DELITOS INFORMÁTICOS: UNA REVISIÓN EN LATINOAMÉRICA

González J.; Bermeo, J.; Villacreses, E.; Guerrero, J.

Universidad Técnica de Machala

jgonzalez@utmachala.edu.ec

RESUMEN

En el presente apartado se aborda el tema de los delitos informáticos, en la sociedad contemporánea que ha adaptado la informática como base para gestionar sus actividades. Es indudable que los avances tecnológicos y el disponer de la información han facilitado el crecimiento de las naciones, pero este progreso ha ido acompañado de nuevas y evolucionadas formas de realizar actividades ilícitas, siendo actos vandálicos más sutiles sin trascendencia física pero un gran daño intangible a los recursos ya sean públicos o privados, esta es una de las razones por las que el objeto de este artículo es el de explicar acerca de los delitos informáticos, sus características, clasificación, la legislación que existe entre los distintos países para constatar qué medidas ha tomado el Ecuador al tratar con esta nueva delincuencia que aún no ha sido procesada adecuadamente dentro del marco legal nacional; como metodología de la investigación se aplica el método confirmatorio, además de ser de tipo descriptiva, de esta manera se llevó a cabo el análisis de diferentes artículos, lo que permitió evaluar e identificar los riesgos presentes en este tipo de delitos; a partir del estudio realizado se concluye que a pesar de los esfuerzos realizados por los diferentes naciones, aún persisten este tipo de prácticas, debido a que en la actualidad las leyes sancionan fútilmente esta traza de delitos.

Palabras clave: Delitos Informáticos, normas jurídicas, seguridad, políticas.

ABSTRACT

This paragraph deals with the issue of computer-related crime, in the contemporary society which has adapted the informatics as basis to manage their activities. There is no doubt that technological advances and the availability of information have made the growth of Nations easier, but this progress has been accompanied by new and evolving forms of illegal activities, which becomes more subtle vandalism without physical transcendence but a great and intangible harm to resources, no matter whether they are public or private, this is one of the reasons why the objective of this article is to explain about cybercrime, its characteristics, classification, and the current legislation from other countries to verify what actions have been taken in Ecuador around dealing with this new crime that has not been processed the proper way within the National regulations. The confirmatory method has been applied as researching methodology, besides being descriptive type. Various related articles have been analyzed, which has allowed the researchers to identify and evaluate the potential risks of this type of crime. According to the research done, it might be concluded that in spite of the great effort

of the countries to stop it, this type of crime still remains since, regulations slightly sanction it.

Keywords: Computer-related crime, legal rules, security policies.

INTRODUCCIÓN

En la actualidad los equipos informáticos no solo son utilizados como herramientas auxiliares ante las diversas actividades que se ejercen diariamente, sino que también se ubican en un nivel que permite obtener y conseguir información, por lo que son consideradas como medios de comunicación, gracias a ello la informática se encuentra presente en casi todos las actividades de las personas y son utilizadas en tareas que antes únicamente se realizaban de forma manual, esto conlleva a que se digitalice la información siendo almacenada en PCs, servidores o medios virtuales, dejándola propensa a ser suscitada sin autorización.

La evolución en el manejo, potencia y versatilidad del software-equipos informáticos ha sido tan rápida que antes se podía tener la entera certeza que nadie era capaz de hurtar información personal, sin embargo esto es pasado, debido a la globalización de los procesos la explosión de las industrias computacionales e informáticas ha permitido la creación de un sistema, que puede guardar grandes cantidades de información y transmitirla en muy poco tiempo, cada vez más personas acceden a dichos contenidos, sin que las legislaciones sean capaces de regularlos.

Los progresos tecnológicos a nivel mundial, así como el incremento de la capacidad de almacenamiento que tienen los equipos electrónicos en la actualidad, hacen más difíciles las tareas de control, es muy difícil legislar tal cantidad de dispositivos a la par con la conducta de sus usuarios que además están influenciados por las presiones sociales que incitan a las masas a buscar nuevas formas de obtener dinero, bajo este contexto abordar el estudio que tienen las actividades informáticas en delitos, resulta un asunto complejo para quien busca determinar el impacto de las nuevas tecnologías en los entornos sociales. Es decir, el desarrollo y la masificación de las nuevas tecnologías en la informática, han contribuido a los estudios que en ámbito jurídico buscan regular estas actividades con la meta de crear accionantes legales por medio del debido proceso den solución a conflictos enmarcados en el contexto descrito anteriormente.

