > Norton Personal Firewall > Norton Personal Firewall, o hacer doble clic en el icono Norton Personal Firewall del escritorio.



Configuración de las opciones de Norton Personal Firewall

Existen varias opciones que se pueden configurar en Norton Personal Firewall. Por ejemplo, puede optar por que Norton Personal Firewall se inicie automáticamente al encender el sistema.

Acceso a las opciones de Norton Personal Firewall:

- En la parte superior de la ventana de Norton Personal Firewall, haga clic en Opciones.

Actualización de Norton Personal Firewall utilizando LiveUpdate

LiveUpdate se conecta a Symantec a través de Internet para ver si hay actualizaciones disponibles del programa Norton Personal Firewall y también busca actualizaciones para la protección de Internet.

Symantec no cobra las actualizaciones del programa Norton Personal Firewall. Cuando caduque su suscripción gratuita, se aplicará una tarifa para la actualización de su protección en Internet . Sólo es necesario pagar los gastos normales de acceso a Internet.

Si se conecta a Internet a través de AOL, CompuServe o Prodigy Internet, primero tiene que conectarse a Internet y luego ejecutar LiveUpdate.

Para actualizar Norton Personal Firewall mediante LiveUpdate:

- 1 En la parte superior de la ventana de Norton Personal Firewall, haga clic en LiveUpdate.
- 2 Siga las instrucciones que aparecen en pantalla.

Acerca de su suscripción

Norton Personal Firewall precisa información actualizada para proteger el sistema contra nuevas amenazas a la seguridad. Actualice Norton Personal Firewall semanalmente y mantendrá su sistema seguro con la protección más reciente de Symantec.

La suscripción ofrece Norton Personal Firewall con la más reciente información sobre seguridad para mantener protegido el sistema:

- Normas de firewall que le protegen de los últimos programas de caballo de Troya y zombis, como Back Orifice y Trinoo.
- Listas de las últimas aplicaciones que utilizan Internet. Estas listas hacen posible que Norton Personal Firewall cree automáticamente normas de firewall cuando se usan aplicaciones de Internet. Véase [“Creación automática de normas de firewall”](#) en la página 18.

No es necesario registrar el producto para comenzar a disfrutar de la suscripción. Cuando llegue el momento de renovarla, haga clic en LiveUpdate para obtener las instrucciones de renovación.

Es importante mantener su suscripción al día. Norton Personal Firewall no puede protegerle de las nuevas amenazas sin información actualizada de Symantec.

Uso de la Ayuda para saber más sobre Norton Personal Firewall

Norton Personal Firewall viene provisto de un extenso sistema de ayuda en pantalla que le proporciona instrucciones detalladas sobre cómo utilizar todos los programas de Norton Personal Firewall.

Norton Personal Firewall ofrece tres tipos de ayuda:

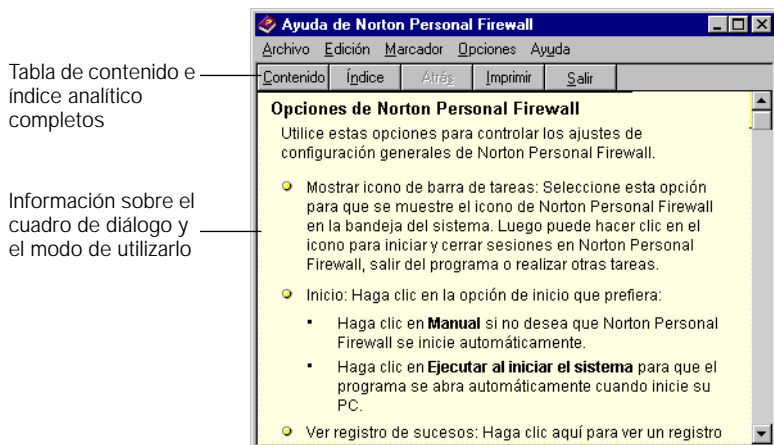
- Ayuda en los cuadros de diálogo de programas
- Ayuda Cómo
- Ayuda ¿Qué es esto?

Ayuda en los cuadros de diálogo y las ventanas de programas

La ayuda en los cuadros de diálogo proporciona información sobre el propio programa Norton Personal Firewall. Este tipo de ayuda se adapta al contexto, es decir, se refiere al cuadro de diálogo que esté utilizando.

Para obtener ayuda en una ventana o en un cuadro de diálogo:

- Haga clic en el vínculo Más información si hay alguno disponible.
- Haga clic en el botón Ayuda situado en el cuadro de diálogo.



Ayuda Cómo

La ayuda Cómo explica, paso a paso, los procedimientos más habituales de un usuario de Norton Personal Firewall. Puede acceder a estos temas por medio de las fichas Contenido e Índice. Abra la tabla de contenido o el índice analítico haciendo clic en el botón Contenido o Índice situado en la parte superior de cualquier tema de ayuda.

Ayuda ¿Qué es esto?

La ayuda ¿Qué es esto? ofrece una definición breve sobre cualquier componente determinado de una ventana o de un cuadro de diálogo.

Para acceder a la ayuda ¿Qué es esto?:

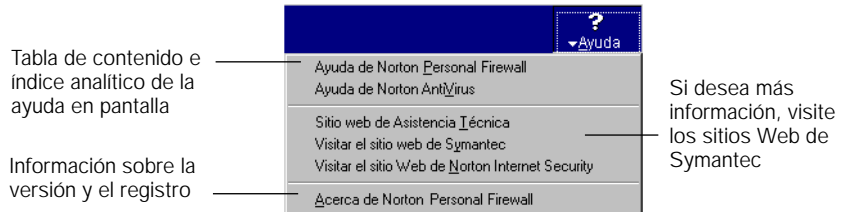
- Haga clic con el botón derecho del ratón en cualquier elemento de un cuadro de diálogo o de una ventana sobre el que necesite ayuda y seleccione ¿Qué es esto?

Obtención de ayuda desde el menú Ayuda

Siempre hay ayuda disponible en la ventana de Norton Personal Firewall.

Para acceder al menú Ayuda:

- En la parte superior de la ventana de Norton Personal Firewall, haga clic en Ayuda.



Personalización de Norton Personal Firewall

Con Norton Personal Firewall, su equipo estará más seguro que la mayoría de los PC en Internet.

Seguridad

Cuanto más tiempo pasa su PC conectado a Internet, especialmente si dispone de una conexión de alta velocidad, más oportunidades tienen los malintencionados piratas informáticos de introducirse en su sistema y hacer estragos: pueden robar archivos de su equipo e incluso dañar su contenido. Norton Personal Firewall le permite disfrutar a fondo de Internet mientras bloquea las agresiones y le avisa de las conexiones no autorizadas y de las tentativas de intrusión.

- El firewall (servidor de seguridad) personal emplea normas para bloquear o autorizar comunicaciones entre su PC e Internet. Le avisa cuando se solicita un tipo nuevo de comunicación y le permite decidir cómo tratarlo.
- La seguridad de subprogramas Java impide o autoriza la ejecución en su PC de dichos subprogramas
- La seguridad de controles ActiveX impide o autoriza la ejecución de los controles ActiveX en su PC. Los controles de ActiveX presentan más riesgo, debido a que pueden tener acceso completo a los datos de su PC.
- Su suscripción mantiene al día las normas de firewall.

Privacidad

Es muy probable que tenga muchos datos personales almacenados en su PC: números de tarjetas de crédito, información sobre cuentas bancarias en línea, así como datos financieros confidenciales. Por ese motivo, Norton Privacy Control le permite designar la información clave que hay que proteger de los sitios Web no seguros. También impide que los servidores Web obtengan su dirección de correo electrónico sin permiso, o que controlen sus actividades en línea a través de cookies.

