DELITOS INFORMÁTICOS:

SU CLASIFICACIÓN Y UNA VISIÓN GENERAL DE LAS MEDIDAS DE ACCIÓN PARA COMBATIRLO

Jesús Alberto Loredo González
Co autor: Aurelio Ramírez Granados
FCFM-UANL
Facultad de Ciencias Físico Matemáticas
Universidad Autónoma de Nuevo León
San Nicolás de los Garza, Nuevo León, México

Resumen:

Con el presente artículo se busca dar a conocer los principales delitos informáticos y los riesgos que estos generan para la sociedad, las empresas y los gobiernos. Asimismo, de las principales leyes que existen en México para tipificar este tipo de delitos y de los acuerdos internacionales de los países han firmado y desarrollado con el fin de combatir este problema.

Palabras claves:

ciberdelincuencia, marco legal, malware, seguridad, tecnología

Delitos informáticos

Antecedentes

Los antecedentes de los delitos informáticos van a la par del desarrollo de las tecnologías de la información. Con el desarrollo de la tecnología, la sociedad se ha visto en un panorama de avance y desarrollo en todas sus áreas; por desgracia, la delincuencia también se ha beneficiado de esto.

Entre los beneficios que ofrece el uso de redes de comunicación a los delincuentes se encuentran: la capacidad de cometer delitos en y desde cualquier parte del planeta, velocidad, gran cantidad de víctimas potenciales y anonimato, entre otros.

Uno de los primeros y más importantes ataques en la historia de Internet se remonta a CREEPER en 1971, escrito por el ingeniero Bob Thomas, es considerado el primer virus informático que afecto a una computadora el cual mostraba un mensaje en los equipos infectados, el cual, si no causaba daño alguno, fue la base para el desarrollo de ataques posteriores con pérdidas multimillonarias, como se menciona en el sitio web de la INTERPOL [1] "se estima que en 2007 y 2008 la ciberdelincuencia tuvo un coste a escala mundial de unos 8.000 millones de USD" [2].

Definición

Es conveniente identificar de forma clara lo que se entiende por delito informático. Existen diversas definiciones respecto; un ejemplo es la definición de Camacho Losa, citada por Leyre Hernández, quien considera como delito informático: “toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor aun cuando no perjudique de forma directa o inmediata a la víctima y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas” [3].

Otra definición destacable es la establecida en el Código Penal para el Estado de Sinaloa en su Artículo 217 [4]:

I. Use o entre a una base de datos, sistema de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información; o

II. Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red [4].

Comete delito informático, la persona que dolosamente y sin derecho:

Una definición más simple que se propone es la siguiente: *Delito informático es el uso de cualquier sistema informático como medio o fin de un delito.* De esta manera se abarcan todas las modalidades delictivas de acuerdo al marco legal de cada país; para esto es conveniente definir qué es un sistema informático.

De acuerdo con el Convenio sobre la Ciberdelincuencia adoptado en Budapest, en 2001: “Por sistema informático se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa." [5]

Esta definición abarca no solo a las computadoras, sino a otros tipos de dispositivos como Data Centers, módems y cualquier otro sistema que permita la ejecución de un programa y/o manipulación de datos.

Por otra parte, la guía del taller de Prevención contra el Delito Cibernético de la Secretaria de Seguridad Pública (SSP) define el delito cibernético como: “Actos u omisiones que sancionan las leyes penales con relación al mal uso de los medios cibernéticos.” [6]

Tipos de delitos informáticos

Los delitos informáticos abarcan una gran variedad de modalidades como se mencionan en la web de la INTERPOL y se enlista a continuación:

- Ataques contra sistemas y datos informáticos
- Usurpación de la identidad
- Distribución de imágenes de agresiones sexuales contra menores
- Estafas a través de Internet
- Intrusión en servicios financieros en línea
- Difusión de virus
- *Botnets* (redes de equipos infectados controlados por usuarios remotos)
- *Phishing* (adquisición fraudulenta de información personal confidencial)

Sin embargo no son los únicos, también existen riesgos relacionados con el uso de las redes sociales y acceso a todo tipo de información tales como:

- Acceso a material inadecuado (ilícito, violento, pornográfico, etc.)
- Adicción - Procrastinación (distracciones para los usuarios)
- Problemas de socialización
- Robos de identidad
- Acoso (pérdida de intimidad)
- Sexting (manejo de contenido erótico)
- *Ciberbullying* (acoso entre menores por diversos medios: móvil, Internet, videojuegos, etc.)
- Cibergrooming (método utilizado por pederastas para contactar con niños y adolescentes en redes sociales o salas de chat)

Delincuentes y objetivos

Así como existen una gran cantidad de delitos relacionados con el uso de sistemas informáticos, también existe una amplia gama de delincuentes. Se definirán dos clasificaciones para estos basado en sus conocimientos técnicos.

