EL EXPERTO

Ciberterrorismo y Hacktivismo Zapatista

Desde el triste suceso del 11 de septiembre pasado, todos hemos sido "bombardeados" por una tremenda ola de noticias sobre el terrorismo, el Al Qaeda, los Talibanes y el mundialmente famoso y temido Bin Laden. No recuerdo un solo día en que no haya aparecido al menos una nota de prensa en periódicos o noticieros relacionada con este tema. Hemos aprendido qué armas tiene el ejército estadounidense: tanques, aviones, tropas, misiles, bombas, etc. También nos dimos cuenta de que los terroristas no usan sólo armas convencionales para sus propósitos, hoy usan aviones suicidas, mañana... quién sabe. La guerra bacteriológica también se volvió una psicosis, especialmente con los ataques de Ántrax en Estados Unidos.

Sin embargo, poco o nada se ha escuchado de otro peligro latente que puede afectar infraestructura de gobierno, militar, privada e incluso recursos básicos de la población en general, como electricidad, agua, gas, etc. Aunque para algunos tal vez se trate de ciencia ficción, el Ciberterrorismo es una realidad tan palpable, que ya lo hemos vivido en México, aunque pocos estén enterados.

El "Ciberterrorismo" puede tener diferentes connotaciones en las que se aprovechan las redes informáticas (Internet, particularmente) para: (a) obtener o transmitir información relacionada con la planeación de ataques terroristas; (b) fomentar e incitar la realización de actos de terrorismo; (c) cometer actos ciberterroristas de diversa índole, 'e pueden consistir principalmente en dañar o ıetrar sistemas informáticos de gobierno y ..quellos que controlan infraestructura básica de una nación. Los ataques más avanzados se pueden llevar a cabo con "armas electrónicas", como bombas de pulsos electromagnéticos (EMP), bombas de radio frecuencia de alta energía (HERF), y bombas de microondas de alto poder (HPM).

Estas armas en conjunto, según el especialista Winn Schwartau, acuñan lo que podría conocerse como el "Pearl Harbor Electrónico". Aunque suenan armas de la Guerra de las Galaxias, por poner un ejemplo, las EMP fueron usadas en la Guerra del Golfo (1991) para neutralizar el equipo informático y de telecomunicaciones de instalaciones Iraquíes con radares de defensa aérea. Estas bombas no causan ningún daño físico a las personas, pero sí son capaces de "destruir" cualquier aparato electrónico o sistema informático que se encuentre dentro de su alcance.

Algunos expertos afirman que Pakistan tiene un centro educacional terrorista de guerra informática, supuestamente con base en Londres. Ciertos grupos árabes han denominado al Internet como "un arma a ser dominada". Los grupos extremistas, milicias y guerrillas pueden intentar ciberasaltos masivos contra el gobierno e infraestructura crítica de un país, como el transporte, la energía y servicios de emergencia.

El "Hacktivismo" es un término que está íntimamente relacionado con el Ciberterrorismo, aunque son distintos, sobre todo por los objetivos que mueven a quienes realizan estas actividades. Este concepto surge de la mezcla de dos palabras "hacking" que genéricamente significa la penetración y/o daño a sistemas informáticos, y "activismo", término que todos conocemos. El "Hacktivismo" entonces, implica que grupos ambientalistas, anti-nucleares, anti-guerras (pro-pacifistas), pro-derechos humanos, globalifóbicos, etc. pueden usar la red para promover ciber-desobediencia civil, manifestaciones electrónicas o ciber-ataques en contra del gobierno.

En 1998, una instalación nuclear de la India fue hackeada después de pruebas de armamento y bombas atómicas. También en el mismo año, un grupo llamado "The Hong Kong Blondes" hackeó la red informática de la Policía China, como forma de protesta en contra de los arrestos políticos.

Tal vez lo que más nos llame la atención, porque nos atañe en lo particular, fue un suceso que combinó las características de Ciberterrorismo y Hacktivismo, ya no sólo fue una manifestación política, sino también buscaba dañar sistemas informáticos de gobierno. En el verano de 1998, un grupo denominado "Electronic Disturbance Theater (EDT)" organizó una serie de "ataques electrónicos" en contra de sitios Web del presidente Ernesto Zedillo, y del presidente Bill Clinton (Pentágono y Casa Blanca), la Embajada Mexicana en Reino Unido, entre otros. El propósito era demostrar solidaridad con los Zapatistas Mexicanos.

El 15 de junio de 1999, el EDT empezó a enviar anuncios a través de Internet incitando a miles de personas a que se uniera en un acto de Desobediencia Civil Electrónica para detener la guerra en Chiapas, México. Brett Stalbaum, uno de los líderes de EDT creó un programa de software llamado "The Zapatista FloodNet" para facilitar los ataques. El 18 de junio 18,615 personas en 46 distintos países, apoyaron desde sus computadoras el ataque masivo ("mítin virtual") contra estos sitios de gobierno de México y Estados Unidos principalmente. Ricardo Domínguez, neoyorquino de padres mexicano, es uno de los principales protagonistas del EDT. Domínguez, junto con miles de manifestantes y el EDT ha dirigido muchos ataques y mítines virtuales contra diferentes organismos y figuras de gobierno. Según importantes fuentes de USA, él es uno de los primeros ciberterroristas del planeta. La relevancia de este hecho hizo que una nota periodística de la Agencia Reuters acreditara el nacimiento del término "Hacktivismo" a los Zapatistas.

Volviendo al tema del ataque terrorista del 11 de Septiembre a Estados Unidos, es interesante el hecho de que varios grupos de hackers se pronunciaron en contra del terrorismo. Kim Schmitz, hombre de negocios Alemán, ex-hacker, ofreció primero una recompensa de $10 millones de dólares a cualquiera que ofreciera información que ayudara a la captura de Bin Laden. Posteriormente un grupo de hackers fundado por Schmitz denominado "Young Intelligent Hackers Against Terror" (pronunciado "YIHAT", muy similar al término Jihad, que en Árabe significa "Guerra Santa"), penetraron en computadoras del AlShamal Islamic Bank en Sudan y recolectaron información de las cuentas de la organización terrorista Al-Queda y de su líder, Osama Bin Laden, la cual fue entregada al FBI.

Por otra parte, el 17 de diciembre pasado se dio a conocer en las noticias que un miembro sospechoso de pertenecer a la red terrorista Al Qaeda, afirmó que militantes Islámicos se infiltraron (consiguieron trabajo) en Microsoft, y sabotearon el nuevo programa "Windows XP". No se sabe con qué propósito lo hicieron, pero para cuando Microsoft lanzó al mercado el XP no se detectó código maligno alguno en el programa.

En fin, estos hechos que parecen ser aislados, y de los cuales no solemos enterarnos en México, deben de tomarse muy en serio por nuestras autoridades. También nosotros debemos tomar conciencia de lo importante que es la cultura de la seguridad informática. La tecnología ha traído tantos beneficios al hombre, como problemas y dolores de cabeza. Es indispensable encontrar un sano equilibrio para vivir mejor.

** Joel A. Gómez Treviño*
es presidente de la AMDI
joelgomez@mail.amdi.org.mx

BUSINESS NORTH MEXICO
Del 11 al 17 de junio, 2001

EL EXPERTO

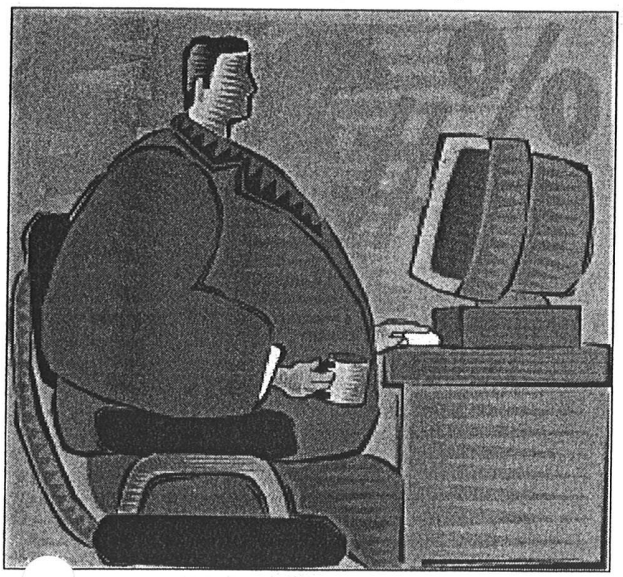
DISEÑE LEGALMENTE SU SITIO

(PRIMERA PARTE)

Joel Gómez Treviño *

La creciente expansión del Internet y las tendencias hacia los negocios electrónicos han propiciado la proliferación de toda clase de sitios Web: de entretenimiento, de información, educativos, gubernamentales, corporativos, marketplaces, portales, subastas, directorios o simples tiendas virtuales. Lo que resulta una verdad incontrovertible es que todo el mundo quiere tener un espacio propio en la Red, desde niños y estudiantes, hasta instituciones gubernamentales y grandes corporativos de empresas.

Cuando un individuo o entidad desea entrar al Internet, probablemente lo primero que hará será buscar y/o contratar un diseñador de páginas Web, o bien una agencia de diseño profesional. Posteriormente decidirá el contenido y el diseño de su página o portal, y finalmente arrancará el proyecto electrónico. Sin embargo, pocas veces, por no decir casi nunca, ni el dueño del sitio, ni el desarrollador del mismo, se ponen a pensar en las consecuencias o implicaciones legales que puede traer el tener una página en internet, o más allá todavía, realizar transacciones electrónicas.



Cuando el dueño o desarrollador si tienen algo de conciencia jurídica, es decir, cuando saben que el sitio debe tener documentos legales, usualmente los buscan en otros sitios, regularmente en inglés, para copiarlos y traducirlos, bajo la creencia de que esto es suficiente para incluirlos en su página Web. La realidad es que esta práctica, lejos de ayudar, perjudica a quienes la adoptan. El derecho y las leyes de cada país son distintos, sobre todo tratándose de México y Estados Unidos, ya que ambos tienen tradiciones (sistemas) jurídicos muy distintos: el romano-germánico y el common law.

Normalmente, los documentos que un sitio que realiza transacciones comerciales necesita son aviso legal (disclaimer), políticas (términos y condiciones) de uso, y las políticas de privacidad y manejo de la información. Debido a lo amplio de cada uno de estos temas, a continuación sólo trataré de realizar una síntesis de los conceptos y contenidos más importantes de los Términos y Condiciones de Uso de un sitio. En una segunda parte, hablaré sobre los otros documentos.

Definiciones. Es importante que al inicio del documento se presente al visitante definiciones que aunque parezcan muy básicas, ayudan a dar una mejor comprensión tanto de los términos que se usarán en el documento y sito web, como del negocio en sí mismo. Es útil definir: a) cuál es o en qué consiste el negocio o portal visitado; b) si existen distintas categorías de usuario o tipo de servicio que se presta; c) qué tipo de transacciones se pueden realizar (compras, ventas, subastas), etc.

Declaraciones del Usuario. El usuario debe reconocer que tiene plena capacidad jurídica y aptitud comercial para negociar, contratar y obligarse en los términos que su relación comercial con otros usuarios (si es un sitio C2C por ejemplo) o con su empresa así lo amerite. También podría ser útlil, como medida informativa meramente, informarle al usuario que conforme a las reformas publicadas en el Diario Oficial de la Federación el 29 de Mayo de 2000, es perfectamente válido contratar electrónicamente.

Aptitud Comercial y Capacidad Jurídica. Como contraparte a lo anterior, es indispensable aclarar que los servicios del sitio Web están dirigidos sólo a personas legalmente capaces para contratar. Si la naturaleza de los bienes o servicios que se venden o promocionan en el sitio requiere de algún requisito adicional (ser adulto por ejemplo), también hay que dejarlo claro.

Registro y Cuenta de Usuario. Hay que especificar cuál es el proceso, si existe, de registro del sitio, así como la conducta que el usuario debe observar respecto a su cuenta y clave de entrada (no compartir información, sólo un usuario por cuenta, derecho del sitio Web de verificar la veracidad de los datos, etc.)

Alcances y Limitaciones. En este punto es vital establecer los lineamientos que delimitan la responsabilidad de la empresa. Aquí debe quedar claro qué cosas, y cuáles no, garantiza el sitio: productos, servicios, promociones, fallas técnicas del servicio o conexión a Internet, etc. Si la empresa es responsable por algún daño que sufra el usuario o consumidor, también debe estipularse.

Responsabilidades de los Usuarios. Esta cláusula puede ser bastante amplia, pero un punto de particular importancia es especificar que el usuario debe adoptar las reglas de conducta o uso del sitio, y deberá ser responsable en caso de afectar o violar derechos de terceros (derechos de autor, de privacidad, de confidencialidad, reputación, etc.)

Cuotas y Cargos. Cualquier pago o cuota que el usuario deba pagar debe quedar definida en este documento, para evitar posteriores confusiones o malos entendidos.

Propiedad Intelectual. Establecer que todos los derechos de autor y de propiedad intelectual (patentes, marcas, etc.) del sitio Web son en todo tiempo propiedad de la empresa, y que el usuario será responsable de cualquier violación a éstos.

