Revista Ciencia UNEMI
Nº 11, Junio 2014, pp. 43 - 50
ISSN: 1390 - 4272

Cómo responder
a un Delito Informático

Resumen

El uso de la tecnología facilita muchas tareas cotidianas, es más fácil comunicarnos, automatizar tareas, realizar negocios online, entre otras actividades; sin embargo en la mayoría de adelantos de la ciencia, la tecnología también está siendo utilizada para cometer actos ilícitos, los cuales son conocidos como delitos Informáticos; en este artículo se expondrá cómo responder ante un incidente de este tipo, aun cuando no se tengan vastosconocimientos informáticos.

Palabras clave: *Seguridad, tecnología, delitos informáticos.*

Abstract

The use of technology makes many of our everyday tasks easier. Nowadays it is easy to be in touch with everyone, to automate tasks, to do business online, among other activities. However in most areas of scientific progress technology is also being used to commit illegal acts, which are known as Cyber Crimes. In this article the authors suggest how users can respond to this kind of incidents, even if they lack vast IT knowledge.

Key words: *Security, Technology, Cyber Crime.*

Recibido: enero, 2013
Aceptado: mayo, 2014

Ing. Enrique Colón Ferruzola Gómez, MGTI[1]
Perito Informático del Consejo Nacional de la Judicatura del Ecuador
eferruzola@peritoinformatico.ec

Abg. Hugo Alexander Cuenca Espinosa[2]
Especialista en Delitos Informáticos y Derecho Informático
info@alexandercuencaespinosa.com

[1]Ingeniero en Informática. Máster en Gerencia de Tecnologías de la Información. Docente de la Universidad de Estatal de Milagro. Consultor Externo de Seguridad de la Información. Investigador Digital. Ponente en temas de Seguridad Informática e Informática Forense.

[2]Abogado de los Tribunales de la República del Ecuador. Especialista en Delitos Informáticos, Inteligencia Informática y Estrategias de Contrainteligencia. Ponente en temas sobre Cibercrimen. Autor del libro "El Delito Informático en el Ecuador una nueva tendencia criminal del Siglo XXI. Su evolución, punibilidad y proceso penal". Presidente de la Sociedad Iberoamericana de Derecho e Informática.

1. INTRODUCCIÓN

Hoy en día vemos que la información y datos almacenados en los equipos informáticos son inseguros, se invierten miles de dólares por parte de empresas a fin de proteger uno de los activos más preciados: la información. Hace algunos meses en Ecuador un experto informático logró "vulnerar" el portal web denominado Dato Seguro, portal que almacena la información personal de los ciudadanos ecuatorianos de "manera segura".

Por medios de comunicación tanto televisivos como periodísticos se dio a conocer que el ciudadano que había vulnerado dicho portal se llama Paúl Moreno, oriundo de la ciudad de Riobamba, quien con ciertos conocimientos informáticos pudo suplantar la identidad del Ec. Rafael Correa, Presidente de la República del Ecuador, en aproximadamente media hora [1], claramente se identifica esto como un robo de identidad electrónica, es decir, para el sistema Dato Seguro el señor Paúl Moreno era el Ec. Rafael Correa y por consiguiente tuvo acceso a varios datos personales de él.

Con este antecedente se puede destacar que la tecnología también está siendo utilizada para cometer actos ilícitos, los cuales son conocidos como delitos Informáticos. En este artículo se expondrá cómo responder ante un incidente de este tipo, aun cuando no se tengan vastos conocimientos informáticos.

2. DESARROLLO

Aunque no hay una definición específica acerca de "Delito Informático", varios tratadistas y doctrinarios en el tema han hecho el esfuerzo por dilucidar un concepto claro y conciso respecto a este ilícito de la nueva era. Es así que entre los más conocidos tenemos las siguientes definiciones:

Nidia Callegari define al *"delito Informático" como "aquel que se da con la ayuda de la informática o de técnicas anexas"* [2], El Departamento de Investigación de la Universidad de México, señala como delitos informáticos *"todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio Informático"* [3]. El italiano Carlos Sarzana, define el Delito Informático como *"cualquier comportamiento criminógeno en que la computadora está involucrada como material, objeto o mero símbolo"* [4], María de la Luz Lima dice que el *"delito electrónico" "en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el Delito Informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin"* [5].

