Debate Jurídico Ecuador. Revista Digital de Ciencias Jurídicas de UNIANDES
Vol. 2 / Nro. 1 / enero-abril / Año. 2019 / pp. 45-59

**ARTÍCULO CIENTÍFICO**

**DERECHO INFORMÁTICO**

# LOS DELITOS INFORMATICOS Y SU INCIDENCIA EN LA PROVINCIA DE PASTAZA

# CRIME AND ITS INCIDENCE IN THE PROVINCE OF PASTAZA

**Velastegui Córdova, Miguel Eduardo [I];**

I. miguelalbo@yahoo.es Universidad Regional Autónoma de los Andes, Puyo, Ecuador

Recibido: 01/07/2018

Aprobado: 21/09/2018

**RESUMEN**

En la actualidad a internet se conectan millones de personas de todo el mundo, llevando excesivo tráfico, generando volúmenes incalculables de información; debido a esa gran demanda de usuarios, se ha dado paso a que personas de distintos lugares del planeta, permanentemente intercambien información de forma deliberada, exponiendo públicamente sus datos que hasta cierto modo comprometen su identidad e integridad. El objetivo de esta investigación corresponde a un análisis crítico reflexivo, sobre el incremento de casos de este tipo de delitos en la Provincia de Pastaza. La metodología aplicada correspondió al paradigma cuali-cuantitativo; técnicas como entrevista y encuesta permitieron recoger información relevante sobre el problema investigado, arrojando resultados alarmantes que ameritan ser investigados. Al tratarse de un tema de actualidad, es necesario realizar acciones concretas, tendientes a disminuir el alto índice de estos delitos, que aqueja a varias personas en la Provincia de Pastaza.

**PALABRAS CLAVE:** Delitos informáticos, fraude, estafa, red, web.

**ABSTRACT**

The internet connects millions of people around the world, carrying excessive traffic, generating incalculable volumes of information; Due to this great demand of users, people from different parts of the planet have been permanently exchanging information in a deliberate way, publicly exposing their data that compromise their identity and integrity to some extent. The objective of this investigation corresponds to a reflexive critical analysis on the increase of cases of this type of crime in the Province of Pastaza. The applied methodology corresponded to the qualitative-quantitative paradigm; techniques such as interview and survey allowed to collect relevant information about the problem under investigation, yielding alarming results that merit investigation. Being a current issue, it is necessary to take concrete actions, tending to reduce the high rate of these crimes, which afflicts several people in the Province of Pastaza.

**KEYWORDS:** Computer crimes, fraud, fraud, network, web**.**

## INTRODUCCIÓN

A partir de la década de los setenta, cuando se envía por primera vez el primer correo electrónico, se produce un nuevo cambio paradigmático en la sociedad (Rodríguez-Acosta, 2018), (Piscitelli, 2002), debido al uso cada vez más frecuente del internet.

El concepto de la web ha ido evolucionando, debido a la calidad de su contenido y a los servicios que se han ido incorporando posteriormente, tales como redes sociales, blogs, foros, chats, sitios de noticas, entre otros; dando la posibilidad de que los usuarios puedan interactuar de forma masiva; creándose grandes grupos de personas, que permanentemente interactúan por este medio, lo que convierten a internet, en la red más grande y con alta demanda en todo el mundo (Torres Moreno, 1998).

La web 2.0, aparece como un nuevo concepto, el mismo que se basa en el trabajo colaborativo de varias personas, la misma que centra la atención en los usuarios, quienes a su vez son los creadores de contenido o colaboradores en una comunidad virtual, sean estos: Redes sociales, wikis, alojamiento de videos, aplicativos webs, blogs, *mashups*, entre otros (Tello Leal, Sosa Reyna, Lucio Castillo, & Flores Morelos, 2010).

