PUNTO SEGURIDAD, SEGURIDAD EN TIC | NÚMERO 6 | MAYO 2010 | *ISSN EN TRÁMITE* | REVISTA BIMESTRAL

Editorial

La revista **.Seguridad** como un esfuerzo de la DGSCA por crear una cultura de la seguridad en cómputo, vuelve con la publicación de su número 6.

Esta edición es dedicada a los **Delitos Cibernéticos**. Debido al auge de las tecnologías, los criminales no pierden la oportunidad de aprovecharse, es entonces cuando la ley debe actuar a favor de los usuarios. Al leer las páginas de esta revista, te podrás enterar del riesgo que pueden correr los menores en Internet además de cómo protegerlos. Se presentan también artículos relacionados con la legislación en delitos cibernéticos en México, los derechos de autor y otro más sobre los acuerdos internacionales en esta materia.

Como siempre, deseamos que la información te resulte útil y que puedas aplicar nuestras recomendaciones para que te encuentres alerta mientras navegas en Internet

Rocío del Pilar Soto Astorga
Departamento de Seguridad en Cómputo

Elsa Díaz Coria

Es ya tan cotidiano hacer uso de la informática que poco nos detenemos a pensar sobre la importancia que tienen los programas de cómputo para que equipos y cientos de procesos digitales funcionen.

Todas las operaciones y comunicaciones que establecemos a través de nuestras PC´s o teléfonos celulares, las funciones automatizadas de maquinaria y equipos actuales y, en general, todos los dispositivos denominados inteligentes, trabajan a través de la aplicación de algún tipo desarrollo de software[1]; lo mismo ocurre con todo lo que hacemos a través de Internet. De hecho, el mundo digital depende de la constante evolución de los programas de cómputo.

El software [1]es un bien intangible y forma parte de las creaciones patrimoniales que están protegidas en el mundo a través de los derechos de Propiedad Intelectual; en nuestro país los desarrollos de software son protegidos a través de la figura de Derechos de Autor.

La Ley Federal del Derecho de Autor define como programa de cómputo o software a *"la expresión original en cualquier forma, lenguaje o código, de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica."*

El Derecho de Autor está regulado por el Estado Mexicano a través del Instituto Nacional del Derecho de Autor (INDAUTOR) quien protege las obras de los creadores y de su derecho a decidir qué destino y uso se da a su obra. www.indautor.gob.mx

Las leyes de Derecho de Autor tipifican como ilegal el uso no autorizado de trabajos creativos -los relacionados con las artes como literatura, música, cine, etc. y en la tecnología a los programas de cómputo; a este delito se le denomina comúnmente como piratería y se considera un delito grave. La piratería se comete en cualquier circunstancia en la que se haga réplica o uso de trabajos protegidos por sus autores sin su autorización, aún cuando en ello no existan objetivos de lucro. El

[1] Información documentada a través de **PiensaANTESdeCOPIAR**, (www.piensaantesdecopiar.com). Las publicaciones de esta página están disponibles para todos y pueden ser consultadas y descargadas de manera gratuita. **PiensaANTESdeCOPIAR**, forma parte de un programa educativo promovido por la BSA (Business Software Alliance) que es la principal organización dedicada a promover un mundo digital seguro y legal.

intercambio de trabajos, archivos o documentos físicos o de ambientes digitales es una de las formas de uso ilícito de estos bienes.

La piratería de software

Los medios digitales facilitan el acceso a la reproducción de cientos de programas de cómputo que se encuentra protegidos ante derechos de autor. El software comercial está protegido bajo esta figura.

El uso de software comercial está amparado a través de una licencia que otorga el fabricante a quien adquiere sus programas. En esta licencia se expresa la capacidad y límites de uso que tiene cada producto de software. Los usuarios deben de apegarse a estas observaciones para no incurrir en un ilícito.

Entre las formas más comunes en las se hace un uso ilegal de los programas de cómputo están:

- Realizar copias de discos de programas de software para venta o distribución gratuita.
- Comprar copias ilegales de software.
- Instalar software prestado.
- Instalar en más de un equipo un programa de cómputo para el cual solamente se tiene una sola licencia de uso.
- Colocar en línea copias de programas de software.
- Descargar programas de software a través de una red de intercambio de archivos Punto a Punto (en inglés se conoce como *peer-to-peer* P2P).