Después de revisar varias definiciones de algunos autores, se selecciona la provista por el Profesor chileno Renato Jijena Leiva, quien menciona en su obra "Chile, La protección penal a la Intimidad y el Delito Informático", que el delito informático es "(...) *toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento automatizado de la misma"* [6].

A definición personal *"el delito informático es toda actividad en la cual se utilizan medios computacionales, telemáticos o electrónicos para el cometimiento de un delito; delitos que constituyen nuevas formas penales que incluyen como elementos primogénitos al internet como instrumento abstracto y a la computadora como instrumento físico"* [7].

El delito informático en sus diferentes tipos es un delito susceptible de ser sancionado por el código penal, siempre y cuando la figura antijurídica se encuentre configurada en el tipo y establecida en un cuerpo normativo. El delito informático dependiendo su resultado deberá tener un alto índice de reprochabilidad para la no reincidencia del mismo.

Dentro de los principales Delitos Informáticos y Delitos Computacionales tenemos:

1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:

- Acceso ilícito a sistemas informáticos.
- Interceptación ilícita de datos informáticos.
- Interferencia en el funcionamiento de un sistema informático.
- Abuso de dispositivos que faciliten la comisión de delitos.

2. Delitos informáticos propios:

- Falsificación informática mediante la introducción, borrada o supresión de datos informáticos.

– Fraude informático mediante la introducción, alteración o borrado de datos informáticos o la interferencia en sistemas informáticos.

3. Delitos relacionados con el contenido:

– Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.

– Delitos relacionados con infracciones de la propiedad intelectual y derechos afines:

– Un ejemplo de este grupo de delitos es la copia y distribución de programas informáticos o piratería informática.

Delitos Informáticos tipificados en la legislación ecuatoriana

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos más conocida como Ley 67, publicada en el R.O. / Sup.557 del 17 de Abril del 2002, tuvo un avance muy importante en el sentido de incluir figuras penales que hagan punibles los ilícitos informáticos, con lo cual, junto al Código Penal, integran normas creadas para la Sociedad de la Información.

Dentro de estas normas promulgadas en la Ley 67 [8], posteriormente incluidas al Código Penal, constan los siguientes ilícitos informáticos [9].

– Art. 57 LCEFEMD: Infracciones informáticas. Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley.

– Art. 58 LCEFEMD, Conc. Art. 202.1 CP: Contra la Información Protegida. El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

– Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.

– La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, serán sancionadas con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

– Si la divulgación o la utilización fraudulenta se realizan por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

– Art.58 últ. inc LCEFEMD, Conc. Art. 202.2 CP: Obtención y utilización no autorizada de información. La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica.

– Art.59 LCEFEMD, Conc. Art. 262 CP: Destrucción Maliciosa de Documentos. Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados sin razón de su cargo.

– Art.60 LCEFEMD, Conc. Art. 353.1 CP: Falsificación electrónica. Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio; alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:

– Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;

– Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;

– Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.
– El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este Capítulo.
– Art.61 LCEFEMD, Conc. Art. 415.1 CP: Daños informáticos. El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.
– La pena de prisión será de tres a cinco años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculado con la defensa nacional.
– Art.61 últ.inc LCEFEMD, Conc. Art. 415.1 CP: Destrucción de instalaciones para transmisión de datos. Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica.
– Art.62 LCEFEMD, Conc. Art. 553.1 CP: Apropiación ilícita. Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.
– Art.62 últ.inc LCEFEMD, Conc. Art. 553.2 CP: Pena. La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios:
-Inutilización de sistemas de alarma o guarda;
-Descubrimiento o descifrado de claves secretas o encriptadas;
-Utilización de tarjetas magnéticas o perforadas;
-Utilización de controles o instrumentos de apertura a distancia; y,
-Violación de seguridades electrónicas, informáticas u otras semejantes.
– Art.63 LCEFEMD, Conc. Art. 563 inc.2 CP: Estafa. Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando medios electrónicos o telemáticos.
– Art.64 LCEFEMD, Conc. Art.606.20 CP: Violación Derecho a la Intimidad. Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

Pero ¿qué hacer si ha sido víctima de este tipo de delitos?

A) Realizando la investigación de manera personal:

Warren G. Kruse II y Jay G. Heiser, esquematizan cuatro fases para la investigación de los delitos informáticos [10]:

1. Evaluar la Situación. Analizar el Alcance de la Investigación y la acción a tomar.

2. Adquirir los Datos. Recopilar, Proteger y Preservar la Evidencia original.

3. Analizar los datos a examinar y correlacionar la evidencia y el contenido digital con los eventos de interés, los cuales ayudarán a resolver el caso.

