Revista Digital Universitaria
10 de septiembre 2004 • Volumen 5 Número 8 • ISSN: 1067-6079

ARTICULO

SEGURIDAD PERSONAL CONTRA DELITOS CIBERNÉTICOS

Luz María Ramírez Romero
Subdirectora de Servicios Web de la Dirección de Sistemas de DGSCA, UNAM.
luzrr@servidor.unam.mx

Fecha de recepción: 4 de agosto de 2004
Fecha de aceptación: 26 de agosto de 2004

© Coordinación de Publicaciones Digitales. DGSCA-UNAM
Se autoriza la reproducción total o parcial de este artículo, siempre y cuando se cite la fuente completa y su dirección electrónica.

http://www.revista.unam.mx/vol.5/num8/art52/art52.htm

SEGURIDAD PERSONAL CONTRA DELITOS CIBERNÉTICOS

RESUMEN

Uno de los grandes beneficios de Internet ha sido compartir y acceder a la información desde diferentes lugares geográficos. Lamentablemente la tecnología asociada a la red tiene el inconveniente de exponer nuestros datos personales, estos pueden ser usados de manera inadecuada. Un ejemplo de ello, puede ser la dirección de correo electrónico que genera el molesto *spam*, mejor conocido como correo basura. En escenarios más complicados, se puede ser víctima de delitos asociados a la distribución de los datos personales a través de la red. Este problema ha cobrado mayor importancia y el uso de esta tecnología se ha hecho más cotidiano. Por ello, las consecuencias de hacer públicos nuestros datos y la manera de evitarlo son temas de gran relevancia en la actualidad y son los aspectos que se abordarán en este artículo.

Palabras clave: servidor proxy, *spam*, spyware, delito, policía cibernética.

PERSONAL SECURITY AGAINST CYBERNETIC DELINQUENCY

ABSTRACT

One of the big benefits of Internet has been the sharing of information as well as the access from different geographical places. Regretfully the technology associated to the network has the inconvenient that it exposes our personal data, and it can be used in non adequate way. An example of this situation is the knowledge of our email. This situation may lead to the receival of the *spam* or garbage messages (spam is also known as non requested mail). In more complicate cases, we can become victims of delinquency associated to the distribution of the personal data through the network. This problem has become more important as the use of this technology has become daily. The consequences of making public our personal data and the ways to avoid it are subjects of this article.

Keywords: proxy server, *spam*, spyware, delinquency, cybernetic police.

© Coordinación de Publicaciones Digitales. DGSCA-UNAM
Se autoriza la reproducción total o parcial de este artículo, siempre y cuando se cite la fuente completa y su dirección electrónica.

10 de septiembre 2004 • Volumen 5 Número 8 • ISSN: 1067-6079

En la actualidad no es común proporcionar información a un extraño, ya sean datos personales como nuestro nombre, dirección, teléfono, nombre de la empresa a la que pertenecemos o correo electrónico. Pese a lo anterior, en Internet se comparte esta información y más. Desafortunadamente se comete el error de confiar a una computadora información personal y no se tiene la certeza de quién la recibe. Algunos de los fraudes cibernéticos realizados han sido producto del exceso de confianza en la red, aunado al abuso de individuos que colocan páginas web con la intención de obtener datos importantes, como puede ser el número confidencial de nuestra tarjeta de crédito.

¿QUÉ DATOS HACEMOS PÚBLICOS EN INTERNET?

- Datos que se proporcionan en los formatos electrónicos en busca de empleo.
- La compra de un *software* gratuito o productos a través de la web, en los que se llena una serie de formas donde se proporciona un sin número de información personal.
- Participaciones en los foros de discusión y *chats*.
- Como usuario de Internet es muy común dejar información de los sitios visitados, la cual puede ser consultada por nuestros compañeros de trabajo.