Al hacer un uso distinto a lo que las licencias de software señalan se comete un acto ilegal. Además se corren riesgos en términos de seguridad informática.

Los sitios de descargas gratuitas en la Web y los discos con software ilegal que se venden en el comercio informal están relacionados con la propagación de virus maliciosos que afectan la integridad de los equipos de cómputo y son capaces de vulnerar la información personal. Esta es una de las vías que la delincuencia informática ha encontrado para cometer fraudes financieros y otros delitos, en donde el daño es contra el patrimonio de los usuarios.

Más información sobre uso de software legal www.bsa.org/mexico

Sergio Andrés Becerril López

La concentración de la información personal en puntos centrales (como oficinas de gobierno, hospitales y escuelas) nos ha hecho considerar las posibles implicaciones de un acceso no autorizado a la misma. En efecto, estos lugares cuentan con toda nuestra información (así como la de muchas otras personas), y la creación de controles para su uso – desde algo trivial como una cerradura hasta medidas de destrucción segura de papeles – es necesaria para asegurar la privacidad de nuestros datos.

El advenimiento de redes de datos, en particular Internet, así como la creciente digitalización de nuestra información, aumenta aún más el riesgo de que dicha información sea comprometida. Aun considerando todas las posibles medidas de seguridad en los sistemas que acceden a los datos, es evidente que una persona autorizada siempre podrá consultar nuestra información. Y precisamente ahí recae un problema fundamental - ¿quién, exactamente, debería estar autorizado?

Un caso clásico, por ejemplo, es el gobierno. Dependiendo de la perspectiva, inclinación política e intereses de la persona a quien se le pregunte, el gobierno debería o no ser una entidad con la habilidad de utilizar la información de la población a la que representa. En este aspecto, así como entre personas, los países tradicionalmente han diferido, y la creación de acuerdos internacionales permite una regularización que es imprescindible para el desarrollo de herramientas y tecnologías legalmente estables.

Ciertamente, el tema no es nuevo, múltiples tratados de derechos humanos reconocen a la privacidad como un derecho. Específicamente, la Declaración Universal de los Derechos Humanos de 1948 declara que:

Nadie deberá estar sujeto a interferencias arbitrarias con su privacidad, familia, hogar o correspondencia, ni a ataques a u su honor o reputación. Todos tienen el derecho de protección bajo la ley de tales interferencias o ataques.

Más recientemente, la Organización de Estados Americanos (a la que pertenece México) proclamó en 1965 la Declaración Americana de Derechos y Obligaciones del hombre, en la cual se demanda la protección de múltiples derechos humanos, incluyendo la privacidad. Es claro entonces que esta situación ha estado en la mente del hombre por años.

Lamentablemente el avance en este rubro es lento y en algunos sectores resulta simplemente imposible. No existe legislación específicamente diseñada para proteger la privacidad de los datos; los avances en el sector se han obtenido al incluir apartados que especifiquen aspectos de privacidad que deben ser considerados a la hora de aplicar la legislación en cuestión.

En esencia, no existe un esfuerzo por definir la privacidad *per se*, sino delinear los límites de otros acuerdos en el aspecto de los datos personales.

Un ejemplo importante se está dando en la generación de ACTA. El Acuerdo Comercial Contra Falsificaciones (*Anti-Counterfeiting Trade Agreement*) la cual, es una legislación que busca "establecer estándares internacionales de aplicación de derechos de propiedad intelectual" en los países participantes, como respuesta "al incremento en comercio internacional de bienes falsificados y obras pirateadas protegidas por *copyright* ".

Evidentemente, esta legislación no tiene como objetivo la preservación de la privacidad de ninguno de los involucrados, sin embargo, sí define específicamente qué medidas tomar para evitar la violación de derechos de autor. Estas medidas incluyen el intercambio de información entre agencias policiacas de los diferentes países miembros, legislación que obligue a los Proveedores de Servicio de Internet (ISPs) a brindar datos de sospechosos sin necesidad de órdenes judiciales, etc.