- Es posible bloquear el envío de datos confidenciales (números de tarjetas de crédito, por ejemplo) a los sitios Web que no sean seguros.
- Los sitios Web utilizan cookies para realizar un seguimiento de sus visitas. Puede bloquear las respuestas a cookies cuando los sitios Web los soliciten.
- Norton Personal Firewall impedirá que el explorador envíe su dirección de correo electrónico así como la dirección del último sitio visitado sin su permiso.
- Puede desactivar las conexiones seguras, para garantizar que los usuarios no autorizados envíen información confidencial.

Personalización de las funciones de seguridad

Para cambiar la configuración de seguridad, abra la ventana Seguridad.

Si desea crear su propia configuración, haga clic en Nivel personalizado

Elija entre seguridad Baja, Media o Alta para esta cuenta

El control deslizante permite seleccionar una configuración de seguridad baja, media o alta. Cuando se cambia la posición del control deslizante, éste varía el nivel de protección.

Configuración de seguridad	Descripción
Alta	<p>Firewall está configurado como Alta, por lo que todo estará bloqueado hasta que decida modificarla.</p> <p>El bloqueo de controles ActiveX y subprogramas Java se configura como Media, lo que significa que recibirá un aviso cada vez que encuentre uno.</p>
Media	<p>Firewall está configurado como Alta, por lo que todo estará bloqueado hasta que decida modificarla.</p> <p>El bloqueo de controles ActiveX y subprogramas Java está configurado como Ninguna, lo que permite ejecutarlos.</p>
Baja	<p>Firewall está configurado como Media, lo que bloquea aquellas aplicaciones que sean perjudiciales.</p> <p>El bloqueo de controles ActiveX y subprogramas Java está configurado como Ninguna, lo que permite ejecutarlos.</p>

Personalización de Norton Personal Firewall

Si desea cambiar la configuración de los niveles de protección del firewall, de Java y de ActiveX, haga clic en Nivel personalizado. Se abrirá el cuadro de diálogo Personalizar la configuración de seguridad.

Norton Personal Firewall tiene tres ajustes: Alta, Media y Ninguna.

Configuración de firewall	Descripción
Alta	Bloquea toda comunicación que el usuario no haya permitido de manera expresa. Éste debe crear reglas para cada aplicación que solicite acceso a Internet.
Media	Bloquea un gran número de puertos utilizados por programas perjudiciales. Sin embargo, puede también bloquear programas útiles que utilizan esos mismos puertos.
Ninguna	Todas las comunicaciones en Internet están permitidas.

Creación automática de normas de firewall

La suscripción a Norton Personal Firewall incluye listas actualizadas de programas conocidos y fiables que se comunican por Internet. Estos programas incluyen, entre otros, exploradores, programas de correo electrónico, juegos y utilidades de red.

Cuando utiliza un programa reconocido por Norton Personal Firewall, Norton Personal Firewall crea automáticamente una norma para dicho programa con la configuración de firewall adecuada. Si desea mantener siempre actualizada la lista de aplicaciones preparadas para Internet, utilice LiveUpdate con regularidad. Véase “[Actualización de Norton Personal Firewall utilizando LiveUpdate](#)” en la página 11.

Uso del Asistente de normas de firewall

El Asistente de normas de firewall le ayuda a configurar el firewall (servidor de seguridad) y le orienta, paso a paso, en la definición de una norma para cada tipo de comunicación que no esté cubierta por las normas vigentes del firewall. Una vez establecida una norma, el firewall la utilizará automáticamente para futuras comunicaciones.

Cuando Norton Personal Firewall se encuentra con que una aplicación para la que carece de normas está intentando establecer una conexión a través de Internet, aparece el Asistente de normas de firewall.

El mensaje de alerta muestra qué aplicación está solicitando acceso a Internet

Bloquear o permitir conexiones sólo una vez

Crear normas de firewall nuevas con el Asistente de normas de firewall

El Asistente de normas de firewall ayuda a tratar las conexiones sospechosas:

- Crear una norma para esta conexión en la base de datos del firewall. Cuando hay una norma establecida para una determinada conexión, el firewall automáticamente la cumple para permitir la conexión o bloquearla.
- Autorizar la conexión en esta ocasión, pero abrir el Asistente de normas de firewall la próxima vez que se solicite la conexión.
- Bloquear la conexión en esta ocasión, pero abrir el Asistente de normas de firewall la próxima vez que se solicite la conexión.

Cuando se hace clic en Configure una norma para el futuro (recomendado), aparece el Asistente de normas de firewall. Éste le da instrucciones paso a paso con el fin de crear una norma de firewall para la aplicación que solicitó la conexión. En caso de que se le plantease cualquier duda sobre las preguntas u opciones del asistente, haga clic en la opción con el botón derecho del ratón y luego haga clic en ¿Qué es esto? y obtendrá información adicional.

Configuración de los niveles de seguridad de Java y de ActiveX

Los subprogramas Java y los controles ActiveX hacen que los sitios Web sean más interactivos y emocionantes. Muchos sitios Web se basan en controles ActiveX y en subprogramas Java para que tanto su formato como su funcionamiento sean los adecuados. La mayor parte de estos programas son seguros y no amenazan el sistema, ni sus datos.

Pero, según como estén programados, los controles ActiveX pueden tener acceso total a sus datos: pueden robar datos del disco duro y transmitirlos a través de Internet mientras el usuario está en línea; o pueden eliminar archivos, interceptar mensajes, capturar contraseñas y hasta obtener números de cuentas bancarias y otros datos importantes.

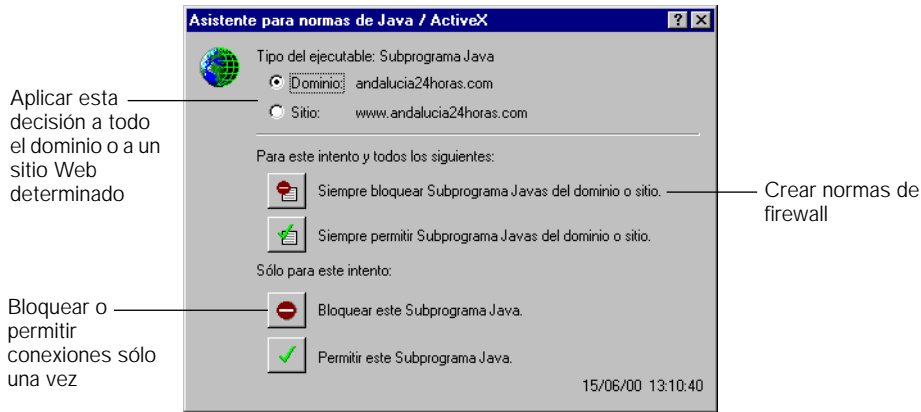
La única manera de evitar que estos programas perniciosos se ejecuten en su PC es impedir que se descarguen. Sin embargo, el bloqueo de subprogramas Java y de controles ActiveX impide que muchos sitios Web se puedan ver o ejecutar correctamente.

En la ventana Nivel personalizado de la configuración de seguridad, las características de seguridad de subprogramas Java y de controles ActiveX tienen tres opciones: Alta, Media y Ninguna.

Configuración de subprogramas Java y controles ActiveX	Descripción
Alta	Impide que el explorador descargue subprogramas Java o controles ActiveX de Internet. Ésta es la opción más segura, pero también la más incómoda. Es posible que los sitios Web basados en estos controles no funcionen adecuadamente con esta configuración.
Media	Activa el Asistente de Java/ActiveX. Este asistente le permite autorizar una regla, bloquearla o crearla para cada subprograma Java o control ActiveX que se descargue. Aunque configurar normas cada vez que se encuentre con un subprograma Java o con un control ActiveX resulte una tarea tediosa, esta opción le permite decidir cuáles de estos programas ejecutar.
Ninguna	Permite que cualquier subprograma Java o control ActiveX se ejecute al descargarlo.