Aceptación, Modificaciones y No Renuncia de los Términos y Condiciones. Los términos de este documento pueden ser modificados eventualmente por la empresa, por lo que el usuario deberá tener la obligación de visitarlos o leerlos con frecuencia para estar enterado de cualquier cambio, o bien la empresa como una cortesía, mas no como obligación, puede enviarles un correo electrónico a los usuarios registrados cada vez que esto suceda para notificarles las modificaciones.

Por último, debo aclarar que lo aquí expresado tiene propósitos meramente informativos, por lo que no constituye de ninguna manera una asesoría legal. Cada sitio Web tiene características y peculiaridades propias, las cuales deben ser revisadas por un abogado para determinar el alcance y contenido de este y otros documentos similares.

** Joel Alejandro Gómez Treviño es presidente de la Academia Mexicana de Derecho Informático (AMDI). (joelgomez@mail.amdi.org.mx)*

BUSINESS NORTH MEXICO
el 9 al 15 de julio, 2001

EL EXPERTO

DISEÑE LEGALMENTE SU SITIO

(SEGUNDA PARTE)

Joel Gómez Treviño

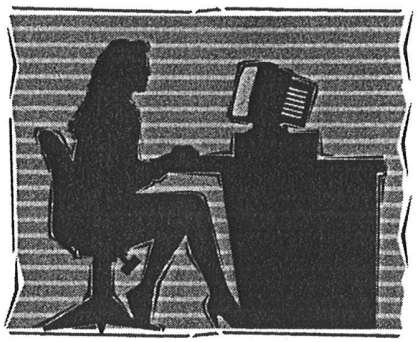
En el artículo anterior vimos cuáles son los puntos más importantes que debe contener los "Términos y Condiciones de Uso" de un sitio Web. En esta ocasión trataremos el tema de "Políticas de Privacidad" para conocer la información que tanto la empresa como el usuario deben tener en mente al diseñar o navegar por un sitio Web.

Para ubicarnos un poco en el contexto de privacidad, es importante conocer que en muchos países del mundo, en donde el comercio electrónico y el Internet están ya en una etapa madura de desarrollo, la mayoría de los grandes portales y sitios que tienen miles y tal vez millones de usuarios registrados, venden a otras empresas las bases de datos que contienen información personal de dichos usuarios.

También aplica para el caso de simples visitantes, en donde mediante el uso de cierta tecnología es posible monitorear los hábitos de consumo, gustos y navegación de los mismos. Estas bases de datos pueden llegar a valer mucho dinero, en función de la cantidad de personas registradas, así como de la calidad y estructura de la información.

El comercio o tráfico de bases de datos genera, en buena medida, la práctica conocida como "spamming" o "correo basura", ya que gracias a que nuestra información personal es compartida con otras empresas, recibimos a diario decenas de e-mails con ofertas y promociones de terceros desconocidos.

Esta situación ha generado descontento y malestar en miles de personas alrededor del mundo, por lo que se han formado organizaciones que buscan proteger al consumidor, e inclusive el gobierno ha creado mecanismos o leyes que limiten o prohíban el uso indiscriminado de información personal o bases de datos.



Es conveniente iniciar la redacción de las Políticas de Privacidad de un sitio Web aclarándole al usuario que la empresa está comprometida a la protección de la privacidad (datos personales) de sus usuarios. El propósito principal de estas políticas debe ser el informarle al usuario o visitante: (I) la clase de información que es posible obtener de él, (II) el uso que el sitio Web podría darle a esa información, (III) los casos en que la empresa divulgará la información a terceros, y lo más importante, (IV) darle al usuario el derecho, si así se desea, de negarse a que revelemos su información a terceros, (V) así como a corregir la misma en caso de error.

¿Cómo se puede obtener información de los usuarios o visitantes? Lo primero que tal vez se nos venga a la mente al leer esta pregunta, son los clásicos cuestionarios que tenemos que llenar para obtener un servicio, gratuito regularmente, tal como correo electrónico, suscripción a servicios de noticias, acceso a publicaciones periódicas, etc.

Las empresas requieren datos que van desde lo básico (nombre, e-mail, edad, sexo, código postal, país), hasta información más personal o detallada (la empresa en que trabajamos, nuestros intereses personales e inclusive el rango de ingresos o sueldo que percibimos).

Sin embargo, la recolección de datos no se limita al cuestionario inicial que llenamos cuando nos inscribimos en algún sitio Web. Hay otras maneras de obtener más información sobre los usuarios. Por ejemplo, una vez que el usuario completa los datos requeridos, se le genera usualmente una "identificación" (nombre de usuario y clave de acceso) para cuando vuelva a entrar al portal. Sus visitas posteriores podrán generarnos datos adicionales, ya que es posible monitorear los banners (publicidad) que el usuario selecciona, así como las compras y gustos de los visitantes, entre otras cosas.

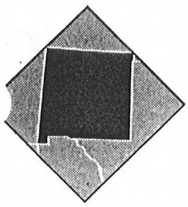
¿Para qué nos sirve dicha información? La información básica obtenida en los cuestionarios de registro ayuda a generar simplemente estadísticas sobre el tipo de usuarios, y la personal o detallada se usa para generar perfiles completos sobre gustos y hábitos de los consumidores o visitantes. Cada vez que la persona acceda a la página electrónica, el sistema podrá reconocer quién es, cuándo fue la última vez que nos visitó, qué artículos ha comprado, qué información suele buscar, qué páginas le gusta navegar, etc. Para lograr esto, en muchas ocasiones las empresas se apoyan en el uso de la tecnología denominada "cookies", que son básicamente pequeños archivos que los sitios instalan en nuestras propias computadoras para poder reconocernos cuando volvamos a visitar el sitio, sin necesidad inclusive de teclear una clave de entrada.

Políticas de Privacidad y Manejo de la Información. Para generar confianza y lealtad a nuestras marcas o portales, es importante ser honesto y transparente con nuestros clientes y usuarios. Hay que revelarles la manera en que obtenemos información de él, para qué la queremos y si la vamos o no a compartir con terceros. También debe declararse que la información proporcionada se mantendrá confidencial. Por ley: (I) hay que respetar la decisión del usuario de no recibir propaganda comercial, (II) debe obtenerse su consentimiento previo para que terceras personas puedan acceder a su información personal contenida en bases de datos, así como para publicar, reproducir, divulgar, comunicar o transmitir dicha información, y (III) debe informarse al consumidor los mecanismos de seguridad que el proveedor (sitio Web) tiene para proteger la información que el usuario proporciona para realizar una transacción electrónica.

Desafortunadamente México está muy lejos de otros países que han desarrollado leyes especiales para proteger la información personal y la privacidad de los usuarios. Sin embargo, la Ley Federal de Protección al Consumidor y la Ley Federal del Derecho de Autor contienen disposiciones para proteger la información, privacidad y seguridad de las personas.

Al igual que el artículo anterior, debo aclarar, que lo aquí expresado tiene propósitos meramente informativos, por lo que no constituye de ninguna manera una asesoría legal. Cada sitio Web tiene características y peculiaridades propias, las cuales deben ser revisadas por un abogado para determinar el alcance y contenido de este y otros documentos similares.

Joel Alejandro Gómez Treviño es presidente de la AMDI. (joelgomez@mail.amdi.org.mx)



NUEVO MEXICO

Combinan acciones Hyaton y Solar Energy

ALBUQUERQUE.- **Hyaton**, que muy pronto adoptará la identidad comercial de **Sun Power Corporation**, anunció la ejecución de acuerdos de intercambio de acciones con **Solar Energy Limited** (SLRE), una empresa pública listada en OTC BB, y tres de sus subsidiarias. Según las condiciones del convenio, la corporación adquirirá el 100% de las acciones de dos compañías privadas, **Sunspring Inc.** y **Renewable Energy Corporation** (RECO). Al cierre de las transacciones de intercambio, Hyaton emitirá 2 millones de acciones comunes y 8 millones de acciones preferenciales para Sunspring y RECO cada uno.

Reportan dividendos accionarios

ALAMOGORDO.- **R. Miles Edgerwood**, presidente y director ejecutivo de Alamogordo Financial Corp., anunció la declaración de un dividendo de 15 centavos por acción de su capital accionario para el trimestre fiscal que terminó el 30 de septiembre. El dividendo será pagadero a los accionistas registrados el 1 de [illegible]bre y será cubierto el 9 de [illegible]. Alamogordo Financial es matriz [illegible] Alamogordo Federal Savings and Loan Association, cuyos depósitos están asegurados por **Federal Deposit Insurance Corp.**

Anuncia Chino Mines despidos

SILVER CITY.- **Chino Mines** anunció el cierre por un período indefinido de su fundidora y mina de Grant County, medida que costará el empleo a 650 trabajadores. **Phelps Dodge** informó que los despidos concluirán el 15 de enero, para dejar una fuerza laboral de 200 personas. Chino Mines, una sociedad entre Phelps Dodge y **Heinsei Minerals**, cerrará temporalmente su fundidora de Hurley y sus operaciones mineras en Santa Rita. Las operaciones de Phelps Dodge en Tyrone no se verán afectadas. Los recortes de fuerza laboral en Nuevo México y Arizona resultarán en una pérdida total de 1,440 puestos de trabajo.

Se oponen a construcción de mina

SANTA FE.- Ante las protestas del pueblo Zuni y oposición de la comunidad ambiental, el Departamento del Interior aparentemente se retractó de su plan para la aprobación de una enorme mina de carbón en el occidente de Nuevo México. La compañía **Salt River Project**, de Arizona, compra la construcción de una mina de 4,000 acres para abastecer de energía a Phoenix. El Pueblo Zuni y las tribus de la zona se oponen a la construcción de la mina alegando que

EL EXPERTO

El caso Microsoft

Joel A. Gómez Treviño

Buen alboroto se ha armado sobre todos los juicios en contra de **Microsoft** (MS) que han iniciado diversas entidades de Gobierno de los Estados Unidos.

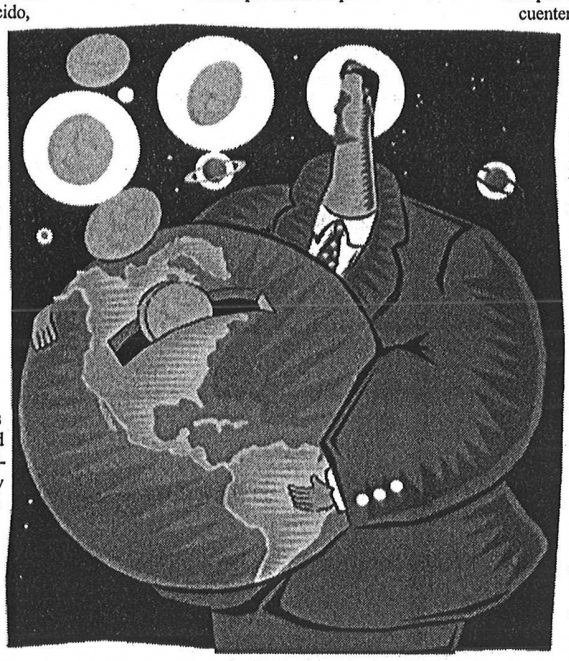
El argumento principal contra este gigante son las prácticas monopólicas ejercidas por la empresa para incorporar a su sistema operativo Windows el programa de Internet Explorer, desplazando así de manera tajante a sus más cercanos competidores como Netscape.

En el juicio contra Microsoft se presentaron diversas pruebas en su contra, algunas de ellas eran cartas o correos electrónicos en donde MS casi "amenazaba" a los grandes fabricantes de equipos de cómputo que si no incluían el Internet Explorer en sus máquinas, les revocaría la licencia para incluir Windows como sistema operativo preestablecido, palabras más, palabras menos. Esto desde luego, traería graves consecuencias para la industria de hardware, pues de poco te serviría comprar una máquina sin el "único" programa standard en el mercado.

No es extraño para nadie que el explosivo crecimiento de MS lo ha convertido en un macro monopolio de la industria del software. Casi es imposible concebir una máquina sin Windows, sin Word, sin Excel, sin Outlook, sin Internet Explorer, etc. Algunos pensarán en Macintosh, pero no vale la pena la comparación... el porcentaje de penetración de la Mac es minúsculo contra las "PC's", y de hecho MS ya también fabrica programas para la Mac. Es un hecho, hoy en día, nadie puede competir contra este gigante de la industria de software.

¿Qué otras consecuencias perjudiciales trae este mercado monopólico? ¿Se ha usted puesto a pensar cuántas veces o qué tan seguido tiene que actualizar su sistema operativo y otros programas de software de MS? Windows 95, Windows 98 (dos versiones), Windows 2000 (tres versiones), Windows Millenium, Windows XP (dos versiones), etc. y no le sigo con la lista de las versiones de office y de internet explorer sólo para no fastidiarlo. Cada actualización cuesta entre $2,500 y $3,500 pesos aproximadmente. "Ah, pues no lo actualizo y listo" dirán algunos... pero no es tan sencillo, si no actualiza el software probablemente en un corto tiempo se quedará obsoleto, porque no podrá intercambiar documentos de negocios con sus socios, proveedores, clientes, distribuidores y demás usuarios que sí actualizaron los famosos programitas.