Resulta importante analizar que de forma paralela a los avances tecnológicos y la influencia que se ha ejercido en el entorno de las personas, se han terminado llevando a cabo comportamientos delincuenciales, que antes no eran posibles de imaginar y en algunos casos de difícil tipificación en las normas penales tradicionales, sin recurrir a aplicaciones analógicas prohibidas por el principio de legalidad.

Los delitos informáticos se han desarrollado al mismo tiempo que las tecnologías de la información, con el auge de las tecnologías, la sociedad se ha visto sumergida en un avance y desarrollo en cada una de sus áreas, donde la delincuencia también se ha visto beneficiada, ahora tienen la capacidad de cometer un acto ilegal desde

cualquier lugar del mundo, con gran acceso informático, a más de la ventaja del anonimato.

Las razones mencionadas son las que demuestran la importancia del tema de la investigación acerca de las nuevas formas jurídicas, siendo de esta manera que la documentación presente ha fijado la tarea de explicar acerca de los delitos informáticos, sus características, clasificación, la legislación que existe entre los distintos países en contraste con las medidas consideradas hasta ahora en las normativas nacionales para linealizar el mejor camino a tomar para tratar con esa nueva forma de delincuencia.

DESARROLLO CONCEPTUAL

Delitos informáticos

El término delito informático se utilizó por primera vez a finales de los años noventa, a medida que Internet se extendía por el mundo. Con el uso del internet, se dio inicio a nuevos problemas por lo que las naciones que conforman el grupo denominado G8, mantuvieron una reunión en Lyon, Francia, con el propósito de estudiar estos problemas emergentes relacionados con la delincuencia que migraron sus actividades al internet. En la reunión se utilizó el término delito informático para describir de forma imprecisa aquellos delitos que se cometieron con el uso de redes informáticas. Al mismo tiempo, y guiado por los participantes en el grupo de Lyón, el Consejo Europeo comenzó a diseñar el Tratado sobre Delito Informático (Alcívar, Domenech & Ortíz, 2015),

Al delito informático se lo puede definir como cualquier actividad en la cual a través del uso de las computadoras, para cometer un delito, estos pueden constituirse en nuevas formas penales donde se incluyen como elementos primarios al internet y a la computadora como instrumentos físico. 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 (Ferruzola, 2014).

Es importante mencionar que la criminalidad informática tiene un alcance mayor y puede incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos en los cuales ordenadores y redes han sido utilizados como medio. Con el desarrollo de la programación y de Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados (Alcívar, Domenech, & Ortíz, 2015).

Se hace importante la implementación de medidas preventivas, estas pueden ser de carácter administrativo o penal que debe ser considerado para evitar que este tipo de delito crezca a dimensiones considerables. No cabe duda que el desarrollo tecnológico actual ha traído ventajas para las personas, pero a su vez esto ha venido acompañado hechos delictivos siendo necesaria tomar acciones para estudiar e indagar su accionar delictivo (Herrera, 2014).

Como medida preventiva y de seguridad es indispensable que al momento de realizar cualquier tipo de transacción mediante el uso de internet, siendo clave las medidas de seguridad en las creaciones de los sitios web que permitan a los usuarios realizar sus actividades y transacciones con seguridad (Lara & Albán, 2017).

A nivel de América Latina, estas actividades delictivas han tenido un gran crecimiento, el incremento de la delincuencia informática de debe a un gran número de factores que hacen que la tipificación del delito sea una tarea compleja. De esta manera el incremento de la tecnología en las actividades, tanto para los usuarios como para los delincuentes, sumado al escaso conocimiento sobre cómo protegerse y actuar ante los diferentes delitos de los cuales pueden ser víctimas (Temperi, 2013).