Uso del Asistente de Java/ActiveX

Norton Personal Firewall contiene un Asistente de Java/ActiveX que le permite configurar normas para diferentes sitios. Puede bloquear los subprogramas Java y los Controles ActiveX que no le merezcan confianza y autorizar aquéllos que le parezcan seguros.



Si el Asistente de Java/ActiveX está activado, sólo aparece cuando el usuario visita un sitio Web que intenta utilizar una de estas tecnologías.

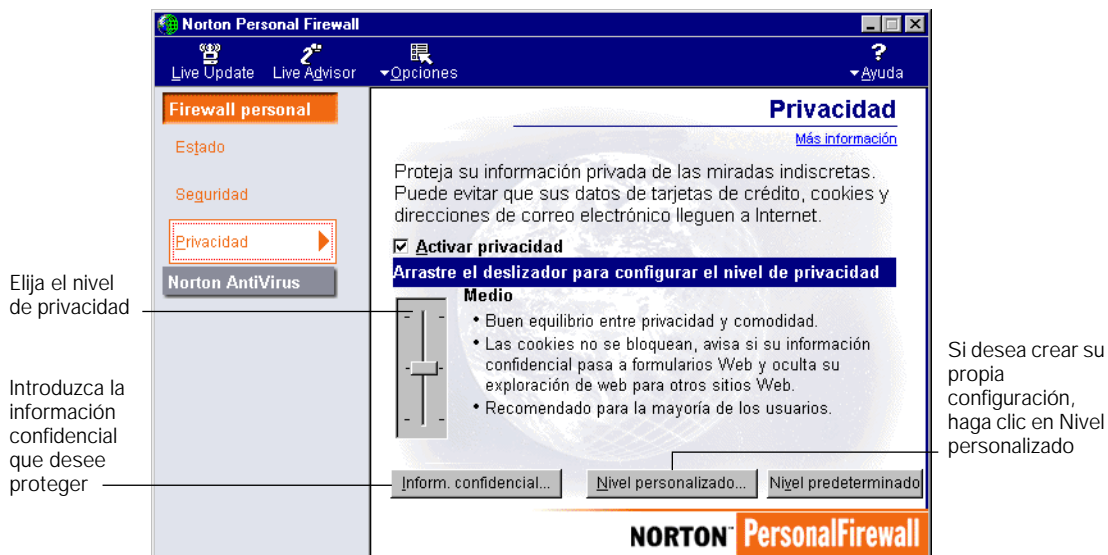
¿Quiero bloquear un dominio o un sitio?

Los dominios pueden incluir varios sitios pudiendo ser mucho más grandes que estos últimos. Al bloquear un dominio como dominio.com, también se bloquean todos los sitios Web incluidos en ese dominio, tales como ventas.dominio.com o inversor.dominio.com, así como dominio.com. Asimismo, se bloquearán todas las páginas Web de cada uno de dichos sitios.

Al bloquear sólo un sitio, se bloquean todas las páginas Web que contiene. Sin embargo, no se bloquean los otros sitios del dominio. Por ejemplo, si bloquea invertir.dominio.com, no se bloquean ni ventas.dominio.com ni inversor.dominio.com.

Protección de la privacidad

Las funciones de seguridad de un equipo no siempre pueden proteger su identidad u otro tipo de información personal. Los equipos y los sitios Web recogen una gran cantidad de información personal mientras el usuario navega por Internet. Norton Privacy Control le ayuda a proteger su privacidad evitando estos tipos de intrusiones.



El control deslizante permite seleccionar una configuración de privacidad baja, media o alta.

Bloqueo de información confidencial

Hay muchos sitios Web que solicitan información personal. Alguien puede, involuntariamente, dejar escapar información que ponga en peligro su privacidad o permita que otros le roben.

Norton Personal Firewall le permite crear una lista de datos personales. Cuando se introduce información en dicha lista, Norton Personal Firewall impide que toda información procedente de comunicaciones no seguras se introduzca en el Web.

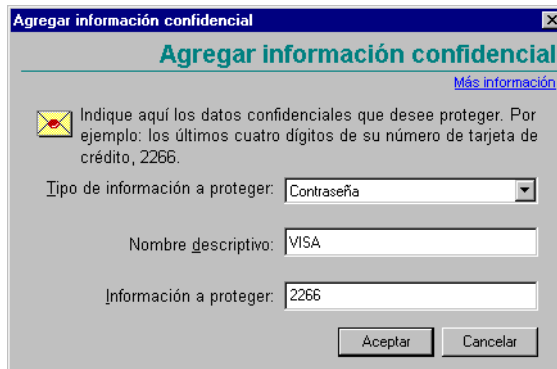
Si le preocupa introducir información personal en el programa, introduzca sólo información parcial. Por ejemplo, en lugar de un número completo de identificación o de tarjeta de crédito, escriba sólo los últimos dígitos. Norton Personal Firewall bloqueará esa parte del número, lo que impedirá que su número de tarjeta de crédito se transmita a un sitio Web.

Para bloquear información personal de sitios Web no seguros:

- 1 Abra Norton Personal Firewall.
- 2 En la parte izquierda de la ventana Norton Personal Firewall, haga clic en Privacidad.
- 3 Ajuste el control deslizante en Media de manera que muestre un aviso cada vez que alguien trate de enviar información protegida a través de una conexión Web no segura. Coloque el control deslizante en Alta si desea bloquear permanentemente la información confidencial.

Para introducir la información confidencial que debe bloquearse:

- 1 Abra Norton Personal Firewall.
- 2 En la parte izquierda de la ventana Norton Personal Firewall, haga clic en Privacidad.
- 3 Haga clic en Información confidencial.
- 4 En el cuadro de diálogo Información confidencial, haga clic en Agregar.



Agregar información confidencial

[Más información](#)

Indique aquí los datos confidenciales que desee proteger. Por ejemplo: los últimos cuatro dígitos de su número de tarjeta de crédito, 2266.

Tipo de información a proteger:

Nombre descriptivo:

Información a proteger:

- 5 En el cuadro de diálogo Agregar información confidencial, escoja una categoría del cuadro Tipo de información a proteger.
- 6 En el campo Nombre descriptivo, escriba una definición que le ayude a recordar por qué está protegiendo los datos.
- 7 En el campo Información a proteger, introduzca la información que no desea enviar a través de conexiones Web no seguras.

Sugerencias sobre el bloqueo de información confidencial

No introduzca el número completo de una tarjeta de crédito o de identificación, sino sólo una parte. Esto evita que esa parte del número se transmita a sitios Web no seguros, con lo que se está protegiendo todo el número. Por ejemplo, si introduce los últimos 4 dígitos de su número de teléfono, impedirá que el número de teléfono completo se envíe por Internet.

Dado que Norton Personal Firewall bloquea los datos personales tal y como se introducen en el programa, se recomienda introducir sólo parte del número. Por ejemplo, puede escribir un número de teléfono como 888-555-1234, pero también sin guiones (8885551234) o con espacios (888 555 1234), o incluso en dos o más casillas separadas. Un denominador común de todos estos formatos es que las últimas cuatro cifras (1234) siempre están juntas. Por lo tanto, sólo con proteger los últimos 4 dígitos conseguirá una protección más elevada que si protege todo el número.