A medida que han incrementado los servicios en la web, también han incrementado los delitos relacionados al uso de esta tecnología y medio de comunicación. Para (Suarez-Sánchez, 2009) el delito informático puede ser definido como una ”conducta delictiva a través de medios o elementos informáticos, o a los comportamientos ilícitos en los que aquellos sean su objeto,

sino también a la afectación de la información *per se* cómo bien jurídico tutelado, diferente de los intereses jurídicos tradicionales" (pág. 73).

Albazuri-Romero (2002), considera a los delitos informáticos como "aquella acción dolosa, anti jurídica que provoca un perjuicio a personas o entidades, que se da por vías informáticas y en la que intervienen dispositivos o programas informáticos que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet" (pág. 1).

Por su parte, el abogado David Narváez considera que no se debería hablar de delitos informáticos, sino mas bien se debería hablar de infracciones informáticas, principalmente por que muchas de los actos humanos antijurídicos en los que pueden intervenir sistemas informáticos únicamente podrían ser considerados como contravenciones (Narváez-Montenegro, 2015, pág. 53).

Como características principales de este tipo de delitos, se puede mencionar las siguientes: 1) son acciones ocupacionales, 2) son operaciones de oportunidad, 3) ofrecen posibilidades de tiempo y espacio, 4) existen muchos casos y pocas las denuncias presentadas, 5) presentan muchas dificultades para su comprobación, 6) son tendientes a proliferar cada vez más (Téllez-Valdéz, 2008, pág. 188).

Dentro de los delitos informáticos se identifican dos clases: a) los delitos que causan mayor impacto en las organizaciones tales como fraudes y sabotajes y b) los más difíciles de detectar; debido a que son producidos generalmente por personas que laboran en las mismas empresas, las cuales tienen conocimiento de las configuraciones de las plataformas tecnológicas; frecuentemente en cooperación con los mismos empleados y con terceros.

A criterio de Narváez-Montenegro (2015), no existe un criterio común para la clasificación de los delitos informáticos, de ahí que este autor clasifica a las infracciones informáticas en: 1) acceso indebido, 2) daño a sistemas informáticos, 3) registro indebido de pulsaciones, 4) transacciones que afectan al sistema financiero, 5) delitos contra la intimidad y el honor, 6) delitos informáticos de afectación social, 7) delitos informáticos contra la propiedad intelectual, 8) estafa informática, 9) intercepción de datos informáticos, 10) pornografía infantil, 11) falsedad, 12) usurpación de identidad en redes sociales y direcciones electrónicas, 13) hostigamiento psicológico, 14) de las tecnologías y herramientas informáticas y 15) de la instrucción libre.

Los atacantes informáticos son personas con altos niveles de conocimiento, expertos en seguridad informática, redes, conectividad, programación de sistemas, protocolos de

comunicaciones, entre otras áreas; los mismos que aprovechando de su conocimiento y habilidad cometen este tipo de delitos, generando serios problemas a personas y a las organizaciones en general.

Dentro de los tipos de atacantes más conocidos están los *hackers*, *cracker*, *crasher, phisher, sniffer*, ciberterroristas, l*ammers* (Salcedo, Fernández, & Castellanos , 2012). Los métodos y técnicas que utilizan los delincuentes informáticos, no son las mismas que utiliza la delincuencia común; ya que, para el cometimiento del delito, necesitan experticia tecnológica, herramientas, medios electrónicos y programas informáticos. Dentro de las técnicas utilizadas para la realización de un delito informático se puede mencionar las siguientes: phishing, ingeniería social, *pharming, skimming, sniffing, spoofing, brute force*, *grooming, ciberbullying, sexting*, entre otros (Salcedo, Fernández, & Castellanos , 2012).

**Normativa legal ecuatoriana**.

El lunes 10 de febrero del 2014, fue publicado en Registro Oficial No 180 el Código Integral Penal (COIP) y entra en vigencia completa a partir del 10 de agosto de 2014.