El navegar por la red implica un intercambio de información, no sólo obtienen nuestra dirección de IP, sino también cuáles son las páginas web que se han visitado, qué temas son de nuestra preferencia o qué tipo de navegador estamos utilizando. La información es tan valiosa, que algunos administradores de sitios web programan sus páginas para almacenar en archivos de texto (*cookies*) en nuestros propios equipos de cómputo, información que posteriormente leerán para ofrecernos algún producto o servicio. Así, los publicistas han aprovechado la información que van recolectando para hacernos llegar el famoso *spam*, el cual es molesto, ya que invade el espacio destinado para nuestros mensajes e incluso pagamos el costo de permanecer más tiempo conectados al leer o borrar estos mensajes basura. De acuerdo con José Armando Aguilar quien escribió el artículo "*Fraudes por Internet*" <http://www.profeco.gob.mx/html/revista/publicaciones/fraudes_inter_abr04.pdf> destaca que el correo electrónico *spam* es una de las técnicas más socorridas para cometer un fraude. Por este medio, se hace llegar un mensaje a las personas sobre viajes que alguien regala a cambio de revelar información personal o privada.

El valor de la información es tan alto que los *hackers*, se han tomado la molestia de violar la seguridad de nuestros equipos de cómputo para entrar a nuestro disco duro y copiar información. Mucha de esta información puede ser el archivo con el diseño de un nuevo producto en nuestra empresa, o bien, nuestros *passwords* o el número confidencial para acceder a la información de nuestra tarjeta de crédito. En escenarios más complicados, los niños son un público que desconoce los peligros de navegar en la red e interactúan con personas de las que saben poco o nada de ellos; este problema se refleja en secuestros, venta o explotación sexual. Otro delito importante que se lleva a cabo a partir del conocimiento de datos personales es el robo de identidad. A través de la obtención de los datos de la cuenta de crédito de un internauta, el defraudador puede efectuar compras de productos y servicios utilizando la cuenta de la que obtuvo información.

Los hechos expuestos desanimarían a cualquiera de seguir utilizando Internet, sin embargo es pertinente señalar que se han desarrollado técnicas y servicios con el objetivo de proteger la información. Asimismo se pueden tomar medidas para prevenir estos problemas a pesar de hacer pública gran parte de nuestra información sin nuestra voluntad o consentimiento expreso.

© Coordinación de Publicaciones Digitales. DGSCA-UNAM
Se autoriza la reproducción total o parcial de este artículo, siempre y cuando se cite la fuente completa y su dirección electrónica.

EL SECRETO DE LOS DATOS PERSONALES

Fundamentos Legales del Derecho a la Privacidad

El lector se preguntará si todo este uso indiscriminado de la información que publicamos consciente o inconscientemente es legal.

De acuerdo al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos <http://www.miredespa.com/wmaton/Other/Legal/Constitutions/Mexico/Spanish/constitution-mex.html> que aborda el tema del Derecho a la intimidad se establece que "nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento…"

Asimismo, hay leyes que regulan el *spam*, como la Ley Federal de Protección al Consumidor (artículos 16, 17, 18 y 18bis).

Ley Federal de Protección al Consumidor
<http://www.profeco.gob.mx/html/juridico/lfpc/lfpc_1.htm>

ARTÍCULO 16

Los proveedores y empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios están obligados a informar gratuitamente a cualquier persona que lo solicite si mantienen información acerca de ella. De existir dicha información, deberán ponerla a su disposición si ella misma o su representante lo solicita, e informar acerca de qué información han compartido con terceros y la identidad de esos terceros, así como las recomendaciones que hayan efectuado. La respuesta a cada solicitud deberá darse dentro de los treinta días siguientes a su presentación.

En caso de existir alguna ambigüedad o inexactitud en la información de un consumidor, éste se la deberá hacer notar al proveedor o a la empresa, quien deberá efectuar dentro de un plazo de treinta días contados a partir de la fecha en que se le haya hecho la solicitud, las correcciones que fundadamente indique el consumidor, e informar las correcciones a los terceros a quienes les haya entregado dicha información. Para los efectos de esta ley, se entiende por fines mercadotécnicos o publicitarios el ofrecimiento y promoción de bienes, productos o servicios a consumidores.

Ley Federal de Protección al Consumidor
<http://www.profeco.gob.mx/html/juridico/lfpc/lfpc_1.htm>

ARTÍCULO 17

En la publicidad que se envíe a los consumidores se deberá indicar el nombre, domicilio, teléfono y en su defecto, la dirección electrónica del proveedor o de la empresa que envíe la publicidad a nombre del proveedor y de la Procuraduría.