En buena medida, estas prácticas monopólicas han propiciado la piratería del software en México, ya que los precios son tan inaccesibles para muchos, que no dudan en comprar un CD pirata. La industria de computadoras y periféricos (hardware) se ha distinguido en los últimos años por ir a la baja en sus precios. Las computadoras, las impresoras, la memoria RAM, los quemadores, los escáners, etc. son cada día más baratos. Sin embargo, la industria del software es la única que crece en precio constantemente. ¿Por qué? Simple, siendo sólo una empresa (prácticamente) la que tiene el control total la industria, MS tiene libertad total de fijar unilateralmente los precios, no hay competencia.



Si esto le parece poco, pues aún no termino. ¿Alguna vez ha escuchado el término "patch"? Los patchs son archivos que genera MS y pone a disposición del público para ser copiados y ejecutados en sus máquinas. El objetivo principal de estos programas es corregir una enormidad de fallas y defectos que tienen los programas de software de MS. Le invito a que visite la página de Internet de Microsoft para que se entere, tal vez por primera vez, el montón de patchs que usted debe bajar de Internet (lo cual le puede tomar horas, y tal vez hasta días) para tener funcionando sus programas de manera adecuada. Dicho de otra manera, pagamos miles de pesos a MS por comprar programas defectuosos, que frecuentemente nos causan problemas en nuestras máquinas, que se traducen en pérdida de tiempo y de dinero. Supongo que a Microsoft lo único que le interesa es sacar lo más pronto posible al mercado nuevos productos, aunque no estén completamente probados y libres de defectos, con tal de seguir recibiendo jugosos ingresos.

Ya para rematar, digo, terminar, pues le comento que los servidores de Internet de MS, denominados IIS (Internet Information Service) son los favoritos de los hackers y los más vulnerables a virus. No en vano hace unas semanas, una enorme empresa de consultoría (Gartner) hizo un anuncio público en donde recomendaba a sus clientes no seguir usando plataformas de MS, debido a los grandes problemas de seguridad que tenían sus programas y servidores.

Ahora sí no sé cuál sea la moraleja del artículo, pero sí le voy a dejar una frase para reflexionar ¿los beneficios de usar MS son mayores a los perjuicios?.

Me despido, tengo que cerrar mi Word, el Office y el Windows antes de salir de la oficina... si, yo también uso Microsoft, ¡no me queda de otra!

Joel A. Gómez Treviño es presidente de la Academia Mexicana de Derecho Informático,A.C. (joelgomez@mail.amdi.org.mx)

CALIFORNIA

Globalstar estrangulado

SAN DIEGO.- La compañía de telefonía móvil vía satellite, **Globalstar**, informó que había registrado una pérdida neta de $3.8 mil millones de dólares durante el año pasado y podría buscar la protección del capítulo de bancarrota si no es capaz de realizar un severo plan de reestructuración. Globalstar fue fundado en 1991 por la firma satelital **Loral Space & Communications** y **Qualcomm**. Loral es propiedad del 38% de la compañía y Qualcomm tiene ahora menos del 6%.

En quiebra el conocimiento

SAN DIEGO.- Store of Knowledge, la cual opera tres tiendas en este condado en afiliación con **KPBS-TV**, recurrió a la protección del capítulo 11 de la ley de Bancarrotas bankruptcy protection y anunció que cerrará sus 91 locales de su red a nivel nacional. KPBS informó que no habrá recuperación alguna en la compañía de productos educacionales, aunque se recibirá algún dinero por concepto de permitir el uso de logo y marca en algunos locales. Durante su socieadad a lo largo de seis años con Store of Knowledge, la estación pública de televisión estimó que había aportado cerca de $300,000 dólares.

[illegible]ca de 30 empleados de Store of [illegible]ledge en San Diego serán liquida[illegible] en el transcurso de los próximos tres meses.

On-Point pone demanda

SAN MARCOS.- On-Point Technology Systems anunció que ha interpuesto una demanda por daños y perjuicios debido a la fallida compra de de la división de lotería a GTech Corp, de Rhode Island. La compañía ubicada en San Marcos iba a pagar $50,000 dólares en efectivo y 316,667 acciones como parte del acuerdo, el cual se ubicó en un monto total de un millón de dólares. Sin embargo, de acuerdo al precio de acciones de hoy, el trato se ubicaría en $445,800 dólares, lo que provocó el retiro de la oferta, con la consecuente demanda de On-Point para que se cumpla el trato original.

Despide Miva a trabajadores

SAN DIEGO.- Miva Corp, una compañía de esta ciudad que produce software para e-commerce, despidió a 21 trabajadores la semana pasada como consecuencia de las últimas bajas ventas registradas en el sector de tecnología. El corte laboral incluyó a miembros del consejo de directores. El director de la

EL EXPERTO

El fin de lo gratuito...

Joel Alejandro Gómez Treviño*

Desde hace un par de meses ha causado tremendo revuelo el caso de Napster en los tribunales estadounidenses. Napster es una empresa punto com creada en California, Estados Unidos en el mes de mayo de 1999.

Ellos se auto denominan como "la comunidad en línea más grande y diversa de amantes de música en la historia" y como "la comunidad para *compartir* archivos líder en el mundo". La aplicación de software de Napster permite a millones de usuarios en todo el mundo localizar y *compartir* archivos de música de manera sencilla y conveniente.

Pero… ¿cuál es el problema con esta empresa? Pues precisamente lo que he venido resaltando desde el inicio de este artículo: el simple hecho de *¡compartir*! Hace poco escuché a un conferencista decir: "¿Si yo comparto algo con mi vecino es ilegal? ¡Claro que no! nunca lo ha sido, entonces, porqué arman tanto alboroto con esto de Napster?" La situación no es así de simple como parece, ya que las bondades aparentes del vocablo *compartir*, en este caso en particular, transgreden los denominados Derechos de Autor.

Sin ánimo de entrar en una discusión meramente teórica, sino más bien con la intención de adentrarnos un poco en los conceptos de derechos de autor, me permito parafrasear al Jurista Mexicano Fernando Serrano, quien afirma que las normas del derecho de autor nunca han sido normas mercantiles ni económicas. Su finalidad ha sido siempre de mucha mayor trascendencia, son normas jurídicas destinadas a *dignificar la labor del creador de las obras, de modo que a través de su respeto y su remuneración puedan generar un ambiente apto para tales creaciones*. Dicho de otra manera, uno de los objetivos principales de las leyes sobre derechos de autor, es el proteger a los autores para fomentar la creatividad .

Para ilustrar o convertir estos conceptos de la doctrina a la realidad, hagámonos la siguiente pregunta: si millones de personas en la red pueden *compartir* las canciones y la música que los artistas y compositores realizan, sin pagar un sólo centavo por ello ¿cuál es el incentivo de los artistas para seguir creando, para seguir componiendo, para seguir cantando o tocando música? La respuesta es sencilla: ¡ninguno!

No sé ustedes, pero si yo fuera cantante, compositor o empresario de dicha industria, y supiera de antemano que mis creaciones van a ser libremente copiadas, alteradas y distribuidas a millones de personas, definitivamente cambiaba de oficio.

Volviendo al tema de Napster, según una sentencia dictada el 12 de febrero del año en curso por un panel de 3 jueces de la Corte Federal de Apelaciones de los Estados Unidos, esta empresa que permite a l usuarios grabar música de la red sin pagar derechos autor, no podrá comercializar dicho material y debe vigilar su sistema, bajo pena de multa. Esta Corte me cionó que la posibilidad de descargar música gratuit mente a través de Napster *perjudica necesariamente l intentos de los titulares del derecho de autor de cobr por tales descargas*.

Conscientes de que esta medida podría obligarlos clausurar el servicio, Napster está intentando moviliz a sus usuarios, pidiéndoles que envíen correos electr nicos al Congreso de los Estados Unidos para que és apoye a Napster, así como *bombardear* a las empres disqueras con correos para que cambien su actitud.

Las empresas disqueras y las grandes asociacion que representan los intereses de la industria musical discográfica en varias partes del mundo, aplaudieron decisión de la Corte, y exigieron a Napster que si verdad quieren que su negocio sea legítimo, que dete ga las violaciones y las tácticas dilatorias en la Corte.

La Asociación Americana de Empresas Disquer preguntó a Napster si apoyaría la ejecución y el cumpl miento a las leyes de derechos de autor contra otros tios en Internet que ofrecen el copiado gratuito de arch vos. Pero la industria disquera no se ha conformado c esta demanda contra Napster, sino que han tomado gunas medidas drásticas en su contra.

Napster llegó a tal grado de desesperación o ac rralamiento, que ofreció un billón de dólares a principales casas disqueras independientes, con la e peranza de que ellos se desistan de la demanda p violaciones a derechos de autor que amenaza con ac bar el servicio gratuito de compartición de cancion por Internet.

La controvertida empresa también afirmó que ot de las medidas que tomará a partir del próximo veran será la de cobrar una cuota mensual.

La moraleja de esta triste historia, tanto para los er presarios como para los usuarios de Internet la podem plasmar con las siguientes reflexiones:

1.- La era del Internet gratuito está por extingu se; los proveedores de acceso a Internet gratuitos e tán quebrando todos los días, los proveedores de n ticias e información ya están cobrando las suscripci nes, los emails gratuitos cada vez tienen menos fu ciones para buscar que el usuario contrate servici *premium*, etc.

2.- El Internet ha venido a revolucionar no sólo comunicaciones, sino también la educación y la mar ra de hacer negocios. Sin embargo, hay que tener p sente que nada es gratis en esta vida, todos los servici siempre tienen un costo que de alguna manera se tra fiere al consumidor final .

3.- Tanto en el mundo real como en el mundo v tual, todos los individuos somos libres, pero recor mos que la libertad es relativa, porque ésta termina d de se vulneran los derechos de otros. Aprendamos a vir en esta gran comunidad mundial que es el Intern Aprendamos a compartir, pero respetando el trab ajeno, respetando los derechos de autor, para que ot también respeten nuestros derechos.

** Joel Alejandro Gómez Trevi*
joelgomez@mail.umdi.org

TAMAULIPAS

No se ejercieron $70,000 mdp

TAMPICO.- Cerca de $70,000 millones de pesos para obra pública no se ejercieron en la entidad como consecuencia de algunas denominadas lagunas que presentaba la Ley de Obras Públicas y Servicios, que a su vez provocaron problemas de interpretación de la normatividad que terminaron por frenar los procesos de licitación de los proyectos de infraestructura contemplados para el estado de Tamaulipas. La Cámara Mexicana de la Industria de la Construcción pugnará para que se apliquen los recursos federales.

Propondrían Ley para imporar ropa usada

REYNOSA.-El dirigente de la **Asociación de Tianguistas de Tamaulipas**, Marcelo Chong Delgado, sugirió legalizar la importación de ropa usada, con el propósito de erradicar la incertidumbre por los operativos de decomiso [illegible] los impuestos correspondientes. La asociación que encabeza planea una próxima reunión con legisladores federales de Tamaulipas a fin de proponerles la creación de una ley que permita importar dicho producto de EU.

Comercio exterior a la alza en NL

NUEVO LAREDO.- La Aduana de esta ciudad fronteriza informó que a pesar de los acontecimientos del pasado 11 de septiembre en Estados Unidos, el movimiento de exportaciones e importaciones no decreció, y por el contrario, hasta se registró un incremento, comparativamente con el año 2000. El movimiento de importaciones durante el 2001 ascendió a 960,704 movimientos, un incremento del 5.01% comparado con los 914,891 que se realizaron en el 2000. Los únicos meses en que se registró una baja fue en agosto, septiembre y noviembre.

Atemorizan delincuentes

NUEVO LAREDO.- **La Asociación de Joyeros** de esta ciudad está decidida a proteger su patrimonio, que en lo que va del mes se ha visto severamente dañado, ante los constantes asaltos a sus negocios. El más reciente lo sufrió la joyería **"Big Ben"**, que se unió a la lista de los 9 atracos, en su mayoría perpetrados con lujo de violencia. Aldo [illegible]zar Ramírez, presidente de la agrupación, advirtió que exigirán a las autoridades policiacas poner fin a esta ola de delincuencia.

EL EXPERTO

E-mail e Internet en el trabajo: ¿Permitirlo o Prohibirlo?

Joel A. Gómez Treviño

Si pudiéramos definir a una empresa tradicional, por no decir obsoleta, en términos de tecnología y comunicación, hablaríamos de un local que cuenta con teléfono, fax (o telex inclusive), máquina de escribir, y para comunicarse utilizan el correo postal y servicios de mensajería privada. En cambio, una empresa moderna, además de lo anterior, sin duda utiliza correo electrónico, una intranet/extranet, Internet, líneas dedicadas (ISDN), videoconferencias, comunicaciones satelitales y sus ejecutivos cuentan con tecnología de punta (palms, laptops, celulares, bipers, etc.)