Por un lado tenemos a los expertos en seguridad informática a los que es común referirse con término de "*hacker*". Una definición del término es la que brinda el Oxford English Dictionary (OED): "Una persona que usa su habilidad con las computadoras para tratar de obtener acceso no autorizado a los archivos informáticos o redes." [7]

En primera instancia, esta definición asocia una conducta delictiva a todo *hacker*; pero en el ámbito informático tales se clasifican en dos tipos:

- *White hat hacker*: Se dedican a buscar vulnerabilidades en redes y sistemas sin realizar un uso malicioso de estas y posteriormente reportando los fallos. Las formas en que se monetiza esta actividad son varias: se busca reputación en el sector, sistema de recompensas, trabajando como consultor o responsable de seguridad en una compañía.
- *Black hat Hacker*: individuos con amplios conocimientos informáticos que buscan romper la seguridad de un sistema buscando una ganancia, ya se obtener bases de datos para su posterior venta en el mercado negro, venta de "xploits" (vulnerabilidades de seguridad), robo de identidad, cuentas bancarias, etc.

Otro tipo de delincuentes que son aquellos que hacen uso del anonimato en internet con el fin de realizar conductas poco éticas: acoso, cyberbullying, estafas, pornografía infantil, turismo sexual, etc.

Herramientas

Los delincuentes con conocimientos técnicos desarrollan herramientas que les permitan llevar a cabo sus objetivos, a este tipo de herramientas se les conoce como Malware y de acuerdo con el glosario en línea de Panda Security: "Cualquier programa, documento o mensaje, susceptible de causar perjuicios a los usuarios de sistemas informáticos. Contracción de las palabras *malicious software* (software malicioso)." [8]

En Internet, este tipo de amenazas crecen y evolucionan día a día, por lo que las compañías de antivirus trabajan constantemente en sus laboratorios, ofrecen soluciones dirigidas a diferentes tipos de usuarios tales como hogares y oficinas pequeñas, o al sector industrial y empresarial.

Un ejemplo de la protección que se ofrece es la siguiente lista de las principales categorías de riesgo para las cuales la firma antivirus alemana AVIRA ofrece protección:

- *Adware* (muestra contenido publicitario en las actividades del usuario)
- *Spyware* (Recopila datos personales y los envía a un tercero sin consentimiento del usuario)
- Aplicaciones de origen dudoso (programas que pueden poner en riesgo el equipo)
- *Software* de control *backdoor* (Permiten el acceso remoto al equipo)
- Ficheros con extensión oculta (Malware que se oculta dentro de otro tipo de archivo para evitar ser detectado)
- Programas de marcación telefónica con coste (generan cargos en la factura de manera fraudulenta)
- Suplantación de identidad (*phishing*)
- Programas que dañan la esfera privada (*Software* que mermar la seguridad del sistema)
- Programas broma

- Juegos (distracción en el entorno laboral)
- *Software* engañoso (hacen creer el usuario que esta vulnerable y lo persuaden para comprar soluciones)
- Utilidades de compresión poco habituales (archivos generados de manera sospechosa) [9]

Riesgo social

Desde siempre las relaciones sociales han sido un punto clave en la vida de las personas. Tener la facilidad de contactar con cualquier persona en cualquier parte del mundo ha contribuido a la globalización y al mismo tiempo ha generado una serie de riesgos.

Existen una serie de conductas identificadas que ponen en riesgo la integridad física y emocional de los afectados. A continuación se enlistarán algunas de las más graves:

Ciberbullying

Acoso que se da entre menores mediante insultos, humillaciones, amenazas a través de redes sociales u otros medios de comunicación.