Es evidente que este tipo de provisiones son peligrosas para la privacidad de la información de todos los que utilizamos Internet. Por ello, varios grupos internacionales han ejercido presión sobre el comité de ACTA para que incluyan restricciones bien delineadas con el objetivo de salvaguardar los datos privados de las personas involucradas. Es en parte debido a la original falta de consideración acerca de la privacidad de los datos que ACTA ha sido rechazada en su iteración actual, principalmente por organismos europeos – el parlamento de la Unión Europea contó con 663 votos en contra el 10 de Marzo de 2010 con 13 a favor.

Los países participantes en ACTA incluyen a los miembros de la Unión Europea, Estados Unidos de América, Japón, Canadá, México, y otros.

Probablemente los principales avances en privacidad referentes específicamente a información digital son, la Convención para la Protección de Individuos con respecto al Procesamiento Automático de Datos Personales (Consejo de Europa, 1981) y los Lineamientos que Rigen la Protección de la Privacidad y Transporte de Flujos de Datos de Información Personal (OECD, 1980). Aunque tienen ya 30 años de antigüedad, estos dos documentos han establecido las bases para la protección de la información digital en múltiples leyes internacionales. Ninguno es un estatuto legal, sino más bien una serie de acuerdos diseñados para estimular la protección de los datos privados.

En esencia, estos documentos (así como los que se han basado en ellos) requieren que la información sea:

- Obtenida legal y justamente
- Utilizada solo para el propósito originalmente especificado

- Adecuada, relevante y no excesiva a su propósito
- Correcta y actualizada
- Accesible al sujeto (dueño de la información)
- Almacenada de manera segura;
- Destruida una vez que haya cumplido su propósito

La OECD (Organización para Cooperación y Desarrollo Económico, *Organisation for Economic Co-Operation and Development*) cuenta con 30 países miembros entre los que se encuentra México.

Referencias:

http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559062&als[theme]=Data%20Protection%20and%20Privacy%20Laws
http://privacy.org/
http://www.michaelgeist.ca/content/view/3660/125/
http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html
http://www.euractiv.com/en/health/meps-defy-commission-internet-piracy-agreement-news-326215
http://www.laquadrature.net/en/european-privacy-protection-authority-condemns-acta

Jorge Christian Durán Lara

Muchos de nosotros podemos recordar cómo era cursar los estudios de primaría, secundaria, medios superiores y hasta superiores sin una conexión a Internet, una como a la que hoy en día tenemos acceso cada uno de nosotros y más impresionante aún, cada uno de nuestros niños. Era muy común acudir a las bibliotecas, libros o material de consulta. En esta primera década del siglo XXI hemos tenido a nuestro alcance una cantidad casi infinita de información a través de la web, y es muy cierto que se puede encontrar información confiable e información sin valor alguno. No obstante nos hemos puesto a pensar ¿Quiénes son las personas más desprotegidas y vulnerables del ventajoso y al mismo tiempo desventajoso mundo de Internet?

Es conveniente pensar por un momento cuál es el uso que le damos al Internet actualmente. Por mencionar algunos usamos el correo electrónico, hacemos búsquedas en línea, utilizamos redes sociales, practicamos el comercio electrónico, intercambiamos mensajes escritos y de voz, visualizamos videos e imágenes, entre otros. Sin embargo, todos los anteriores no son exclusivos de los adultos, es decir, cualquiera los puede usar, incluyendo menores de edad y particularmente los niños.

Los niños y adolescentes utilizan el Internet, en su mayoría, para complementar sus estudios, interactuar en redes sociales, utilizar mensajería instantánea, establecer conferencias de audio y video, jugar videojuegos, ver videos e imágenes y, escuchar música en línea.

Gran parte de estas actividades también las llevamos a cabo los adultos, sin embargo, ¿alguna vez nos hemos puesto a pensar cuáles son las amenazas que corren los más pequeños del hogar al utilizar estas nuevas herramientas tecnológicas?

Los niños y adolescentes podrían estar en riesgo de experimentar algunos de los siguientes peligros.