Sabemos que algunos de los principales factores para que una empresa sea exitosa y competitiva son: (a) excelente comunicación, tanto interna (empleados, gerentes, directivos) como externa (clientes, proveedores, distribuidores); (b) uso eficiente de recursos (humanos y materiales); y finalmente (c) un ambiente de trabajo positivo que motive a los empleados a rendir el máximo en sus labores cotidianas.

Sin duda las ventajas del uso del correo electrónico en el trabajo son muchas. La comunicación interna se vuelve ágil y efectiva, directa al destinatario final, reduce tiempos de respuesta y ahorra costos de papel e impresión. También facilita la comunicación externa con clientes y proveedores, la colocación de pedidos y órdenes de compra y la retroalimentación directa con el consumidor. Podría seguir hablando de las ventajas del email, del internet y de las nuevas tecnologías, pero creo que todos las conocemos, así que pasemos al tema central del artículo.

Pensemos en una situación hipotética. Usted, empresario responsable, propietario o directivo de una empresa moderna, ha decidido realizar una Auditoria Informática en su empresa. Los auditores, después de revisar todas las computadoras, periféricos y demás equipo informático que se encuentra en sus instalaciones, encontraron los siguientes problemas críticos:

(a) material pornográfico en discos duros; (b) páginas electrónicas con contenido sexual marcadas como "favoritos" (bookmarks), o visitadas recientemente, según se detectó en el historial de navegación de varias PC's; (c) archivos no legibles, encriptados con software que no es de la empresa; (d) mediante correos electrónicos, un empleado acosaba sexualmente de manera continua a varias empleadas; (e) considerables recursos de la empresa fueron utilizados con propósitos personales, de esparcimiento o ajenos al negocio; (f) desarrollo de programas de software que no pertenecen a la empresa; (g) cantidades significativas de programas de software sin la licencia correspondiente ("piratas"); (h) muchos programas de software fueron descargados (copiados) del Internet; (i) varios empleados enviaron correos electrónicos, usando las cuentas de la empresa y firmando con el nombre de la misma, que contenían material pornográfico, propaganda política, mensajes subversivos, etc.

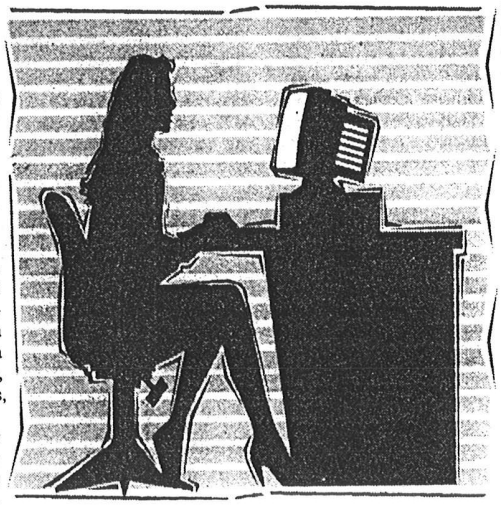
Estos son sólo algunos de los muchos y diversos hallazgos que se pueden encontrar en una Auditoria Informática. Los problemas derivados de estas situaciones pueden afectarle tanto externa como internamente: se compromete la integridad de los sistemas informáticos de la empresa por virus y otros tipos de acceso no autorizados (caballos de troya, back orifice, etc.), mala imagen ante la sociedad o clientes por e-mails con contenidos inapropiados, personal gastando tiempo y recursos de la empresa al navegar por Internet con fines personales, secretos industriales o información confidencial puede circular libremente y salir de la empresa con facilidad, responsabilidad jurídica por tener software pirata, demandas por difamación u hostigamiento (acoso sexual), etc.

Usted ha recibido un reporte detallado con los problemas críticos ante citados. Ahora, ¿qué va a hacer?, ¿cuál es su reacción?, ¿qué ideas le cruzan por su mente? "Voy a cortar el Internet, voy a quitarles el e-mail externo a los empleados, voy a colocar cámaras de video detrás de cada empleado para ver lo que hace, voy a monitorear los correos electrónicos que entren y salgan de la empresa, voy a despedir a quien sorprenda usando Internet en horas de trabajo".

Cuidado, estos son terrenos escabrosos, y si usted decide tomar cualquiera de estas acciones podría traer problemas no deseados, tanto jurídicos como de ambiente laboral: molestias entre los empleados, clima de inseguridad e incertidumbre laboral, violaciones a la privacidad e intimidad de sus empleados, problemas laborales (despidos "injustificados"), etc.

Vamos a suponer que usted decida monitorear el uso de recursos informáticos y de comunicación de su empresa. Actualmente se puede monitorear casi todo: llamadas telefónicas internas y externas, correo de voz, correos electrónicos, computadoras (discos duros, pantallas, espacio en red, archivos eliminados que se quedan en memoria de respaldo), navegación en Internet (history, cookies, archivos temporales), personas que entran a la empresa e inclusive a ciertas áreas (tarjetas de acceso), cámaras de video, micrófonos, etc.

Esta decisión generaría interesantes consecuencias. Primero, usted necesitará dedicar recursos económicos y humanos para realizar estas labores, que quizás no estén contemplados en su presupuesto operativo o planeación de recursos humanos. Segundo, generará molestias en sus empleados, pues se sentirán invadidos en su privacidad y vigilados como si fueran delincuentes. Tercero, aunque hasta la fecha la legislación mexicana es muy vaga al respecto, ya existen muchos casos internacionales en que patrones han despedido empleados por uso no autorizado de e-mails o Internet, y posteriormente el empleado demanda por despido injustificado. Hace algunos meses, un tribunal francés determinó que era ilegal que un patrón monitoreara los correos electrónicos de los empleados, aunque así lo estableciera en sus políticas o en sus contratos laborales. Tarde que temprano, México tendrá que legislar al respecto y podría verse influido por las tendencias internacionales.



Por otra parte, si decide simplemente cerrar todos los accesos a Internet, correo electrónico, etc., pues usted estaría encerrando a la empresa en una caja de cristal que dificilmente le permitirá competir con empresas vanguardistas, con tecnología de punta y sobre todo con una comunicación eficiente y ágil.

¿Qué hacer entonces? Las soluciones eclécticas a veces son las más útiles, ya que buscan tomar lo mejor de varias alternativas. En otras palabras, encontrar el equilibrio siempre es importante. Mis recomendaciones son las siguientes: 1. *Lo primero es iniciar una campaña de concientización y cultura del* uso de recursos informáticos de la empresa. Propicie el ambiente de "libertad con responsabilidad". Deles a los empleados que lo necesiten, acceso a Internet y correo electrónico, pero haga hincapié en su uso responsable para poder seguir aprovechando estas ventajas. 2. Elabore una "Política de Uso y Acceso a Sistemas Informáticos" para que pueda determinar con detalle cómo quiere que se utilicen sus recursos. Esta Política debe incluir: el uso de computadoras, dispositivos portátiles de almacenamiento (diskettes, zips, CD's), correo electrónico e Internet; acciones de monitoreo, si existen; medidas disciplinarias en caso de violación y procedimientos de despidos en casos extremos. Luego informe a sus empleados de esta política, entrégueles una copia y de ser posible, hágales firmar un breve documento en el que afirmen conocerla y se comprometan a cumplirla. 3. Realice de manera anual o semestral auditorias informáticas, con el fin de detectar usos inapropiados o acciones que no se apeguen a su Política. 4. Si mediante estas auditorias o revisiones periódicas usted detecta irregularidades, podría optar por iniciar actividades de monitoreo más formales, tratando siempre de respetar la intimidad del usuario e informarle a los empleados que están siendo monitoreados de manera aleatoria. 5. También es recomendable redactar y planear políticas de seguridad informática, así como de uso y acceso a información confidencial de la empresa.

En la elaboración y redacción de estas políticas, siempre es indispensable que gerentes o directivos de las siguientes áreas participen: recursos humanos, sistemas y jurídico. Recuerde que es sumamente conveniente que en su empresa fomente y arraigue el principio de "libertad con responsabilidad" entre sus empleados. Eso le evitará muchos problemas y propiciará un ambiente positivo y de seguridad laboral.

Joel A. Gómez Treviño es presidente de la Academia Mexicana de Derecho Informático, A.C.
joelgomez@mail.amdi.org.mx

BUSINESS NORTH MEXICO
Del 14 al 20 de mayo, 2001

EL EXPERTO

Estafas.com

Los fraudes por Internet se acrecentaron el último año 14% y usted debe saber cómo evitarlos

Joel Gómez Treviño*

Juan Maxon, un residente de Colorado, Estados Unidos, estaba muy ansioso por comprar un DVD el otoño pasado. Sabía que Internet tenía muchos sitios en donde se pueden rematar artículos de todo tipo, así que decidió entrar a uno de los más populares: **Ebay**. Fácilmente dio con un vendedor, aparentemente nuevo en Ebay, pues no tenía ningún comentario en su perfil de retroalimentación.

A Maxon pareció no importarle el hecho, pues el anuncio parecía muy profesional. Max ofreció $500 dólares por el DVD y ganó la subasta.

Pagó mediante "PayPal", el mecanismo de pago ofrecido por el sitio y aceptado por el vendedor. Sin embargo, nunca recibió el DVD. Juan no fue la única víctima, el mismo vendedor subastó más de 500 artículos a 200 personas, y jamás entregó uno sólo. La víctima estima que el estafador se hizo de unos $40,000 dólares por subastas "ganadoras".

Ebay rápidamente suspendió al usuario para evitar que realizara más transacciones, cosa que no ayuda de mucho puesto que el estafador lo único que tiene que hacer es volver a registrarse con un nombre de usuario distinto. ¿Le suena esto a un cuento? Pues lamento informarle que no lo es, lo relatado es un caso real, esto sucede todos los días en la red.

De acuerdo a la Comisión Federal de Comercio de los Estados Unidos, los delitos relacionados con Internet se incrementaron un 14% en el 2000; la agencia federal recibió más de 18,700 quejas en el 1999, y tal cifra brincó a 21,400 en el 2000. Sin embargo estas cifras distan mucho de representar le triste realidad, ya que muchos consumidores están tan avergonzados de haber caído en fraudes tan simples, que no presentan queja de ningún tipo.

El fraude por Internet continuará creciendo mientras nuevos usuarios de computadora entren en línea, ellos son los vulnerables, comenta un experto. Los engaños siempre han proliferado en la red porque es muy fácil llegar a millones de consumidores.

Internet Fraud Watch, un programa de la Liga Nacional de Consumidores en Estados Unidos, publicó estadísticas en las que el 78% de todas las quejas reportadas a IFW están relacionadas con subastas. Aunque también se han incrementado ventas fraudulentas de mercancía en otro tipo de sitios (del 3% en el 99 al 10% en el 2000). Los usuarios típicamente son víctimas de sitios con los que hacen negocios por la noche, y a la mañana siguiente ya no están.

Otro tipo de estafas de comercio electrónico son las relacionadas con artículos difíciles de encontrar en el mercado. El ejemplo clásico es lo que sucedió con el "Sony Playstation 2". Dos sitios, ambos basados en New Brunswick, Canada, prometieron a consumidores que tenían muchos de estos aparatos en su inventario. Cientos de consumidores hicieron sus pagos, pero nunca recibieron los artículos.

Pero los fraudes y engaños no se limitan a simples compras al menudeo o subastas. Los hay en casi todas las áreas en las que puede verse involucrado el internet. Hay hackers que en lugar de aprovecharse de debilidades en los sistemas informáticos de las empresas, se aprovechan de las "debilidades mentales" de sus empleados.

Existen casos en donde estos delincuentes envían mails a empleados de una empresa haciéndose pasar por personal de recursos humanos de la propia empresa: "Estimado Juan Pérez, nuestro sistema de nóminas e información de personal ha sufrido un error grave, y para repararlo necesitamos que nos proporciones tu clave de acceso para darte una nueva una vez que reinstalemos el sistema". Una vez con el password, ¡imaginen qué no puede hacer un hacker!

Los ámbitos financiero y bursátil no se quedan atrás. En el 99, una empresa texana denominada **NEI Webworld**, tenía valuadas sus acciones en 13 centavos de dólar un día viernes. Para el lunes siguiente, las acciones valían $8 dólares, una ganancia de más de 11,000%.

Tres personas fueron responsables del fraude, dos de ellos ex-estudiantes de la Universidad de California en Los Angeles. ¿Cómo lo lograron? Simple, enviaron cientos de correos a "tableros de mensajes" de Yahoo, Raging Bull y otros sitios de inversiones, en donde esparcieron el rumor de que NEI iba a ser adquirida mediante una fusión inversa por una firma privada de California llamada LGC Wireless. Como resultado, los jóvenes se llevaron $360,000 dólares.

No les duró mucho el gusto, pues semanas después la Securities Exchange Comission (SEC) ordenó el congelamiento de sus bienes y el FBI arrestó a los dos principales implicados. La SEC recibe 400 quejas diarias relacionadas con este tipo de fraudes.