4. Informar de la Investigación. Reunir y organizar la Información recopilada y la Redacción del Informe final.

A fin de precautelar y mantener intacta la evidencia, se debe elaborar la cadena de custodia, la cual es un sistema de aseguramiento, que tiene como fin garantizar la autenticidad de la evidencia que se utilizará como "prueba" dentro del proceso. La información mínima que se maneja en la cadena de custodia, para un caso específico, es la siguiente:

- Una hoja de ruta, en donde se anotan los

datos principales sobre descripción de la evidencia.
- Fechas, horas.
- Custodios, identificaciones, cargos y firmas de quien recibe y quien entrega;
- Rótulos que van pegados a los envases de las evidencias, por ejemplo a las bolsas plásticas, sobres de papel, sobres de Manila, frascos, cajas de cartón, etc.;
- Etiquetas que tienen la misma información que los rótulos,
- Detalle de los equipos electrónicos, (número de serie de los equipos, color, estado) que se deben llevar a los laboratorios de análisis [11].

B) Actuando legalmente ante un delito informático

Dentro del campo del Derecho Penal Informático y con la suscitación de un Delito Informático, hay que considerar los siguientes puntos del procedimiento penal:

1. Si el delito fuese de acción pública de instancia oficial y llegase a conocer la autoridad competente llámese Fiscal, el titular único del ejercicio de la acción penal será el Ministerio Público, sin necesidad de denuncia previa. Un ejemplo son los delitos de blanqueo de dinero que se pueden suscitar a través de mecanismos informáticos.
2. Si el delito fuese de acción pública de instancia particular, y se llegase a conocer por denuncia previa, sea escrita u oral, esta deberá ser reconocida por parte del denunciante bajo la condición de que esta posteriormente pueda ser declarada maliciosa o temeraria y, en el caso pertinente los titulares de la acción penal son el Estado y el denunciante llámese agraviado; ejemplo el robo de dinero por acceso ilícito a través de transferencias electrónicas bancarias.
3. Si el delito fuese de acción privada, éste deberá ser interpuesto mediante querella, cumpliendo con los requisitos exigidos en la ley, para posteriormente ser calificada y admitida aperturando la primera etapa del proceso penal que es la instrucción fiscal, debemos ver que la querella es similar a la denuncia, su principal diferencia radica en que la primera es de acción privada y la segunda de acción pública. Cabe indicar que dentro del código de procedimiento penal se precisa qué delitos son de acción privada, así por ejemplo en el caso pertinente las injurias calumniosas y no calumniosas graves, a través de redes sociales cómo Facebook se encuadrarían dentro de esta clase de conductas.
4. Hay que tomar en consideración que la indagación previa no es una etapa del proceso penal, sino una fase pre procesal penal en la cual se buscan indicios, evidencias o hechos que puedan demostrar la existencia material del delito y puedan aperturar la instrucción fiscal como primera etapa del proceso penal.
5. También debemos tomar en consideración que sólo la querella una vez calificada da paso a la instrucción fiscal por ser de acción privada, en cuanto a la denuncia en la acción pública, iniciada la indagación previa y de demostrarse elementos que guíen a la existencia del ilícito, da inicio a la instrucción fiscal, y exclusivamente dentro de esta etapa es decir desde la apertura de la instrucción fiscal y hasta antes de su cierre, el denunciante podrá seguir siendo sujeto del proceso penal, siempre y cuando esté presente la acusación particular que igualmente deberá ser calificada y cumplir los requisitos establecidos en el Art.55 del Código de Procedimiento Penal; de ser el caso que el denunciante no presente la acusación particular dejará de ser sujeto procesal, y únicamente quien tendrá la titularidad y el ejercicio de la acción penal será el Estado.
6. Debemos considerar que los titulares de la acción penal son el Estado y el agraviado llámese perjudicado o denunciante, y el titular del ejercicio de la acción penal es exclusiva y únicamente el Estado, quien ejercerá su potestad jurisdiccional y punitivita para esclarecer el delito y sancionar bajo pena o sanción correspondiente al infractor de la ley.
7. La Indagación Previa tiene un plazo máximo de un año de duración en delitos de acción privada y de dos años en delitos de acción pública. En cuanto a la Instrucción Fiscal tiene una duración de 90 días, y sólo en el caso de incorporar nuevos sospechosos al proceso se podrá prorrogar por 30 días más por sospechoso incluido; por principios de celeridad procesal se consideran hasta 60 días máximos de prórroga.
8. En caso de recopilar indicios y evidencias que demuestren la existencia de un delito informático, el Fiscal a través del Juez y posterior a la Audiencia de Formulación de Cargos