Bloqueo de cookies

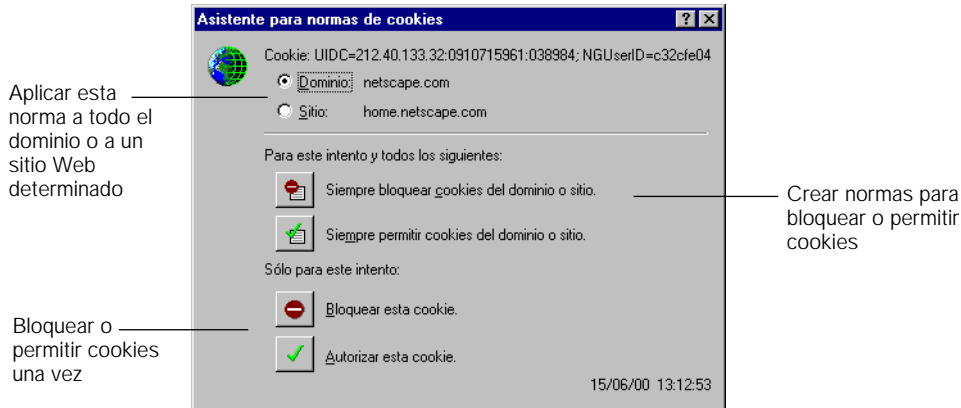
Los cookies son archivos de pequeño tamaño que el explorador guarda en el sistema. En ocasiones, los sitios Web los utilizan como fuente de información que facilita la utilización de dichos sitios.

Los cookies que registran información personal pueden poner en peligro su privacidad permitiendo que terceras personas accedan a esa información sin su permiso. Es posible que contengan suficiente información como para revelar sus hábitos de navegación, o que muestren contraseñas o nombres de inicio de sesión.

Cuando un sitio Web solicita un cookie a su PC, Norton Personal Firewall comprueba que el usuario lo permite, lo está bloqueando o está utilizando el Asistente de cookies para tomar una decisión al respecto.

Uso del Asistente de cookies

El Asistente de cookies establece normas para determinados sitios Web cuando detecta una solicitud de cookie. Puede servirse del asistente para especificar qué sitios Web están autorizados o no a emplear cookies. Cuando el usuario crea una norma para un cookie, Norton Personal Firewall recuerda en qué sitios desea o no autorizar cookies.



Para obtener información sobre el uso de la configuración de dominios o de sitios, consulte “¿Quiero bloquear un dominio o un sitio?” on page 21.

Activación o desactivación de conexiones Web seguras

Cuando el usuario visita un sitio Web seguro, el explorador configura una conexión cifrada con el sitio Web. El firewall no puede detectar la información transmitida a través de una conexión segura, por tratarse de información cifrada. "Cifrada" significa que la información se ha codificado mediante una fórmula matemática, desordenando los datos en un formato ilegible.

Si desea garantizar que no se envíen datos confidenciales a través de conexiones Web seguras, puede bloquear todas las conexiones Web seguras.

Para desactivar las conexiones Web seguras:

- 1 Abra Norton Personal Firewall.
- 2 En la parte izquierda de la ventana Norton Personal Firewall, haga clic en Privacidad.
- 3 Haga clic en Nivel personalizado.
- 4 En el cuadro de diálogo Personalizar la configuración de privacidad, desactive la opción Activar conexiones seguras (https).

Solución de problemas

En este capítulo se resuelven algunas de las dudas que los usuarios avanzados puedan plantearse sobre Norton Personal Firewall.

Preguntas más frecuentes

¿Cómo se desactiva Norton Personal Firewall?

Pueden existir circunstancias en las que el usuario quiera suspender temporalmente un determinado recurso de protección o incluso todo el producto. Norton Personal Firewall le permite desactivar determinadas funciones sin necesidad de modificar la configuración.

Para desactivar Norton Personal Firewall temporalmente:

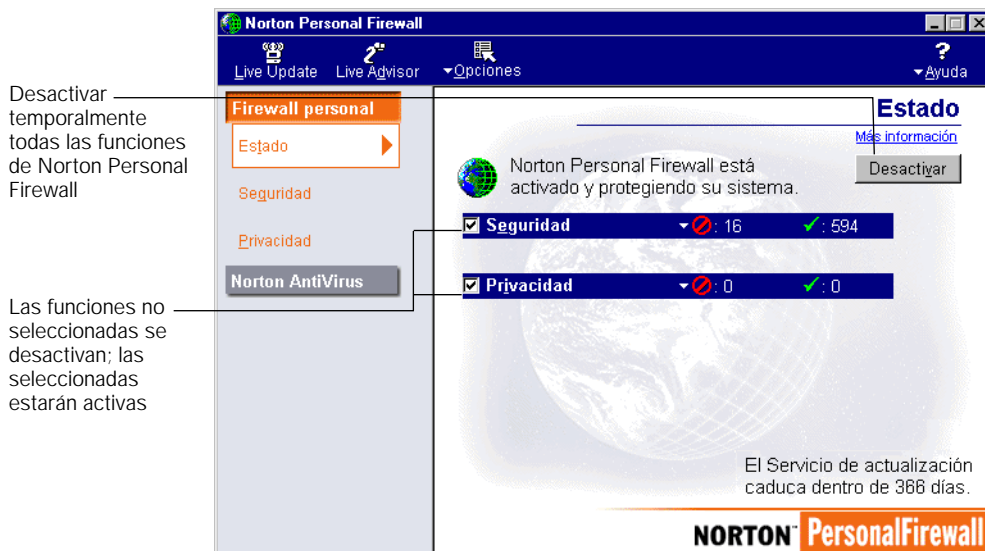
- 1 Abra Norton Personal Firewall.
- 2 En la ventana de estado, haga clic en Desactivar.

También puede desactivar Norton Personal Firewall haciendo clic en el icono Norton Personal Firewall de la bandeja del sistema y haciendo clic en Desactivar.

Norton Personal Firewall estará activado la próxima vez que inicie el sistema.

Para suspender temporalmente Privacidad:

- 1 Abra Norton Personal Firewall.
- 2 En la ventana Estado, compruebe que no se han seleccionado las opciones que desea suspender.



Para salir de Norton Personal Firewall

Aun cuando Norton Personal Firewall no esté abierto, si el icono aparece en la Bandeja de sistema, está todavía protegiendo su sistema. Puede interrumpir la ejecución en segundo plano de Norton Personal Firewall.

Para salir de Norton Personal Firewall:

- 1 En la zona de notificación de la barra de tareas de Windows, haga clic con el botón derecho en el icono de Norton Personal Firewall.
- 2 En el menú que aparece, haga clic en Salir.

¿Por qué no puedo enviar información en línea?

Si no puede enviar información a un sitio Web, es posible que se deba a que Norton Privacy Control está bloqueando la información. Compruebe la lista de Información confidencial en la ventana de Privacidad para ver si la información que está tratando de enviar está bloqueada.

Para comprobar la información de la lista Información personal:

- 1 Abra Norton Personal Firewall.
- 2 En la parte izquierda de la ventana Norton Personal Firewall, haga clic en Privacidad.
- 3 Haga clic en Información confidencial.
Se abrirá la lista de datos que Norton Privacy Control no desea transferir a Internet.

¿Por qué hay problemas de acceso a ese sitio Web?

La ejecución de Norton Personal Firewall puede bloquear determinados elementos de un sitio Web e impedir que sus páginas aparezcan correctamente en la pantalla del explorador. En algunos casos, es posible que el sitio ni siquiera aparezca en pantalla.

Generalmente, esto ocurre cuando Norton Personal Firewall intenta protegerlo de contenidos inapropiados. La mejor solución quizás sea ir a otro sitio Web más adecuado.

Para ver si Norton Personal Firewall está bloqueando el acceso al sitio Web, puede desactivar Norton Personal Firewall y tratar de entrar de nuevo en el sitio Web. Tenga presente que cuando desactiva Norton Personal Firewall, está retirando la protección contra el envío de información privada y la recepción de información inadecuada. Véase “[¿Cómo se desactiva Norton Personal Firewall?](#)” en la página 27. Si sigue sin poder conectarse, quizás haya un problema con Internet o con su proveedor de servicios de Internet.