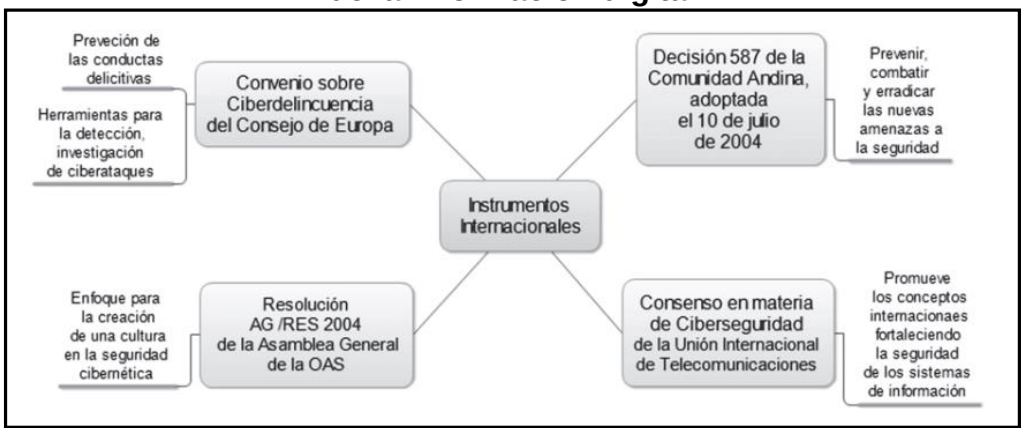
En el Ecuador las investigaciones realizadas acerca de pericia informática son de bajo interés, una de las causas es el desconocimiento del tema por parte de la sociedad, adicional a la falta de procedimientos registrados de delitos informáticos competentes a las autoridades o entidades gubernamentales. La fallas principales de la pericia informática en el Ecuador es la carencia de profesionales que tengan conocimientos informáticos adecuados obteniendo como resultado impunidad de casos, debido a la falta de conocimientos, pocas habilidades idóneas para la utilización de medios tecnológicos en la adquisición de pruebas, y una correcta legislación de acuerdo a los delitos informáticos actuales (Bolaños & Gómez, 2015).

Seguridad

Es indispensable que en el análisis de los hechos al momento de generarse un delito informático con el propósito de cuidar y prevenir sobre los riesgos a lo que pueden incurrir las personas o diferentes instituciones, también es importante la prevención y detección de estos a través de diferentes herramientas que permiten evaluar los problemas más comunes en las estafas presentadas en los ciberataques. Por lo anterior, se debe conocer cómo actuar frente a las diferentes situaciones que se puedan presentar en una entidad y conocer las herramientas de la auditoría en el área informática para la identificación y evaluación de los riesgos presentes en las estafas comunes de los ciberataques financieros (Harnández, Cerquera, & Vanegas, 2015).

El panorama mundial en lo correspondiente a la seguridad cibernética, se han evaluado las tendencias más importantes en lo correspondiente a las amenazas cibernéticas y quienes se ven afectados, quienes pueden ser desde instituciones gubernamentales, hasta empresas privadas y usuarios individuales. Asimismo, en la siguiente figura, se observa los informes generados en los encuentros internacionales asumidos por diversos países, para contrarrestar los ciberataques, en la Fig. 1. Se aprecian los instrumentos internacionales para asegurar la integridad de la información digitalizada.

Figura 1. Instrumentos Internacionales en orientación para el aseguramiento de la información digital



Fuente: Comisión de Regulación de Comunicaciones de la República de Colombia, 2015

Políticas de seguridad informática

Las políticas de seguridad informática se han convertido en una forma de comunicarse con las personas, ya que a través de ellas se establecen canales de comunicación con relación a los recursos y servicios informáticos. Una política de seguridad no puede ser considerada como una descripción técnica de mecanismos, ni tampoco una expresión legal que conlleve a sanciones, sino que más bien es una descripción de lo que se desea proteger y la razón para ello, debido a que cada política de seguridad es un reconocimiento de que la información es uno de los principales activos así como también un motor de intercambio y desarrollo en el ámbito de los negocios. Por tal razón, las políticas de seguridad deben incluir una posición preventiva acerca del uso y limitaciones de los recursos y servicios informáticos.

Tipos de delitos informáticos

De acuerdo a Lara, Martínez & Viollier (2014), se considera para los delitos informáticos las siguientes categorías:

1. El acceso no autorizado: es el acceso sin derecho a un sistema o a una red, donde son violadas las medidas de seguridad, llega también a ser conocido como hacking.