podrá iniciar la Instrucción Fiscal para dar vida al proceso penal como tal; en caso que no hubiesen los elementos de conocimiento sobre la existencia de la infracción, el Fiscal sugerirá el archivo provisional de la causa y para esto recurrirá donde el Juez competente que conoció el delito para que este ordene el archivo del mismo.

9. La prueba informática para que sea considerada como tal dentro del proceso penal y surta efectos de validez jurídica debe seguir lo siguientes parámetros: a) ser solicitada b) ser presentada c) ser practicada d) ser incorporada al expediente del proceso penal, para que al momento de darse la audiencia oral, pública y contradictoria esta sea exhibida con todos los requisitos que la ley exige. La finalidad de la prueba informática es el demostrar la materialidad de la infracción y hacer de esta forma efectivo el IUS PUNIENDI.

10. En caso que la prueba informática requiera pericia alguna, se deberá nombrar un perito informático acreditado por el Consejo Nacional de la Judicatura, o en el caso que de ausencia de uno, se deberá solicitar un perito civil según las reglas establecidas en el Reglamento para la acreditación de peritos del Consejo de la Judicatura. Este peritaje debe ser realizado previamente bajo orden judicial para que la prueba obtenida sea válida.

11. De acuerdo a las estadísticas, sólo el 1% de los casos suscitados sobre delitos informáticos y delitos computacionales pasan a Instrucción Fiscal, el resto queda en Indagación Previa y posteriormente se archiva.

Es importante que al momento de la comisión del delito informático, se mantenga una ordenada cadena de custodia con la ayuda de equipos informáticos forenses para demostrar la veracidad de la evidencia y la legalidad de esta al ser practicada e incorporada como prueba al expediente del proceso

PAIS	ECUADOR		
DELITO	**2011**	**2012**	**2013**
APROPIACIÓN ILÍCITA UTILIZANDO MEDIOS INFORMÁTICOS	3129	2721	458
FALSIFICACIÓN ELECTRÓNICA	127	105	40
ESTAFA UTILIZANDO MEDIOS INFORMÁTICOS	286	60	16
USURPACIÓN TOMAR UN NOMBRE QUE NO LE PERTENECE	1221	1540	514
TOTAL GENERAL	**4764**	**4427**	**1030**

Tabla 1. Estadísticas de Delitos de Acuerdo a la Fiscalía General del Estado
Fuente: Fiscalía General del Estado

La Fiscalía cuenta con la cooperación internacional de la Interpol (por el problema de una o más jurisdicciones), y de manera local con el Servicio de Inteligencia de la Policía Judicial y Contrainteligencia, para las debidas capturas y seguimientos. Esta cooperación internacional es regulada por Red de Contactos 24/7[12], para el TRATAMIENTO DE DATOS.

Además, la Fiscalía mantiene convenios en los cuales el responsable del caso puede solicitar cooperación para la investigación de estos ilícitos a compañías en el extranjero tales como Facebook, Yahoo o Hotmail, entre otros.

3. CONCLUSIONES

Dentro del paradigma que envuelve a los delitos informáticos en el Ecuador, hay una gran problemática que requiere la toma de medidas para solventar y solucionar estos delitos, ya que, en un principio, los delitos informáticos quedan impunes, debido a que no se encuentran incluidos en una normativa específica. En el Código Penal Ecuatoriano que se encuentra vigente, hay pocas figuras que hacen punibles estos delitos, no todas se adecuan al tipo, dejando en la total indefensión al agraviado, ya que al no considerarse como delitos tradicionales en el Código Penal, no se puede establecer una pena o si bien se las es-

tablece será semejante a otro ilícito como un simple robo o hurto.

