Revisión Bibliográfica

Normativa Legal sobre Delitos Informáticos en Ecuador

Legal Regulations on Cybercrimes in Ecuador

Narda J. Ortiz Campos

Instituto Tecnológico Superior "Eloy Alfaro", Ecuador.

La correspondencia sobre este artículo debe ser dirigida a Narda Ortiz Campos.

Email:najioc@hotmail.com

Fecha de recepción: 31 de diciembre de 2018.

Fecha de aceptación: 8 de febrero de 2019.

¿Cómo citar este artículo? (Normas APA): Ortiz Campos, N. J. (2019). Normativa Legal sobre Delitos Informáticos en Ecuador. Revista Científica Hallazgos21, *4*(1), 100- 111. Recuperado de http://revistas.pucese.edu.ec/hallazgos21/

Resumen

El avance tecnológico y la creciente accesibilidad al Internet que tienen las personas en todo el mundo ha sido de utilidad para la masificación en la creación y utilización de diferentes sitios web y APP (aplicaciones). Estas están diseñadas para satisfacer las necesidades de sus usuarios a través de dar tan solo un click; las necesidades suelen ser variadas, desde hacer transacciones bancarias complejas a nivel internacional a simplemente chatear con otra persona en un lugar remoto del planeta. Sin duda alguna, el uso de Internet facilita la vida de los usuarios, pero esos beneficios se tornan peligrosos cuando se infiltran entre los servicios del Internet programas maliciosos que de forma silenciosa pueden dañar no sólo los equipos tecnológicos sino también las finanzas de las personas, empresas y gobiernos. Los programas maliciosos son insertados en los sitios web o APP por delincuentes informáticos que han hecho de las Tecnologías de la Información y Comunicación (TIC) su nueva herramienta para cometer sus actos ilícitos. Cuáles son los tipos de delitos que se generan en la red, qué leyes existen para sancionar los delitos informáticos y cuáles son los problemas para combatir el mismo fueron las interrogantes que motivaron a desarrollar la presente revisión bibliográfica. Al concluir el trabajo se pudo determinar que existen dificultades para combatir los delitos informáticos por la transnacionalidad de los mismos y la incompatibilidad de las leyes a nivel mundial; considerando que en algunos países no existen Leyes para combatir los delitos informáticos y que son millonarias las pérdidas ocasionados por este tipo de delitos.

Palabras clave: delitos informáticos; tipificación; procedimiento penal; tipos de delitos informáticos.

Abstract

The technological advance and the increasing accessibility to the Internet that people have throughout the world has been useful for the massification in the creation and use of different websites and APP (applications). These are designed to meet the needs of its users through giving just one click; The needs are often varied, from complex international banking transactions to simply chatting with another person in a remote part of the world. Undoubtedly, the use of the Internet facilitates the lives of users, but those benefits become dangerous when malicious services infiltrate Internet services that can silently damage not only the technological equipment but also the finances of the people, companies and governments. Malicious programs are inserted into web sites or APP by computer criminals who have made Information and Communication Technologies (ICT) their new tool to commit their illicit acts. What are the types of crimes that are generated in the network, what laws exist to sanction cybercrime and what are the problems to combat it were the questions that motivated the development of this bibliographical review. At the conclusion of the work it was possible to determine that there are difficulties to combat computer crimes due to the transnationality of the same and the incompatibility of laws worldwide; Considering that in some countries there are no Laws to combat computer crimes and that the losses caused by this type of crime are millions.

Keywords: Cybercrime; typing; penal procedure; types of computer crimes.

Normativa Legal sobre Delitos Informáticos en Ecuador

Rincón y Naranjo (2008) plantean que la era actual ha sido denominada como la sociedad del conocimiento, en el que la información ha adquirido un valor económico en tal sentido la informática se ha convertido en una nueva herramienta de poder. A nivel mundial una gran cantidad de personas, empresas, organizaciones e instituciones públicas, privadas y gubernamentales generan, almacenan y obtienen información a través del uso de Internet; un sistema de redes informáticas gigantesco que usa dispositivos tecnológicos. Es sorprendente como esta nueva forma de procesar y transmitir los datos ha dado origen a una gran cantidad de delitos porque "la informática puede ser el objeto del ataque o el medio para cometer otros delitos" (Zambrano, Dueñas, & Macías, 2016, p. 206).