En fin, los fraudes y estafas se dan por cientos todos los días, tanto en el mundo real como en el mundo virtual de la red. ¿Cómo evitar caer en ellos?. Algunos consejos prácticos:

1) No se deje llevar o impresionar por un web site elegante, bien construido, con logotipos oficiales de empresas reconocidas. Los "artistas del engaño" son especialistas en hacer parecer reales los fraudes;
2) Sea escéptico de los sitios que ofrecen precios increíblemente bajos o dicen tener en su inventario productos sumamente difíciles de conseguir;
3) Si va a subastar algo, lea siempre las reseñas o retroalimentación que otros consumidores han proporcionado sobre el vendedor;
4) Nunca pague con órdenes de pago, cheques de caja o cualquier otra opción que haga difícil o imposible el rastrear quién cobra. Use la tarjeta de crédito de preferencia.
5) No confíe en "medicamentos mágicos", premios o regalos consistentes en vacaciones increíbles, planes para trabajar en casa y hacerse millonario.
6) Nunca haga caso de los "correos basura" (spam), ni responda a ellos, ni mucho menos los reenvíe a amistades y conocidos.
7) Haga caso omiso de "consejeros anónimos" que quieran darle tips sobre cómo invertir su dinero.

** Joel A. Gómez Treviño*
joelgomez@mail.amdi.org.mx
Academia Mexicana de Derecho Informático, A.C. http://www.amdi.org.mx

LAGUNA

Invertirán en planta de celulosa

DURANGO.- Empresarios de Corea manifestaron su interés para ejecutar obras en Durango en una planta de celulosa, empaques y envases, y de esta manera abastecer el mercado del vecino país. Sergio Guerrero Mier, gobernador de Durango, destacó que lo anterior se desprende de una gira de trabajo realizada en Asia, donde llevaron a cabo la promoción de las bondades de invertir en la entidad, como infraestructura y mano de obra. Representantes de la empresa como Joongbo Chemical realizarán próximamente una visita a la entidad

Baja producción

TORREÓN.- La sequía que enfrenta la Región Laguna será determinante en la baja en la producción de leche. Los productores tendrán que sujetarse a limitaciones en su crecimiento, derivadas por la falta de agua y por ende, de alimento del ganado. Aunque la Región Lagunera es la primera cuenca lechera con una producción de 1,718 millones 198,735 litros en 2001, y que registra un crecimiento anual del 4%, las expectativas del mismo tendrán a reducir en el presente año, destacó Felipe Cedillo Vela, presidente de la Unión [illegible]era Regional de La Laguna

Capacitan a mineros

LERDO.- Las compañías del sector minero, en especial las relacionadas con el mármol, están impulsando acciones para el mantenimiento preventivo de la industria. Como parte del proyecto están ejerciendo actividades para la exploración y explotación de la bentonita. El Fideicomiso de Fomento Minero (Fifomi) en la Región Laguna comunicó que en este plan [illegible]rticipan más de 35 empresas, las [illegible]uales a su vez desarrollan programas de capacitación sobre el mantenimiento preventivo y de explotación de bentonita.

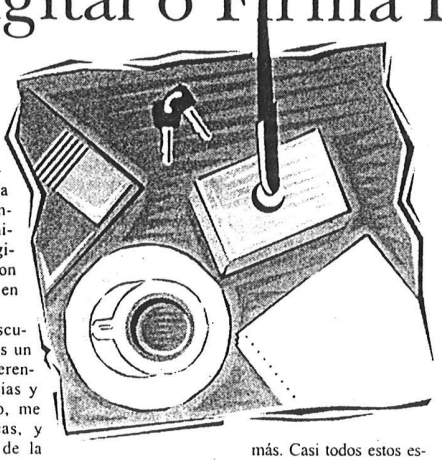
Rechazan pagar alumbrado

TORREÓN.- Las maquiladoras de la Región Laguna descartan realizar pagos por el servicio de alumbrado público. Hasta el momento, dos de las empresas más grandes, Siete Leguas y Pami, se han amparado con resultados positivos por lo cual fueron eximidas de pagar el Derecho de Alumbrado Público (DAP). El pago tendrá que ser asumido por el Ayuntamiento, se trata de cubrir una factura más elevada por consumo de energía eléctrica. En el sector industrial el consumo de energía representa el 7%.

EL EXPERTO

¿Firma Digital o Firma Electrónica?

Joel A. Gómez Treviño



Tremenda propaganda y publicidad se le ha hecho recientemente a la "firma digital". Revistas, periódicos y artículos en Internet nos han bombardeado de las maravillosas ventajas de la "firma digital". Algunos han afirmado inclusive que para que el comercio electrónico prospere, es necesario usar la "firma digital", por lo que es indispensable contar con un marco regulatorio que valide su uso en transacciones comerciales.

Un momento, pero yo también he escuchado el término "firma electrónica". ¿Es un sinónimo de "firma digital"? ¿Existen diferencias? En la realidad, sí existen diferencias y son considerables. Como buen abogado, me gustan las definiciones técnico-jurídicas, y además ahora que estuvo de moda lo de la "Cumbre de la ONU en Monterrey", pues aprovecharé para tratar de diferenciar estos conceptos con perspectivas de organismos internacionales, para luego resumir en un lenguaje claro ambos términos.

La Ley Modelo de la **Comisión de las Naciones Unidas** para el Derecho Mercantil Internacional (CNUDMI) sobre Firmas Electrónicas, determina que "por firma electrónica se entenderán los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos".

Otra definición interesante es la de la Ley de Firmas Electrónicas en el Comercio Nacional y Global de Estados Unidos, la cual establece que "el término firma electrónica significa un sonido, símbolo o proceso electrónico, adherido o lógicamente asociado con un contrato u otro archivo y ejecutado o adoptado por una persona con la intención de firmar el archivo."

Finalmente, la Directiva 1999/93/CE del Parlamento Europeo y del Consejo por la que se establece un marco comunitario para la firma electrónica, estipula como definición de firma electrónica: "los datos en forma electrónica anexos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación."

En resumen, y desde mi punto de vista personal, tenemos los siguientes elementos comunes que definen a la **FIRMA ELECTRÓNICA**:

> 1) Esta formada por datos, sonidos o símbolos electrónicos,
> 2) Que están adheridos o asociados a un documento o contrato,
> 3) Con el objeto de indicar la intención de firmar el documento, o bien para servir como medio de autenticación.

Ahora bien, para definir la "firma digital", recurriré a la legislación de los Estados Unidos, ya que tienen una extensa cantidad de leyes en materia de firma digital, tanto a nivel federal como estatal especialmente. En la legislación estatal de los Estados Unidos, existen tres grandes tendencias para definir a la firma digital.

Por razones de espacio, me pasaré directamente a la tendencia maximalista, que es la que siguen la mayoría de Estados de la Unión Americana, tales como: Arizona, Florida, Illinois, Indiana, y otros 11 más. Casi todos estos estados definen a la firma digital como "un tipo de firma electrónica que transforma un mensaje usando un criptosistema (sistema criptográfico) asimétrico para que la persona que tenga el mensaje inicial y la llave pública del signatario pueda determinar con exactitud:

(a) si la transformación fue creada usando la llave privada que corresponde a la llave pública del firmante.

(b) si el mensaje inicial ha sido alterado desde que la transformación fue hecha."

Algunos especialistas y algunas legislaciones, en lugar de "firma digital" usan el término "firma electrónica avanzada", como lo hace la Directiva del Parlamento Europeo sobre firma electrónica. Conceptualmente estos términos son casi sinónimos, dadas las características y elementos propios de cada uno. En México, una de las propuestas que se discute actualmente en la Comisión de Comercio de la Cámara de Diputados, usa el término "firma electrónica avanzada".

Concluyendo, la firma digital es un tipo de firma electrónica que usa tecnología de encripción asimétrica (o "PKI" por sus siglas en inglés) para crear un juego de llaves digitales únicas (una pública y otra privada), que cuando se usan juntas proveen a la comunicación electrónica de los siguientes elementos (de seguridad en su mayoría): privacidad, integridad, autenticación y no repudiación.

La firma electrónica es entonces el género, mientras la firma digital es sólo una especie dentro del universo de firmas electrónicas. Podríamos citar varios ejemplos de "tipos de firma electrónica": reconocimiento de voz o huella digital, tecnología biométrica, digitalización de firma autógrafa, o sistemas combinados.

A pesar de la enorme publicidad que se le ha dado a la firma digital, muchos especialistas opinan que la tecnología PKI está muerta o que la firma digital tiene serias desventajas y debilidades.

La creencia popular nos indica que la "firma digital" es una "nueva tecnología" necesaria para que el e-commerce pueda desarrollarse y prosperar. Esto dista mucho de la realidad. En 1976, Whitfield Diffie y Martin Hellman desarrollaron el concepto de criptografía asimétrica de llave pública (PKI), aunque no fue un sistema funcional y comercial hasta que apareció el sistema (y empresa) "Seguridad de Datos RSA" (nombrado así por sus autores: Rivest, Shamir y Adleman). Como podemos ver, es evidente que la tecnología de firma digital ha existido durante mucho tiempo, suficiente para que la comunidad empresarial la haya adoptado como un estándar en el comercio electrónico, cosa que no ha sucedido por muy diversas razones.

Hay mucha literatura que habla maravillas y enormes ventajas de la firma digital, sin embargo la inmensa mayoría de esta literatura, y las promociones para su adopción ante legislaturas y sectores empresariales de diversos países, es llevada a cabo por empresas que venden sistemas de PKI o firma digital. Es lógico entonces, que intenten convencernos a todos de las bondades del PKI.

Algunas razones por las que especialistas opinan que el PKI está muerto, además de la anterior claro está, son:

1.- El PKI no está siendo usado, casi ningún contrato establece el uso de PKI como obligatorio para transacciones electrónicas. Visite cualquier sitio web que le venga a su mente, cualquiera estará feliz de aceptarle un pedido u orden de compra, tenga usted un certificado digital o no. Muchos millones de dólares se mueven en comercio electrónico B2C y B2B hoy en día, muy pocas empresas o sitios web usan la firma digital como un requisito para hacer negocios.

2.- La firma digital implica el uso de llaves públicas y privadas. Estas llaves son en realidad un conjunto de bytes (o bien un conjunto de caracteres de cierta longitud) que necesitan estar almacenados en algún dispositivo: un disco duro, un diskette, una computadora portátil o inclusive en tarjetas inteligentes. Lo cierto es que la mayoría de usuarios almacenan sus llaves en su computadora personal. Estando ahí, las llaves están sujetas a innumerables riesgos de seguridad: a) ataques de virus u otros programas maliciosos (caballos de troya), b) un hacker puede penetrar la computadora y usar o copiar la llave, c) si la computadora está en una empresa o lugar "público", cualquier persona (no sólo el titular de la llave) puede tener acceso a la PC y por consiguiente tendrá acceso a las llaves públicas y privadas, etc.

3.- Cada vez más países, potencias y organizaciones internacionales (EUA, CNUDMI {ONU}, UE) se han pronunciado a favor de leyes "tecnológicamente neutras". Recientemente los Estados Unidos, con el objeto de dar fin a toda una serie de problemas con legislaciones estatales sobre firma digital, adoptó y publicó la "Ley de Firmas Electrónicas para el Comercio Nacional y Global", la cual establece que los Estados podrán emitir disposiciones que modifiquen esta ley, siempre y cuando el uso de la firma electrónica no esté condicionado a la implementación o aplicación de alguna tecnología en particular.

En conclusión, México no necesita de la "firma digital" para que el comercio electrónico pueda explotar y desarrollarse, aunque tal vez los proveedores de sistemas PKI o "firmas y certificados digitales", si necesiten del comercio electrónico para que sus negocios puedan prosperar. Lo que necesita nuestro país es una legislación tecnológicamente neutra sobre firmas electrónicas, para evitar que la ley quede obsoleta en el corto lapso en el que las tecnologías evolucionan, entre muchos otros factores. Ojalá que pronto contemos con una legislación que promueva el comercio electrónico, y que esté acorde a las tendencias regulatorias globales.

Joel A. Gómez Treviño es presidente de la Academia Mexicana de Derecho Informático, A.C. (AMDI)
joelgomez@mail.amdi.org.mx

BAJA CALIFORNIA

Proponen emitir bonos

TIJUANA.- El Consejo de Desarrollo Económico de Tijuana (CDT), destacó que existe la posibilidad de que se acepte la propuesta de emisión de bonos, donde si el municipio opera este esquema, se podrán financiar proyectos como el Centro de Convenciones.
Pedro Delgado, director de proyectos del CDT, señaló que la emisión de bonos por autoridades municipales o estatales sería una alternativa para financiar proyectos, lo que resulta viable, ya que este esquema es utilizado por el estado de Guanajuato.

Deben ser precios iguales

La Cámara Nacional de Comercio (Canaco) de Tijuana, reportó que al año los mexicanos gastan en San Diego $4,000 millones de dólares, sin que hasta el momento se dé una solución por parte de las autoridades a esta fuga de divisas. Para la Canaco de Tijuana, las ciudades de la frontera, deben tener una homologación de precios con sus competidores de Estados Unidos. La fuga de con- dores se da en primer instan- ausa del precio de la gasoli- a es más barata en Estados Unidos.

