

La privacidad en el mundo cibernético:

Las reglas básicas para navegar por Internet

Fuente: <http://www.privacyrights.org/spanish/pi18.htm>

Página Informativa 18: La privacidad en Internet

Derecho de Autor © 1995-2006.
Privacy Rights Clearinghouse / UCAN
June 1995. Revised July 2002.

Para navegar por Internet solamente necesita una computadora y un módem. Y si cuenta con estos requisitos, entonces forma parte de un creciente número de cibernautas.

El Internet ofrece muchos beneficios. Le brinda acceso a una amplia gama de servicios informativos, desde entretenimiento hasta sitios para realizar sus compras. A través de servicios como correo electrónico, mensajero instantáneo y cuartos de chateo, el Internet nos permite comunicarnos con amistades, familiares y desconocidos de una manera inimaginable hace una década.

Pero el Internet también amenaza la privacidad, y el no conocer las "reglas básicas" para navegar el Internet, podría ocasionarle problemas graves.

Esta guía se divide en cuatro secciones:

- Parte uno: Las expectativas sobre la privacidad y el Internet
- Parte dos: Monitoreo y rastreo
- Parte tres: Consejos para salvaguardar su privacidad
- Parte cuatro: Recursos adicionales

PARTE UNO: LAS EXPECTATIVAS SOBRE LA PRIVACIDAD Y EL INTERNET

¿Qué son las "comunicaciones en línea"?

Las comunicaciones en línea son comunicaciones hechas por medio de una computadora y a través de una línea telefónica, cable o un sistema inalámbrico. Algunos ejemplos de este tipo de comunicaciones son las conexiones al Internet por medio de proveedores como [America Online](#) o [Earthlink](#). Este tipo de comunicaciones también se llevan a cabo en los centros de informática de bibliotecas públicas o de centros de computación públicos. Cada día hay más aparatos inalámbricos con acceso al Internet, como pagers o programadores digitales personales (Personal Digital Assistants o PDAs). (Para conocer un directorio de proveedores consulte la sección de Recursos Adicionales al final de este documento).

Hay inquietudes sobre la privacidad en Internet ya que toda información enviada por medio de este sistema global puede pasar, antes de llegar a su destino, por docenas de computadoras, todas con su propio administrador o dueño capaz de interceptar y almacenar información. Asimismo, su propio proveedor puede rastrear su actividad en línea.

¿Qué debe esperarse en cuanto a la privacidad en Internet?

Por lo general, la privacidad en Internet depende del tipo de actividad que usted realiza. Algunas actividades en línea que parecen ser privadas no lo son. *No existe ninguna actividad cibernética que garantice absoluta privacidad.* Esta guía ofrece consejos para maximizar la privacidad y para evitar errores comunes.

Actividades Públicas

Existen actividades cibernéticas abiertas al público que no ofrecen ninguna garantía en cuanto a la privacidad. De acuerdo a leyes federales, cualquier persona puede consultar o divulgar comunicación electrónica si está "al alcance" del público. ([Electronic Communications Privacy Act, 18 USC § 2511\(2\)\(g\)\(I\)](#)).

Newsgroups y / o foros. Antes de participar en un foro o grupo de noticias, considere que cualquier persona puede capturar, copiar y almacenar todo lo que usted escriba; su nombre, correo electrónico e incluso información sobre su proveedor de Internet están incrustados en el mensaje mismo.

La mayoría de estos mensajes se archivan fácilmente en sitios accesibles como <http://groups.google.com>. Por lo tanto, todo mensaje que usted teclee en Internet puede ser leído por cualquier persona en cualquier momento - incluso muchos años después de que se escribió el mensaje original. Antes de participar en un foro público, considere que podría ser leído por un empleador o un miembro de la familia. (Vea Recursos Adicionales al final de esta guía).

Listas de distribución. Existen algunas funciones que permiten que su mensaje sea distribuido a múltiples usuarios. Los boletines cibernéticos o las listas de distribución tienen como destino un grupo específico de suscriptores. Si usted desea contestar un correo a un individuo de estos grupos, asegúrese de que esté dirigido sólo a la persona indicada y no a la lista completa de suscriptores.