- Exposición inadvertida de contenido no apropiado en forma de imágenes, videos o contenido. Los ejemplos más ilustrativos son los sitios de pornografía y violencia.
- Contacto con vicios como pueden ser las drogas y juegos en línea.
- Encuentro con pedófilos en salas de *chat*, mensajeros instantáneos, por correo electrónico y redes sociales. Y más grave aún que se presente un encuentro cara a cara.
- Intimidación y acoso en línea.
- Revelación de información personal y privada.
- Infección por programas espía y virus.
- Comercialismo excesivo por medio de anuncios de productos, servicios y sitios web.
- Descargas ilegales como pueden ser archivos de música y video protegidos por derechos de autor.

Es muy posible que ahora algún padre de familia quiera llegar a su casa y apagar la computadora de sus hijos directamente y sin preguntar; o al menos eliminar la conexión a Internet. Estudios afirman que dichos riesgos son verdaderos pero existen formas de controlarlos mediante tareas simples y sanas que los padres de familia pueden poner en práctica para evitar que sus hijos sean un blanco más. Algunos consejos prácticos para los padres son los siguientes:

- Como figura paterna debes ver a Internet como una herramienta para el buen desarrollo de tu hijo y no descalificarlo bajo la falsa idea de que solo encontrarán cosas malas. Toma conciencia de que es un instrumento que lo ayuda en sus estudios, a acortar distancias y aprovechar mejor el tiempo.
- Debes educar a tus hijos pequeños para que naveguen con una persona adulta presente. Si el chico ya es un cibernauta bien formado será difícil que te acepte, en ese caso inténtalo buscando sitios que puedan ser de su interés y muéstraselos para que poco a poco pueda aceptar tu presencia mientras navega.
- Es muy recomendable utilizar filtros de seguridad para limitar la navegación de tus hijos. Algunos navegadores poseen esta característica. También es posible obtener un filtrado de sitios a través de tu proveedor de servicios de Internet.
- Así como en la vida real educas a tu hijo para que no hable ni le preste atención a gente extraña o desconocida, debes instruirlo para que se comporte de la misma manera en el mundo digital. En los mensajeros instantáneos, correo electrónico y redes sociales existen también esas personas desconocidas con intensiones maliciosas. Se han dado casos en México de que el pedófilo[2] logra envolver a los menores en su juego para que estos posen semidesnudos frente a una cámara y ellos puedan verlos, posteriormente el pedófilo insiste en un encuentro personal, en algunas ocasiones estos menores acceden y ocurre lo peor. A la práctica de contactar al menor por Internet y envolverlo en un juego de confianza se le conoce como *grooming*.
- Trata de educar a tu hijo para solo utilice el Internet en un horario definido, recomendablemente cuando estés tú, al igual crea en él la costumbre de utilizarlo por un período razonable de tiempo.
- Como padre tienes la tarea de ubicar físicamente la computadora en una zona del hogar donde tengas fácil acceso o inclusive donde los niños puedan ser constantemente inspeccionados, aunque sea de reojo.
- Si tu caso es que no puedes estar en casa cuando tu hijo navega, te sugiero que lo dejes utilizar una cuenta de usuario limitada en el equipo para navegar, además de que revises el historial de navegación periódicamente. A continuación en la Figura 1 se muestra como crear una cuenta limitada mientras en las Figuras 2 y 3 se muestra como consultar el historial en Internet Explorer, ambos sobre Windows 7.

[2] Sujeto adulto que experimenta atracción sexual o erótica hacia niños o adolescentes