Si bien el *bullying* se inició en las escuelas y parques; hoy día se ha expandido a las redes sociales donde no existe la vigilancia de los padres, los menores se ven emocionalmente afectados y sin la confianza de comentar sus problemas.

Sexting

El término hace referencia al uso de móviles para mantener charlas de índole sexual, donde voluntariamente se genera contenido que implique una situación erótica o sexual.

Si bien en ningún momento se obliga a la persona a posar y la mayoría de las veces se busca mantener el anonimato, existe un riesgo de identificación lo que resultaría en serios problemas sociales, de acoso y/o extorsión.

Acceso a material inadecuado

La Internet nos permite acceder a una enorme cantidad de información de todo tipo, normalmente basta con teclear en algún motor de búsqueda lo que nos interesa y en seguida se despliegan miles de resultados. Los proveedores de este servicio siempre buscan mantener fuera de sus resultados el contenido no apto para el usuario. Pero fuera de ese contenido indexado existe otra parte de la red.

Conocida como *Deep Web* (Internet profunda) es el conjunto de sitios que contienen material potencialmente peligroso para el usuario, no solo de índole sexual, también existen, videos *snuff* (grabaciones de asesinatos, violaciones, torturas y otros crímenes reales), mercado negro *online* (tráfico de armas, drogas, trata de personas, etc), contratación de asesinos, no existen límites para la gravedad del contenido que se puede encontrar.

Pornografía infantil

El problema de la pornografía infantil es quizás el más grave que enfrenta la sociedad; las víctimas quedan marcadas de por vida y por daños físicos y/o emocionales. Combatir esto debe ser una tarea de suma importancia para cualquier gobierno.

Los pederastas han hecho uso de las tecnologías de la información por las diferentes ventajas facilitan la realización de esta actividad:

- **Anonimato:** La facilidad de cambiar de identidad dentro de foros en internet dificulta el seguimiento de las acciones de un mismo sujeto.
- **Cifrado:** Herramientas que ofrecen métodos de cifrado (incluso a grado militar) para la información que aseguran que ninguna otra persona tenga acceso, y por tanto pruebas, a menos que se conozca una contraseña.
- **Dificultad de rastreo:** Si bien es posible obtener cierta información acerca de la fecha de acceso, ubicación y dispositivos utilizados, usuarios avanzados pueden hacer uso de programas con los que se pueden falsear estos registros.

Riesgo empresarial

Schneier, 2004, citado por Del Pino: "Si Ud. piensa que la tecnología puede resolver sus problemas de seguridad, entonces Ud. no entiende los problemas de seguridad y tampoco entiende la tecnología". [10] Esto refleja perfectamente el problema de la seguridad informática que se enfrenta todas las organizaciones.

En un ambiente donde los riesgos avanzan a gran velocidad como lo es Internet no existen soluciones de seguridad definitivas, por lo que todas las empresas, sin importar giro, tamaño o ubicación son susceptibles de recibir ataques informáticos. Para brindar un mejor panorama se listará una serie de casos:

PlayStation Network. Abril 2011

En una entrada en el blog corporativo de PlayStation, Patrick Seybold, Sr. Director de la compañía, publicó un comunicado para todos los clientes de los servicios PlayStation Network (PSN) and Qriocity en el cual se explica que información de los usuarios se vio comprometida entre el 17 y 19 de abril de 2011 por una intrusión ilegal y no autorizada en la red de la compañía.

Se mencionan las medias de respuesta que tomo la compañía:

- Desactivación temporal de los servicio
- Contratación de una empresa externa para protección y llevar a cabo una investigación
- Adoptar medidas rápidas para fortalecer la seguridad de la infraestructura
- Asimismo, se proporcionó información para que las personas afectadas permanezcan atentas a los movimientos de sus cuentas para evitar robos de identidad o pérdidas financieras. [11]

Entre la información que se cree fue comprometida se encuentran: nombres, direcciones (ciudad, estado, código postal), país, dirección de correo electrónico y fecha de nacimiento. También se cree estuvieron en riesgo los datos de las tarjetas de crédito de los usuarios.

Stuxnet. Junio 2012

Se cree que Stuxnet puede ser el primer paso hacia una ciberguerra, constituye uno de los virus informáticos más poderosos hasta la fecha. Más que virus se les denomina ciberarmas por su complejidad y la precisión de los objetivos.