Directorios de suscriptores. No suponga que su cuenta con un proveedor de Internet es privada. La mayoría de estos proveedores dan a conocer públicamente información sobre sus usuarios. Además, algunos de estos directorios pueden contener información personal adicional. Sin embargo, la mayoría de estos servicios ofrecen a sus usuarios la opción de quitar sus nombres de dichos directorios.

Registro de un sitio. Muchas personas obtienen su propio sitio en Internet, por ejemplo www.XYZfamilia.org. Estos registros son información pública. Cualquier persona puede saber quién es el dueño de una página utilizando un servicio como www.checkdomain.com o www.internic.net/whois.html. Para ver qué tan fácil es el proceso, realice una prueba con nuestro sitio, www.privacyrights.org. Cuando usted registre una dirección, tenga precaución de no utilizar su correo electrónico personal ni indicar su lugar de residencia. Sin embargo, mantenga una línea de comunicación abierta para que puedan avisarle cuando tenga que renovar el registro de la página.

"Actividades semi-privadas"

Debido a que el acceso a algunos foros está restringido a las personas que cuentan con códigos de seguridad, la comunicación que se lleva a cabo dentro de ellas aparenta ser privada. Pero ése no es el caso. Aunque la comunicación en estos foros está restringida a miembros autorizados, es totalmente legal que los administradores del foro capturen y divulguen la información posteriormente.

Como ejemplo, puede citarse el *chat* o conversación en línea, donde los participantes teclean mensajes que aparecen instantáneamente en los monitores de otras personas. Es común que las compañías que proveen servicio de Internet clasifiquen esta información como privada. Sin embargo, los usuarios pueden capturar, almacenar y transmitir los mensajes en cualquier momento. Asimismo, estas actividades cuentan con las mismas excepciones de monitoreo que se aplican a los correos electrónicos privados (Vea la siguiente sección). Para obtener consejos para chatear, visite "Ángeles Cibernéticos" en la página www.cyberangels.org/101/chat/index.html.

"Servicios Privados"

La mayoría de compañías que proveen servicio de Internet ofrecen algún tipo de comunicación "privada". La ley federal Electronic Communications Privacy Act (ECPA por sus siglas en inglés), dicta que está prohibido, bajo determinadas circunstancias, que una persona lea y divulgue el contenido de cualquier tipo de comunicación electrónica (18 USC § 2511). Esta ley abarca el uso del correo electrónico.

La ley, sin embargo, es compleja, tiene muchas excepciones y distingue entre mensajes en pleno tránsito y mensajes ya almacenados. Los ya almacenados cuentan con menos protección que aquellos que son interceptados. A continuación se incluyen otras excepciones:

- Los proveedores de Internet tienen el derecho de consultar correos electrónicos privados si se sospecha que el emisor tiene la intención de agredir al sistema o a otro usuario. Está generalmente prohibido monitorear al azar el correo electrónico de una persona.
- Los proveedores de Internet tienen el derecho de tomar y divulgar los mensajes electrónicos *sólo* si el emisor o el receptor están de acuerdo en ello. Muchas de estas compañías solicitan el consentimiento de los usuarios cuando éstos contratan el servicio.
- Toda compañía tiene el derecho de inspeccionar los mensajes electrónicos de sus empleados cuando éstos utilizan el sistema de correo electrónico de la empresa. Por lo tanto, los correos que se mandan desde el trabajo no son privados. Se ha determinado, por medio de varios juicios, que los empleadores tienen el derecho de monitorear los mensajes electrónicos de sus empleados. (Sobre el monitoreo de los empleados, consulte la Página Informativa 7 de PRC en www.privacyrights.org/fs/fs7-work.htm)
- Las compañías pueden ser obligadas a difundir información privada como resultado de un juicio o un citatorio.

- La ley USA PATRIOT Act, aprobada por el Congreso tras los ataques terroristas del 11 de septiembre de 2001, afecta a la ley de comunicaciones ECPA y su jurisdicción cibernética. Asimismo, amplía el tipo de archivos electrónicos que pueden solicitarse sin la orden de un juez. Para obtener más información sobre la ley USA PATRIOT Act, visite los siguientes sitios: Electronic Frontier Foundation (www.eff.org); Electronic Privacy Information Center (www.epic.org); Center for Democracy and Technology (www.cdt.org) y American Civil Liberties Union (www.aclu.org).