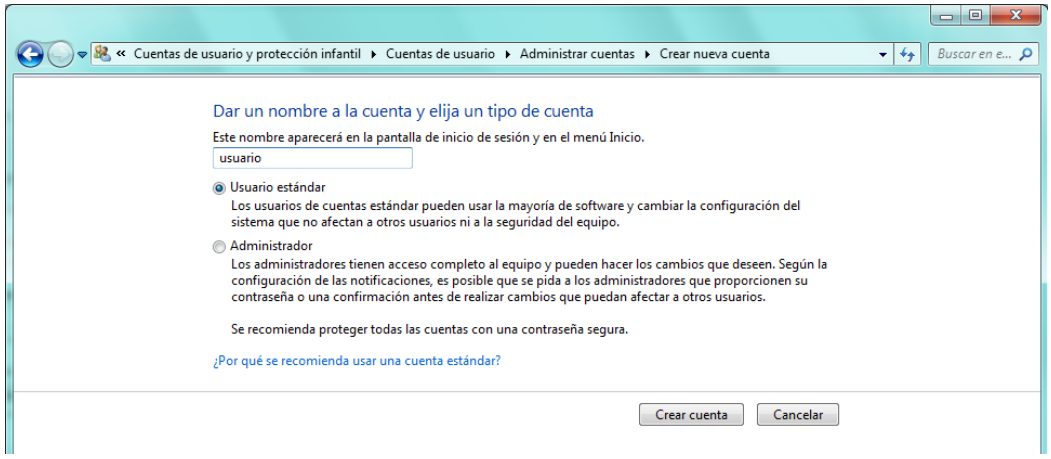

Figura1. Creación de una cuenta limitada en Windows 7.

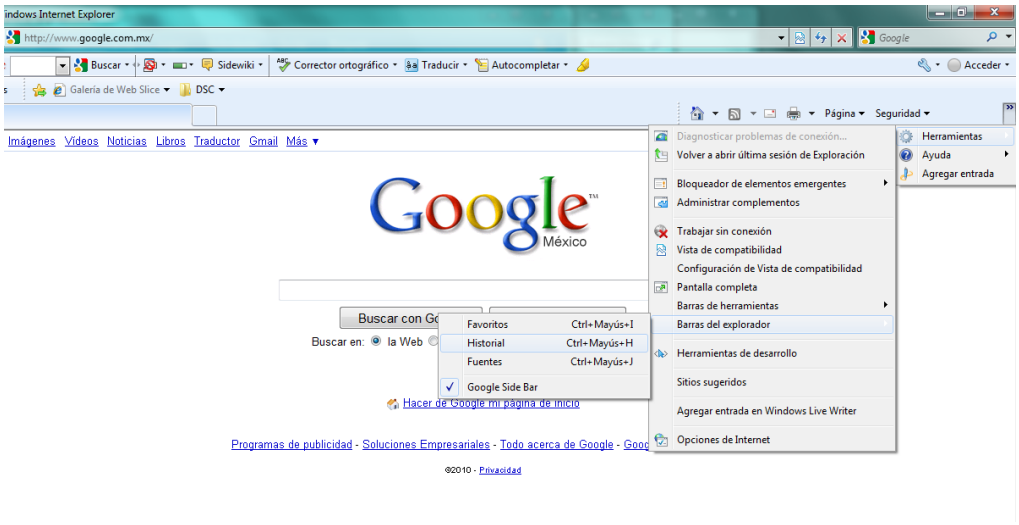

Figura2. Menú para acceder al historial de Internet Explorer 8.