Según Téllez (2008) los delitos informáticos son conductas típicas, antijurídicas y culpables que tienen a las computadoras como instrumento o fin (p.188). Internacionalmente existen diferentes designaciones para la terminología delitos informáticos, tales como, delitos electrónicos, cibercrimen, ciberdelitos, delitos relacionados con las computadoras, crímenes por computadora, entre otros. El término más usado por los autores en la doctrina del derecho penal informático es el de delito informático. Los delitos informáticos ya están tipificados en el marco jurídico legal del Ecuador, en la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas y en el Código Orgánico Integral Penal (COIP).

No se puede sancionar un delito si éste no está debidamente tipificado en el marco legal; es decir, que toda conducta que atente contra la armonía y la tranquilidad del conglomerado social debe estar normalizada, ya que no es posible su sanción a través de analogías. Por esta razón, se precisa la creación de tipos penales sancionatorios de los nuevos delitos ilícitos producto del avance tecnológico como los que se desarrollan a través del internet estos son el ciberbulling, ciberataques, subastas y ventas ilegales en internet, uso de redes robot o zombi, etc.

La estructura del delito está conformado por la tipicidad, antijuricidad y la culpabilidad. "A través de la tipicidad es posible brindar garantías jurídicas, políticas y sociales a los ciudadanos del mundo" (Rincón & Naranjo, 2008, pp. 54 - 60).

La tipificación del delito informático en la ley penal responde a elementos tales como el sujeto o autor de la conducta ilícita o delictiva; el medio, el sistema informático; y el objeto, el bien que produce el beneficio económico o ilícito (Zambrano et al., 2016, p. 206).

Método

Para la realización de esta revisión bibliográfica se procedió a buscar y a descargar información sobre la temática seleccionada en google, google scholar y google libros. Como criterio de búsqueda se utilizaron las palabras clave "delitos informáticos", "delitos informáticos + leyes", "tipos de delitos informáticos", "cibercrimen + Ecuador", "derecho informático", y "delitos informáticos + retos". Luego de revisar el contenido de aquellos artículos, libros o sitios web que fueron descargados, se seleccionaron solo aquellos que se consideraron originales y de importancia para el desarrollo de la redacción del presente artículo. También se realizó una base de datos en la cual se registraron los datos concernientes al año de publicación, autores, nombre y resumen de cada uno de los archivos descargados,

con el propósito de tener una ayuda memoria que permitiera encaminar el reciente trabajo.

Desarrollo

Los delitos informáticos en Latinoamérica están en crecimiento, según Temperini, citado en Zambrano et al. (2016): Los países ubicados en esta región no tienen un marco legal homogéneo aplicable a los delitos de esta índole, por tal motivo es complicado combatirlos.

La pirámide Kelseniana es una representación gráfica que establece el orden de aplicación jerárquica de las normas jurídicas de un país. En el Ecuador esta representación esta prescrita en la Constitución de la Republica del año 2008 en el artículo 425 el cual expresa que:

> El orden jerárquico de aplicación de las normas será el siguiente: La Constitución; los tratados y convenios internacionales; las leyes orgánicas; las leyes ordinarias; las normas regionales y las ordenanzas distritales; los decretos y reglamentos; las ordenanzas; los acuerdos y las resoluciones; y los demás actos y decisiones de los poderes públicos.
>
> En caso de conflicto entre normas de distinta jerarquía, la Corte Constitucional, las juezas y jueces, autoridades administrativas y servidoras y servidores públicos, lo resolverán mediante la aplicación de la norma jerárquica superior. La jerarquía normativa considerará, en lo que corresponda, el principio de competencia, en especial la titularidad de las competencias exclusivas de los gobiernos autónomos descentralizados (p.126).

Considerando el orden jerárquico establecido en el artículo 425 se analizará la normativa vigente sobre delitos informáticos en el Ecuador.

1. **Constitución de la República del Ecuador:** Vaca (2017) los delitos informáticos dentro de la carta magna de la nación no son mencionados de forma específica, sin embargo, dentro de la constitución existen ciertos bienes jurídicos protegidos que son parte de este tipo de conductas estos son el acceso universal a las tecnologías de información y comunicación incluido en el artículo 16, y el derecho a la intimidad personal y familiar incorporado en el artículo 66 (p.37).