La falencia no sería sólo de quien juzga, sino también del órgano administrador de justicia, pues en Ecuador existen pocos cursos o seminarios de actualización dirigidos a jueces, fiscales y demás funcionarios públicos sobre este tipo de delitos. Además muchas empresas ocultan y no denuncian este tipo de delitos, por cuanto consideran que esto afectaría su imagen; es por este motivo que las reales estadísticas de los delitos informáticos no salen a la luz pública.

4. RECOMENDACIONES PARA EVITAR SER VÍCTIMA DE LOS DELITOS INFORMÁTICOS

1. Tener instalado en sus equipos informáticos un antivirus y antispyware con licencia y actualizados.
2. Tener instalado en nuestros equipos informáticos las actualizaciones recientes de seguridad.
3. Para acceder a cuentas bancarias y de correo electrónico, utilizar el teclado virtual para mayor seguridad.
4. No acceder a páginas de contenido pornográfico, ya que en su mayoría contienen virus.
5. Evitar descargar programas gratuitos porque la mayoría son infecciosos.
6. Evitar instalar programas crackeados, piratas o con parches.
7. Realizar un análisis con el antivirus actualizado de todo dispositivo de almacenamiento de información que conectemos a nuestro equipo.
8. Revisar con cautela los correos que tengamos en la bandeja de entrada, estos pueden ser spam, contener código malicioso que nos puede redireccionar a un sitio falso donde al ingresar nuestros datos podemos ser víctimas de robo de información.
9. Tenga cuidado con los negocios, promociones, inversiones y regalos por internet, la mayoría de veces contienen virus o son estafas.
10. No proporcionar nunca información personal sobre ti a través de internet a personas desconocidas, evitar tomar fotos de tarjetas de crédito, cédula, DNI, pasaporte o visa y subirlo a redes sociales como Instagram, Facebook o Twitter.
11. No responder a mensajes de anuncios o cadenas en los que se incluyan mensajes agresivos, obscenos o amenazantes. No pactes citas con personas desconocidas.
12. Instale la computadora en un área de fácil acceso a todos los miembros de la casa, para poder vigilar su uso por los menores. Si sus hijos son pequeños no les permita entrar en chats y redes sociales sin tener a un adulto presente. No permita que sus hijos pacten citas por Internet.
13. No envíe información bancaria o crediticia a través de correos electrónicos, los bancos nunca solicitan este tipo de información por medio de un correo electrónico o mensajes de texto.
14. Cuando cree su clave, use siempre palabras combinadas con números, letras y símbolos diferentes, no utilices datos personales, nombre de hijos o familiares.
15. Muchos hackers utilizan noticias curiosas o impactantes para lanzar infecciones, troyanos, malware a través de enlaces a páginas web, por lo que no es recomendable abrir los documentos.
16. No descargar software del cual no se tenga plena confianza de que son sitios seguros ni tampoco abrir archivos o postales de desconocidos enviados a los correos, las direcciones seguras son una forma de verificar que el sitio a donde se ingrese es verídico, la forma de reconocerlos es que la página empiece con https:/

Referencias Bibliográficas

[1]. Coyote, P. (2012). www. DatoSeguro.gob.ec NO es seguro. Consultado en: http://www.ecualug.org/?q=20121126/blog/paulcoyote/wwwdatosegurogobec_no_es_seguro
[2]. Conde O'Donnell, H.; González P., C. y Heredia M., A. (2009). El delito informático. Consultado en: http://dmi.uib.es/~dmiamp/TEGP/Tema%202/Delito%20informatico%20I%20pres.pdf
[3]. Conde O'Donnell, H.; González P., C. y Heredia M., A.: Ídem.
[4]. Conde O'Donnell, H.; González P., C. y Heredia M., A.: Ídem.
[5]. Conde O'Donnell, H.; González P., C. y Heredia M., A.: Ídem.
[6]. Leiva Jijena, R. (1992). Chile, la protección penal de la intimidad y el delito informático. Chile: Editorial Andrés Bello, p. 225.
[7]. Cuenca Espinoza., A. "EL DELITO INFORMÁTICO EN EL ECUADOR", Revista Ruptura. N°56; Ecuador 2013, p. 220
[8]. Registro Oficial / Sup.557 del 17 de Abril del 2002
[9]. Registro Oficial / Sup.557 del 17 de Abril del 2002: Ídem.
[10]. Kruse II, W. G. & Heiser, J. (2002). Computer Forensics: Incident Response Essentials. EE.UU: Addison Wesley Pub Co Inc.
[1]. Acurio Del Pino, S. Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Versión 2.0
[12]. NOTA: Interpol ha creado el sistema mundial de comunicación policial I-24/7 a fin de conectar entre sí a los funcionarios encargados de la aplicación de la ley de todos los países miembros, lo que permite a los usuarios autorizados intercambiar información policial vital y acceder a las bases de datos y a los servicios de INTERPOL 24 horas al día.