Stuxnet fue escrito orientado a los sistemas de control industrial utilizados en tuberías de gas y diversas plantas de energía. El objetivo final es reprogramar los sistemas para obtener el control sobre la infraestructura, para esto se vale de diversos componentes implementados por los programadores aprovechando todo tipo de vulnerabilidades.

Unas pocas semanas después de Stuxnet fue detectado en todo el mundo, una serie de ataques consiguió sacar de operación temporalmente 1,000 de las 5,000 centrifugadoras que Irán tenía destinadas a la purificación de uranio. [12]

En un artículo publicado por el diario estadounidense *The New York Times*, se afirma que el presidente Barack Obama ordenó ataques informáticos contra las instalaciones iraníes de enriquecimiento de uranio, valiéndose del gusano Stuxnet desarrollado por los E.E. U.U. e Israel con el fin de frenar el programa nuclear de Irán. Expertos en informática concuerdan en que el desarrollo de tal arma necesitó de meses de investigación y colaboración entre expertos de diversas áreas, recursos de los que solo un gobierno podría disponer. [13]

Actualmente todas las operaciones de una organización dependen en mayor o menor grado de un sistema informáticos por lo que se vuelven un blanco de ataque para los ciberdelincuentes, estos casos son solo un ejemplo de las consecuencias que podría tener un ataque y revelan la importancia de contar un sistema de seguridad que permita reducir la exposición a este tipo de riesgos.

Marco legal

Normas regulatorias

En México se han dictado diversas leyes para regular y castigar este tipo de delitos, entre las principales se encuentran:

El Código Penal Federal en su Título Noveno referente a la Revelación de secretos y acceso ilícito a sistemas y equipos de informática:

- **Artículo 211 Bis.** A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una **intervención de comunicación privada**, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.
- **Artículo 211 bis 1.** 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 multa. [14]

Al que **sin autorización conozca o copie información** contenida en sistemas o equipos de informática protegidos por algún **mecanismo de seguridad**, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

De igual forma en el Artículo 211 bis 2 a bis 5 se en listan los delitos, y correspondientes condenas, cometidos en equipos informáticos propiedad del Estado, materia de seguridad pública e instituciones que integran el sistema financiero.

Otra regulación existente se encuentra en el Código Penal para el Estado de Sinaloa en su artículo

217, mencionado anteriormente, se establece que al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa [4].

Por último, se mencionará del Código Penal Del Distrito Federal en su Título Décimo Quinto - Capítulo III referente al Fraude:

- **Artículo 231. XIV.** Para obtener algún beneficio para sí o para un tercero, por cualquier medio accese, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la Institución. [15]

Acuerdos internacionales

Estos acuerdos son un primer paso para unificar esfuerzos en contra de estas actividades y si bien existen muchas cosas que mejorar son una buena guía para cualquier Estado que analice el establecimiento de una legislación al respecto.

Convenio sobre la ciberdelincuencia

Firmado en Budapest, el 23 de noviembre de 2001, por los Estados miembros del Consejo de Europa, en cual México participa como observador permanente, se reconoce el problema de la ciberdelincuencia y la necesidad de una cooperativa trasnacional para abordarlo. En el cual se definen diferentes aspectos como:

- Definición de los delitos informáticos
- Medidas que deben adoptar en sus legislaciones cada uno de los países miembros
- Jurisdicción sobre la información
- Facilitar información entre los Estados de ser necesario en alguna investigación

Asimismo, en su artículo 9 se hace mención de los delitos relacionados con la pornografía infantil con el cual se busca clasificar como delito los actos de: producción, oferta, difusión, adquisición y posesión de material pornográfico en el que se involucre un menor en cualquier sistema informático.

Proyecto de Stanford

El Centro Internacional de la Seguridad y la Cooperación (CISAC) de Stanford publicó el Proyecto de Convención Internacional para Mejorar la Seguridad de la Delincuencia en el Ciberespacio y el Terrorismo, conocido como Proyecto de Stanford, con el cual se busca un convenio multilateral entre las naciones en materia de delito informático y terrorismo. Es de destacar los artículos:

- Artículo 6. Asistencia Legal Mutua
- Artículo 7. Extradición
- Artículo 12. Agencia de Protección de la Infraestructura de Información (AIIP)
- Artículo 14. Informes anuales de los Estados Partes [16]

La AIIP como organismo internacional integrado por todos los Estados Partes en calidad de Miembros, actuaría como un eje central para asegurar la ejecución de los objetivos de tal Convenio.