2. **Tratados Internacionales:** En el año 2001 el Consejo de Europa elaboro el convenio de Budapest sobre la ciberdelincuencia, en él se establecen normas de cooperación internacional para realizar procesos penales que ayuden a combatir los delitos informáticos; pues el avance de la tecnología ha permitido que los delincuentes informáticos inventen nuevas formas de delinquir. A pesar de las aportaciones jurídicas, legales y técnicas que implica el estar suscrito al convenio de Budapest el Ecuador es uno de los pocos países de Sudamérica que no se ha adherido a este acuerdo, lo que implica una gran limitación en la realización de investigaciones y en la lucha contra el delito informático.

Sin embargo, existen otros convenios internacionales que atacan en áreas específicas a los delitos informáticos y en los que está suscrito el Ecuador algunos de ellos son:

- El convenio de Berna sobre los derechos de autor, que fue ratificado en

nuestro país por la Ley 22195 ratificado el 09 de octubre de 1991[1]

- La Convención para la Protección y Producción de Phonogramas de 1971 ratificado el 04 de junio de 1974[2]
- Convenio de París en 1999[3], en él se establecen los derechos de autor con respecto a propiedad industrial (patentes, marcas, etc.).
- Convenio internacional de telecomunicaciones, suscrito en Nairobi - Kenya, el 6 de noviembre de 1982 y sus protocolos adicionales y el protocolo facultativo para la solución obligatoria de controversias[4]

3. **Código Orgánico Integral Penal:** La reforma del COIP del año 2014 en el artículo 190 establece que:

> el uso de un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de ésta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años (p.30).

En el COIP no están tipificado los nuevos delitos informáticos (ciberbulling, ciberataques, subastas y ventas ilegales en internet, uso de redes robot o zombi, etc) que surgen del ingenio criminógeno de los delincuentes informáticos. Sin embargo, la penalización de un mayor número de delitos se puede lograr si se los observa desde la óptica de los autores Bolaños y Gómez. Estos autores realizan un análisis de los delitos informáticos tipificados en el COIP relacionándolos con su área de estudio, lo que permite esta clasificación es la correcta aplicación del principio de legalidad para sancionar de forma adecuada los delitos y brindar asistencia legal a las víctimas del ciberecrimen.

Las áreas de estudios establecidas por Bolaños y Gómez (2015) con sus respectivos artículos son: 1) violación a los derechos humanos, diversas formas de explotación articulo 103; 2)delitos contra el derecho a la intimidad personal y familiar artículos 178,179 y 180; 3) delitos contra el derecho al honor y buen nombre articulo 182; 4) delitos contra el derecho a la propiedad artículos 190,191,192,193,194 y 195; 5) delitos contra el derecho a la integridad articulo 298; 6) prueba, disposiciones generales artículos 453 y 454; 7) delitos contra la seguridad de los activos, sistemas de información y comunicación artículos 229,230,231,232,233 y 234; 8) actualizaciones especiales de investigación artículos 475,476 y 477;9) Medios de prueba articulo 498; 10) documentos, reglas generales artículos 499 y 500 ; y 11) la pericia, reglas generales artículo.

4. **Ley de Comercio Electrónico, Mensaje de datos y Firmas Electrónicas:** La Organización de Cooperación y Desarrollo Económico (OCDE), la ONU y la UNESCO son algunas de las organizaciones que a nivel mundial trabajan en combatir la delincuencia informática, para ello

[1] https://www.wipo.int/treaties/es/remarks.jsp?cnty_id=945C (19-02-2019)

[2] https://www.wipo.int/treaties/es/remarks.jsp?cnty_id=945C (19-02-2019)

[3] https://www.wipo.int/pressroom/es/prdocs/2000/wipo_upd_2000_82.html (19-02-2019)

[4] https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Convenio-Internacional-de-Telecomunicaciones.pdf (19-02-2019)

establecen directrices genéricas que ayuden a los países en la tipificación de los delitos informáticos en sus normativas legales.

Ecuador se basó en el modelo de ley establecida por la Comisión de las Naciones Unidas para una ley Comercial Internacional (UNCITRAL) para incluir la tipificación de los delitos informáticos en la reforma a la Ley de Comercio Electrónico, Mensaje de datos y Firmas Electrónicas aprobada en el año 2002. Esta ley tiene como objetivo

regular los mensajes de datos, las firmas electrónicas, los servicios de certificación, la contratación electrónica y telemática, la presentación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas (p.1).