En resumen: existen diferentes compañías que ofrecen servicios de Internet y que cuentan con acceso a correos electrónicos. Sus mensajes pueden ser consultados por el personal de dichas compañías con algunas excepciones a la ley ECPA. Las autoridades pueden consultar información personal suya sin su consentimiento. Asimismo, las compañías pueden ver cualquier mensaje electrónico si el emisor o el receptor lo autorizan.

PARTE DOS: MONITOREO Y RASTREO DE LA ACTIVIDAD EN INTERNET

¿Pueden las compañías que ofrecen servicio de Internet consultar y archivar mi actividad en línea?

Sí. Mucha gente asume que navegar por Internet es una actividad anónima. *No lo es.* Casi todo lo que se transmite por Internet puede archivarse, incluso los mensajes en foros o los archivos que consulta el subscriber y las páginas que visita. Los proveedores de Internet y los operadores de sitios tienen la capacidad de recopilar dicha información.

Cookies. Muchos sitios de Internet depositan en su disco duro bloques de información conocidos como *cookies*, o galletas, que contienen datos sobre su visita a una determinada página electrónica. Cuando usted regresa al sitio, la información contenida en la galleta reconocerá sus datos. El sitio entonces podrá ofrecerle productos o publicidad de acuerdo a sus intereses personales, con base en el contenido de la galleta.

La mayoría de las galletas son utilizadas sólo por el sitio que colocó dicha información en su computadora. Sin embargo, existen galletas de terceras personas que transmiten información suya a compañías de publicidad. Estos negocios comparten sus datos con otras compañías publicitarias. Su navegador de Internet le ofrece a usted la capacidad de detectar y borrar galletas, incluyendo aquellas de terceras personas. (Obtenga más información sobre cómo bloquear las galletas al final de esta guía en la sección de Recursos Adicionales.

Bichos cibernéticos. Un bicho cibernético o *web bug* es una gráfica en un sitio o un mensaje electrónico "mejorado" que permite a terceras personas monitorear quién consultó el mensaje o la página. La gráfica puede ser de un tamaño fácilmente visible o casi invisible, del tamaño de un pixel. A los correos electrónicos que incluyen gráficas como páginas de internet se les conoce como mensajes mejorados, o también son conocidos como correos estilizados o de HTML. El bicho cibernético puede confirmar cuando usted consulta un mensaje o visita una página y archivar la información, incluso la dirección IP del usuario. La dirección IP de un usuario es un número de varios dígitos

que identifica a todos los aparatos conectados al Internet, como su computadora y la impresora.

Usted puede evitar los bichos cibernéticos si lee sus correos mientras está desconectado de Internet. Esta opción la ofrecen la mayoría de los programas. Otra opción es instalar un programa que detecta los bichos. Conozca más sobre los bichos cibernéticos en www.bugnosis.org. Aquí podrá descargar gratis un programa de detección. Muchos de los programas que detectan galletas de terceras personas también pueden detectar bichos cibernéticos. La última versión de Microsoft Internet Explorer permite a los usuarios desconectar las galletas de terceras personas y los bichos cibernéticos.

Los usos de la mercadotecnia y el spam. La información sobre los patrones de conducta de las personas que navegan por Internet es una valiosa y potencial fuente de ingresos para operadores de servicios de Internet y administradores de sitios. Los comerciantes pueden utilizar dicha información para desarrollar listas específicas de usuarios con gustos y comportamientos similares. Esta información también puede resultar en correos electrónicos no solicitados conocidos como spam. Asimismo, esta información puede resultar penosa para los usuarios que han consultado sitios controversiales o delicados.

Navegadores. Es importante estar al tanto de la información que transmiten a computadoras remotas los programas que usted utiliza para navegar por Internet. Los navegadores más utilizados son Netscape Navigator y Microsoft Internet Explorer.

La mayoría de los navegadores dan a conocer a los administradores de sitios información sobre su proveedor de servicio de Internet y otras páginas que usted ha visitado. Algunos navegadores, especialmente aquellos que no cuentan con las nuevas medidas de seguridad, son susceptibles de dar a conocer el correo electrónico de un usuario, teléfono y otra información contenida en su "agenda", en el caso de que el navegador también trabaje en conjunto con su correo electrónico. (Vea una demostración sobre la información que trasmite su navegador en la sección Recursos Adicionales).