Falta personal

MEXICALI.- El nuevo administrador de la Aduana de Mexicali, Enrique Hernández Navarro, reconoció que falta más personal en la Aduana, al señalar que se enfrentó a problemas de desorganización ante la ausencia de un titular. El administrador enfatizó que de llegarse a dar casos comprobados de corrupción, se harán cambios en la Aduana.
Hernández Navarro, quien es egresado de la UANL y trabajó en **Vitro** durante 25 años, sucedió a Gerardo Rocha Centeno, quien dejó de laborar en la Aduana hace dos meses.

Peligrarían aguinaldos

MEXICALI.- Gustavo de Hoyos Walther, presidente de **Coparmex** en Mexicali, señaló que el crédito al salario afectará al empleado, porque en el corto plazo el cheque vendrá más reducido en cantidad. En mediano plazo las empresas ante la imposibilidad de absorber ese costo, tendrán que retener de manera retroactiva todos los impuestos que anteriormente no los retuvieron. Por lo que existe la posibilidad que no llegue aguinaldo a los empleados, en el caso de las compañías calculen así el crédito al salario, para no afectar el ingreso normal de los empleados.

EL EXPERTO

La nueva e-economía: *Mitos y realidades*

Aunque parezca increíble, hay empresas como la texana Enron que sí está haciendo dinero en Internet

Joel A. Gómez Treviño

Mucho se ha escrito y platicado sobre los "fracasos.com" y la aparente época de crisis por la que pasa el Internet. Hay quienes afirman que el comercio electrónico es un sueño, o peor aún, un gran fiasco. Otros afirman que el Internet será sólo un medio electrónico para mejorar particularmente la comunicación de los negocios, más no una herramienta para hacer negocios.

Cuando llegó a México el boom del comercio electrónico, literalmente todo el mundo quería tener una punto com. Desde entonces, la historia se repite una y otra vez...

El objetivo. Perseguir el codiciado sueño americano, hacerse mi-llonario de la noche a la mañana abriendo una empresa en Internet.

Los jugadores. Son tres primordialmente: los emprendedores, los inversionistas y los consumidores. Entre los primeros, usualmente encontramos a los siguientes: a) jóvenes ejecutivos, con carreras brillantes, e inclusive con postgrados en el extranjero; b) recién egresados, que sin mucho que perder, pretenden correr antes de aprender a gatear; c) los juniors, quienes teniendo el apoyo de su apellido y una familia adinerada, se quieren comer el mundo "a mordidas".

En el exclusivo mundo de los inversionistas, también hay de todo: a) familiares y "ángeles" que con fe ciega buscan apoyar iniciativas novedosas; b) incubadoras, muchas de ellas buscando adueñarse de las mejores ideas y dejar a los jóvenes emprendedores en calidad de empleados; c) inversionistas con amplio "colmillo" para detectar sólo las ideas con posibilidades reales de éxito. Y al final, li-teralmente al final, quedan los consumidores, quienes son usados como bandera de una lucha que muchas veces no tiene causa ni beneficio.

La estrategia. Casi todos los emprendedores promueven y prometen a los inversionistas el mismo "cuento de hadas": ganancias mi-llonarias en un corto período de tiempo. Además, los emprendedores suelen convertirse en hábiles negocia-dores, y buscan recibir todo tipo de asesorías (financieras, fiscales, contables, legales, etc.) de manera gratuita, ofreciendo a cambio al consultor acciones y hasta un puesto directivo en su empresa. Eso sí, en las punto com todos quieren ser y de hecho son "directores", y no sólo de título, pues los sueldos que suelen auto-asignarse también andan por las "nubes". Por si fuera poco, como el Internet es global, pues las punto com también quieren ser globales, y olvidándose de la omnipresencia y otras bondades que nos brinda a todos la Web, los emprendedores se van de viaje por el mundo a abrir oficinas reales para un negocio virtual.

El resultado. Fracasos.com a la orden del día. Gracias a este mundo de excesos, avaricia, engaños y sueños guajiros, el comercio electrónico está pasando por una de sus mayores debacles, su credibilidad ante quienes le dan vida: inversionistas y consumidores.

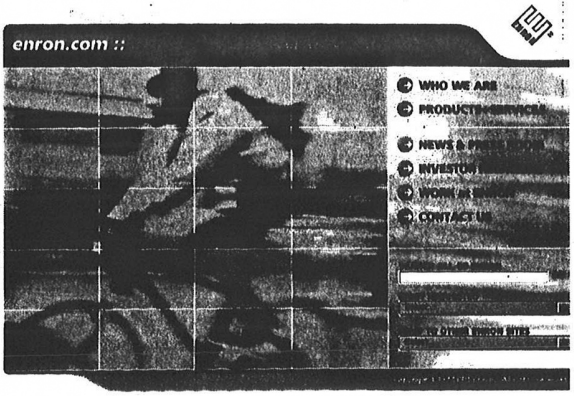
Realidades. No sólo en México hay problemas. Aún las empresas estadounidenses más populares en Internet tienen graves dificultades financieras. Estadísticas recientes muestran que entre los meses de abril y julio del presente año, más de 210 empresas punto com cerraron sus puertas. En lo que va del 2001 la cifra es de 367. En julio de 2001, Webvan, una popular empresa que vendía abarrotes por Internet con base en California, solicitó declararse en quiebra. La empresa llegó a estar cotizada en $1.2 billones de dólares. En noviembre de 1999, durante la Oferta Inicial de Compra (IPO, por sus siglas en inglés) en la bolsa de valores, sus acciones llegaron a valer $30 dólares cada una. El pasado 13 de julio, las mismas valían 6 centavos.

A pesar de toda esta ola de publicidad negativa para el Internet y el comercio electrónico, estoy convencido de que ambos llegaron para quedarse. Los actuales problemas pueden tener muy diversas causas. Probablemente muchos de ellos se deben a una visión y esquemas poco adecuados de los negocios electrónicos. Las empresas exitosas no se hacen de la noche a la mañana, se construyen a base de esfuerzo, experiencia y un proceso de mejora continua.

No todo es fracaso en Internet. Existen también casos de éxito. Una conocida revista estadounidense, en su ejemplar de septiembre de 2001, publicó 50 empresas que están haciendo dinero en Internet. A la cabeza aparece **Enron.com**, empresa texana dedicada al comercio de energéticos (gas y electricidad, entre otros). Enron realiza más de 4,000 transacciones diarias en promedio, de un monto aproximado de $500,000 dólares cada una. El año pasado tuvo ventas que ascendieron a los $101 billones de dólares. En el segundo puesto está UPS, que está obteniendo grandes ganancias, gracias a su división de e-Logística. Otros ejemplos de empresas exitosas en Internet son **General Electric, American Express, Dell Computer, IBM, Boeing, Procter & Gamble, Fedex, Office Depot, Hewlett-Packard, General Motors, Avon, Barnes & Noble, Wal-Mart** y **Carrier.**

En esta lista podemos apreciar fácilmente un común denominador: todas las empresas son "brick & mortar", como dicen los "gringos", es decir, son de "ladrillo y cemento". Todas son empresas reales, con experiencia y sólida trayectoria, que encontraron en Internet un medio idóneo para ahorrar costos, mejorar comunicación, expandir su mercado, etc. Que esto sirva de ejemplo a nuestras empresas mexicanas. Y si tienen la duda sobre si en el resto de las 50 empresas existe alguna "punto com" virtual, de esas que nacieron de la nada de la noche a la mañana, pues lo siento, pero desafortunadamente al menos en esa lista no aparece ninguna con esas características. Claro, esto no significa que no puedan existir empresas punto com innovadoras que tengan éxito en la nueva e-economía, simplemente revela una clara tendencia: quienes hoy por hoy tienen éxito en la Red, son las empresas "click & mortar".

Joel Alejandro Gómez Treviño es presidente de la Academia Mexicana de Derecho Informático, A.C. (joelgomez@mail.amdi.org.mx)



CALIFORNIA

Financia Mercury Air Group obligaciones

LOS ANGELES.- **Mercury Air Group Inc.** anunció que accedió a un financiamiento por $71 millones 500 mil dólares a través de la aseguranza de obligaciones subordinadas convertibles. Dichas obligaciones, que serán compradas por una firma europea de inversión por un monto nominal principal de $110 millones de dólares, vencerán el 30 de septiembre de 2021 y llevarán una tasa de interés del 7% anual sobre el monto nominal principal. El interés será pagadero trimestralmente. Las obligaciones serán convertibles en acciones comunes de Mercury Air Group a partir del 30 de septiembre de 2004 a $21.50 por acción. Mercury es proveedor de combustibles de aviación, servicios de transporte, logística, personal, equipo y servicios de apoyo a las líneas aéreas nacionales e internacionales.

Davis da moratoria a gravámen en Internet

SACRAMENTO.- El gobernador Gray Davis extendió formalmente el pasado lía [illegible] tual moratoria a los mpu[illegible] nuevos y discriminatorios al efrendar el proyecto de ley SB 394, ó ıcta de Libertad Tributaria en Internet le California. La moratoria debía expirar l mes próximo. **A&A**, la asociación más rande de la industria de las tecnologías vanzadas, e **ITFA**, manifestaron su onfianza de que la extensión de la ıoratoria impositiva estimulará el crei-imiento del comercio electrónico. La 'FA prohibe los impuestos específicos e acceso e impide la suplementación e gravámenes locales de acceso a ıternet a través de cientos de jurisdicones tributarias en todo el estado.

)avis aprueba)royecto de $2 mdd

ACRAMENTO.- El gobernador Gray avis anunció la aprobación de un ıanciamiento de bajo costo por $1.96 i-llones de dólares para la ciudad de rawley del **Banco de Desarrollo conómico e Infraestructura de alifornia** (CIEDB). Los fondos del IEDB darán asistencia a la ciudad para :tualizar su Planta de Tratamiento de guas Residuales e instalar una línea drenaje para servicio del nuevo cams de la **Universidad Estatal de San ego**. A su vez, las mejoras en la plande tratamiento beneficiarán a una ıeva planta de procesamiento de cárcos de BP Ventures que iniciará eraciones a finales del año. BP ntures prevé crear 600 puestos de baj[illegible] mpo completo en la comudad.

EL EXPERTO

La próxima guerra es informática

Joel A. Gómez Treviño

Hace apenas unos días me decidí a instalar en mi computadora portátil un software de los denominados **"firewall"**. Estos programas tienen la finalidad de proteger la información de tu computadora contra "ataques externos", o dicho de otra manera, son sistemas de seguridad informática.

Cada vez que escuchamos temas relacionados con virus, hackers y demás ciberdelincuentes, muchos solemos pensar que sólo se trata de una paranoia por la seguridad en Internet. Lo más triste de todo es que de paranoia no tiene nada, es una cruda realidad: la gran Red está llena de cibervándalos y criminales.

En la antigua Grecia se ideó un mecanismo para penetrar las ciudades amuralladas: el caballo de Troya. Este gigantesco equino de madera, inocente en apariencia, atrajo la curiosidad de los habitantes de la ciudad. Lo introdujeron a la ciudad, y con él llegó su destrucción y conquista, ya que sus entrañas se encontraban llenas de soldados enemigos que inundaron sus calles con fatal sigilo.

Pues bien, mientras escribo este artículo he sido atacado más de 30 veces, 16 de las cuales han sido intentos de entrar a mi computadora mediante el "SubSeven Trojan Horse". Los Troyanos, nombrados así por el mitológico "Caballo de Troya", son programas disfrazados de programas normales, pero que en realidad contienen un código para penetrar en un sistema de cómputo. Los Troyanos más típicos son aquéllos que roban passwords (claves de acceso), instalan un virus, reformatean el disco duro, etc.

Una clase muy popular de Troyanos son los de "Acceso Remoto". Estos son programas que le permiten a un hacker el control total de tu computadora de manera remota. Otros también muy recurridos son los "Back Orifice", una herramienta de "puerta trasera" desarrollada desde agosto de 1998 por un grupo de hackers conocidos como "El Culto de la Vaca Muerta". Este "orificio trasero" implica que tu computadora ha sido analizada, mas no elegida como un objetivo de ataque. Esto significa que un atacante está analizando miles de máquinas con la esperanza de encontrar alguna que haya sido infectada con este Troyano. Al igual que con el Caballo de Troya anterior, con el Back Orifice los hackers no buscan a un individuo en particular, sino buscan en cientos de máquinas simultáneamente para ver en cuál pueden entrar.

Durante el fin de semana recibí cientos de ataques, pero algunos en particular me llamaron la atención. Hubo un hacker que en un lapso menor a una hora intentó penetrar a mi computadora más de 170 veces. La cuenta no creció sólo porque me tuve que desconectar de Interenet. Desde una computadora conectada por módem en la ciudad de Cambridge, Massachussets, durante cada minuto este individuo analizaba 3 o 4 distintas maneras de entrar a mi laptop, principalmente buscando puertos abiertos. Otros ciberdelincuentes intentaron entrar a mi máquina desde lugares tan remotos como Asia, Europa, Dinamarca, y también, porqué no decirlo, desde México. Otro que me sorprendió fue el de un atacante que se encontraba conectado a un servidor cuya dirección de Internet (IP) pertenece al **Commercail Bank Delovaya Moskva**, ¡en Rusia!