En el Artículo 103 del COIP, hace referencia a la pornografía con utilización de niñas, niños o adolescentes, donde textualmente dice:

> La persona que fotografíe, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o adolescentes en actitud sexual; será sancionada con pena privativa de libertad de trece a dieciséis años (COIP. Reg. Ofi. No 180, 2014).

El Artículo 104 del mismo cuerpo legal, expresa sobre la comercialización de pornografía con utilización de niñas, niños o adolescentes, estableciendo una sanción de diez a trece años. En los referidos Artículos hace mención a las diversas formas de explotación, como la producción y/o elaboración de material pornográfico con utilización de niños, niñas o adolescentes y a su vez en el Art. 104 se refiere a la comercialización de la pornografía; siendo estos delitos graves que atentan contra el pudor de niños, niñas y adolescentes.

Por su parte el Artículo 173 se refiere al contacto con finalidad sexual con menores de dieciocho años por medios electrónicos.

> La persona que a través de un medio electrónico o telemático proponga concertar un encuentro con una persona menor de dieciocho años, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento con finalidad sexual o

> erótica, será sancionada con pena privativa de libertad de uno a tres años (COIP. Reg. Ofi. No 180, 2014).

Además, en el Artículo 174 habla sobre la oferta de servicios sexuales con menores de dieciocho años por medios electrónicos, en donde hace referencia a "la persona, que utilice o facilite el correo electrónico, chat, mensajería instantánea, redes sociales, blogs, foto blogs, juegos en red o cualquier otro medio electrónico o telemático para ofrecer servicios sexuales con menores de dieciocho años de edad, será sancionada con pena privativa de libertad de siete a diez años.

Delitos contra el derecho a la intimidad personal y familiar.

En el Artículo 178 del COIP, nos habla sobre la violación a la intimidad, donde literalmente dice:

> La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años (COIP. Reg. Ofi. No 180, 2014).

El Artículo 180 del mismo código hace referencia a la difusión de información de circulación restringida y establece una sanción de pena privativa de libertad de uno a tres años.

**Delitos contra el derecho a la propiedad.**

El Artículo 186 del COIP hace referencia a la Estafa:

> La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años (COIP. Reg. Ofi. No 180, 2014)

Este es uno de los delitos más comunes que se desarrolla con gran magnitud en internet, e inclusive hasta en las redes celulares, ya que, a través de engaños, inducen a las víctimas a revelar información personal o patrimonial, en este caso revelación de cuantas, de usuarios, contraseñas, cuentas bancarias o tarjetas de crédito, para ser perjudicados.

El abuso de confianza según el Artículo 187 del mismo código manifiesta que:

> La persona que disponga, para sí o una tercera, de dinero, bienes o activos patrimoniales entregados con la condición de restituirlos o usarlos de un modo determinado, será sancionada con pena privativa de libertad de uno a tres años (COIP. Reg. Ofi. No 180, 2014)

El abuso de confianza es un delito informático, difícil de detectar, ya que, en la mayoría de los casos, es cometido por el mismo personal que labora en la organización, con la finalidad de favorecerse personalmente o para terceros, utilizando procedimientos fraudulentos que ocasionan grandes inconvenientes a las empresas u organizaciones y numerosas pérdidas económicas. Por lo que es necesario tomar en cuenta la implementación de políticas de seguridad tanto internas, como externas en el uso de los sistemas de información.

El Artículo 190 del COIP, se refiere a la apropiación fraudulenta por medios electrónicos; en el que manifiesta lo siguiente:

> La persona que utilice fraudulentamente 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 esta 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 (COIP. Reg. Ofi. No 180, 2014).

El fraude informático, es otra de las actividades ilícitas que se cometen en varias organizaciones, con el fin de apropiarse de algún bien ajeno, ya sea por manipulación de datos a la entrada, como a la salida, y en algunos casos inclusive modificando la programación de los sistemas de información, ya sea por los propios funcionarios de la misma organización o expertos que actúan desde el exterior, ocasionando graves perjuicios, principalmente económicos, en otros casos los fraudes informáticos, también se dan desde escenarios políticos.