Política de privacidad y sellos cibernéticos. La Comisión Federal de Comercio (Federal Trade Commission) recomienda a los administradores de todo sitio comercial que den a conocer su política de privacidad en su página de Internet. La mayoría de los sitios cuentan con información sobre sus prácticas de recaudación de información. Busque un "sello de aprobación de privacidad" conocido como TRUSTe (www.truste.org) en la primera página del sitio. A los participantes del programa TRUSTe se les requiere que den a conocer su política de privacidad y que se sometan a auditorías.

Las siguientes asociaciones ofrecen otros tipos de sellos de aprobación: Council of Better Business Bureaus (BBB) www.bbbonline.org; American Institute of Certified Public Accountants, WebTrust, www.cpawebtrust.org y Entertainment Software Rating Board, www.esrb.org/privacy_stmt.asp.

Monitoreo en el trabajo. Las personas con acceso al Internet en el trabajo deben estar conscientes de que los empleadores rastrean cada vez más los sitios que visitan sus empleados. Asegúrese de verificar la política de privacidad de su compañía.

Recomiende que se desarrolle una en el caso de que no exista. (Obtenga más información sobre otros aspectos del rastreo en la Página Informativa 7, www.privacyrights.org/fs/fs7-work.htm. Conozca más sobre el manejo de información en www.privacyrights.org/fs/fs12-ih2.htm

El acceso de las autoridades. Las autoridades pueden obtener acceso a los archivos con la información de los suscriptores con una orden judicial que demuestre que los datos son relevantes en una investigación criminal vigente (Communications Assistance for Law Enforcement Act, 18 USC § 2703(d)). Esta ley previene que las autoridades la utilicen para llevar a cabo "expediciones de pesca", en donde los funcionarios de gobierno esperan encontrar por accidente violaciones a la ley. Sin embargo, estos estatutos han sido debilitados gracias a la nueva ley USA PATRIOT Act, aprobada en noviembre del 2001 tras los ataques del 11 de septiembre.

¿Pueden las compañías cibernéticas consultar información almacenada en mi computadora sin que yo me dé cuenta?

Sí. Numerosos proveedores comerciales de Internet como AOL descargan automáticamente gráficas y programas nuevos en la computadora del usuario. En estos casos se le notifica al suscriptor. Sin embargo, existen otras intrusiones no tan claras. Algunos reportajes noticiosos han documentado que algunos proveedores han admitido, tanto accidental como intencionalmente, haber entrado a los sistemas duros de computadoras personales. Las compañías por lo general justifican dichas prácticas como una manera de mejorar el servicio al cliente.

Es difícil detectar este tipo de intrusiones. Es responsabilidad suya estar consciente de este potencial abuso a la privacidad e investigar ampliamente sobre cualquier servicio antes de suscribirse. Asegúrese siempre de leer la política de privacidad y el contrato de cualquier servicio que usted pretende utilizar.

¿Pueden los piratas obtener acceso a mi computadora?

Un creciente número de usuarios está conectado al Internet por medio de módems de cable y conexiones DSL a base de una línea telefónica. La vulnerabilidad a los ataques de piratas, o *hackers*, se agudiza cuando los usuarios utilizan el servicio de *broadband*, es decir que están "siempre conectados". Aconsejamos el uso de "paredes de fuego" para monitorear la actividad en la red y limitarla sólo a las actividades autorizadas. También debe consultarse la página de Internet del proveedor para proteger su computadora desconectando programas innecesarios e instalando nuevas medidas de seguridad. El sitio Zonelabs provee una "pared de fuego" gratis en su página www.zonelabs.com.

¿Cuáles son los artefactos espía y cómo puedo saber si están instalados en mi computadora?

Los artefactos espía son programas o aparatos que rastrean la actividad electrónica. Las compañías de software instalaron este tipo de programas en las computadoras para obtener más ingresos. Hay dos tipos de programas: de "monitoreo" y de "diagnóstico". El primero fue diseñado para que empleadores y padres de familia pudieran monitorear la actividad electrónica de sus subordinados e hijos, respectivamente. El servicio se

utilizó para otorgar acceso a documentos por medio de contraseñas y para evitar el uso inapropiado de la red. Los programas de "diagnóstico" son utilizados por compañías de software para archivar errores y hábitos de uso para mejorar la siguiente generación del software. El usuario, sin embargo, desconoce el hecho de que este tipo de programas estén instalados en su computadora. La sección de Recursos Adicionales al final de esta guía provee información sobre cómo localizar y quitar este tipo de programas.