Otra bibliografía consultada

1. Cuenca E., A. (2012). Una nueva tendencia criminal del Siglo XXI. Su evolución, punibilidad y proceso penal. Editorial Ruptura, Revista Ruptura N°56. Pontificia Universidad Católica del Ecuador. Facultad de Jurisprudencia.
2. Código Penal, Quito, Corporación de Estudios y Publicaciones, Año 2009.
3. Código de Procedimiento Penal, Quito, Corporación de Estudios y Publicaciones, Año 2009.
4. Ley orgánica de Transparencia y Acceso a la Información pública, Quito, Corporación de Estudios y Publicaciones, Año 2008.
5. Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de datos, Quito, Corporación de Estudios y Publicaciones, Año 2002.
6. Ley de Propiedad intelectual, Quito, Corporación de Estudios y Publicaciones, Año 2007.
7. Ley Especial de Telecomunicaciones, Quito, Corporación de Estudios y Publicaciones, Año 2013.
8. Ley Orgánica de Control Constitucional, Quito, Corporación de Estudios y Publicaciones, Año 2011.
9. Reglamento de la Superintendencia de Bancos y Seguros, Quito, SBS, Año 2011.
10. CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR, Quito, Corporación de Estudios y Publicaciones, Año 2011.
11. Páez, J. J. y Acurio del Pino, S. (2010). Derecho y Nuevas Tecnologías. Quito: Editora Corporación de Estudios y Publicaciones.
12. Márquez E., C.. (2003). El Delito Informático. Bogotá: Editorial Leyer.
13. Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de datos, Quito, R.O. Suplemento 557 de 17-ABR-2002, Año 2002.
14. Página web del Municipio de Quito destruida por "crackers" - Archivo Histórico; Quito, editorial diario hoy, 6-XII-2001.
15. Mensajes de datos; Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI), Año 2000.
16. Ley de Firma electrónica chilena, Santiago, Año 2003.
17. Primer borrador proyecto de ley para Código Orgánico Integral Penal; Asamblea Constituyente, 2011.
18. Recovery Labs. (En línea). Delitos informáticos info. Consultado en: http://delitosinformaticos.info/delitos_informaticos/definicion.html
19. GIGATRIBE, GigaTribe brings private P2P sharing to U.S, Estados Unidos, CNET News, Año 2008.
20. Brenner, S. (2010). Gigatribe and the 4th Amendment, Estados Unidos.
21. Araujo, M. P. (2012). Apuntes de delitos en particular, Quito.
22. Zambrano, R. (2012). Delitos Informáticos Contemplados en la Ley Ecuatoriana. Consultado en: http://www.cec.espol.edu.ec/blog/rzambrano/files/2012/08/DELITOS-INFORM%C3%81TICOS-CONTEMPLADOS-EN-LA-LEY-ECUATORIANA.pdf
23. Huilcapi, A. (2009). El Delito Informático. Consultado en: http://www.derechoecuador.com/index.php?option=com_content&task=view&id=3091&Itemid=426
24. Levene,R. y Chiaravalloti, A. (2009). Delitos Informáticos. Consultado en: http://www.derechoecuador.com/index.php?option=com_content&task=view&id=3925&Itemid=426
25. Dr. Beltrán, F y Dra. Beltrán, S. (2010) Derecho Informático. Consultado en: http://www.derechoecuador.com/index.php?option=com_content&view=article&id=4980:derecho-informatico&catid=42:derecho-informatico&Itemid=420
26. Dr. Yánez, P. (2005). Infracciones electrónicas en el Procedimiento Penal. Consultado en: http://www.derechoecuador.com/index2.php?option=com_content&do_pdf=1&id=3090
27. Dr. Páez, J. (2009). Peritaje e Infracciones Electrónicas. Consultado en: http://www.derechoecuador.com/index2.php?option=com_content&do_pdf=1&id=5174
28. Consejo de Europa (2001). Convenio sobre la CiberDelincuencia. Consultado en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_Ciberdelincuencia.pdf