Otros documentos y limitaciones

Existen diversos documentos que reflejan el esfuerzo de diferentes países y organizaciones tal como el Cybercrime Legislation Toolkit de la Unión Internacional de Telecomunicaciones (ITU) que busca dar un marco de referencia para los Estados con el fin crear una legislación eficaz que permita enfrentar estos delitos.

La Ley Modelo de la Commonwealth sobre Delitos Informáticos, que al igual que el Convenio de Budapest, contiene disposiciones sobre material penal, procesal y de cooperativa internacional para sus actuales 54 países miembros [17].

Una de las principales limitaciones que presentan estos acuerdos es la reducida cantidad de países miembros con los que cuenta, a abril de 2010 la Convención sobre el Delito Cibernético del Consejo de Europa tenía el más amplio alcance: ha sido firmada por 46 Estados y ratificada por 26 [18], son los países desarrollados quienes cuentan con la experiencia y los recursos que demanda la implementación de este tipo de acuerdos.

Un vacío legal en países sin las competencias necesarias para la persecución ofrece una oportunidad para los delincuentes quienes pueden causar estragos muchas veces con solo contar con un ordenador y una conexión a internet sin importar mucho donde se encuentre al momento de realizar un ataque.

Medios de persecución

En México la policía cibernética de la Policía Federal Preventiva es la encargada atender los delitos relacionados con las computadoras y atención de

denuncias de delitos sexuales contra menores, para esto cuentan una formación especial que les permita resolver las dificultades que supone perseguir delincuentes por Internet.

Análisis Forense Digital

Una vez que se define e implementa un marco legal, es necesario establecer medidas de persecución y acción con lo que se hace referencia al "Análisis Forense Digital" el cual Miguel López delgado lo define como: "Un conjunto de principios y técnicas que comprende el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias digitales y que llegado el caso puedan ser aceptadas legalmente en un proceso judicial." [19]

Como disciplina ofrece las herramientas para obtener y presentar evidencia digital ante un juez por lo cual es de vital importancia que las investigaciones sean realizadas por experto en el área.

Exigencias técnicas: Reto Forense

Un ejemplo de las exigencias técnicas del análisis forense digital y por consecuencia la persecución de delitos informáticos es el Reto Forense llevado a cabo en conjunto por RedIRIS, Red de Comunicaciones Avanzadas de la Comunidad Academia y Científica Española, y el UNAM-CERT, Equipo de Respuesta a Incidentes de Seguridad en Cómputo de la Universidad Nacional Autónoma de México, con el objetivo de contribuir a mejorar el conocimiento sobre cómputo forense. [20]

Durante el reto, los participantes realizan el análisis de un sistema comprometido por un acceso no autorizado; el objetivo es presentar un resumen ejecutivo (leguaje común) y un informe técnico donde se detalla el análisis y el uso de herramientas para determinar lo ocurrido en el sistema analizado; con un vocabulario lleno de tecnicismos. Este tipo de análisis refleja el reto que enfrentan las correspondientes unidades de investigación y la necesidad de profesionistas.

Cultura en la Red

Regulación del contenido

Laura Chinchilla Miranda, Presidente de la República de Costa Rica establece (2012): "La única limitación que debe experimentar la internet, es la limitación que nos impone nuestro propio sentido de responsabilidad."

A falta de capacidades para regular el contenido en la web, tanto por el volumen de datos, el número de usuarios y problemas de jurisdicción, el crear conciencia del uso responsable de Internet se ha vuelto un punto clave para la convivencia en una sociedad virtual, tanto para los ciudadanos como para empresas. Por ejemplo, cientos de empresas manejan información confidencial de sus clientes y es su responsabilidad asegurar la integridad de la información la cual puede caer en manos de grupos criminales quienes la utilizan para extorsiones telefónicas, suplantación de identidad, espionaje, etc.