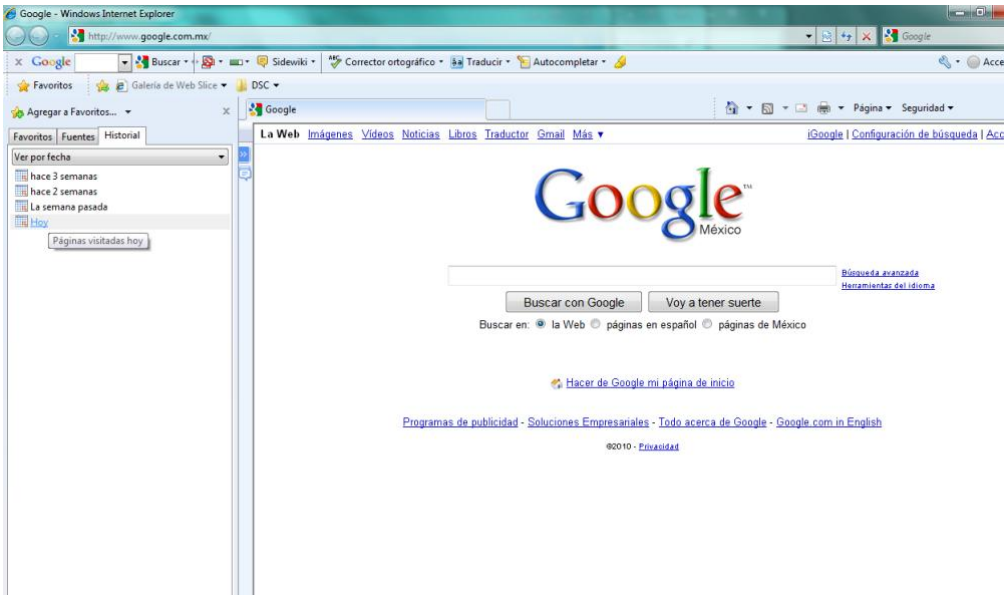

Figura3. Aspecto de la barra historial, parte derecha de la imagen.

Las figuras paternas del hogar deben tomar precauciones y mantenerse informados de las amenazas y peligros para los menores. En la web existen también sitios de odio generalizado que pueden ser visitados por los niños, los cuales les transmiten ideas racistas y de odio hacia ciertos sectores de la población; por supuesto no nos gustaría que en las escuelas exista discriminación alguna por parte de los mismos compañeros de clase. Otro ejemplo de riesgos se da por medio de los mensajes vía celular, por los cuales los menores pueden enviarse toda clase de mensajes. Se ha observado una práctica que los especialistas han catalogado como *sexting*, esta consiste en el envío de mensajes de texto con contenido erótico, una variante más grave aún se presenta cuando los mensajes se envían con fotos y videos eróticos.

A pesar de que los delitos de pornografía infantil están tipificados y son perseguidos por la Policía Cibernética de la SSP federal, las entidades encargadas de juzgarlas no poseen el conocimiento para catalogar las acciones que el atacante ha desempeñado a través de Internet.
Por todo esto te recordamos que debes permanecer informado, no solo de los beneficios que Internet ofrece, sino también de las amenazas que existen. Para poder acceder a contenido útil de seguridad informática se recomienda visitar la sección de usuario casero del UNAM-CERT, esta entidad también cuenta con material dirigido a los niños.

http://www.seguridad.unam.mx/usuario-casero/

Referencias:

http://www.consumer.es/web/es/tecnologia/internet/2008/11/12/180713.php
http://www.imbiomed.com.mx/1/1/articulos.php?method=showDetail&id_articulo=53603&id_seccion=3348&id_ejemplar=5424&id_revista=17
http://www.eldeber.net/internetninos.htm
http://www.scielo.cl/scielo.php?pid=S0370-41062005000200006&script=sci_arttext
http://www.vidadigitalradio.com/consejos-uso-internet-ninos/
http://www.terra.es/tecnologia/articulo/html/tec16579.htm
http://www.munimadrid.es/UnidadWeb/Contenidos/Publicaciones/TemaEconomia/GuiaNuevasTecnologias/Tictac-Chiqui.pdf
http://arstechnica.com/tech-policy/news/2010/03/online-presence-of-hate-terrorist-groups-up-20.ars
http://es.wikipedia.org/wiki/Sexting
http://www.getsafeonline.org/nqcontent.cfm?a_id=1124
http://mx.news.yahoo.com/s/21032010/90/n-mexico-pederastas-refugian-internet-atraer-menores.html

Criminalística Aplicada en la Seguridad de Tecnologías de Información y Comunicaciones

Oscar Manuel Lira Arteaga

En nuestro país, la falta de aplicación de procedimientos de investigación forense en conductas delictivas que utilizan como medio las Tecnologías de la Información y Comunicación (TIC's) acordes a las normas de investigación establecidas por organizaciones internacionales tales como la SWGDE3 y apegadas a la legislación de nuestro país, provocan que la persecución de éste tipo de delitos no sea resuelta en todos los casos de manera exitosa por los actores que intervienen en la maquinaria de procuración de justicia (Jueces, Agentes del Ministerio Público, Peritos y Policía Investigadora). Sin embargo, es importante señalar que si bien delitos como la pornografía infantil, fraude, extorsión, falsificación, robo de información, alteración de información, espionaje, secuestro, amenazas, entre otros, que actualmente utilizan las nuevas tecnologías como medio, son delitos bien definidos en nuestras leyes y han existido en la mayoría de los casos mucho antes de la invención de los medios de comunicación, procesamiento y almacenamiento de datos de manera digital en medios magnéticos, electrónicos u ópticos.