El consumidor podrá exigir directamente a proveedores específicos y a empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, no ser molestado en su domicilio, lugar de trabajo, dirección electrónica o por cualquier otro medio, para ofrecerle bienes, productos o servicios, y que no le envíen publicidad. Asimismo, el consumidor podrá exigir en todo momento a proveedores y a empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, que la información relativa a él mismo no sea cedida o transmitida a terceros, salvo que dicha cesión o transmisión sea determinada por una autoridad judicial.

© Coordinación de Publicaciones Digitales. DGSCA-UNAM
Se autoriza la reproducción total o parcial de este artículo, siempre y cuando se cite la fuente completa y su dirección electrónica.

10 de septiembre 2004 • Volumen 5 Número 8 • ISSN: 1067-6079

Ley Federal de Protección al Consumidor
<http://www.profeco.gob.mx/html/juridico/lfpc/lfpc_1.htm>

ARTÍCULO 18

La Procuraduría podrá llevar, en su caso, un registro público de consumidores que no deseen que su información sea utilizada para fines mercadotécnicos o publicitarios. Los consumidores podrán comunicar por escrito o por correo electrónico a la Procuraduría su solicitud de inscripción en dicho registro, el cual será gratuito.

ARTÍCULO18 bis. Queda prohibido a los proveedores y a las empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios y a sus clientes, utilizar la información relativa a los consumidores con fines diferentes a los mercadotécnicos o publicitarios, así como enviar publicidad a los consumidores que expresamente les hubieren manifestado su voluntad de no recibirla o que estén inscritos en el registro a que se refiere el artículo anterior. Los proveedores que sean objeto de publicidad son corresponsables del manejo de la información de consumidores cuando dicha publicidad la envíen a través de terceros.

Asimismo la Ley Federal de Protección al Consumidor contempla los derechos de los consumidores cuando realizan transacciones en el web.

Ley Federal de Protección al Consumidor Artículos relativos al derecho de privacía.
<http://www.profeco.gob.mx/html/juridico/lfpc/lfpc_8bis.htm>

Capítulo VIII bis. De los derechos de los consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología.

ARTÍCULO 76 bis. Las disposiciones del presente capítulo aplican a las relaciones entre proveedores y consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología. En la celebración de dichas transacciones se cumplirá con lo siguiente:

I. El proveedor utilizará la información proporcionada por el consumidor en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente;

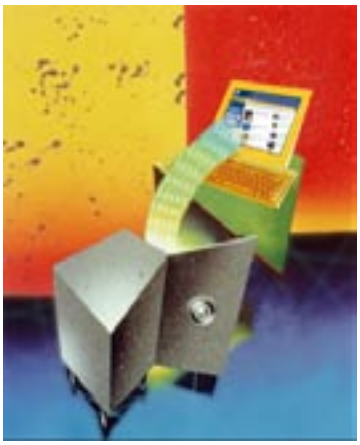
II. El proveedor utilizará alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el consumidor e informará a éste, previamente a la celebración de la transacción, de las características generales de dichos elementos;

VI. El proveedor respetará la decisión del consumidor en cuanto a la cantidad y calidad de los productos que desea recibir, así como la de no recibir avisos comerciales; y,

VII. El proveedor deberá abstenerse de utilizar estrategias de venta o publicitarias que no proporcionen al consumidor información clara y suficiente sobre los servicios ofrecidos, en especial tratándose de prácticas de mercadotecnia dirigidas a la población vulnerable, como los niños, ancianos y enfermos, incorporando mecanismos que adviertan cuando la información no sea apta para esa población.

© Coordinación de Publicaciones Digitales. DGSCA-UNAM
Se autoriza la reproducción total o parcial de este artículo, siempre y cuando se cite la fuente completa y su dirección electrónica.

TECNOLOGÍA DE SEGURIDAD DIGITAL



La primera actividad de protección es la regla de oro del trabajo en computadoras, es decir, efectuar respaldos de nuestra información en dispositivos como memorias *flash* (dispositivos que se conectan al puerto USB de la computadora y que son portátiles y muy confiables) o discos compactos.

Los prestadores de servicios en Internet han incorporado técnicas, funciones y tecnología para proteger los datos de sus clientes (*PET*, *Privacy Enhancing Technologies* o Tecnologías habilitadoras de Privacidad).