2. El daño a los datos o programas informáticos: es el borrado, descomposición, deterioro o supresión de datos o programas informáticos sin que la persona tenga derecho a realizar esa acción.

3. El sabotaje informático: se refiere a la introducción, alteración, eliminación de datos o programas, la interferencia a los sistemas informáticos con el propósito de ser un obstáculo en el funcionamiento de las redes.

4. La interceptación no autorizada: se refiere a la captación que se realiza sin autorización a través de mecanismos tecnológicos.

5. El espionaje informático: se entiende como la adquisición, revelación, transferencia de información confidencial de tipo comercial sin que se tenga la debida autorización, con el propósito de causar pérdidas económicas o de obtener algún beneficio.

Delitos informáticos y normas jurídicas

Las normas que rigen las actividades que se realizan por medio del internet y el cual resulta insuficiente ante las diversas actividades que se llevan a cabo por medio de la red. Las diferentes nacionalidades que se concentran y las diferentes posturas que asumen frente a la regulación del internet en general, lo que ha llegado a convertirse en un reto de tipo jurídico para el derecho nacional e internacional (Arévalo, Navarro, García, & Casas, 2011).

Es importante que se ponga en conocimiento de las dificultades que se atraviesa para lograr la comprobación de este tipo de delitos, debido al volumen de los mismos y a la posibilidad de que el autor utilice una falsa identidad lo que dificulta su localización a través de la red, especialmente cuando estas se encuentran situadas en el extranjero. Esto conduce a que sea difícil determinar el lugar de cometimiento del delito, el cual es un elemento del que depende la competencia territorial e inclusive la jurisdicción de las autoridades judiciales (Picotti, 2013).

La preocupación generada a nivel mundial, se encuentra impulsando y apresurando cualquier tipo de acción local, donde se incluyen compromisos multilaterales y bilaterales, con el propósito de combatir esta gran amenaza, en la actualidad ningún país, ni siquiera el de mayor desarrollo permanece inmune ante esta amenaza (Sorj, 2013).

En la actualidad existen dos organismos internacionales que se encuentran relacionados con el combate a este tipo de crímenes; el Convenio de Budapest y las Naciones Unidas por medio de la Comisión de Prevención del Delito y Justicia Penal; el cual se convirtió en el primer tratado internacional sobre este tipo de delitos, donde también se considera algunos procedimientos como la búsqueda de las redes informáticas y la intercepción legal (Argüelles, 2016).

La Comisión de Prevención del Delito y Justicia Penal (1992) es el órgano principal del sistema de las Naciones Unidas para formular políticas y recomendaciones sobre cuestiones de la justicia penal, incluida la trata de seres humanos, los crímenes transnacionales y los aspectos de la prevención del terrorismo. La Comisión supervisa el uso y la aplicación de las normas de las Naciones Unidas relativas a estas cuestiones y guía el desarrollo de políticas para abordar nuevas cuestiones (Argüelles, 2016).

Delitos informáticos en el Ecuador

En Ecuador, como en todos los países, existen delitos informáticos, en el 2013, se registró un aumento en la cantidad de quejas cibernéticas de los ciudadanos en las autoridades nacionales en Ecuador. Los ciudadanos reportaron casos relacionados con ataques de interceptación ilegales sobre la integridad de la información, dispositivos de abuso de sistemas, ciber falsificación, fraude informático, pornografía infantil y delitos contra la propiedad intelectual. Desde el 10 de agosto, cuando entró en vigencia el Código Orgánico Integral Penal, hasta el 31 de mayo del 2015, se registraron 626 denuncias por delitos informáticos en la Dirección de Política Criminal de la Fiscalía General (López, 2017).

MATERIALES Y MÉTODOS

La investigación nace a partir de un estudio confirmatorio mediante la investigación mixta en el uso de metodología cualitativa y cuantitativa. La investigación mediante métodos mixtos ha sido muy utilizada para estudiar los delitos informáticos mientras que los estudios exploratorios cualitativos, seguidos de estudios confirmatorios, han sido comunes y concurrentes (Pereira, 2011).