Previsión en el hogar

Es importante regular el contenido que los menores pueden visitar; actualmente existen diversos software que facilitan la tarea de seleccionar y filtrar aquellas páginas con contenidos que consideren impropios, pero más importante aún es darse cuenta del tipo y tiempo de uso que los menores dedican cuando se encuentran frente a una computadora.

Cada padre de familia debe advertir a sus hijos de las ventajas y peligros de la *web*, fomentando en ellos una conciencia ética y responsable sobre su uso.

Conclusiones

A medida que las actividades digitales toman protagonismo en nuestras vidas, nos vemos expuestos a nuevos riegos y mantener un ambiente de comunicación seguro para todos los usuarios es el principal reto para los gobiernos de los países en vías de desarrollo tal es el caso de México, el cual, ha dado el primer paso con la implementación de un marco regulatorio que permita frenar el crecimiento exponencial de los delitos informáticos en últimos años.

Referencias

[1] T. Meltzer & S. Phillips. "From the first email to the first YouTube video: a definitive internet history" *The Guardian*. 23 octubre 2009.

[2] Internacional Criminal Police Organization. INTERPOL. Recuperado de: http://www.interpol.int/es/Criminalidad/Delincuencia-informática/Ciberdelincuencia. Último acceso: 11 febrero 2013.

[3] L. Hernández Díaz, "El delito informático". *Eguzkilore. Cuaderno del Instituto Vasco de Criminología*. nº 23. pp. 227-243. 2009.

[4] Código Penal para el Estado de Sinaloa, Estado de Sinaloa,. Última reforma publicado P.O. 25 abril 2012.

[5] Consejo de Europa, Convenio Sobre la Ciberdelincuencia, Budapest. 2001.

[6] Secretaría de Seguridad Pública. "Guía del Taller Prevención contra el Delito Cibernético". 2012.

[7] Oxford University Press. "hacker". Oxford Dictionaries, Oxford Dictionaries. 2010.

[8] Panda Security, S.L. "Panda Security". 2013. Recuperado de: http://www.pandasecurity.com/spain/homeusers/security-info/glossary/. Último acceso: 11 febrero 2011.

[9] Avira Operations GmbH & Co. KG., "Centro de ayuda - Avira Free Antivirus". 2012.

[10] S. Acurio Del Pino. Delitos Informáticos: Generalidades. 2007.

[11] P. Seybold. "PlayStation.Blog". 26 abril 2011. Recuperado de: http://blog.us.playstation.com/2011/04/26/update-on-playstation-network-and-qriocity/. Último acceso: 11 febrero 2013.

[12] N. Falliere, M. Liam O & C. Eric. "W32.Stuxnet Dossier". *Symantec Corporation*. 2011.

[13] D. E. Sanger. "Obama Order Sped Up Wave of Cyberattacks Against Iran". *The New York Times*. 1 june 2012.

[14] Código Penal Federal. Última reforma publicada DOF 25 enero 2013.

[15] Código penal del Distrito federal. Última reforma publicada en la Gaceta Oficial del Distrito Federal: 3 agosto 2012.

[16] S. E. Goodman & A. D. Sofaer. "Proposal for an International Convention on Cyber Crime and Terrorism, A". 2000.

[17] Commonwealth Secretariat. "Member States - Commonwealth". Recuperado de: http://www.thecommonwealth.org. Último acceso: 20 marzo 2013.

[18] Oficina de las Naciones Unidas contra la Droga y el Delito. "Ficha Informativa 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal". Salvador, Brasil. 12 a 19 abril 2010.

[19] M. López Delgado, «Analisis Forense Digital,» Universidad Nacional de Educación a Distancia - España, 2007.

[20] Subdirección de Seguridad de la Información - UNAM, «Resultados Reto Forense Episodio III,» [En línea]. Available: http://www.seguridad.unam.mx/eventos/reto/. [Último acceso: 04 marzo 2013].

Datos de los autores:

Jesús Alberto Loredo González

Licenciado en Informática Administrativa, egresa de la Facultad de Contaduría y Administración.

Email: alphaproxy@myopera.com, jesus.loredogn@uanl.edu.mx

Maestro Asesor:

Ing. Aurelio Ramírez Granados

Email: raurelio56@yahoo.com.mx