Los delitos informáticos regulados por la Ley de Comercio Electrónico, Mensaje de datos y Firmas Electrónicas están en el Capítulo I del Título V, artículos del 57 al 64; Según Sosa (2005) estas disposiciones están encaminadas a modificar el COIP, y sancionan los siguientes delitos: 1) la violación al derecho a la intimidad en documentos con soporte electrónico (Art. 58 y 64); 2) la violación o divulgación de información secreta contenida en documentos con soporte electrónico (Art. 58); 3) La obtención y utilización no autorizada de información (Art. 58); 4) la destrucción o supresión de documentos con soporte electrónico por parte de personas que tuvieren su resguardo a cargo (Art. 59); 5) la falsificación electrónica (Art. 60); 6)- los daños informáticos (Art. 61), 7) la apropiación ilícita (Art. 62) y, 8) la estafa utilizando medios electrónicos o telemáticos (Art. 63) (párr. 9).

La investigación de los delitos informáticos no es similar a la de un delito común y "es deber del Estado y en especial del Ministerio Público el de promover las dinámicas sociales, jurídicas, tecnológicas, policiales, o de cualquier otra índole para hacer frente de forma eficaz al problema de la delincuencia informática" (Acurio, 2015, p. 4; Hernández, 2016). Los principales retos que tiene la Fiscalía del Estado para combatir los delitos informáticos son: implementar una unidad especializada contra el cibercrimen; capacitar al personal que intervienen en las investigaciones del delito informático; y, socializar a la ciudadanía de las leyes contra el delito informático (pp.31-32). Existen otros retos para combatir los delitos informáticos. Ureta (2009) pone de manifiesto que en el marco legal del Ecuador se evidencian la falta de infraestructura y tecnologías adecuadas en los entes u organismos de investigación (Ministerio de Público, policía judicial);y la ausencia de firmas de convenios y tratados internacionales que le permita manejar la transnacionalidad de los delitos (pp. 86-93).

Según el congreso de las Naciones Unidas (2010) sobre las novedades recientes en el uso de la ciencia y la tecnología por los delincuentes y por las autoridades competentes en la lucha contra la delincuencia, incluido el delito cibernético, a nivel internacional existen problemas para combatir los delitos informáticos y establece los siguientes retos:

La incertidumbre del alcance: uno de los principales retos relacionados con el delito cibernético es la no existencia de información fehaciente sobre la trascendencia del problema y sobre las detenciones, los enjuiciamientos y las condenas correspondientes; sin esos antecedentes, es difícil cuantificar el impacto del delito cibernético en la sociedad y elaborar estrategias para combatirlo.

La dimensión transnacional: los delitos informáticos que se cometen a través de Internet suelen tener una dimensión transnacional; es decir, que el delincuente está en un país y las victimas en otro. Esto presenta una dificultad en la hora de combatir los ciberdelitos, puesto que existe el principio de territorialidad que impide que se puedan hacer investigaciones acerca de un delito con características de transnacionalidad. Otra dificultad importante se relaciona con el poco tiempo disponible para llevar a cabo las investigaciones de los delitos informáticos transnacionales. Para solucionar esta dificultad es necesario que exista una cooperación eficaz entre las autoridades de diferentes países y que se establezcan procesos ágiles para realizar las investigaciones con rapidez y eficiencia.

Las diferencias en los enfoques jurídicos nacionales: en el congreso de las Naciones Unidas se instauraron dos criterios para enfrentar la dimensión del delito cibernético transnacional:

1) la compatibilidad de la legislación: todos los países deberían suscribirse a organizaciones internacionales que tengan tipificados los delitos cibernéticos para poder combatirlos. Algunos ejemplos de tratados internacionales son el Commonwealth, la Comunidad Económica de los Estados de África Occidental (CEDEAO), la Unión Europea y el Consejo de Europa, y

2) la territorialización: consiste en restringir el acceso a Internet; es decir, que los proveedores de servicios de Internet puedan bloquear el ingreso de los usuarios finales a sitios web que tienen contenido indebido según las leyes.