Los materiales utilizados en el desarrollo del artículo son principalmente los siguientes:

- Papers indexados tomados de bases de datos certificadas.
- Normativas jurídicas afines al tratamiento de delitos informáticos.
- Documentaciones donde se detallen casos particulares sobre medidas legales que se han tomado en favor de tratar algún delito informático.
- Leyes nacionales e internacionales que describan accionantes relacionadas al proceso para tratar delincuencia informática.

Los procesos investigativos empleados en la obtención de la información son:

- **Análisis Comparativo:** Es necesario para contrastar e interpretar las medidas que se ha tomado en casos afines a nivel internacional mediante la lectura crítica de artículos que mencionen el delito informático.
- **Observación:** Permite apreciar el contexto nacional o local sobre la temática, sirve para analizar desde una perspectiva objetiva las medidas a considerar para tratar a los delitos informativos en función del peligro que representan para la sociedad nacional.
- **Descripción:** Facilita la comprensión de la temática, gracias a que es clave para identificar los riesgos que representan los delitos informáticos en base a un síntesis clara y concisa.
- **Método cualitativo-cuantitativo:** Se requiere para medir en base a datos internacionales la incidencia de los delitos informáticos en la sociedad, dando una evaluación cualitativa sobre los riesgos de este tipo de delitos en la sociedad ecuatoriana.

Para llevar a cabo la investigación en la cual se identifican y se evalúan los riesgos presentes en los delitos informáticos se realizó la búsqueda en diferentes bases de datos de artículos científicos, y en páginas de internet de fuentes confiables, que permitan a partir de las investigaciones realizadas detectar los procesos generados, los riegos latentes y las herramientas utilizadas en las legislaciones de los diferentes países.

DISCUSIÓN DE RESULTADOS

Se pretende describir las características de cada una de las leyes de la región en donde es posible encontrar similitudes y diferencias entre cada una de ellas, y así analizar como los países enfrentan la lucha contra la criminalidad informática, luego se imparte una síntesis contextual de los delitos informáticos a nivel nacional, describiendo como ha reaccionado el país ante estaos actos ilícitos. En la tabla 1 se resume los delitos y medidas que han considerado los países latinos para combatir la ciberdelincuencia.

Figura 3. Principales causas de los ciberdelitos a nivel nacional

Delito	País	Gestiones Realizadas
Ciberpornografía Violación de secretos y privacidad Daños a documentos, programas o sistemas operativos Estafa y fraudes	Argentina	Prioriza la firma digital y documentos privados, modificando su código penal para sancionar delitos informáticos.
Daños o hurto en sistemas de información	Chile	Regula la firma digital y documentos electrónicos en la administración del estado.
Obstaculización ilegitima de sistemas informáticos Interrupción de datos informáticos Daño informático Uso de software malicioso Violación de datos personales Hurto por medios informáticos Transferencias no consentida de activos	Colombia	Formó la le de protección de la información de Datos, se agregaron varios artículos que permiten penalizar acciones ilícitas referentes a la informática
Violaciones electrónicas Fraude Informático Sabotaje de redes en internet	Costa Rica	Se creó leyes para tipificar ciberdelitos.
Comercialización de pornografía Infantil Derechos de autor-intelectuales	Paraguay	Crea nuevos tipos penales y ejercer regulación en el proceder de las investigaciones, tífica delitos

Sabotaje de computadoras Alteración de datos Operaciones fraudulentas		cibernéticos, amalgame leyes para que la policía actué sin ataduras legales
Contenido Pornográfico Divulgación de información confidencial	Uruguay	No posee leyes especificas contra delitos informáticos
Robo de información personal Reproducción de programas informáticos Acceso no autorizado a dispositivos Interrupción de servicios telemáticos o informáticas a entidades públicas Imágenes sexuales protagonizadas por menores	Brasil	Implementó leyes para legislar delitos informáticos, dando la potestad de ser iniciada por la persona o entidad ofendida.
Son considerados como delitos comunes	Bolivia	Sanciones y acciones se incluyen en el código penal no posee una ley específica
Sanciona toda conducta delictiva	Venezuela	Ofrece definiciones y conceptos ante delitos informáticos, es una de las leyes más completas- complejas.
Revelación ilegal de bases de datos Interceptación ilegal de datos Transferencia electrónica de dinero ilegal Ataques a integridad de sistemas informáticos Acceso a sistemas de telecomunicaciones Acoso sexual y pornografía infantil	Ecuador	Se implementó el Código Orgánico Integral Penal desde el 2014, que contempla y sanciona delitos informáticos