PARTE TRES: CONSEJOS PARA SALVAGUARDAR SU PRIVACIDAD EN INTERNET

¿Qué puedo hacer para proteger mi privacidad en Internet?

Es fácil suponer que sus actividades en Internet son privadas, especialmente cuando usted está solo en su casa "surfeando" la red, mandando correos electrónicos y participando en foros. Pero esté consciente de que alguien puede monitorear sus actividades e interceptar sus mensajes en el incontrolable mundo del Internet.

1. Su cuenta está tan protegida como su **contraseña** lo permita. Elija contraseñas que no tengan sentido utilizando una combinación de palabras mayúsculas, minúsculas, números y símbolos, como tY8%uX. No utilice la misma contraseña - o variaciones de la misma - en otros programas. Una manera de crear una contraseña fácil de recordar es utilizar la primera y última letra de su poema favorito. Utilice números y símbolos de puntuación entre las letras. "Blanca nieves y los siete enanos" sería b*ni7en\$.s.

Cambie su contraseña con frecuencia. No permita que otras personas lo observen teclear su contraseña. No escriba su contraseña ni coloque dicha información en su monitor. Si debe de escribir su contraseña, tome medidas para esconder la información.

2. Consulte la **política de privacidad** del proveedor de Internet que utilice. La mayoría de estos proveedores dan a conocer su política de privacidad en sus sitios electrónicos o en otros tipos de documentación. Cuando esté consultando el Internet, busque las políticas de privacidad de las páginas que visite. También busque sellos de aprobación como TRUSTe o BBBOnline. Evite utilizar el sitio si no encuentra un logo que respalde la privacidad o si no está de acuerdo con la política al respecto.

3. Revise los **ajustes de galletas o cookies**. Ya pasó la época en que los navegadores escondían sus galletas sin opción para los usuarios. Hoy usted puede aceptar, rechazar o seleccionar las galletas de las páginas en las cuales usted está interesado. Tenga cuidado cuando modifique sus galletas ya que puede borrar algunas de sitios en los que usted confía. Es posible crear una función que limite las galletas de sitios que usted no conoce.

4. Busque otras opciones. Investigue todo lo posible de un servicio antes de usarlo. Haga preguntas dentro de un foro o algo similar. Consulte buscadores de grupos como <http://groups.google.com> para encontrar discusiones archivadas sobre el servicio que usted está considerando adquirir. Las malas reputaciones se difunden rápidamente por Internet. Si otras personas han tenido malas experiencias, usted sabrá qué hacer.

5. Suponga que toda comunicación en Internet **no es privada** a menos que utilice programas decodificadores especiales (encryption programs). Sin embargo, la mayor

parte de los programas decodificadores son difíciles de manejar y puede resultar problemático. Si no utiliza estos programas, recomendamos que por lo menos tome las siguientes precauciones: No dé información personal, teléfono, contraseña, dirección, número de tarjeta de crédito, de Seguro Social, información sobre su salud, fecha de nacimiento, etcétera en los cuartos de chateo, foros, correos electrónicos o biografías cibernéticas).

6. Tenga cuidado con **software que se carga automáticamente** y que lo inscribe a su lista de usuarios. Por lo general, estos programas solicitan información personal como datos financieros y después descargan esta información en el servicio. Estos programas pudieran tener la capacidad de consultar los archivos de su computadora sin que usted se dé cuenta. Contacte a estos servicios para utilizar otros métodos de suscripción.

7. Tome en cuenta que cualquier mensaje que usted teclee en Internet puede ser **archivado** y grabado. Es posible buscar y descubrir mensajes que alguien ha colocado en foros. (Vea <http://groups.google.com>). Antes de teclear algo, pregúntese si le gustaría *quedar ligado* a su mensaje público, ya sea por un empleador, un familiar o un comerciante. Utilice un seudónimo o un correo electrónico anónimo cuando participe en foros públicos. Considere obtener una dirección electrónica por medio de proveedores gratis como www.hotmail.com o www.yahoo.com. Registre un correo electrónico que no lo identifique y utilícelo cuando participe en foros públicos.