**Delitos contra el derecho a la identidad.**

Los Artículos que hacen referencia a estos delitos corresponden al 211 y 212 del mismo código mencionado, en el cual el primero trata sobre el uso de programas informáticos para cometer un delito en o que tiene que ver a los datos de identidad de una persona.

Mientras que el Art. 212 habla sobre la suplantación de identidad. Particularmente el delito de suplantación de identidad, también se ha convertido en un delito común en el escenario de las redes sociales e internet, ya que a menudo se conoce de casos sobre personas inescrupulosas que crean cuentas falsas en redes sociales, haciéndose pasar por otras, para causar perjuicios en la victima suplantada, o con la finalidad de obtener algún beneficio personal o para terceras personas, en la mayoría de casos quedando en la impunidad debido a la escaza intervención de especialistas sobre este tipo de delitos.

**Delitos contra la seguridad de los activos de los sistemas de información y comunicación**

El Artículo 229 del COIP, trata de la revelación ilegal de base de datos, dice lo siguiente:

> la persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años (COIP. Reg. Ofi. No 180, 2014).

La revelación de bases de datos de las organizaciones o empresas, está considerada como una infracción grave, ya que violenta los principios de confidencialidad y reserva, permitiendo que se divulgue información de carácter privado, como bases de datos de clientes, bases de datos de correos electrónicos, así como también secretos de empresa, entre otros; generalmente con fines comerciales o políticos. Se califica de secreto porque al tratarse de informaciones conocidas por un circulo limitado de personas y oculto para otras. La información dotada de un verdadero valor estratégico y patrimonial, en el ámbito de la empresa y del mercado es configurada como un verdadero valor económico.

El Artículo 230, del mismo código, nos habla sobre la Interceptación ilegal de datos, la misma que será sancionada con pena privativa de libertad de tres a cinco años (COIP. Reg. Ofi. No 180, 2014). En el mencionado Artículo de hace referencia al espionaje informático, donde se incluye las formas de acceso no autorizado a un sistema de información. El acceso puede darse de forma directa, por un mismo empleado quien accede de forma no autorizada, lo que se conoce como riesgo interno; pero también puede ocurrir de forma remota. El delincuente informático aprovecha la falta de medidas de seguridad, para obtener acceso o puede descubrir las deficiencias en las medidas existentes de seguridad. Generalmente los hackers

se hacen pasar por usuarios legítimos del sistema, debido a que los usuarios utilizan contraseñas comunes y saben poco o nada de políticas de seguridad.

Sobre el delito de Transferencia electrónica de activo patrimonial, el Artículo 231 del COIP indica:

> La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años (COIP. Reg. Ofi. No 180, 2014).

El Artículo anteriormente citado, hace referencia al fraude informático, donde personas que tienen acceso a la información, o al código fuente de los sistemas, modifican datos tanto de entrada como de salida, con la finalidad de apropiarse de lo ajeno; ya sea para beneficio personal o para terceros. Además, han existido casos donde las personas encargadas de los sistemas, alteran los procedimientos para generar resultados que les favorezcan. Del mismo modo los propios funcionarios abusan de la confianza para manipular las cuentas que han sido otorgadas a las autoridades competentes.

El Artículo 232 nos ilustra sobre el ataque a la integridad de sistemas informáticos y dice:

> La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años (COIP. Reg. Ofi. No 180, 2014).

Este tipo de delitos, hace referencia a las conductas dirigidas a causar daños físicos o lógicos de los sistemas de información, bien sea por cuestiones de índole política, o por intentar eliminar las pruebas que le responsabilizan de algún acto ilegal que se ha cometido en alguna organización.