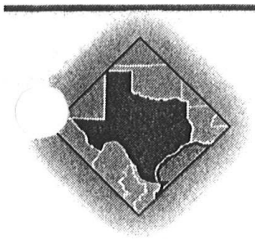
Bueno, pero muchos se preguntarán: ¿qué interés pueden tener estos ciber-terroristas en la modesta computadora de Pito Pérez (léase, un servidor)? Usualmente pensamos que los hackers sólo buscan computadoras de bancos o grandes empresas, para obtener dinero mediante transacciones fraudulentas o robar información confidencial. La realidad puede ser muy distante a este pensamiento. Hay millones de hackers en potencia en todo el mundo, comúnmente jóvenes estudiantes cuyo principal pasatiempo es merodear por Internet, aprendiendo nuevas formas de penetrar y husmear en computadoras ajenas. Uno de los objetivos de muchos de ellos, sobre todo de quienes sí desean causar daño, puede ser el penetrar en tu máquina para desde ahí perpetrar un ataque a otra, y cuando las autoridades busquen el rastro llegarán a ti, y probablemente te señalarán como principal sospechoso de la agresión.

Se rumora que el Gobierno de los Estados Unidos, derivado de los recientes ataques a Nueva York y Washington, está haciendo un llamado al pueblo de los Estados Unidos para desincentivarlos a que usen el Internet durante algún tiempo. La razón, creen que hay muchos hackers y creadores de virus pueden estar planeando un ataque informático masivo a instituciones públicas y privadas para desestabilizar al país. Recordemos que todos, absolutamente todos los servicios (agua, drenaje, electricidad, puertos, aeropuertos, gas, etc.) están controlados por computadoras, eso sin mencionar al propio Gobierno y la milicia, que también dependen al 100% de las computadoras, el Internet y otras redes privadas. Un virus o hacker bien infiltrado, podría causar un verdadero caos.

Y en México, ¿somos vulnerables a estos tipos de ataques? Pues la respuesta es bastante obvia: SI, y ¡MUCHO! La cultura de la seguridad informática en nuestro país es muy pobre. Y por si esto fuera poco, nuestro glorioso Código Penal Federal sólo nos "protege" contra ataques a sistemas informáticos que estén protegidos con algún mecanismo de seguridad, el cual, para variar, no está definido en la Ley.

Por si las dudas, la mejor recomendación que le puedo hacer es simple: compre inmediamente algún programa de software (firewall) para proteger sus sistemas de cómputo. Hay de todos tamaños, colores y sabores. Algunos caseros o personales tienen un rango de precio que oscila entre los $40 y $80 dólares. Un precio sin duda bajísimo en comparación de lo que puede perder si llega a ser atacado. Instalando un firewall logrará dos beneficios: proteger su información contra la mayoría de los ataques (tampoco son perfectos) y poder ser sujeto de "protección" bajo los términos actuales de nuestra legislación en México.

Joel Alejandro Gómez Treviño es presidente de la Academia Mexicana de Derecho Informático, A.C. (joelgomez@mail.amdi.org.mx).



TEXAS

Adquisición de Combined y Lifeline

AUSTIN.- **Citizens Inc**. anunció un acuerdo definitivo para la adquisición de las acciones en circulación de **Combined Underwriters Life Insurance Company** y **Lifeline Underwriters Life Insurance Company** por acciones comunes Clase A de Citizens a ser ofrecidas a través de un prospecto. Tanto Combined como Lifeline son miembros del Walden P. Little Group, de Tyler, Texas. El acuerdo está sujeto a la aprobación de los accionistas de ambas y a las sanciones de las autoridades regulatorias del estado. El intercambio será efectuado en base a un valor de mercado de $8.64 dólares por acción de Combined y $5.00 dólares por acción de Lifeline.

Inician obras en el aeropuerto de McKinney

MCKINNEY,.- **Crossmark** echó a andar obras de construcción de su nuevo hangar de 10,200 pies cuadrados para su flota corporativa. Las obras de expansión son parte del plan del Aeropuerto de McKinney para atraer más compañías en busca de servicios com[illegible]les de aviación. La Corporación de[illegible]ollo Económico de McKinney est[illegible]ajando estrechamente con **WingsPoint Development** en el Aeropuerto de McKinney para la construcción de nuevas pistas y hangares. Cossmark se suma a **Texas Instruments**, **Fleming Foods**, **Lattimore Materials** y **United American Insurance** en el uso del aeropuerto como sus instalaciones de aviación corporativa.

Adquiere a la federal Northern NEF

DALLAS.- **CompuCom Systems**, proveedor líder de servicios de integración de sistemas y subcontratación de tecnologías de la información, anunció la adquisición de **Northern NEF**, un integrador de sistemas y proveedor de soluciones federal. Con sede en Colorado Springs, Northern NEF ofrece servicios como ingeniería de sistemas, desarrollo, integración prueba y capacitación en software, así como servicios de apoyo en administración de programas a varias dependencias civiles y de defensa del Gobierno federal.

Demandan empleados a Enron

HOUSTON.- En una demanda colectiva fincada el 20 de noviembre ante un tribunal federal de distrito, empleados de **Enron Corp**. denunciaron que la compañía puso en riesgo sus fondos para el retiro, ocasionando que muchos empleados perdieran cientos de miles de dólares prácticamente de la noche a la mañana. La denuncia refiere también que, después del sorpresivo anuncio de pérdidas para el tercer trimestre, Enron sus[illegible]ó ilegalmente los planes para el ret[illegible]us empleados, imposibilitándole[illegible]roteger sus fondos de una

EL EXPERTO

Las tarjetas inteligentes

Joel A. Gómez Treviño

Hace unos días recibí un curioso paquete por mensajería privada. Venía de Estados Unidos... "Uy, cuidado con el Ántrax!" pensé, bromeándome a mí mismo. El clásico sobre de cartón de las empresas de mensajería lucía débil, su contenido se sentía pequeño. De hecho, sólo tenía otro sobre adentro, del tamaño de los que usualmente recibimos por correo. Al abrirlo, mi sorpresa fue grata, no sólo porque tenía mi renovación de la tarjeta **American Express** (emitida en Estados Unidos, aclaro), sino porque esta tarjeta luce muy distinta a comparación de las tradicionales, es una mezcla de una tarjeta de crédito y una... **LADATEL**! Sí, me refiero a las tarjetas telefónicas. En otras palabras, además de la banda magnética, esta tarjeta llamada "Blue" por American Express (AE), tiene un microchip integrado, idéntico en apariencia, tamaño y posición al de las tarjetas LADATEL.

Aunque venía un folleto explicando sus características dentro del sobre, preferí meterme a navegar al sitio de Internet de esta empresa para conocer un poco sobre "Blue". Resulta que este chip inteligente contiene un certificado de autenticidad, para proveer mayor seguridad al hacer compras por Internet. Es un sistema de seguridad tripartita en realidad, pues debes combinar el chip inteligente de la tarjeta, con tu NIP y el sistema de "Pagos Privados" de AE. La seguridad radica en que este sistema genera un número seguro temporal, para cada transacción realizada en línea, evitando así estar manejando tu número de tarjeta de crédito por Internet.

Algunos estarán pensando ahora: ¿pero cómo va a "leer" la computadora este chip de mi tarjeta? Pues muy buena pregunta... para que esto funcione, es necesario adquirir o comprar un lector de tarjetas de AE, que a decir verdad, son bastante portátiles y económicos. Hay una versión gratuita, otra de $25 dólares y una tercera que viene integrada en un teclado para computadora a un precio de $59 dólares. Una vez instalado este lector en tu computadora, puedes "bloquearlo" para que el chip de tu tarjeta pueda ser utilizada sólo desde tu PC. Bastante seguro y útil en caso de que sufras robo o extravío.

No soy experto en tarjetas inteligentes ni en sistemas electrónicos de pago, pero sí estoy enterado de que el anteriormente descrito no es el único uso que se les da a estos chips, que dan nacimiento a las que hoy conocemos como "tarjetas inteligentes".

Para los lectores que viven en Monterrey, no sé si recuerden que hace algún tiempo hubo un "programa piloto" en el municipio de San Pedro llamado **"VISA Cash"**. Esta empresa sacó al mercado estas tarjetas, que también tenían un chip inteligente. La diferencia con el ejemplo anterior estriba precisamente en el uso, ya que la tarjeta "VISA Cash" era más o menos lo que su nombre indica: "efectivo electrónico". Sí, tenías que depositar la cantidad que desearas en un banco, y ellos a su vez te "cargaban" la tarjeta con dicha cantidad de dinero. Era como traer efectivo, ya que si perdías la tarjeta, cualquiera podría usarla (sin firmas ni NIP's de por medio) como si trajera billetes en mano.

La tarjeta venía acompañada con un pequeño dispositivo en forma de llavero, que en realidad era un lector del chip, que permitía conocer la cantidad de dinero que contenía la tarjeta y el monto de la última transacción realizada. Esta tarjeta se promocionaba como un medio eficaz para hacer compras por montos pequeños, evitando así cargar morralla o dinero en efectivo inclusive.

Pese a la gran publicidad que se le hizo, no les duró mucho el gusto. Desconozco la razón del fracaso de este sistema electrónico de pagos, pero en lo personal, desde el punto de vista del usuario, dos eran los grandes problemas de VISA Cash: (1) sólo era aceptada por ciertos establecimientos que contaban con el aparato lector de tarjetas, y (2) cada vez que ibas al banco a tratar de "re-cargar" la tarjeta, casi siempre la respuesta era la misma: "no hay sistema", "no está funcionando el aparato que carga las tarjetas", etc.

Hablando de estas tarjetas inteligentes, tal vez el ejemplo más antiguo y mejor aceptado en un mercado específico es **"Mondex"**, un sistema de dinero electrónico que provee un equivalente electrónico directo del efectivo, que trae beneficios convincentes a los consumidores y comerciantes (europeos) que hacen negocios en el mundo virtual. Al igual que "Blue", Mondex opera por medio de una tarjeta plástica con un chip inteligente inserto. En realidad este es un sistema que mezcla algunos beneficios de "Blue" y "VISA Cash", ya que además de almacenar información ("dinero") en el chip para realizar compras en el mundo real, puede usarse también para hacer compras en línea con altos estándares de seguridad, y sin necesidad de revelar datos personales.

Mondex tiene otra característica interesante: es accesible a todos, inclusive al mercado joven y a aquellos que no tienen una cuenta bancaria. Este sistema electrónico permite la transferencia de valores (dinero) directamente entre comerciantes y consumidores (o entre consumidor y consumidor), sin necesidad de una autorización bancaria, como es el caso de las tarjetas de crédito. Mondex también ofrece soluciones para la Televisión Digital, el Internet y el comercio electrónico móvil (a través de telefonía celular). Este sistema está diseñado para hacer pagos de bajo valor en cualquier parte, sea un café, el metro, una pequeña tienda, o en la web.

Sin duda, uno de los principales problemas para que el comercio electrónico en México explote todo su potencial, radica en los mecanismos de pago disponibles actualmente para hacer transacciones en línea. El medio tradicional para pagar en Internet es la tarjeta de crédito. Sin embargo, sabemos que en México es muy limitado el número de personas que tienen las características para ser titulares de una tarjeta de crédito, particularmente los jóvenes y estudiantes, que de alguna manera son los principales compradores potenciales en la web.

Es necesario que nuestro país cuente con un adecuado medio electrónico de pago para que el comercio electrónico pueda desarrollarse a plenitud. Tal vez las tarjetas inteligentes puedan ser una solución viable, o al menos sería deseable que cualquier tarjeta de débito pueda usarse para hacer pagos en Internet, como ya lo ha promovido un banco mexicano hace algunos meses. Esta es una tarea titánica que implica recursos y un gran cambio cultural. Es importante seguir fomentando, entre otras cosas, los medios electrónicos de pago, para que el comercio electrónico prospere en México.

Joel A. Gómez Treviño es presidente de la Academia Mexicana de Derecho Informático.
joelgomez@mail.amdi.org.mx

Mejora IMSA su rendimiento

ADOPTA LA EMPRESA REGIOMONTANA LAS SOLUCIONES DE PRECISE, A FIN DE OPTIMIZAR EL RENDIMIENTO DE SU AMBIENTE SAP R/3

Precise Software Solutions, líder en optimización de negocios mediante la gestión de rendimiento de sus aplicaciones, fue seleccionada por la compañía regiomontana **IMSA**, el mayor productor mexicano de acero procesado. IMSA, la más grande división de Grupo IMSA, compañía tenedora industrial diversificada de $2,200 millones de dólares, usará las soluciones de Precise para optimizar el rendimiento de su ambiente SAP R/3.

Localizada en cuatro plantas y 14 centros de distribución en todo México, la infraestructura SAP de IMSA [illegible] y aplicaciones financieras.