Puede ser un bloqueo de cookies

Para aparecer correctamente en pantalla, muchos sitios Web necesitan que los cookies estén activados. Si tiene activado el bloqueo de cookies y la página Web aparece en blanco, desbloquee los cookies y vuelva a entrar en la página.

Para desbloquear los cookies:

- 1 Abra Norton Personal Firewall.
- 2 En la parte izquierda de la ventana Norton Personal Firewall, haga clic en Privacidad.
- 3 Haga clic en Nivel personalizado.
- 4 Configure Bloqueo de cookies como Medio o Ninguno.

Puede ser una norma de firewall

Es posible que una norma de firewall esté bloqueando el sitio Web. Cuando esto sucede, suele aparecer un mensaje indicándole que no se pudo realizar la conexión. Se pueden ver las normas de firewall que se han configurado y deducir si una norma está bloqueando el sitio. Véase [“¿Cómo reviso o cambio las normas de firewall?”](#) en la página 36.

Puede ser un bloqueo de ActiveX o de Java

Algunos sitios Web muestran sólo controles ActiveX o subprogramas Java. Si el usuario los está bloqueando, se muestra una página en blanco. Véase [“Configuración de los niveles de seguridad de Java y de ActiveX”](#) en la página 19.

Puede ser un bloqueo de script

Algunos sitios Web utilizan scripts de Java en sus controles de navegación y otros lugares. Si Norton Personal Firewall está bloqueando scripts de Java o VB, esto puede causar problemas con dichos sitios Web.

Para suspender el bloqueo de scripts de Java o de VB:

- 1 Abra Norton Personal Firewall.
- 2 En la parte superior de la ventana Norton Personal Firewall, haga clic en Opciones.
- 3 Haga clic en Opciones avanzadas.
- 4 En la ficha Web, haga clic en la ficha Contenido activo.
- 5 En la lista de sitios Web, haga clic en el sitio que vaya a cambiar, o haga clic en Predeterminados para cambiar todos los sitios Web que no figuran en la lista.
- 6 Debajo de Script, haga clic en Permitir la ejecución de todos los scripts.

¿Por qué FTP no funciona en los exploradores antiguos?

Las versiones antiguas de exploradores utilizan cualquier puerto para abrir conexiones FTP. De forma predeterminada, Norton Personal Firewall bloquea las conexiones Internet en puertos no estándar.

Para solucionar temporalmente este problema, desactive la parte de seguridad de Norton Personal Firewall. Véase “[¿Cómo se desactiva Norton Personal Firewall?](#)” en la página 27.

Para resolver este problema de una vez por todas, instale la versión más reciente de su explorador.

¿Cómo puede un sitio Web obtener información sobre mi explorador?

Las configuraciones de Privacidad de su explorador impiden que se envíe información de navegación. Sin embargo, algunos sitios de diagnósticos en Internet pueden enviar información de explorador incluso si las configuraciones de Privacidad del explorador están bloqueando la información:

- Si no está bloqueando Java, ActiveX o scripts, es posible que el sitio esté utilizando uno de estos métodos para obtener la información. Véase “[Configuración de los niveles de seguridad de Java y de ActiveX](#)” en la página 19.
- Algunas veces, cuando los servidores de Web no obtienen la información del explorador, simplemente utilizan la última parte de la información que recibieron. Es posible ver los datos de la última persona que visitó el sitio.

¿Qué son conexiones de entrada y de salida?

Una conexión de entrada se produce cuando otro equipo en Internet intenta conectarse a su PC. Las conexiones de salida ocurren cuando un programa de su propio PC intenta realizar una conexión con un equipo externo. Una vez establecida la conexión, sea ésta de entrada o de salida, los datos pueden circular en ambos sentidos a través de la conexión.

Preguntas sobre redes domésticas

Aunque Norton Personal Firewall puede utilizarse en una red doméstica, está diseñado para proteger un solo equipo. Es posible que la instalación de Norton Personal Firewall en un solo equipo no proteja a otros equipos de la red frente a las amenazas de Internet.

Si tiene más de una estación de trabajo conectada a Internet, adquiera e instale Norton Personal Firewall en cada una de ellas.

¿Cómo trabaja el firewall con conexiones de Internet compartidas?

Si Norton Personal Firewall se instala en el equipo que está conectado a Internet, funcionará tal y como se describe en este manual. Sin embargo, ignora toda la comunicación que se envía a los equipos que comparten la conexión, a menos que se haya instalado en los mismos.

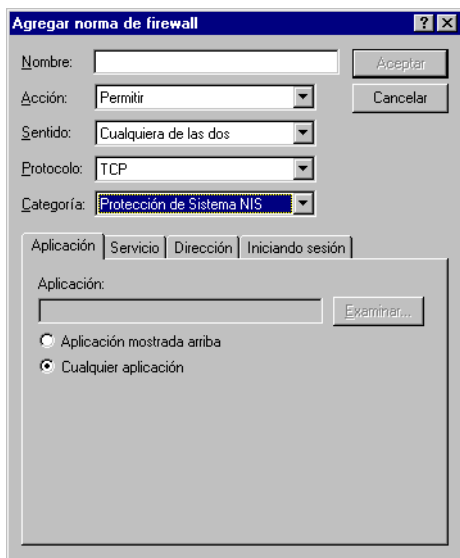
Adquiera e instale Norton Personal Firewall en todos los equipos que compartan la conexión a Internet.

¿Cómo trabaja el firewall con archivos e impresoras compartidos?

Norton Personal Firewall contiene normas de firewall predeterminadas que permiten compartir archivos e impresoras en redes NetBEUI. Si está usando una red basada en TCP/IP, deberá configurar al firewall para que reconozca los demás equipos de la red.

Para configurar el firewall de manera que reconozca a los otros equipos de la red:

- 1 Abra Norton Personal Firewall.
- 2 En la parte superior de la ventana de Norton Personal Firewall, haga clic en Opciones.
- 3 Haga clic en Opciones avanzadas.
- 4 En la ficha Firewall, haga clic en Agregar.



- 5 Dé un nombre descriptivo al equipo que está configurando.
- 6 En el campo Acción, haga clic en Permitir.
- 7 En el campo Sentido, haga clic en Cualquiera de las dos.
- 8 En el campo Protocolo, haga clic en TCP o en UDP.
- 9 En el campo Categoría, haga clic en Protección de sistema NIS.
- 10 En la ficha Aplicación, haga clic en Cualquier aplicación.
- 11 En la ficha Servicio, dentro de Servicio remoto, haga clic en Cualquier servicio. En Servicio local, haga clic en Cualquier servicio.

- 12 En la ficha Dirección, en Dirección remota, haga clic en Dirección del host y escriba la dirección TCP del otro equipo.
 - Si está configurando más de una máquina con esta norma, haga clic en Intervalo de direcciones e introduzca el intervalo de direcciones de su red local.
 - Si está usando dos tarjetas de red, una conectada a Internet y la otra conectada a la red doméstica, en Dirección local haga clic en Dirección del host y escriba la dirección del equipo que ejecuta Norton Personal Firewall.

Esto permite cualquier comunicación en esa tarjeta de red. Las otras normas de firewall se aplican a la tarjeta de red conectada a Internet.

Después de hacer clic en Aceptar, aparecerá la nueva norma de firewall al final de la lista de firewall. Desplace la norma de firewall hacia el inicio de la lista si desea que se ejecute en primer lugar.

Para mover la norma de firewall al inicio de la lista:

- 1 Haga clic en la nueva norma de firewall.
- 2 Haga clic varias veces en la flecha hacia arriba hasta que la norma aparezca al principio de la lista.

¿Cómo se utiliza Norton Personal Firewall con un servidor proxy?