8. Utilizar **el comando "borrar" o "delete"** no significa que su correo desaparecerá ya que aún puede consultarse por medio de programas de copias de seguridad. Algunos programas pueden consultar mensajes borrados de su disco duro. Si usted desea borrar permanentemente mensajes y otros documentos de su computadora, considere utilizar programas gratuitos como los que se encuentran en <http://cleanup.stevengould.org/> u otros programas generales como Norton's Cleansweep (<http://www.symantec.com/sabu/ncs/>) o Helix Software's Nuts & Bolts (<http://www.helixsoftware.com>).

9. Su **biografía en Internet**. Si usted crea una, considere que podrá ser consultada por cualquiera. Es mejor no crear una biografía si por alguna razón usted debe de salvaguardar su identidad. Solicite a su proveedor de Internet que lo excluya de su directorio electrónico.

10. Tome en cuenta que si usted publica información personal **en su página de Internet**, los comerciantes y otros podrán obtener su dirección, número telefónico, correo electrónico y otra información que usted provea. Si está preocupado por su privacidad, sea discreto en su página de Internet.

11. Esté consciente de los **peligros sociales** que existen en Internet: acosos, vergüenzas, ataques verbales o ser víctima de correos spam (mensajes no solicitados). Las mujeres pueden quedar vulnerables si el nombre de su correo electrónico puede distinguirse como femenino. Considere utilizar seudónimos y direcciones electrónicas que no indiquen su sexo.

12. Si sus **hijos** utilizan el Internet, asegúrese de enseñarles los usos apropiados para salvaguardar la privacidad. Hágales saber de los peligros de dar a conocer información

sobre ellos mismos y su familia. (Vea la sección de Recursos Adicionales para obtener detalles).

13. Utilice sólo **sitios seguros** cuando transmita información sensible por Internet. Asegúrese de que la transmisión sea segura cuando utilice su tarjeta de crédito en un sitio de compras. Busque un candado cerrado en la parte inferior derecha de su página. Asimismo, asegúrese de que la dirección electrónica de la página contenga una "s" después del http en la parte superior de la página. Para conocer más consejos para hacer compras en Internet visite www.privacyrights.org/fs/fs23-shopping.htm.

14. Esté consciente de las actividades en línea que dejan **huellas electrónicas**. Su proveedor de Internet puede determinar qué tipo de buscadores utiliza, qué tipos de sitios visita y la fecha, hora y duración de sus sesiones en Internet. Los administradores de los sitios pueden monitorear sus actividades colocando galletas en su computadora. Pueden obtener más información suya si usted se registra en su sitio. Su navegador también puede transmitir información a otros sitios.

Usted puede evitar dejar huellas al utilizar servicios de "anonimato". Aproveche las herramientas disponibles para proteger su privacidad, conocidas generalmente como tecnologías de protección a la privacidad. Aquí se ofrecen explicaciones sobre **codificadores, anonymous remailers o correos anónimos, servicios de surfeo en el anonimato y protección de información almacenada**. Conozca más sobre estos servicios en la sección de Recursos Adicionales.

Codificación. Es un método capaz de codificar un correo electrónico o un documento de manera en que sólo las personas indicadas puedan decodificarlo y leerlo. Este método permite a los usuarios codificar información privada, transmitirla, almacenarla y difundirla sin la preocupación de que sea leída por otras personas. Existen programas de codificación como PGP (Pretty Good Privacy) y están disponibles por Internet.

Correos anónimos. Es relativamente fácil determinar el nombre y dirección electrónica de cualquier persona que trasmite un correo electrónico o que participa en un foro público. Existe un programa llamado "anonymous remailers" que consiste en recibir un mensaje electrónico, quitar información que pudiera identificar a un usuario, y mandarlo a su destino apropiado.

Servicios anónimos para navegar por Internet: Estos servicios combinan las funciones de "remailers", direcciones electrónicas desechables y aquellas de servidores "proxy" para esconder su identidad y transferir información entre su navegador y una página de Internet.

Software para proteger y almacenar información. Los programas de seguridad ayudan a prevenir el acceso no autorizado a documentos dentro de su computadora. Por ejemplo, existen algunos programas que codifican todos los directorios de su computadora con diferentes contraseñas para que sólo la persona indicada pueda abrirlas. Estos programas pueden incluir "rastreadores" que archivan toda actividad en el disco duro de su computadora. Un ejemplo de este tipo de programas es Steganos Security Suite, www.steganos.com/en/sss/features.htm

PARTE CUATRO: RECURSOS ADICIONALES

Existen varias organizaciones sin fines de lucro que pertenecen a grupos que abogan por los derechos de los usuarios de Internet. También proveen información extensa sobre temas de privacidad en Internet.