La delincuencia organizada: la delincuencia organizada usa la tecnología para delinquir. Algunos ejemplos de delitos informáticos que realizan los grupos organizados son la piratería de programas informáticos y otras formas de violación de los derechos del autor. Sin embargo, en el ámbito del ciberespacio los grupos organizados cometen sus fechorías en pornografía infantil y los delitos relacionados con la identidad. La convención contra la delincuencia organizada establece ciertas características de los grupos organizados que cometen delitos cibernéticos:

a) los grupos dedicados al delito cibernético suelen tener una estructura más flexible y abierta;

b) los grupos que cometen delitos cibernéticos son con frecuencia mucho más pequeños que los grupos delictivos organizados tradicionales;

c) en muchos casos, los miembros de los grupos se comunican entre sí exclusivamente en forma electrónica, sin tener nunca encuentros personales (pp. 2-11).

Los retos para combatir el delito informático del Ecuador están intrínsecos a los establecidos por las Naciones Unidas lo que convierte al cibercrimen en una mal que aqueja a gran parte de la humanidad. Es importante que los países puedan aunar esfuerzos y superar estos retos para lograr disminuir las grandes pérdidas económicas, proteger a las personas, estados y empresas de los cibercriminales.

Tipos de Delitos Informáticos

Atendiendo la modernidad tecnológica que usan los criminales para afectar los bienes jurídicos personales se presentarán algunos de los delitos informáticos que generan mayores pérdidas económicas y sociales a nivel internacional.

Ciberterrorismo: Nye, citado en De la Corte & Blanco (2014), define al ciberterrorismo como acciones ofensivas que se planifican y realizan tomando como blanco gobiernos, estados, sectores de población o poblaciones enteras con el fin

de coaccionar e intimidar o generar un profundo impacto psicológico. Esto afectaría a la información, sistemas, programas, datos informatizados e infraestructuras críticos.

Los ciberterroristas hacen uso de las tecnologías de la comunicación e información (TIC) para el cometimiento de sus delitos. La oficina de las Naciones Unidas contra la droga y el delito (UNODC, 2013) establece que los grupos terroristas utilizan el Internet para realizar las siguientes tareas: "la propaganda (incluidos el reclutamiento, la radicalización y la incitación al terrorismo); la financiación; el adiestramiento; la planificación (por medio de comunicaciones secretas o de dominio público); la ejecución; y los ataques cibernéticos" (p. 3).

Pornografía infantil: el convenio de Budapest define como pornografía infantil a todo material pornográfico que contenga la representación visual de un menor comportándose de una forma sexualmente explícita; una persona que aparezca con un menor comportándose de una forma sexualmente explicita; imágenes realistas que representan a un menor comportándose de una forma sexualmente explícita. La definición de menor estará bajo la concepción que tenga cada país; por ejemplo, en los países europeos se entiende que un menor es una persona que tiene hasta 18 años de edad; sin embargo, en Australia un menor es un adolecente que tiene hasta 16 años (Convenio sobre la Ciberdelincuencia, 2001). En Ecuador son menores de edad los jóvenes que tienen menos de 18 años.

De igual forma en el convenio se establecen los delitos relacionados con la pornografía infantil. Estos son:

a) la producción de pornografía infantil con vistas a su difusión por medio de un sistema informático;

b) la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático;

c) la difusión o transmisión de pornografía infantil por medio de un sistema informático;

d) la adquisición de pornografía infantil por medio de un sistema informática para uno mismo o para otra persona;

e) la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.

Ruiz (2017) afirma que hoy en día la pornografía infantil es uno de los negocios que genera más dinero en la red, pues el Internet ha permitido su fácil expansión y ha limitado la identificación y localización de los responsables de este hecho delictivo. "Según un estudio realizado por la Universidad de Porstmouth, el 80% del tráfico generado en la 'deep web' está relacionado con sitios web de pornografía infantil" (Tecnoxplora, 2015).

Delitos Contra la Propiedad Intelectual: La propiedad intelectual se relaciona con las creaciones de la mente: invenciones, obras literarias y artísticas, así como símbolos, nombres e imágenes utilizados en el comercio. Las legislaciones protegen a la propiedad intelectual a través de las patentes, el derecho de autor y las marcas (Organización Mundial de la Propiedad Intelectual, 2018).

Moisés (2018) expone que los derechos de autor integran los derechos de reproducción (capacidad exclusiva de autorizar la duplicación), la distribución (autorización a un tercero para la puesta a disposición del público del original o copias), la comunicación pública (el autoriza el número de personas que pueden ingresar a la obra) y la transformación (autorizar posibles trabajos derivados de la obra).