En el caso particular en nuestro país, existen vacíos legislativos importantes específicamente en el control de los proveedores de servicios de Internet y fabricantes de programas de cómputo, los cuales imposibilitan en algunos casos a los investigadores la obtención de la evidencia suficiente para la persecución y aplicación del castigo a los responsables directos e indirectos de lo que se empieza a conocer mundialmente como ciberdelitos.

En nuestro país debemos de identificar a estos ciberdelitos como "CONDUCTAS DELICTIVAS COMETIDAS A TRAVÉS DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES" y que se identifican como fraude, sabotaje, robo, acceso no autorizado a sistemas informáticos, entre otras en el Código Federal de Procedimientos Penales de nuestro país.

En relación con el desarrollo y utilización de programas de cómputo y sistemas operativos, es de considerar que desde su concepción implican altos riesgos de estabilidad y seguridad de los datos que procesan dando como resultado un alto nivel de vulnerabilidad que al cabo del tiempo se traduce en pérdidas millonarias a los consumidores finales ya sea a consecuencia de la pérdida de su información o por los altos costos de mantenimiento y soporte de las aplicaciones informáticas.

De lo anterior es fácil comprender que en la actualidad los consumidores no cuentan con la transparencia y elementos suficientes por parte de los fabricantes de programas de cómputo para poder realizar la elección de una aplicación con base en sus propios estándares de calidad y seguridad y no con base en los propios de cada fabricante.

[3] Grupo de Trabajo Científico en Evidencia Digital (SWGDE, Scientific Working Group on Digital Evidence) http://68.156.151.124/

En éste momento la pregunta obligada sería:

¿De dónde vienen o qué factores propician los delitos cometidos a través de tecnologías de la información y comunicaciones? y ¿Cómo se combaten éste tipo de conductas?

Bien, ante la constante evolución, tanto de la sociedad como de su entorno ideológico, económico, social y tecnológico, surgen distintas tendencias y conductas delictivas cometidas por mentes criminales que de alguna manera encuentran la forma de adaptarse y aprovecharse de la candidez del momento de su época con la finalidad de obtener un beneficio y violentando las garantías individuales de terceras personas. En auxilio a las autoridades responsables de la procuración y aplicación de justicia surge una ciencia, la cual busca mediante la aplicación de metodología aplicada a la investigación, reconstruir la verdad histórica de los hechos después que se ha cometido un "presunto acto delictuoso", esta es la **Criminalística**.

Sin embargo, el Criminalista forma parte de un equipo de trabajo dependiente, que partiendo de las circunstancias de los hechos en torno a un delito, necesitará de la pericia de los involucrados tanto en materia legal como en ciencias físicas y naturales. Al día de hoy, los medios y los métodos utilizados para cometer un delito, han evolucionado a la par de la sociedad y hoy más que en otras épocas, las nuevas tecnologías y su capacidad para procesar, comunicar y almacenar de manera masiva datos e información e inclusive controlar sistemas vitales, han sido testigos del nacimiento de un nuevo perfil criminal que las utiliza para burlar las medidas de seguridad implementadas incluso por los corporativos que nunca pensaron estar al alcance de un criminal. Sin embargo, es importante no perder la objetividad del delito, esto es, el hecho de poder cometer un fraude financiero mediante la falsificación de un documento con técnicas de impresión serigráficas o a través de la red, aprovechando las diferentes vulnerabilidades de los sistemas electrónicos bancarios, no hace diferencia en cuanto a la tipificación del delito: fraude. En otras palabras, el robo, el engaño, el asesinato, explotación y prostitución de menores, entre otros, han existido seguramente desde que nuestros primeros antepasados formaron grupos sociales en los cuales se albergaron los primeros individuos con mentes criminales.