Una de las tecnologías PET más importantes es el cifrado de la información sensible que viaja por la red, lo cual nos da la confianza de que sólo el receptor podrá leer nuestro número de tarjeta de crédito -por citar un ejemplo- y deja inhabilitados a los administradores de todas las computadoras intermedias por las que pasan los mensajes de datos para comprender el contenido del mensaje.

Hay organismos internacionales que han emitido recomendaciones para que los administradores de sitios web serios y que se guían con ética, determinen y publiquen en sus páginas, las políticas de privacidad de la información que tienen. Un ejemplo de políticas de privacidad lo podemos analizar en el sitio de Amazon en donde se indica qué tipo de información se solicitará al usuario, con qué fines se utilizará y con qué organizaciones se compartirá a fin de llevar a cabo la transacción de venta de artículos: <http://www.amazon.com/exec/obidos/tg/browse/-/468496/103-8340879-4935060>.

En el artículo de la Procuraduría Federal del Consumidor (PROFECO) sobre Comercio Electrónico Seguro, se hace hincapié en que el consumidor debe antes de efectuar una transacción en línea, verificar entre otras cosas, las políticas de seguridad de la información que le proporcionará al proveedor. Ya que al efectuar la compra, el consumidor proporcionará su nombre, dirección, número telefónico o número de tarjeta de crédito. <http://www.profeco.gob.mx/html/revista/publicaciones/seguro_ce_may04.pdf>.

Las políticas de privacidad deben indicarle al usuario qué se hará con la información personal que introduzca a través de un formulario web para la compra de algún artículo, ya que en algunas ocasiones, el proveedor puede compartir o vender esta información a otras personas.

También se han creado sellos de aprobación de organismos como TRUSTe <http://www.truste.org>, que implica que los administradores que colocan el sello en sus páginas web, tienen políticas de privacidad que hacen del conocimiento del público y que además se sujetan a auditorias para efectivamente comprobar que respetan y siguen estas políticas.

Sellos que dan credibilidad a las políticas de privacidad de los sitios web son:

© Coordinación de Publicaciones Digitales. DGSCA-UNAM
Se autoriza la reproducción total o parcial de este artículo, siempre y cuando se cite la fuente completa y su dirección electrónica.

10 de septiembre 2004 • Volumen 5 Número 8 • ISSN: 1067-6079

TRUSTe: <http://www.truste.org>

BBB: <http://www.bbbonline.org>

WebTrust: <http://www.cpawebtrust.org>

En el ámbito laboral, también se deben establecer políticas de privacidad y hacerlas del conocimiento de los empleados, esto con la finalidad de evitar descontentos y sorpresas desagradables en las evaluaciones del personal.

Es importante mencionar que las políticas de privacidad no sólo deben abarcar los medios electrónicos y la Internet, sino que también deben contemplar qué empleados tienen acceso a la información y las acciones permitidas a los empleados para el uso de dicha información. *Privacy Rights Clearinghouse* <http://www.privacyrights.org>, recomienda a las empresas, crear conciencia en sus empleados sobre la importancia en el manejo de la información y sobre las políticas de uso de la misma, así como de las sanciones para quién utilice con otros fines los datos de los usuarios o para quién tenga algún descuido con los datos que maneja.

También es tema de consideración de los administradores web, solicitar la información directamente del usuario y no recolectarla de manera automática, a partir de las variables de ambiente de las sesiones web o a partir de otros medios como generación de bitácoras.

Para protegernos de los *hackers* es importante que instalemos un *firewall* sencillo y que instalemos las actualizaciones del *software* que utilizamos, como el navegador de web, el sistema operativo o el cliente de correo electrónico. Asimismo es recomendable no entrar a páginas sobre *hackers*, *software* pirata o sitios web pornográficos, ya que en muchas ocasiones estas páginas web guardan en nuestra computadora *spyware*, o *software* que monitorea lo que hacemos y además reporta estos datos a sus creadores, vía Internet.

Para detectar y borrar *Spyware* hay programas como el *Ad-aware*, que buscan el *Spyware* en la memoria, el registro de *windows* y el disco duro <http://www.lavasoftusa.com>. También se recomienda deshabilitar el uso de *cookies* en el navegador, o bien, borrar las *cookies* periódicamente.