- **Center for Democracy and Technology**

(Centro para la democracia y la tecnología)

1634 I St. N.W. #1100, Washington, DC 20006

Teléfono: 202-637-9800.

E-mail: info@cdt.org.

Web: www.cdt.org

- **Computer Professionals for Social Responsibility**

(Asociación de Profesionistas por la Responsabilidad Social)

P.O Box 717, Palo Alto, CA 94302

Teléfono: 415-322-3778

E-mail: cpsr@cpsr.org

Web: www.cpsr.org.

- **Electronic Frontier Foundation**

(Fundación de las Fronteras Electrónicas)

454 Shotwell St., San Francisco, CA 94110

Teléfono: 415-436-9333

E-mail: eff@eff.org

Web: www.eff.org.

- **Electronic Privacy Information Center**

(Centro de Información sobre la Privacidad Electrónica)

1718 Connecticut Ave. N.W., Suite 200, Washington, DC 20009

Teléfono: 202-483-1140

E-mail: info@epic.org

Web: www.epic.org.

- **PrivacyActivism**

(Activismo y Privacidad)

Teléfono: 415-225-1730

E-mail: info@privacyactivism.org

Web: www.privacyactivism.org

- **Privacy Foundation**

(Fundación de la Privacidad)

University of Denver, Mary Reed Bldg.

2199 South University Blvd.

Denver, CO 80208

Teléfono: 303-871-4971

E-mail: info@privacyfoundation.org

Web: www.privacyfoundation.org

- **Privacy Rights Clearinghouse**

(Centro de Derechos por la Privacidad)

3100 5th Ave., Suite B, San Diego, CA 92103

Teléfono: 619-298-3396

Contacto: www.privacyrights.org/qwertyuiopasdfghjkl.php

Web: www.privacyrights.org.

La **Comisión Federal de Comercio** es la principal dependencia federal que regula la privacidad en Internet. La página de Internet de esta dependencia provee información extensa sobre la política pública y también ofrece consejos a los consumidores.

- **Federal Trade Commission**

(Comisión Federal de Comercio)

600 Pennsylvania Ave. N.W.

Washington, DC 20580

En Internet: www.ftc.gov/privacy/index.html

El sitio federal para consumidores: www.consumer.gov

Varios grupos de interés público han patrocinado la guía **Computer Privacy Guide** www.consumerprivacyguide.org. El sitio ofrece consejos, un glosario de términos y videos didácticos con instrucciones sobre cómo aprovechar las funciones relacionadas con la privacidad que ofrecen los programas que usted utiliza en Internet.

Existen **boletines informativos** sobre la privacidad en Internet:

- *Computer Privacy Digest*: Puede consultarse como un Usenet newsgroup en *comp.society.privacy*. Puede recibirlo a través de correos electrónicos. Suscríbese mandando un correo electrónico al moderador a: comp-privacy-request@uwm.edu. En Internet: www.uwm.edu/Org/comp-privacy.
- *Privacy Forum*: Para obtener información sobre las suscripciones, escriba un correo electrónico a privacy-request@vortex.com. Teclee las palabras "subscribe privacy" en el mensaje. En Internet: www.vortex.com/privacy.
- Algunos de los grupos de interés indicados arriba ofrecen boletines informativos sobre temas legislativos, últimas noticias, publicaciones, tópicos internacionales y más. Puede suscribirse en las siguientes páginas de Internet:
 - Center for Democracy and Technology, www.cdt.org/publications
 - Electronic Frontier Foundation, www.eff.org/effector
 - Electronic Privacy Information Center, www.epic.org/alert/subscription.htm

Los siguientes **sitios** contienen información sobre la privacidad en Internet:

Correos electrónicos anónimos: Para obtener información sobre los programas de correos electrónicos anónimos consulte las siguientes preguntas frecuentes compiladas por Andre Bacard en www.andrebacard.com/remail.html.