Se observa que se ha generalizado las definiciones, leyes y contramedidas para tratar contra delitos informáticos, principalmente se busca sancionar, evitar y procesar este tipo de actos, entre los países se destaca Paraguay que no solo ha incursionado en reformas legales al dotar de poder al cuerpo policial para actuar sino que legisla de una forma íntegra proporcionando incisos que amalgaman sus reglamentaciones facilitando la labor nacional de actuar; además propone nuevos métodos investigativos para combatir abiertamente los ciberdelitos.

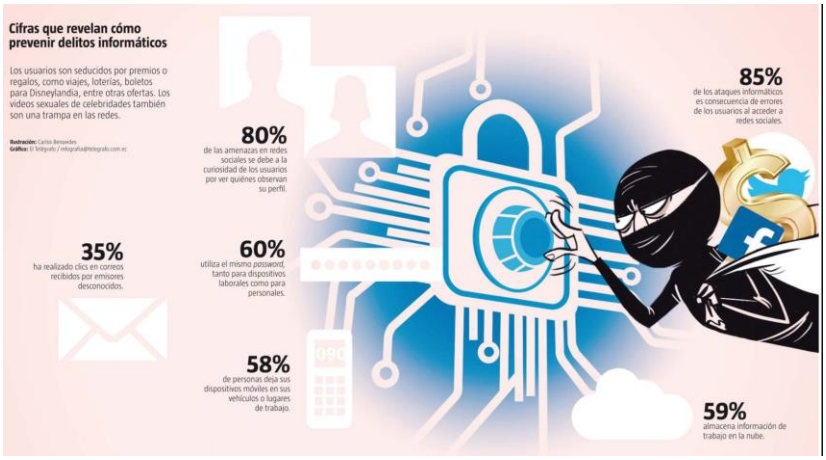
Colombia también ha derogado medidas legales contra actos vandálicos cibernéticos priorizando la proyección de los datos e información personal, Venezuela ha dotado de leyes más completas dando potestad a todos sus departamentos para interceptar y procesar estos actos sin ataduras legales pertinentes; además a manera general los

países latinos han implementado leyes para proteger la información de entidades públicas, combatir la pornografía infantil, caracterizando la firma digital e integración de seguridad informática a sistemas de bases de datos. Estas medidas si bien son eficaces aun no son suficientes para frenar en su totalidad a los delitos informáticos debido a que operan a gran escala y de múltiples formas dificultando así capturar a los culpables o tomar acciones competentes.

En Ecuador, la Fiscalía General del Estado registró 530 delitos informáticos en los primeros cinco meses de 2016, en el mismo período del año anterior se presentaron 635 denuncias. Las cifras evidencian una disminución. En Guayas hubo 18 casos; Pichincha, 145; Manabí, 24; El Oro, 22; en el resto de provincias se registró una cantidad menor. La mayoría de denuncias (368) corresponde al delito de "apropiación fraudulenta por medios electrónicos".

Un estudio elaborado por la Policía Nacional, Interpol, el centro de respuesta a Incidentes Informáticos de Ecuador (Ecucert), con el soporte de organismos similares de América Latina, indica que el 85% de los ataques a los sistemas informáticos son causados por errores de los consumidores, quienes no toman precauciones al acceder a las redes sociales, utilizar el correo electrónico, y en el uso de usuario y contraseña (El Telégrafo, 2016).

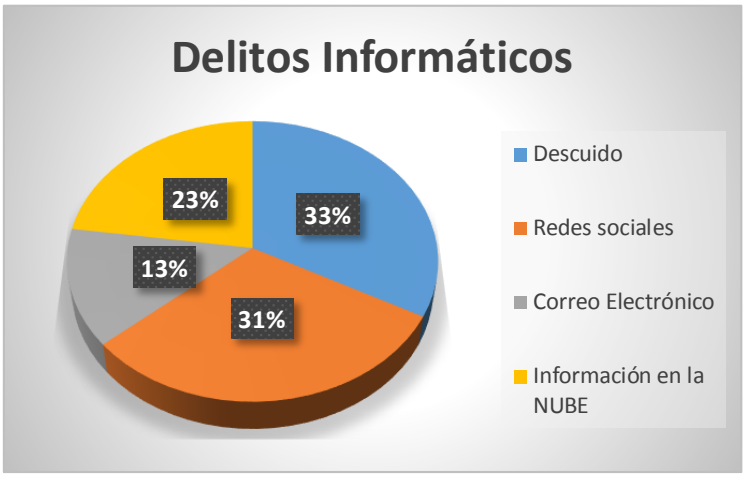
Figura 2. Ciberdelitos en Ecuador durante el año 2016