El acceso no consentido a un sistema informático, telemático o de telecomunicaciones consta en el Artículo 234, el mismo que manifiesta:

> La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente

> el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años (COIP. Reg. Ofi. No 180, 2014).

A esta actividad se le conoce también como el intrusismo informático, el mismo que se produce, cuando personas ingresan ilegalmente a los sistemas de información suplantando la identidad de los usuarios autorizados, o a su vez por medios remotos con la utilización de herramientas para el efecto. En otros casos violentan las seguridades de los centros de información para cometer este tipo de delito y apoderarse de la información objetiva.

## MÉTODOS

El presente Artículo constituye un análisis crítico-reflexivo sobre la problemática que conllevan los delitos informáticos. Los métodos utilizados en la presente investigación van en correspondencia con la modalidad “cuali-cuantitativa”, a más de la utilización de tipos, técnicas e instrumentos de investigación, para la recolección de datos.

Se realizó observaciones individuales, en cada uno de los elementos del objeto de estudio para luego, realizar generalizaciones, cuyo contenido sobrepasa el de los hechos inicialmente observados.

Se tomó en cuenta los procesos delincuenciales aparentemente aislados, para formular una concepción más amplia de los delitos informáticos en la provincia de Pastaza.

Se desarrolló un proceso de búsqueda selectiva de información en libros, Artículos científicos, revistas y sitios de internet; para fundamentar el objeto de estudios de la presente investigación.

Para poder extraer los datos de la realidad, utilizando técnicas de recolección de datos, de un grupo involucrado en el universo de esta investigación, se realizó entrevistas, que permitieron, recoger información relacionada al tema de investigación, aplicada a profesionales del derecho con experticia en el área de esta investigación.

La encuesta, permitió recolectar información de las variables de la presente investigación, mediante un cuestionario, aplicadas a una muestra representativa, para conocer su opinión y valoración.

## RESULTADOS

En base a la investigación realizada, es importante destacar algunos resultados que han sido publicados en medios nacionales e internacionales sobre el crecimiento de este tipo de delitos,

siendo la excepción la Provincia de Pastaza, que no cuenta con un estudio objetivo ni estadísticas de casos reportados en la Provincia.

Al respecto se presentan los siguientes resultados.

En primer momento se expone una tabla con los Artículos en el COIP que tratan sobre los delitos informáticos, cuales son dichos delitos y la sanción establecida.

Tabla 1. Delitos informáticos COIP

| Artículo | Delito | Sanción |
|---|---|---|
| 174 | Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos. | 7 a 10 años |
| 178 | Violación a la intimidad | 1 a 3 años |
| 186 | Estafa | 5 a 7 años |
| 190 | Apropiación fraudulenta por medios electrónicos | 1 a 3 años |
| 191 | Reprogramación o modificación de información de equipos terminales móviles | 1 a 3 años |
| 192 | Intercambio, comercialización o compra de información de equipos terminales móviles | 1 a 3 años |
| 193 | Reemplazo de identificación de terminales móviles | 1 a 3 años |
| 194 | Comercialización ilícita de terminales móviles | 1 a 3 años |
| 195 | Infraestructura ilícita | 1 a 3 años |
| 229 | Revelación ilegal de base de datos | 1 a 3 años |
| 230 | Interceptación ilegal de datos | 3 a 5 años |
| 231 | Transferencia electrónica de activo patrimonial | 3 a 5 años |
| 232 | Ataque a la integridad de sistemas informáticos | 3 a 5 años |
| 233 | Delitos contra la información pública reservada legalmente | 5 a 7 años |
| 234 | Acceso no consentido a un sistema informático, telemático o de telecomunicaciones | 3 a 5 años |

Fuente: Elaboración propia a partir de (COIP. Reg. Ofi. No 180, 2014).