Desafortunadamente, nuestro país no ha sido la excepción en relación al incremento de conductas delictivas cometidas mediante la utilización de TIC's sobre todo en relación a secuestros, extorsiones, falsificación y fraudes financieros cometidos a través de Internet. De lo anterior, se desprende la necesidad de tomar en cuenta los fundamentos de esta rama de la ciencia, con la finalidad de establecer una nueva especialidad criminalística dedicada al estudio, investigación y esclarecimiento de actos probablemente delictivos que utilizan como medio y objeto las TIC's. Con este planteamiento se busca conjuntar los elementos necesarios para que el Perito en esta materia se encuentre capacitado para dar fundamento técnico acorde a la legislación de nuestro país para las posibles evidencias que, en su oportunidad, serán presentadas por el Agente del Ministerio Público ante un Juez.

Para lograr lo anterior, será necesario estandarizar metodologías y técnicas de investigación de éste tipo de delitos así como aplicar cambios legislativos que permitan no solo definir delitos que se cometen a través de estos medios, sino establecer los mecanismos para controlar los medios que sirven de enlace o que permiten la comunicación entre un dispositivo emisor y un receptor. Es también necesario definir a los responsables de su administración para que la información que queda registrada y que permite establecer el origen y destino de una comunicación a través de una red informática, pueda ser almacenada con la finalidad de que los responsables de una investigación cuenten con los elementos necesarios para localizar al responsable de cometer un acto delictivo. En éste momento cabe aclarar que, en relación a la telefonía móvil y fija, hoy se cuenta con lo necesario para ser muy eficientes en la investigación de delitos cometidos por éstos medios gracias a los cambios en la Ley Federal de Telecomunicaciones en donde por ejemplo (en el artículo 44) los proveedores de servicios de comunicaciones deben almacenar la información de conexión por un periodo de 12 meses, identificar la posición geoestacionaria de dispositivo móvil y en su caso brindar la información a la autoridad correspondiente en un plazo no mayor a 72 horas, entre otros puntos. En la Figura 1 y con la finalidad de establecer de manera clara lo antes expuesto, presentamos una tabla de los delitos que se castigan en nuestro país con fundamento al Código Penal Federal así como su relación con los medios utilizados (códigos maliciosos, ingeniería social, *phishing*, *pharming*, entre otros).

Figura 1.

De la Figura 1. se desprende la necesidad por parte de maestros, abogados, ministerios públicos y jueces, de romper paradigmas en relación a temas relacionados con las nuevas tecnologías, e intentar comprender la relación entre el medio utilizado para cometer la conducta delictiva, la definición de la conducta delictiva y después su identificación como un delito castigado por nuestras leyes.

DIRECTORIO

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

Dr. José Narro Robles
Rector

Dr. Sergio Alcocer Martínez de Castros
Secretario General

DIRECCIÓN GENERAL DE SERVICIOS DE
CÓMPUTO ACADÉMICO

Dr. Ignacio de Jesús Ania Briseño
Director

M. en C. Ma. de Lourdes Velázquez Pastrana
Directora de Telecomunicaciones

Ing. Rubén Aquino Luna
Subdirección de Seguridad de la Información
UNAM-CERT

2010 D.R. Universidad Nacional Autónoma de México
Revista elaborada por la
Dirección General de Servicios de Cómputo Académico

CRÉDITOS

PUNTO SEGURIDAD, DEFENSA DIGITAL

M en I. Rocío del Pilar Soto Astorga
Edición

Sergio Andrés Becerril López
Jorge Christian Durán Lara
Oscar Manuel Lira Arteaga
Elsa Díaz Coria
Colaboraciones

Ing. Rubén Aquino Luna
Subdirección de Seguridad de la Información
UNAM-CERT

Rocío del Pilar Soto Astorga
Rubén Aquino Luna
Revisión de Contenidos

Act. Guillermo Chávez Sánchez
Coordinación de Edición Digital

Diana Chávez González
Coordinación de la Producción Digital

Lic. Lizbeth Luna González
Dolores Montiel García
L.D.C.V. Carolina Silva Bretón
Diseño Gráfico

Liliana Minerva Mendoza Castillo
Formación

2010 D.R. Universidad Nacional Autónoma de México
Revista elaborada por la
Dirección General de Servicios de Cómputo Académico