Los servidores proxy son equipos que actúan como única conexión a una red mayor. Si está usando un servidor proxy, quizás tenga que especificar el puerto que la red utiliza para las comunicaciones Web (http). Esto permite a Norton Personal Firewall supervisar la actividad en la Web.

Para supervisar un puerto específico para las comunicaciones Web:

- 1 Abra Norton Personal Firewall.
- 2 En la parte superior de la ventana Norton Personal Firewall, haga clic en Opciones.
- 3 Haga clic en Opciones avanzadas.
- 4 En la ficha Otros, en la lista Puertos HTTP, haga clic en Agregar.
- 5 Introduzca el número del puerto que desee supervisar.

Consulte las instrucciones que siguió al configurar el servidor proxy para determinar qué puertos han de comprobarse.

Preguntas sobre firewall

Encontrará la información técnica sobre el firewall y la configuración del mismo en la Ayuda de Norton Personal Firewall.

Para abrir la Ayuda:

- 1 Abra Norton Personal Firewall.
- 2 En la parte superior de la ventana de Norton Personal Firewall, haga clic en Ayuda.
- 3 En el menú que aparece, haga clic en Ayuda de Norton Personal Firewall.

¿Por qué no aparece el Asistente de normas de firewall?

El Asistente de normas aparece cuando el firewall (servidor de seguridad) detecta que un programa está tratando de acceder a Internet y no existen normas previas que bloqueen o permitan la conexión del programa a la red. En Norton Personal Firewall, hay varias zonas en las que se puede bloquear un programa de forma que no aparezca el Asistente de normas de firewall.

Utilice esta lista de verificación para asegurarse de que el Asistente de normas de firewall aparece cuando se necesita:

- Active el asistente para normas. Véase [“Uso del Asistente de normas de firewall”](#) en la página 18.
- En la ventana Seguridad, asegúrese de que el firewall está activado. Puede mover el control deslizante Seguridad hasta Alta o configurar el firewall como Alta en Nivel personalizado.

- Asegúrese de que no hay normas previas que afecten al programa que quiere usar. Véase “¿Cómo reviso o cambio las normas de firewall?” en la página 36. Si ya existe una norma, es posible que ya la haya creado con el Asistente de normas de firewall. O bien, si Activar creación automática de normas de firewall se ha seleccionado, Norton Personal Firewall habrá creado automáticamente la norma. Véase “Creación automática de normas de firewall” en la página 18.
- Cuando alguien explora puertos no utilizados del sistema, es posible configurar Norton Personal Firewall para que no lo alerte a menos que la conexión se lleve a cabo satisfactoriamente. Esto puede reducir el número de mensajes de alerta que reciba.

¿Cómo reviso o cambio las normas de firewall?

Siempre que se crean normas de firewall, éstas aparecen en la ventana Configuración de Norton Personal Firewall. Esta ventana permite revisar y cambiar las normas de firewall en la base de datos de firewall.

Las flechas que apuntan hacia el equipo permiten comunicaciones de entrada.

Las flechas que apuntan en sentido opuesto al equipo permiten comunicaciones de salida.

Las flechas bloqueadas muestran normas que impiden comunicaciones de entrada o de salida.

Ajusta el orden en que se ejecutan las normas de firewall.

Norma de firewall	Resumen de la acción de la norma
<input checked="" type="checkbox"/> Default Inbound ICMP	ICMP: Destino inalcanzable
<input checked="" type="checkbox"/> Default Outbound ICMP	ICMP: cualquier tipo
<input checked="" type="checkbox"/> Default Inbound DNS	domain
<input checked="" type="checkbox"/> Default Outbound DNS	domain
<input checked="" type="checkbox"/> Default Inbound Bootp	bootpc
<input checked="" type="checkbox"/> Default Outbound Bootp	bootp
<input checked="" type="checkbox"/> Default Inbound NetBIOS	nbdatagram, nbname
<input checked="" type="checkbox"/> Default Outbound NetBIOS	nbdatagram, nbname
<input checked="" type="checkbox"/> Default Inbound Loopback	localhost
<input checked="" type="checkbox"/> Default Outbound Loopback	localhost
<input type="checkbox"/> Block access to secure sites	https
<input checked="" type="checkbox"/> Default Inbound Authentication	auth
<input checked="" type="checkbox"/> Default Block Inbound and Outbound ICMP	ICMP: cualquier tipo
<input checked="" type="checkbox"/> Default Block NetBIOS Networking	nbssession
<input checked="" type="checkbox"/> Windows Explorer HTTP rule	http, 81, 82, 83, https, socks, htt...

Para revisar o modificar normas individuales de firewall:

- 1 Abra Norton Personal Firewall.
- 2 En la parte superior de la ventana Norton Personal Firewall, haga clic en Opciones.
- 3 Haga clic en Opciones avanzadas.
- 4 En la ficha Firewall, haga clic en la norma que desea ver.
- 5 Haga clic en Modificar.

Las normas de firewall pueden permitir, bloquear o ignorar la información que entra al equipo, o que sale del mismo.

Cada ficha contiene configuraciones adicionales

El firewall puede controlar diferentes protocolos; la mayor parte de las comunicaciones en Internet se realizan a través de TCP

Puede bloquear o permitir determinadas categorías de aplicaciones

Si dos normas de firewall tratan del mismo asunto, ¿cuál se ejecuta?

Cuando Norton Personal Firewall detecta que un programa está intentando acceder a Internet, revisa la lista de normas de firewall para ver si hay alguna instrucción que permita la conexión o la bloquee. Tan pronto como la encuentra, detiene la búsqueda. Si existe una norma que deba ejecutarse antes que otra, es posible alterar el orden de las mismas.

Para cambiar el orden de las normas:

- 1 Abra Norton Personal Firewall.
- 2 En la parte superior de la ventana Norton Personal Firewall, haga clic en Opciones.
- 3 Haga clic en Opciones avanzadas.
- 4 En la ficha Firewall, haga clic en la norma que desee desplazar.
- 5 Haga clic en flecha hacia arriba o en la flecha hacia abajo para desplazar la norma seleccionada.

¿Para qué sirven las normas de firewall predeterminadas?

Hay diversas normas predeterminadas ya configuradas en el firewall cuando se instala por primera vez. Esta lista predeterminada se adapta a las opciones que el usuario configura en la ventana Seguridad:

- Las normas predeterminadas de entrada DNS y las normas predeterminadas de salida DNS permiten el uso del Servicio de nombres de dominio (DNS) para la conexión a Internet. El DNS convierte las direcciones de sitios Web de nombres de host como `ww.symantec.com` en direcciones IP tales como `127.0.0.1`.
- Las normas predeterminadas del BOOTP de entrada y las normas predeterminadas del BOOTP de salida permiten el uso del servicio BOOTP. BOOTP es la abreviatura para el protocolo Bootstrap, que permite a un equipo descubrir su propia dirección IP.
- Las normas predeterminadas del bucle invertido de entrada y del bucle invertido de salida permiten que su equipo se conecte sí mismo mientras se comprueban las conexiones de red.
- Las normas de ICMP de entrada y de ICMP de salida permiten el envío de mensajes ICMP. El protocolo ICMP permite a su PC determinar cómo enviar información en una red como Internet.
- Existen otras muchas normas predeterminadas que bloquean programas conocidos de caballo de Troya, tales como Back Orifice y NetBus.

Si elimino las normas predeterminadas de firewall, ¿puedo recuperarlas?

Sí, pero primero el usuario ha de eliminar todas las normas existentes, incluida cualquier norma personalizada que haya creado.