1.- En Ecuador no existen datos ni estudios sobre la afectación económica producida por los delitos informáticos. De acuerdo al criterio de (Zambrano-Mendieta, Dueñas-Zambrano, & Macías-Ordoñez, 2016), en el Ecuador del año 2009 al 2013 se registraron un total de 3,143 casos, esto a pesar de que se conoce que el 80% de los delitos informáticos no son reportados, en cuanto al índice delictivo (pág.210).

2.- Ecuador ocupa el tercer lugar después de México con el 92 % y Bolivia con el 85 %, lo que a criterio de la ONU se produce como consecuencia de la falta de una cultura de denuncia (Zambrano-Mendieta, Dueñas-Zambrano, & Macías-Ordoñez, 2016).

3.- En un estudio “Delitos Informáticos en Latinoamérica del Centro de Estudios de Justicia de las Américas”, publicado en el año 2013, se explica que el nivel de sanción penal por esta clase de delitos en el Ecuador es del 63%. Esto en base a un análisis de las leyes promulgadas.

4.- Según un estudio de la Federación Latinoamericana de Bancos (FELABAN) presentado en el año 2015 por su secretario general, Giorgio Trettenero, indica que “el 98,5% de los riesgos bancarios en América Latina y el Caribe son digitales o informáticos, los robos en las oficinas bancarias, los asaltos a mano armada, han pasado a ser el 1,5 % del problema, antes el riesgo era físico y patrimonial, hoy en día, el riesgo es digital, informático" (Agencia EFE, 2015).

5.- Cuatro de los 10 procesados en el caso que investiga la inscripción fraudulenta de 366 títulos profesionales en la Secretaría Nacional de Educación Superior (SENESCYT) y la obtención ilegal de 600 licencias de conducir en la Agencia Nacional de Tránsito (CNT) se sometieron al procedimiento abreviado y fueron condenados a dos años de cárcel por este delito (Lahora, 2016)

6.- Según datos de la Fiscalía de enero a mayo del 2016 se han denunciado 530 delitos informáticos. De eso, 368 fueron de apropiación fraudulenta por medios electrónicos.

7.- Informes internacionales advierten que en el Ecuador los delitos informáticos crecieron del 26% al 45% en los últimos años. La entidad refiere que los delitos informáticos son la transferencia ilícita de dinero, la apropiación fraudulenta de datos personales, la interceptación ilegal de datos, la pornografía infantil, el acoso sexual.

8.- En la provincia de Pastaza, en la Fiscalía Provincial, no existe un informe sobre el número de casos identificados como “delitos informáticos”; tampoco cuentan con una unidad de delitos informáticos, que se encargue del proceso de investigación de este tipo de delitos; más por el contrario se conoce que han existido algunos casos denunciados relacionados a estafas, abuso de confianza, calumnias e injurias a través de las redes sociales, las mismas que en su mayoría aún se encuentran en etapa de indagación previa.

9.- Los resultados de la encuesta aplicada a un grupo de 200 personas de la ciudad de Puyo, donde se les consulta, si tienen conocimiento sobre la existencia de este tipo de delitos informáticos, nos muestran los siguientes resultados:

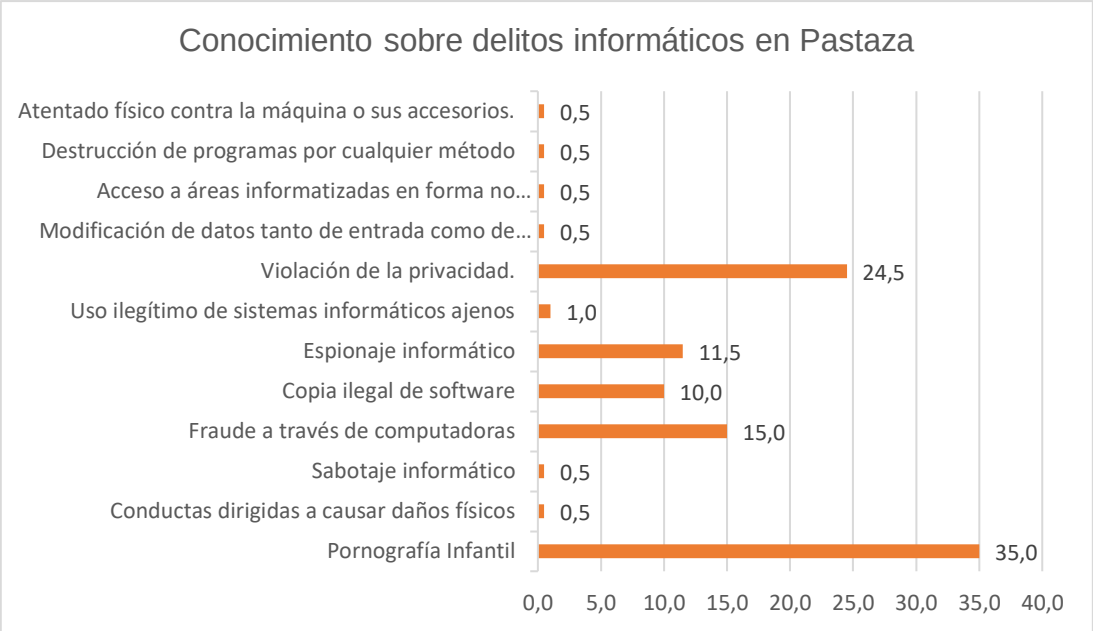



Figura 1. Conocimiento sobre delitos informáticos en Pastaza.

Fuente: Elaboración propia, 2017.

De acuerdo a los resultados presentados, podríamos manifestar, que, en la ciudad de Puyo, provincia de Pastaza, existe poco conocimiento sobre los delitos informáticos, pero por otro lado si conocen sobre la existencia de casos de utilización de material pornográfico en internet, así como también la violación a la privacidad, de la misma manera conocen que existen casos de fraudes a través de computadores, espionaje informático y copia ilegal de software.

## DISCUSIÓN

Los delitos informáticos van en aumento en todo el mundo (Noguera, 2012), esto es innegable, ya que el uso de las tecnologías de la información y la comunicación se van generalizando a nivel mundial. Esto ha permitido el aparecimiento de conductas contra las normas judiciales establecidas en los diferentes países. Muchos autores denominan delitos informáticos a las a las acciones antijurídicas, pero según el criterio del autor de este Artículo es muy importante tomar en cuenta lo que menciona (Narváez-Montenegro, 2015), ya que este autor no dice que debería denominarse delitos informáticos, sino mas bien, infracciones informáticas, lo cual es muy interesante, ya que bajo su criterio y basándose en la legislación ecuatoriana, hay una serie de contravenciones que no son delitos.

El Código Orgánico Integral Penal, ha actualizado ostensiblemente la situación sobre la parte sustantiva de los delitos informáticos, pero lógicamente debido al aparecimiento vertiginoso de nuevas tecnologías día a día, se requiere una actualización de los articulados que tratan sobre este tema.

La ciudad de Puyo no se escapa al accionar delincuencial utilizando medios electrónicos e informáticos, por este motivo se decidió realizar una encuesta a 200 personas, preguntando sobre los delitos informáticos y en forma especial el tipo de delitos informáticos, en dicha encuesta se tuvo como resultado que la mayoría de personas consideran que el uso de los medios informáticos para generar pornografía infantil, es el principal delito, pero no se consideró si los servidores en los cuales se alojan datos (fotos, videos) de menores se encuentran en la provincia de Pastaza, además no se tiene en cuenta si los niños utilizados en la generación de la información pornográfica corresponden a la provincia en mención. De ahí que, debería realizarse una búsqueda más adecuada de la información sobre el tema.

Otra limitación de la investigación tiene que ver con la adquisición de información mediante entrevistas a autoridades de la provincia en general y forma específica con aquellos que tengan que ver con los principales delitos que se mencionan en el COIP.