Las leyes que protegen la propiedad intelectual son insuficientes y no pueden

amparar las obras en el nuevo marco de la sociedad de la información e Internet. El Internet les ha permitido a los autores generar muchas ganancias, facilitando la mayor distribución de sus obras; sin embargo, la red presenta una cara oscura al no permitirle al autor controlar el número de copias o reproducciones que se hacen de su obra. Existen 3 modelos principales de difusión ilegal de contenidos en la red. Estos son las redes P2P, la centralización de contenidos (centran contenidos para los cuales no tienen licencia para su distribución) y la agregación de enlaces (Moises, 2018, pp. 11-23).

Delitos de calumnias e injurias: el Internet proporciona la difusión universal de difamaciones, calumnias e injurias. Injuriar y calumniar en Internet supone dar "publicidad" a los insultos, lo cual agrava la calificación de los mismos, puesto que el daño causado a la víctima es mayor que si se lleva a cabo en un ámbito acotado o privado. "Cuando alguien se excede en el ejercicio de su libertad de expresión entramos en el ámbito del delito" (García, 2015, párr. 2).

Las estafas, subastas y ventas ilegales en Internet: las estafas electrónicas "consistente en la manipulación informática o artificio similar que, concurriendo ánimo de lucro, consiga una transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero" (Iglesis, 2018, p. 7).

Según Oxman (2013) el *phising*, *pharming* y el *money mules* son formas de estafas informáticas que se dan en la red. A través del phishing los delincuentes obtienen los datos personales y/o financieros de la víctima por medio del envío masivo de correos electrónicos con enlaces a páginas web falsas en las que se imita el contenido o la imagen de una entidad financiera o bancaria. Sin embargo, el pharming utiliza otro tipo de mecanismo para realizar las estafas, pues en este caso los malhechores manipulan las direcciones DNS que son utilizadas por el usuario redireccionando a éste a la navegación de sitios web que son falsos y han sido creados con el objetivo de defraudar; por lo general la ejecución de este tipo de delitos lo realiza un grupo de vándalos transnacionales. En último lugar, con los anglicismos "money-mules", "phishing-mules" o "pharming-mules", hace referencia a una conducta de colaboración que opera con posterioridad a la consumación de la defraudación patrimonial. Ella consiste, esencialmente, en poner a disposición de los estafadores (*scammers*) el dinero obtenido por éstos a través del phishing o pharming la obtención ilícita de datos confidenciales asociados a cuentas (pp. 212-219).

BBC Mundo (2017) plantea que las ventas ilegales se dan ampliamente en la Internet profunda; allí se puede encontrar cualquier artículo ilegal y obtenerlo con facilidad. Los cibercriminales, ciberterroristas, *hackers*, entre otros tipos de delincuentes, son los que navegan por el Internet profundo o *darknet* para cometer sus actos dolosos. Los cinco productos más vendidos son drogas, armas, identificaciones y dinero falso, software para hacker y pornografía infantil.

Conclusiones

La mayoría de los delitos informáticos se dan porque los delincuentes usan la ingeniería social en sus víctimas; es decir, los delincuentes fingen tener empatía con sus víctimas para lograr que ellas se enlacen emocionalmente con ellos y por medio de este vínculo logran cumplir su cometido.

Las empresas públicas y privadas del Ecuador no tienen implantado un sistema de gestión de seguridad que les permita

mitigar el impacto de un ataque informático interno o externo.

En los sitios oficiales de los entes gubernamentales ecuatorianos encargados de combatir los delitos informáticos no existen estadísticas actuales sobre el impacto que provoca el mismo, lo que dificulta establecer cifras con relación al número de víctimas, tipos de delitos más efectuados y pérdidas económicas; esta falencia también imposibilita el poder definir estrategias que le permitan al estado combatir los delitos informáticos de forma efectiva.

El robo, hurto, estafa, pornografía, contrabando, entre otros delitos tradicionales, en la actualidad se realizan a través del uso de herramientas informáticas y del Internet. Estos delitos son cometidos por delincuentes que tienen un buen dominio en el uso de las TIC. Los delitos más graves como el narcotráfico, trata de blancas y pornografía infantil son cometidos en la Internet profunda, también llamada Internet oscura.