Se recomienda usar un pseudónimo para participar en *chats* y foros de discusión. En el sitio web de la Policía Cibernética <http://www.ssp.gob.mx/application?pageid=pcibernetica> se recomienda que este pseudónimo sea creado con la intención de ocultar el sexo y edad de la persona, además de que se deben evitar palabras provocativas que inviten a otros a enviarnos mensajes ofensivos o poco apropiados. Se debe instruir a los niños y adolescentes sobre los peligros de proporcionar información a desconocidos en Internet y más aun, debemos insistirles de no tener encuentros físicos con personas que "conocemos virtualmente" a través del *chat*. No se debe de olvidar que en realidad no se sabe quién está en la otra computadora.

© Coordinación de Publicaciones Digitales. DGSCA-UNAM
Se autoriza la reproducción total o parcial de este artículo, siempre y cuando se cite la fuente completa y su dirección electrónica.

Asimismo es conveniente utilizar servicios anonimizadores, que protegen nuestra identidad, para navegar sitios web. Para utilizar estos servicios, primero se debe entrar a su página y colocar en ella el URL de la página que se desea visitar. Éste servicio protegerá nuestra identidad, al funcionar como un puente entre la página objetivo y nosotros. Es en este punto importante recalcar que si alguien intenta algún acto fraudulento utilizando un anonimizador, siempre hay forma de rastrearlo, ya que el anonimizador sí conocerá la identidad de quién accede, asimismo los Proveedores de Servicios de Internet, tendrán el registro de la fecha, hora y tiempo por el que se utiliza el servicio.

OCULTANDO NUESTRA IDENTIDAD

Para quienes tenemos una dirección IP fija, nos puede resultar muy útil utilizar los servicios de navegación anónima a fin de disminuir la cantidad de *spam* que recibimos en nuestro buzón de correo electrónico.

Una de las técnicas que nos proporciona anonimato en la navegación es el "Servicio Anonimizador" o *Anonymizer*.

El servicio más popular de anonimización es: <http://www.anonymizer.com/>.

Para utilizar los servicios anonimizadores, primero se debe cargar en el navegador web la página del servicio y después se le debe indicar el URL que se desea visitar anónimamente.

Hay anonimizadores gratuitos y otros que cobran por el servicio. El inconveniente de utilizar este producto es que la transferencia de información hacia nuestra computadora será más lenta, ya que la información debe pasar primero por un intermediario antes de llegar a nuestro equipo.

Además, la información es cifrada o encriptada por el anonimizador, lo cual consume tiempo de procesamiento y agrega información a los mensajes de datos, lo que contribuye a hacer más lento el servicio, pero estas características ofrecen más seguridad. Otra característica no deseada de los anonimizadores es que agregan publicidad a las páginas que estamos visitando.

Otra forma de lograr la navegación anónima es a través de "*Servidores Proxy*". El servidor *proxy* también funciona como intermediario, solicitando las páginas web y haciéndolas llegar a nuestro equipo.

Las diferencias de los servidores *proxy* respecto a los servicios anonimizadores son que no filtran *cookies*, *applets*, ni código malicioso. Otra diferencia importante es que no todos son anónimos, algunos permiten que la otra parte obtenga la dirección IP desde la cuál nos conectamos. Al igual que los anonimizadores, los proxies reducen la velocidad en la recepción de información.

© Coordinación de Publicaciones Digitales. DGSCA-UNAM
Se autoriza la reproducción total o parcial de este artículo, siempre y cuando se cite la fuente completa y su dirección electrónica.

10 de septiembre 2004 • Volumen 5 Número 8 • ISSN: 1067-6079

ORGANISMOS REGULADORES EN MÉXICO

- ***Policía Cibernética*** <http://www.ssp.gob.mx/application?pageid=pcibernetica>

  Órgano creado en diciembre de 2002, que depende de la Policía Federal Preventiva. Las principales funciones de esta institución son: detectar fraudes, falsificaciones, intrusión en sistemas de cómputo, pornografía infantil, y amenazas, entre otros. También está dentro de sus funciones la identificación, monitoreo, rastreo y localización de todas aquéllas manifestaciones delictivas tanto en el territorio nacional como fuera de él. Esta última atribución de la Policía Cibernética es de capital importancia, puesto que los fraudes y delitos en Internet suelen traspasar las fronteras de los países y se convierten en delitos transfronterizos.