Para recuperar las normas predeterminadas de firewall originales:

- 1 Elimine todas las normas de firewall.
- 2 Busque el archivo firewall.dat en su PC.
Para abrir el programa de búsqueda, haga clic en el botón Inicio de Windows y seleccione Buscar > archivos o carpetas.
- 3 Cuando lo encuentre, cambie su nombre por firewall.reg.
- 4 Haga doble clic en el archivo firewall.reg para incorporarlo al Registro de Windows.

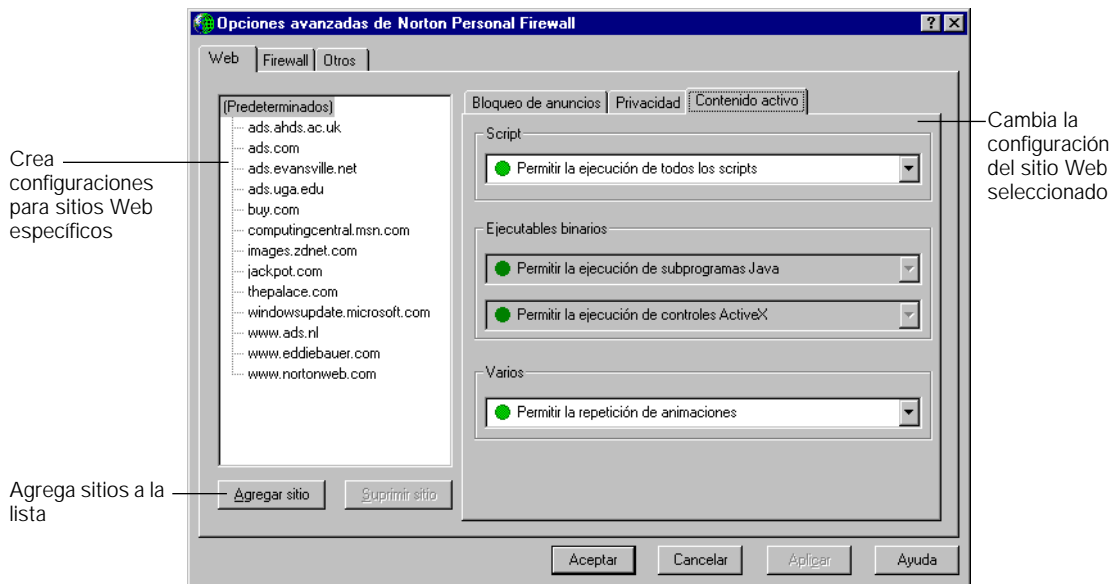
¿Puedo crear configuraciones para determinados sitios Web?

Se pueden crear configuraciones de Privacidad y Contenido activo para determinados sitios Web a través del cuadro de Configuración de Norton Personal Firewall. Primero, configure Norton Personal Firewall de la forma en que quiere aplicarlo en general a todos los sitios Web. A continuación, siga estas instrucciones para crear normas o configuraciones para sitios Web específicos.

Para crear configuraciones para sitios Web específicos:

- 1 Abra Norton Personal Firewall.
- 2 En la parte superior de la ventana Norton Personal Firewall, haga clic en Opciones.

3 Haga clic en Opciones avanzadas.



4 En la ficha Web, haga clic en Agregar sitio e introduzca la dirección del sitio Web cuya configuración desea modificar.

Haga clic en Aceptar y el nuevo sitio aparecerá en la lista de sitios Web.

5 En la lista de sitios Web, haga clic en el sitio Web que va a modificar.

6 Haga clic en la ficha Privacidad o Contenido activo y modifique la configuración de ese sitio.

La ventana muestra la configuración de cualquier sitio Web seleccionado en la lista Web. Si selecciona Predeterminados, la ventana mostrará las configuraciones de todos los sitios Web que no estén en la lista.

Í N D I C E

A

- abandonar el programa 28
- ActiveX 8, 19
- actualizar protección 11
- AOL 11
- asistente
 - Asistente de cookies 25
 - Asistente de Java/ActiveX 21
 - Asistente de normas de firewall 18, 35
- ayuda 12-14
- Ayuda ¿Qué es esto? 13
- ayuda en pantalla 12-14

B

- bloqueo
 - cookies 24-25
 - dominios o sitios 21
 - información confidencial 22-24
 - información sobre el explorador 31

C

- cdstart.exe 10
- cerrar el programa 28
- compartir conexiones de Internet 32
- conexiones de entrada 32
- conexiones de salida 32
- conexiones, de entrada y de salida 32
- confidencial, información 9
- configuración
 - firewall 17-21
 - privacidad 22-25
 - seguridad 16-21
- cookies 9, 24-25
- creación
 - normas de firewall 18
 - Normas de Java/ActiveX 21
 - normas para cookies 25

D

- detener el programa 28
- doméstica, red 32
- dominio 21

F

- firewall
 - configuración 17-21
 - creación de normas 18
- firewall.dat 39

I

- icono 10
- información confidencial 9
- información sobre el explorador 31
- iniciar el programa 10
- instalación 10

L

- LiveAdvisor 43
- LiveUpdate 11

M

- menú Inicio 10

N

- normas de firewall
 - lista predeterminada 38
 - modificación 36
 - orden 37
 - restauración de predeterminados 39
 - revisión 36
- Norton Personal Firewall 8, 17-21
- Norton Privacy 9, 22-25

O

opciones, configuración 11

P

protección de información personal 22-24

protección, actualizar 11

R

red doméstica 32

renovación de la suscripción 11

requisitos 9

requisitos de sistema 9

restauración de las normas predeterminadas de
firewall. 39

S

salir del programa 28

seguridad

 ActiveX 19

 subprogramas Java 19

servidor proxy 34

subprogramas Java 8, 19

suscripción 11

Soluciones de servicio y asistencia de Symantec

Symantec desea ofrecer el mejor servicio en todo el mundo. Nuestro objetivo es proporcionarle una asistencia profesional para la utilización de nuestro software y servicios, dondequiera que esté.

La asistencia técnica y la atención al Cliente varían según el país. Si tiene alguna pregunta respecto a los servicios descritos a continuación, por favor consulte la sección "Servicio y asistencia en todo el mundo" al final de este capítulo o la tarjeta de Servicio y Asistencia incluida en el paquete.

Cómo registrar su producto Symantec

Para registrar su producto Symantec, rellene la tarjeta de registro incluida dentro del mismo, escaoge la etiqueta adecuada:

También puede registrarse por módem durante el proceso de instalación (si su software ofrece esta posibilidad).

En México, también puede registrarse enviando por fax su tarjeta de registro al 52 (5) 661 7975.

Disco de actualización de definiciones de virus

Si no dispone de un módem para obtener los archivos de definiciones de virus a través de Internet, CompuServe o America Online, puede pedir actualizaciones periódicas a Symantec por correo. Es necesario pagar una cuota para obtener este servicio.

Puede hacer el pedido de las siguientes formas:

- En México, llame al 52 (5) 661 6120, o envíe un correo electrónico a Supportmex@symantec.com.
- En los Estados Unidos, llame al (800) 441 7234.
- En cualquier otra parte, llame a su distribuidor oficial de Symantec.

Asistencia técnica

Symantec ofrece una serie de opciones de asistencia técnica adaptadas a sus necesidades específicas para ayudarle a obtener el máximo provecho de su software.

World Wide Web

El sitio web de Symantec (<http://service.symantec.com>) es la vía de acceso a una serie de soluciones de asistencia técnica en línea, donde encontrará los siguientes servicios:

Solucionador de problemas interactivo

El solucionador de problemas interactivo en línea de Symantec (conocido con el Support Genie) le ayuda a resolver problemas y obtener respuestas sobre muchos productos de Symantec.

Bases de conocimiento del producto

Las bases de conocimiento del producto le permiten hacer búsquedas en miles de documentos utilizados por los técnicos de Symantec para responder a las preguntas de los usuarios.