Fuente: El Telégrafo, 2016.

Desde que entró en vigencia el Código Orgánico Integral Penal se contempla y sanciona los delitos informáticos como: la revelación ilegal de base de datos, la interceptación ilegal de datos, la transferencia electrónica de dinero obtenido de forma ilegal, el ataque a la integridad de sistemas informáticos, los accesos no consentidos a un sistema telemático o de telecomunicaciones, la pornografía infantil y el acoso sexual (Policia Nacional del Ecuador, 2015). En la figura 3 se expresa el porcentaje de las causas que facilitan los delitos informáticos en el Ecuador.

Figura 3. Principales causas de los ciberdelitos a nivel nacional



Fuente: Yepez Flores & González Sánchez (2017)

El Ecuador se ha quedado atrás en la aplicación de leyes, las medidas tomadas son algo rígidas e impiden el pleno desempeño de las autoridades locales, se debe en parte a que no se acostumbra a usar licencias ni respetar derechos de autor, solo se reacciona ante pérdidas económicas, no obstante solo los bancos y entidades financieran se protegen contra tales vulnerbaildiades.

La reforma en el Código Orgánico Integral Penal ha dado los lineamientos para actuar, ejecutar el debido proceso contra ciberdelicos; sin embargo, no es versátil frente a la abundancia de estos actos, solo en el 2016 se registraron 530 casos, donde la mayor parte se efectuan por descuido propio de los usuarios, dejando contraseñas, olvidando celulares, aceptando correos electrónicos a desconocidos, usando una misma cuenta para varios servicios informáticos, 23% son delitos intencionados contra bases de datos en la Nube realizados por hackers que buscan enriquecerse ilegalmente, 31% se registran, estafan o actos fraudulentos mediante las redes sociales.

El país necesita concientizar a la población sobre el uso de los recursos informáticos y ha de tomar con seriedad los riesgos que estos conllevan no solo a nivel personal ni económico sino en el desempeño mismo de la sociedad que es altmente vulnerable a golpes delictivos en el ciberespacio por la falencia en sus sistemas de seguridad y la falta de accionantes para contraatacar a este tipo de delincuencia.

Los delitos informáticos son muy comunes en la actualidad, los delincuentes hacen uso de diferentes modalidades en la red para actividades delincuenciales, como incurrir en hurtos, estafas o interferencias por medio de las redes hacia las personas o cualquier entidad. Este es uno de los principales motivos por los que se han llegado a diseñar innumerables mecanismos de control y prevención para evitar este tipo de actividades, de tal manera que toda institución, sea esta pública o privada desarrolla políticas o procedimientos ante actividades que resulten sospechosas.

Es importante el control en todas las actividades que se realicen dentro de las organizaciones, especialmente con sus empleados en cuanto a la documentación que ingresa y sale de las oficinas, en los correos electrónicos y en el uso de las redes. Un factor a considerar es la seguridad de las organizaciones para evitar cualquier tipo de interferencia y uso no autorizado de información confidencial.

Un tema relevante también lo es el estar al tanto del cometimiento de esta tipo de delitos, el desconocimiento ha sido la causa principal de tantos perjuicios, impunidad ante los delitos y de desorientación. El uso de las redes es muy amplio y los delincuentes se encuentran más que capacitados para cometer delitos donde su ubicación y sanción resulta con dificultades si las personas carecen de los medios y conocimientos adecuados (Arocena & Esparza, 2017).