Navegación anónima. Hay numerosos sitios comerciales que ofrecen herramientas para navegar el Internet anónimamente, incluyendo www.anonymizer.com, www.freedom.net, y www.ultimate-anonymity.com. Estos servicios fueron analizados en www.Webveil.com.

Niños. Si sus hijos utilizan el Internet, solicite gratuitamente un panfleto titulado "Child Safety on the Information Highway" (Seguridad para niños en Internet). El panfleto es cortesía del National Center for Missing and Exploited Children. Teléfono: 800-843-5678. En Internet: www.safekids.com.

Conozca más sobre los programas de "supervisión paterna" en la página de "Resources for Internet Parents" (Recursos sobre el Internet para padres) en www.netparents.org.

La Comisión Federal de Comercio cuenta con recursos extensos para padres y niños. Visite www.ftc.gov/bcp/online/edcams/kidzprivacy/index.html. Conozca más sobre la ley Children's Online Privacy Protection Act en www.ftc.gov/privacy/index.html. También puede consultar la Página Informativa 21 titulada "Children in Cyberspace" (Los niños en Internet) en www.privacyrights.org/fs/fs21-children.htm.

Cookies o "galletas". Aprenda más sobre las maneras de bloquear las galletas y cómo utilizar otros tipos de filtros cibernéticos. Visite: www.junkbusters.com, www.consumerprivacyguide.org, www.cookiecentral.com, y www.spamblocked.com/proxomitron.

Demostraciones. Si desea ver una demostración sobre qué tipo de información puede ser capturada de su disco duro por medio de un navegador cuando usted está en Internet visite www.privacy.net/analyze.

Codificación. Para conocer más sobre el programa comercial de codificación PGP, visite www.pgp.com. Para obtener información sobre los programas de PGP, visite el centro de distribución MIT Distribution Center en <http://web.mit.edu/network/pgp.html> y su página central International PGP Home Page en www.pgpi.org.

Glosario. Para obtener un diccionario sobre la terminología cibernética, visite el Center for Democracy and Technology en www.consumerprivacyguide.org/glossary. Privacy Foundation también cuenta con un glosario de términos: www.privacyfoundation.org/resources/glossary.asp.

Proveedores de servicios de Internet: Para obtener un directorio de proveedores, consulte el Boardwatch's Directory of Internet Service Providers en www.boardwatch.com/ASP/Search/NationalISP.asp.

Extraer su nombre de listas. Para extraer su nombre de la lista de galletas que se comparte entre comerciantes, visite la página de Network Advertising Initiative en www.networkadvertising.org.

Tecnología para mejorar la privacidad. El sitio de EPIC cuenta con una sección de programas que ofrecen barreras adicionales de protección cuando usted navega por Internet. La página es www.epic.org/privacy/tools.html. Asimismo, visite la sección de enlaces titulada Privacy Links de Privacy Rights Clearinhouse, donde encontrará información sobre programas, herramientas y productos: www.privacyrights.org/links.htm.

Buscadores. Algunos buscadores son: www.google.com, www.northernlight.com, www.dogpile.com, www.lycos.com y www.yahoo.com. Estos buscadores lo ayudarán a encontrar casi todo tipo de información por medio de palabras clave, nombres personales y nombres de organizaciones. Para encontrar mensajes en foros públicos, visite Google en <http://groups.google.com>. La página www.paml.net provee un buscador de otros tipos de discusiones cibernéticas que no necesariamente son consideradas públicas. Los autores de estos mensajes no siempre saben que dicha información está siendo archivada.

Spam. Encuentre consejos sobre cómo reducir mensajes electrónicos no-solicitados en www.spamcom.net o www.stop-spam.org. La Página Informativa 20 ofrece una lista adicional de listas de internet que ofrecen consejos para detener el spam: www.privacyrights.org/fs/fs20-spam.htm. Para conocer más sobre las leyes relacionadas con el spam, visite www.spamlaws.com.

Programas de espionaje. Ad-Aware es un programa gratuito capaz de detectar y remover software de espionaje de la memoria de su computadora y de su disco duro: www.lavasoft.de. Otras herramientas similares pueden encontrarse en la página de enlaces de PRC www.privacyrights.org/links.htm#tools.

Aclaración: Hemos proporcionado los nombres y direcciones de varios sitios comerciales en esta guía. Dicha mención no implica patrocinio de nuestra parte.