FAQ

Los documentos de Preguntas frecuentes, conocidos como FAQ, incluyen preguntas realizadas con frecuencia y claras respuestas para productos específicos.

Grupos de discusión

Los grupos de discusión proporcionan un foro donde puede hacer preguntas y recibir respuestas de los técnicos de asistencia en línea de Symantec.

FTP

Apunte su navegador hacia <http://service.symantec.com> para buscar y descargar notas técnicas y actualizaciones de software. También puede hacer clic en el botón LiveUpdate en los programas que incluyan esta opción para descargar e instalar automáticamente las actualizaciones de software y definiciones de virus.

Otras opciones de asistencia de Symantec son:

America Online	Escriba la palabra clave SYMANTEC para acceder al foro de Symantec
CompuServe	Este servicio le permite intercambiar informaciones con miembros de Symantec y con otros clientes de productos Symantec. Para acceder al forum de Symantec en CompuServe, escriba (GO SYMANTEC). Para más información sobre la configuración de acceso necesaria, póngase en contacto directamente con Compuserve.
BBS de Symantec	<p>La BBS de Symantec ofrece un forum de Atención al Cliente, programas de dominio público y shareware, así como una lista de los problemas más comunes (FAQ); asimismo propone un servicio de asistencia técnica donde puede intercambiar información y experiencias directamente con otros clientes. La configuración necesaria para acceder a nuestra BBS es la siguiente: 8 bits de datos, 1 bit de parada, sin paridad.</p> <p>EE.UU. (14.400 baud) Tel +1 (541) 984-3366</p> <p>EE.UU. (28.800 baud) Tel +1 (541) 484-6669</p>
Sistema de recuperación automática de faxes	<p>El sistema automatizado de fax de Symantec está disponible las 24 horas del día. Le permitirá recibir información general sobre nuestros productos así como sobre actualizaciones y notas técnicas.</p> <p>EE.UU. Tel +1 (541) 984-2490</p> <p>ESPAÑA +34 (91) 662 4021</p>
Servidor de Acceso Remoto (RAS) en México	En México, puede beneficiarse del Servidor de Acceso Remoto de Symantec. En primer lugar, póngase en contacto con el Centro de asistencia, en el 52 (5) 661 6120, para obtener un ID de usuario y una contraseña para el servidor RAS. A continuación, marque el servidor RAS en el 52 (5) 662 0558.
Asistencia StandardCare	Si no tiene acceso a Internet, aproveche la posibilidad de recibir asistencia técnica telefónica ofrecida a todos los usuarios registrados de Symantec.

Asistencia para versiones anteriores o suspendidas

Cuando sale una nueva versión del software, los usuarios registrados recibirán información sobre la actualización del producto por correo. Se ofrecerá asistencia telefónica para la versión anterior durante los 6 meses posteriores a la entrega de la nueva versión. Se puede seguir obteniendo información técnica a través de la asistencia en línea.

Cuando Symantec anuncia que un producto ya no se venderá, la asistencia técnica será suspendida 60 días después. La asistencia para este tipo de productos sólo estará disponible a través de servicios en línea. Consulte la sección "Asistencia técnica" para conocer las opciones de los servicios en línea.

Servicio al Cliente

El departamento de Servicio al Cliente de Symantec también puede ayudarle en aquellas cuestiones que no son técnicas. Llame al Servicio al Cliente para:

- Pedir una actualización.
- Suscribirse a la Solución de asistencia técnica que desee.
- Obtener información sobre productos o discos de demostración.
- Obtener información sobre distribuidores y localización de los productos Symantec.
- Pedir la sustitución de partes del producto defectuosas o no incluidas (CD, disquetes, manuales, etc.).
- Actualizar su registro del producto con cambios de nombre o dirección.

También puede visitar el Servicio al Cliente en línea en www.symantec.com/custserv para obtener las últimas FAQ, saber el estado de su pedido o devolución, o para enviar una consulta al grupo de discusión del Servicio al Cliente.

Servicio y asistencia en todo el mundo

Symantec proporciona Asistencia técnica y Servicio al Cliente en todo el mundo. Los servicios varían según el país e incluyen Socios Internacionales que representan a Symantec en aquellas regiones que no disponen de una oficina de Symantec. Si desea obtener información general, por favor póngase en contacto con la Oficina de Servicio y Asistencia de Symantec de su región.

Oficinas de Servicio y Asistencia

MEXICO

Insurgentes Sur 1871-602
Col. Guadalupe Inn
C.P. 01120 México D.F.

Número de servicio de Atención al Cliente y ventas

Tel: +52 (5) 661 7978
Fax: +52 (5) 661 7975
RAS: +52 (5) 662 0558
Web: www.symantec.com/region/la/where.html

Servicio y soporte

Tel: +52 (5) 661 6120 +01-800-711-8443
Fax: +52 (5) 661 8819
RAS: +52 (5) 662 0558
Web: <http://service.symantec.com>
E-mail: supportmex@symantec.com

ARGENTINA,

CHILE,

URUGUAY

Symantec Región Sur
Cerrito 1054 - piso 9
1010 Buenos Aires
Argentina
Tel: +54 (11) 4811 7526
Fax: +54 (11) 4811 7495
Web: www.symantec.com/region/la/where.html

Número de servicio de Atención al Cliente y soporte

Tel: +54 (11) 4315 0889
Fax: +54 (11) 4314 3434
Web: <http://service.symantec.com>

COLOMBIA,
VENEZUELA,
EL CARÍBE
y otros países
LATINOAMERICANOS

Symantec Latin America
2501 Colorado, Suite 300
Santa Monica, CA 90404
EE.UU.

Número de servicio de Atención al Cliente y ventas

Web: www.symantec.com/region/la/where.html

Servicio y soporte

Tel: +1 (541) 334 6054 (EE.UU.)
Fax: +1 (541) 984 8020 (EE.UU.)
Web: <http://service.symantec.com>

NORTEAMÉRICA

Symantec Corporation
175 W. Broadway
Eugene, OR, 97401

(800) 441 7234 (EE.UU. y Canadá)
(541) 334 60 54 (otras ubicaciones)
Fax: (541) 984 8020

Servicio de recuperación automática
de faxes

(800) 554 4403
(541) 984 2490

BRASIL

Symantec Brazil
Av. Juruce, 302- cj 11
Sao Paulo - SP
04080 011 Brazil

Número de servicio de Atención al Cliente y ventas

Tel: +55 (11) 5561 0284
Fax: +55 (11) 530 8869
Email: atendimentobr@symantec.com
Web: <http://www.symantec.com.br/region/br/where.html>

Servicio y soporte

Tel: +55 (11) 531 7577
Fax: +55 (11) 530 8869
Email: suportebr@Symantec.com
Web: <http://service.symantec.com/>
BBS: +55 (11) 531 7382

EUROPA

Symantec Europe 31 (71) 408 3111
Schipholweg 103
2316 XC LEIDEN
Holanda

Servicio de recuperación 31 (71) 535 32 55
automática de faxes

ESPAÑA

Número de servicio de Atención al Cliente

Tel: +34 (91) 662 4413

FOD:+34 (91) 662 4021

Soporte Técnico

Tel:

34 (91) 662 5255

La mayoría de los Socios Internacionales ofrecen Servicio al Cliente y Asistencia técnica para los productos de Symantec en su propia lengua. Si desea obtener más información sobre otras ubicaciones, por favor llame al servicio de recuperación automática de faxes del Servicio de asistencia en los Estados Unidos en el +1 (541) 984 2490, seleccione la Opción 2, y pida el documento 1400.

Hemos hecho todo lo posible por asegurar la exactitud de esta información. Sin embargo, la información aquí contenida está sujeta a cambios sin previa notificación. Symantec Corp. se reserva el derecho de realizar estos cambios sin previo aviso.