CONCLUSIONES

Resulta evidente que en la mayoría de los países estudiados, aún persisten en algunos casos los vacíos legales con respecto a la regulación del uso de la información a partir de los diferentes medios de comunicación. A pesar que han sido múltiples los esfuerzos de los gobiernos en la lucha contra este tipo de delitos, donde se incluye la piratería, difusión de pornografía infantil, así como el uso inadecuado de la información con diferentes fines; lamentablemente aún persisten este tipo de prácticas.

Los delitos informáticos no se pueden erradicar de un día para otro, pero si es posible y urgente legislar y aplicar la ley para el combate a estos delitos con más rigor, pues aunque las autoridades competentes pongan a disposición de un Ministerio Público a estas bandas delictivas o actores individuales, lamentablemente no se tienen elementos suficientes para atribuirles en algunos casos responsabilidades por la falta de claridad en las leyes.

A nivel nacional se detectan varias falencias en el sistema jurídico que no prioriza el accionar publico frente a estos actos que sumado a la falta de conocimiento de la población, ocasiona un medio fácil para los ciberdelitos gracias a que no se protege la integridad de la información virtual ni se respetan espacios intelectuales.

Las medidas a tomar en el Ecuador deben ser claras, en primera instancia capacitar a la ciudadanía sobre realidad de estos delitos, implementar reformar a su código penal para actuar libremente mediante la aplicación de leyes dinámicas que se actualicen según se detecten el modo de operar de los responsables, además mejorar los sistemas de seguridad a nivel nacional en todos los entornos virtuales no solo en bancos sino en sitios gubernamentales y aplicar códigos para regular el uso de las redes sociales al ejecutar dichos actos vandálicos.

REFERENCIAS BIBLIOGRÁFICAS

Alcívar, C., Domenech, G. & Ortíz, C. (2015). La seguridad jurídica frente a los delitos informáticos. *Avances*, 10(*12*), 41-57.

Arévalo, P., Navarro, J., García, F., & Casas, C. (2011). Modelos de regulación jurídica de las redes sociales virtuales. *Revista VIA IURIS,* 11, 109-135.

Argüelles, M. (2016). Retos de la legislación informática en México. *Computación y Sistemas,* 20(*4*), 827-831.

Arocena, L. & Esparza, I. (2017). Los retos procesales de la criminalidad informatica desde una perspectiva española. *NOVUM JUS,* 11(*1*), 39-72.

Bolaños, F. & Gómez. (2015). Estudio cualitativo de la relación de las leyes y la pericia informática en el Ecuador. *ReCIBE,* 4(*3*), 1-32.

El Telegráfo. (2016). *85% de los delitos informáticos ocurre por descuido del usuario.* Quito: El Telégrafo.

Ferruzola, E. (2014). ¿Cómo responder a un delito informático? *Ciencia Unemi*, 11, 43-50.

Harnández, L., Cerquera, J. & Vanegas, J. (2015). Riesgos presentes en los ciberataques: un análisis a partir de herramientas de auditoria forense. *Pensamiento Republicano*, 3, 57-76.

Herrera, R. (2014). Breve análisis y algunas observaciones al delito informatico. *Revista de Investigación Jurídica de Estudiantes*, 5(*5*), 1-12.

Lara, E. & Albán, L. (2017). Los riesgos de las transacciones bancarias por Internet. *Revista Publicando*, 10(*1*), 62-74.
Lara, J., Martínez, M. & Viollier, P. (2014). Hacia una regulación de los delitos informáticos basada en la evidencia. *Revista Chilena de Derecho y Tecnología*, 3(*1*), 101-137.

López, M. (2017). Hacking ético. Vulnerabilidad de Sistemas Operativos en el acceso por contraseñas. *Revista Publicando*, 10(*1*), 31-51.

Pereira, Z. (2011). Los diseños de método mixto en la investigación en educación: Una experiencia concreta. *Educare*, 15(*1*), 15-29.

Picotti, L. (2013). Los derechos fundamentales en el uso y abuso de las redes sociales en Italia: aspectos penales (II). *IDP,* 17, 63-76.

Policia Nacional del Ecuador. (2015). *Delitos informáticos o ciberdelitos*. Quito: Policía Ecuador.

Sorj, B. (2013). Brasil y América Latina: ¿Qué Liderazgo es Posible? *Plataforma Demócratica.*

Temperi, M. (2013). *Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado.* Argentina: Universidad Nacional del Litoral.