"Las invaluables soluciones de Precise nos permiten optimizar el rendimiento de nuestro ambiente SAP R/3. Ahora podemos identificar rápidamente los embotellamientos de procesamiento y resolver problemas con mayor rapidez y eficacia", señaló Javier Cantú, gerente de bases de datos e infraestructura de tecnologías de la información en IMSA.

IMSA aplica las soluciones de Precise, diseñadas específicamente pensando en el ambiente SAP R/3, para monitorear y afinar proactivamente su ambiente de producción, al tiempo que mantiene todas sus aplicaciones funcionando con fluidez y disposición continua para más de 900 usuarios finales.

"Precise ha mejorado el rendimiento de nuestro ambiente SAP R/3, [illegible]

"Escogimos a Precise en parte por nuestra sociedad e integración con EMC, que nos brinda una perspectiva completa correlacionada del rendimiento de las aplicaciones a lo largo de toda la infraestructura, partiendo del servidor de aplicaciones hasta la base de datos o un dispositivo de almacenamiento EMC Symmetrix específico", añadió.

"Hoy, una transacción de manufactura que antes nos llevaba 40 minutos, toma apenas unos segundos", precisó Javier Cantú. IMSA usa Precisa también para la alerta y monitoreo en tiempo real, el envío de alarmas por radiolocalizador para notificar a Cantú y a su equipo BASIS cuando se exceden los umbrales de rendimiento, dándoles las advertencias e información necesarias para eliminar cualquier [illegible]

tamente competitivas, como IMSA, se apoyan en procesos eficientes de tecnologías de la información para maximizar sus recursos y rentabilidad", manifestó Andrew Bird, vicepresidente ejecutivo de comercialización de Precise Software Solutions. Grupo IMSA, fundado en 1936, maneja cuatro operaciones fundamentales: productos procesados de acero; baterías automotrices y productos afines; aluminio y productos relacionados; y acero y productos plásticos de construcción. Cuenta con plantas de manufactura en México, Estados Unidos, Centro y Sudamérica, y exporta a los cinco continentes.

Precise Software Solutions, con sede en Westwood, Massachusetts, se dedica a aportar soluciones destinadas a mejorar drásticamente el [illegible]

CALIFORNIA

Reportan sobre víctimas energéticas

SACRAMENTO.- La Asociación de Manufactura y Tecnología de California (CMTA, por su siglas en inglés) publicó la primera de lo que serán las listas mensuales de empresas que han sufrido el impacto de la crisis de energía en el estado. La lista, llamada, "Energy Casualty Report", menciona docenas de empresas que han tenido que suspender su producción, despedir personal o sufrir otras problemas a consecuencia de los aumentos en los precios de la electricidad. La asociación dice que cuando la comisión estatal cambió el esquema de precios en junio, transfirió cientos de millones de dólares en costos de consumidores residenciales a empresas. Las tarifas en algunos casos aumentaron hasta 190%. Entre otras cosas, la CMTA exige que empresas tengan la opción de controlar sus costos con acceso directo a proveedores de energía o generación propia. El reporte se puede leer en www.cmta.net/casualty_report.

Se expande Instill

REDWOOD CITY.- Instill Corporation, un proveedor líder de servicios de logística para la industria de servicios de comida, agregó $12 millones de dólares a su fondo de financiamiento y anunció que adquirido Global Food Exchange tlanta, en una transacción que le mitirá crecer en el área de eComercio dentro del sector. Instill ha recibido un total de $84 millones de dólares de sus inversio-nistas Altos Ventures, Applebee's International, Charles River Ventures, JP Morgan Partners, Mayfield Fund, Octane Capital Management, Ohio Partners, Piper Jaffray y Procter & Gamble.

Ampliará servicios

VISTA.- Paramount International Telecommunications firmó un acuerdo con Qwest Communications, en el cual Paramount proveerá servicios a clientes, incluyendo la de operadora en línea en México, Canadá y Estados Unidos. Paramount provee sistemas de telecomunicaciones a hoteles, hospitales y otras instituciones y empresas grandes. Paramount también podrá utilizar la plataforma de Qwest para llamadas a EU, originadas en Europa.

Llega Netro a México

SAN JOSÉ.- Netro Corp. anunció que arrancó operaciones en México, ofreciendo a empresas de telecomunicaciones tecnología que les permite conectar a sus clientes (empresas pequenas y medianas, principalmente) a banda ancha para conexiones de alta velocidad. La empresa dijo que el mercado en México para equipo de acceso a banda ancha crecerá en los siguientes tres años 600%, a más de $250 millones de dólares.

EL EXPERTO

Virus, hackers y gobierno

Joel Gómez Treviño *

El pasado 17 de julio de 2001, el Sircam infectó a miles de computadoras en todo el mundo. Este virus se propaga a través de correos electrónicos, llegando en la forma de un archivo adjunto ("attachment"), disfrazado como un documento de Word o Excel. Al ser ejecutado el archivo, el virus buscaba un archivo al azar en la computadora, luego usaba la lista de contactos del programa de correo de la misma para reenviarse a toda la lista, con el archivo elegido al azar y el propio virus.

El Sircam ocasiona entonces, tres tipos de daños: I) revela información (confidencial, en ocasiones) al enviar a otros algún documento que elija de la PC; II) se esparce fácilmente por e-mail usando la lista de contactos de la computadora infectada, copiando y redistribuyendo nuevos archivos de diferentes usuarios en cada ocasión; y III) el 5% de las ocasiones borra todos los archivos del disco duro y el 3% de las veces llena el disco duro con archivos de texto.

Este virus es de los llamados "gusanos" y se presume que es de origen mexicano, porque en una línea del código del Sircam aparece la leyenda: "[SirCam Version 1.0 Copyright ¬ 2000 2rP Made in / Hecho en - Cuitzeo, Michoacan Mexico]".

El 19 de julio de 2001, en menos de 14 horas, más de 359,000 computadoras en 50 países del mundo fueron atacadas por el gusano (virus) llamado "Red Code". En su momento más crítico, 2,000 nuevos servidores eran infectados cada minuto. El 43% de los servidores infectados fueron estadounidenses. El 19% de los dominios ".net" y el 14% de los dominios ".com" fueron afectados también por el Red Code. Este virus atacó sólo servidores Microsoft y provocaba la "denegación de servicios" de dichos servidores.

Un día antes de que se esparciera el Sircam, un supuesto hacker ruso de nombre Dmitry Sklyarov fue detenido por el FBI en las Vegas, después de dar una exposición en la Conferencia de Hackers "DefCon". Adobe, empresa estadounidense, acusó al programador ruso por haber creado un software capaz de romper la encriptación que protegía uno de sus programas (formatos) más recientes: eBook.

Estas historias, aunque suenen a fantasía o película de ciencia ficción, no son más que la cruda realidad que vivimos desde hace algunos años, a raíz del boom informático.

Es conocido que las autoridades de otros países, en particular las de Estados Unidos, a través del FBI, son pro-activas en la búsqueda, cacería y arresto de ciberdelincuentes, como los ya famosos "hackers" o "crackers". Esto no lo hacen desde un par de años atrás, sino desde hace más de una década. El 15 de enero de 1990, Día de Martín Luther King, el sistema telefónico de AT&T se colapsó gracias a un "super hacker": Kevin Mitnick.

Desafortunadamente nunca se levantaron cargos contra nadie por tal incidente, tal vez porque no se pudo comprobar el ilícito, pero si hubo una impresionante búsqueda policiaca de este sujeto. En 1999 en China, las autoridades arrestaron a 51 personas por "hackear" (violar o penetrar ilícitamente) el sistema de cómputo de los ferrocarriles, justo un mes antes de que sentenciaran a muerte a dos hermanos por robo electrónico bancario.

¿Y el Gobierno Mexicano, qué hace o ha hecho al respecto? Sinceramente, creo que muy poco o tal vez nada. Pero no echemos toda la culpa a las autoridades, porque buena parte de ella es nuestra. En nuestro país vivimos la cultura del "miedo", de la desconfianza al estado de derecho, del pavor a perder imagen o prestigio ante la sociedad.

Es probable que lo primero que haría una empresa mexicana atacada por un hacker, sería ocultar el hecho para no poner en riesgo la lealtad de sus clientes o consumidores. Y si tienen la valentía de denunciar el incidente, probablemente el Ministerio Público o autoridad competente no sabría ni cómo iniciar la investigación. Si las autoridades mexicanas no están capacitadas para tratar con este tipo de cibercriminales, podría ser, tal vez, porque nunca se ha presentado ninguna denuncia por esta clase de atentados, lo cual no significa que no existan o sean pocos.

Si existe legislación sobre delitos informáticos en México, sin embargo, difícilmente podría ser aplicable para sancionar a autores de virus. El Código Penal Federal establece: "al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad se le impondrán de seis meses a dos años de prisión y de cien a trescientos días de multa".

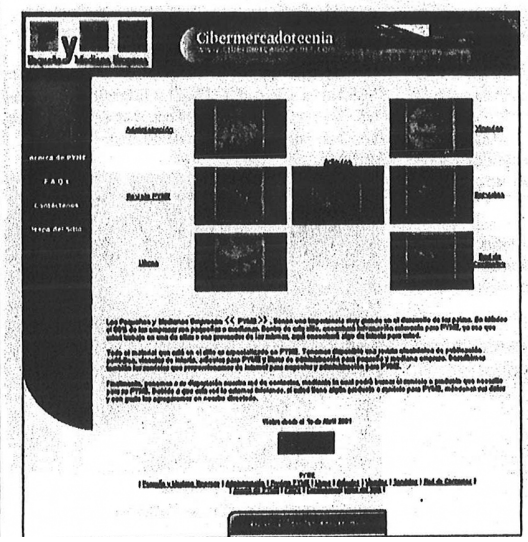
Sería muy complicado encuadrar al tipo penal tales acciones, ya que en primera, de la redacción se desprende que una persona en lo particular modifique, destruya o provoque pérdida de información, actitud típica de un hacker que dirige un ataque específico a una computadora o sistema informático, no así la de un programador de virus, aunque sin duda alguien argumentará que "provocó la pérdida de información de manera indirecta".

Sin embargo, el supuesto que muy pocas veces pudiere darse es el de: "sistemas o equipos informáticos protegidos por algún mecanismo de seguridad". Siendo realistas, en México sólo las grandes empresas tienen, primero la preocupación, y segundo la capacidad económica para instalar firewalls (sistemas de seguridad informática) en sus empresas. La mayoría de las computadoras en nuestro país no cuentan con mecanismos de seguridad. De hecho, no existe una definición en la ley de "mecanismos de seguridad", por lo que no faltará quien opine que un simple password o un antivirus cabe dentro de ese concepto. En resumen, la ley actual es ambigua y se presta a múltiples interpretaciones.

Es labor de todos, legisladores, gobierno, industria y sociedad, el tomar las acciones pertinentes para detener esta ola de terror electrónico. Los legisladores necesitan adecuar el marco legal para tener normas claras y penas severas para los delincuentes informáticos. El gobierno debe preocuparse por capacitar a los cuerpos policiacos y tener unidades especializadas de investigación en materia informática. La industria debe denunciar cualquier ataque e incidente, por pequeño que sea, tanto al CERT México (Computer Emergency Response Team) como a las autoridades competentes. La sociedad debe promover ante todas las instancias la cultura de protección informática y respeto al Estado de Derecho.

Joel Alejandro Gómez Treviño es presidente de la AMDI. (joelgomez@mail.amdi.org.mx)

Microregiones para PyME´s



Ricardo Bolaños

La inminente necesidad de una banca que atienda a las PyME´s y a las microempresas nace de la falta de atención de la banca comercial y de desarrollo a este sector. La PyME por su naturaleza y características, normalmente no es sujeto de crédito. El financiamiento logrado es mediante canales informales.

En el más reciente Foro de Apoyo a las Micro, Pequeñas y Medianas Empresas se habló del desarrollo de la banca popular como alternativa de financiamiento a las PyME´s. Este proyecto, si bien interesante está centrado en grupos de alta marginalidad, por lo que no beneficia a todas las PyME´s.

Este programa también busca contribuir a la descentralización de las grandes urbes mediante la creación de microregiones. Este programa de microregiones (250 en total) tiene como objetivo generar nuevos polos de desarrollo mediante la canalización de recursos de diversas dependencias y organismos. Este programa será medido por el impacto social de cada proyecto.

Dentro de este mismo panel, se forma el Plan Puebla-Panamá, mismo que persigue mejorar el ingreso de dicha región. Esta región que tiene elevados índices de fecundidad, mortalidad infantil, analfabetismo, desempleo y empleo informal hace imperiosa la necesidad de buscar un desarrollo sostenido sustentable e integral.

Finalmente se espera lograr la integración de las PyME´s a cadenas productivas. Este hecho se espera lograrse mediante acciones de desarrollo regional, sectorial y de algunas empresas en particular. Dentro de estos programas están iniciativas de legalización de negocios, desarrollo de proveedores, desarrollo de distribuidores, empresas integradoras y agrupamientos industriales. Para esto se destinará un fondo de fomento para la integración de cadenas productivas.

* *Ricardo Bolaños es consultor de PyME's. (ricardob@pyme.com.mx)*