El Ecuador debe

- Adherirse al convenio de Budapest contra la ciberdelincuencia; de esta forma podrá aplicar los principios de la pirámide Kelseniana y llenar los vacíos legales que genera la falta de tipificación de los nuevos delitos informáticos en las leyes nacionales.
- Aprovechar la asistencia penal internacional para combatir la delincuencia informática.
- Educar a los ciudadanos en la prevención de delitos informáticos.

Referencias

Acurio del Pino, S. (2015). Plan Operativo de creación de la Unidad de Delitos Informáticos del Ministerio Público. Recuperado de http://www.oas.org/juridico/spanish/cyb_ecu_plan_operativo.pdf

BBC Mundo. (2017). Finanzas personales. Los 5 productos ilegales que más se venden en internet. Recuperado de http://www.finanzaspersonales.co/consumo-inteligente/articulo/cosas-ilegales-en-internet/60740

Consejo de Europa. (2001). Convenio Sobre La Ciberdelincuencia. Recuperado de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

De la Corte Ibáñez, L., & Blanco Navarro, J. M. (2014). Seguridad nacional, amenazas y respuestas. España: LID .

García, N. N. (2015). Cómo actuar si sufres calumnias e injurias en Internet. Recuperado de https://www.kaspersky.es/blog/como-actuar-si-sufres-calumnias-e-injurias-en-internet/6150/

Hernández Maldonado, K. (2016). Retos de la administración de juesticia penal frente a los delitos informáticos en el Ecuador. Recuperado de http://dspace.udla.edu.ec/bitstream/33000/6439/1/UDLA-EC-TAB-2016-71.pdf

Iglesis, C. F. (2018). La criminalidad en internet. Recuperado de http://abacus.universidadeuropea.es/bitstream/handle/11268/4954/Iglesias_Carballo_2001.pdf?sequence=1

Móises, B. A. (2017). Derecho Público e Internet: la actividad administrativa de regulación de la Red. Madrid: Colección Estudios y Documentos.

Moisés, B. A. (2018). Derecho público y propiedad intelectual: su protección en internet. Madrid: Editorial Reus.

Oficina de las Naciones Unidas contra la Droga y el Delito. (2013). El uso del internet con fines terroristas. Recuperado de https://www.unodc.org/...Internet.../Use_of_Internet_Ebook_SPANISH_for_web.pdf

Organización Mundial de la Propiedad Intelectual. (2018). La OMPI por dentro. Recuperado de http://www.wipo.int/about-wipo/es/

Oxman, N. (2013). Estafas Infromáticas a través de internet acerca de la imputación penal del "phishing" y el "pharming". Revista de derecho de la Pontificia Universidad Católica de Valparaíso, 262.

Rincón Rios, J., & Naranjo Duque, V. (2008). Delito Informático, Electrónico De Las Telecomunicaciones Y De Los Derechos De Autor. Cali: Grupo editorial Ibañez.

Ruiz Larrocha, E. (2017). Nuevas tendencias en los sistemas de información. Buenos Aires: Editorial Centro de Estudios Ramon Areces SA.

Sosa Meza, J. (2005). Aspectos generales y comparados de la Ley de Comercio Electrónico. Recuperado de https://www.derechoecuador.com/aspectos-generales-y-comparados-de-la-ley-de-comercio-electroacutenico

TECNOXPLORA. (2015). El 80% de lo que circula por la internet profunda es pornografía infantil. Recuperado de https://www.lasexta.com/tecnologia-tecnoxplora/internet/que-circula-internet-profunda-pornografia-infantil_2015011257f78f110cf2fd8cc6aa9ddf.html

Téllez Valdés, J. (2008). Derecho informático. México: MC Graw Hill.

Ureta Arreaga, L. A. (2009). Retos a superar en la administración de justicia ante los delitos informáticos en el Ecuador.(Tesis de grado). Escuela Superior Politécnica del Litoral. Guayaquil. Recuperado de https://www.dspace.espol.edu.ec/bitstream/123456789/5792/5/TESIS%20-%20delitos%20informaticos%20en%20ecuador%20y%20administracion%20de%20justicia.pdf

Zambrano Mendieta, J. E., Dueñas Zambrano, K. I., & Macías Ordoñez, L. M. (2016). Delito Informático. Procedimiento Penal en Ecuador. Dominio de las ciencias, 204-215. Recuperado de https://dialnet.unirioja.es/descarga/articulo/5761561.pdf