- ***Procuraduría Federal del Consumidor*** <http://www.profeco.gob.mx/html/inicio/inicio.htm>
  Órgano cuya misión es "procurar la equidad y seguridad en las relaciones de consumo, para favorecer el mejor funcionamiento de los mercados y garantizar los derechos e intereses de los consumidores, mediante acciones de carácter preventivo y correctivo".

ORGANISMOS INTERNACIONALES

- ***Grupo de Expertos en Delito Cibernético*** <http://www.oas.org/juridico/spanish/cybersp_intro.htm> Constituidos en 1999, cuando los Ministros de Justicia o Procuradores Generales de las Américas recomendaron establecer un grupo de expertos intergubernamentales sobre delito cibernético.

- ***Secretaría General de la OEA (Organización de Estados Americanos)***
  En cumplimiento de las resoluciones de la Asamblea General de la OEA, cumple las funciones de Secretaría Técnica y administrativa del Grupo de Expertos en Delito Cibernético.

- ***INTERPOL*** <http://www.oas.org/juridico/english/cyber_links_list.htm>
  En virtud de que los delitos y fraudes en internet rebasan la legislación de un solo país, puesto que las fronteras son rebasadas, a su vez, es necesario valerse de un organismo de jurisdicción internacional como la INTERPOL.

  La INTERPOL existe para hacer un mundo más seguro y su objetivo es combatir el crimen optimizando los esfuerzos de organismos internacionales. <http://www.interpol.int/Public/TechnologyCrime/default.asp>.

© Coordinación de Publicaciones Digitales. DGSCA-UNAM
Se autoriza la reproducción total o parcial de este artículo, siempre y cuando se cite la fuente completa y su dirección electrónica.

CONCLUSIÓN

Por lo anterior se puede dejar claro y reiterar al lector que no debe desalentarse para utilizar Internet. Este medio que permite la difusión de la información conlleva grandes beneficios al brindar acceso a temas muy diversos, así como la posibilidad de contactar gente de diversas partes del mundo de forma económica y sencilla, incluso nos ayuda a realizar trabajo remoto desde nuestro hogar y hacerlo llegar de manera casi inmediata a nuestro centro laboral.

Sin lugar a dudas el objetivo de este trabajo ha sido lograr que el lector tome conciencia de los problemas sociales que tiene el hacer uso de la Internet con exceso de confianza, y de mismo modo se ha percatado de las diversas formas que existen para prevenir situaciones desagradables y complicadas.

© Coordinación de Publicaciones Digitales. DGSCA-UNAM
Se autoriza la reproducción total o parcial de este artículo, siempre y cuando se cite la fuente completa y su dirección electrónica.

10 de septiembre 2004 • Volumen 5 Número 8 • ISSN: 1067-6079

REFERENCIAS ELECTRÓNICAS

- *Privacy Rights Clearinghouse*. [en línea]: Home Page, 30-07-2004. Disponible en: <http://www.privacyrights.org> [Consulta 1 agosto 2004].

- *Policía Cibernética* [en línea]. Secretaría de Seguridad Pública, Policía Cibernética, 2003, Disponible en: <http://www.ssp.gob.mx/application?pageid=pcibernetica> [Consulta 1 agosto 2004].

- *Procuraduría Federal del Consumidor* [en línea]: Página inicial. Disponible en: <http://www.profeco.gob.mx/html/inicio/inicio.htm> [Consulta 1 agosto 2004].

- *Trust-e* [en línea]: Home page, 2004. Disponible en: <http://www.truste.org> [Consulta 1 agosto 2004].

- *A Better Business Bureau Program* [en línea]. Council of Better Business Bureau, 2003. Disponible en: <http://www.bbbonline.org/> [Consulta: 3 agosto 2004].

- *WebTrust* [en línea]: Home page, 2004. Disponible en: <http://www.cpawebtrust.org> [Consulta: 3 agosto 2004].

- *INTERPOL* [en línea]. INTERPOL, Information Technology Crime, 2004. Disponible en: <http://www.interpol.int/Public/TechnologyCrime/default.asp> [Consulta: 3 agosto 2004].

© Coordinación de Publicaciones Digitales. DGSCA-UNAM
Se autoriza la reproducción total o parcial de este artículo, siempre y cuando se cite la fuente completa y su dirección electrónica.