## CONCLUSIONES

- Los delitos informáticos, cada día van en aumento, por lo que es necesario que las personas tengan conocimiento de los mismos, con la finalidad de evitar ser víctimas de este tipo de delitos.
- El delito que mayor impacto que produce en la sociedad en general, es el de la "pornografía infantil", ya que es de conocimiento público; muchos niños, niñas y adolescentes acceden libremente a las redes, principalmente a internet; sin contar que tras de ellos se encuentran los depredadores sexuales que pretenden abusar sexualmente de ellos; ya que no existe un adecuado control parental, ni tampoco escolar.
- Los delitos como difamación y calumnias son comunes en las redes sociales; pero lamentablemente no hay un marco regulatorio que frene estos atropellos, donde pretenden dañar el honor y la honra de las personas o instituciones.
- Los perjuicios económicos que conllevan esta clase de delitos son incalculables, tanto para personas naturales como jurídicas, lo que amerita implementar mejores controles y políticas de seguridad a fin de evitar ser víctimas de estafas y fraudes informáticos.
- El Código Orgánico Integral Penal, recoge algunos tipos de delitos informáticos, aunque no contamos con una ley específica, que regule todas estas conductas antijurídicas en armonía con el avance de la tecnología y este tipo de delincuencia organizada.
- Las Unidades Judiciales de provincias pequeñas, no cuentan con unidades de delitos informáticos, tampoco con especialistas en esta área, para que procedan con una investigación coherente, acorde a las denuncias presentadas de las personas perjudicadas.

**REFERENCIAS**

Agencia EFE. (15 de octubre de 2015). *https://www.efe.com.* Obtenido de https://www.efe.com/efe/america/economia/el-98-5-por-ciento-de-los-riesgos-bancarios-en-america-latina-son-informaticos/20000011-2738875#

Albizuri-Romero, M. B. (2002). El Fraude y la Delincuencia Informática: Un Problema Jurídico y Etico. *Revista UNAM, 3*(2). Obtenido de http://www.revista.unam.mx/vol.3/num2/art3/#1

Campos, J. (15 de Septiembre de 2014). *www.mailxmail.com*. Obtenido de www.mailxmail.com: http://www.mailxmail.com/curso-delitos-informaticos/conceptualizacion-generalidades

COIP. Reg. O. No 180. (2014). *Código Orgánico Integral Penal.* Quito: Nacional.

Lahora. (22 de marzo de 2016). *https://lahora.com.ec.* Obtenido de https://lahora.com.ec/noticia/1101927597/4-sentenciados-en-caso-de-tc3adtulos-falsos

Narváez-Montenegro, B. D. (2015). El delito informático. En F. A. Carrera-Calderón, B. D. Narváez-Montenegro, S. Fiallos, A. Bucaram, & F. Viscaino-Naranjo, *Derecho informático. Conceptos, principios y prácticas* (págs. 51-83). Quito: Jurídica.

Noguera, N. G. (15 de 07 de 2012). *www.delitosinformaticos.com*. Obtenido de www.delitosinformaticos.com: http://www.delitosinformaticos.com/delitos/codigopenal.shtml

Ortega Sánchez, I. (2009). ALFABETIZACIÓN TECNOLÓGICA Y SU INFLUENCIA. *Revista Teoría de la Educación. Educación y Cultura en La Sociedad de la Información*, 5-7.

Piscitelli, A. (2002). *Cibercutluras 2.0. En la era de las máquinas inteligentes.* Buenos Aires: Paidós.

Rodríguez Perrojo, K., & Ronda León, R. (2006). Web semántica: un nuevo enfoque para la organización y recuperación de información en el web. *ECIMED, 13*(6). Obtenido de http://eprints.rclis.org/7961/1/aci030605.pdf

Rodríguez-Acosta, B. M. (2018). Los negocios realizados por internet, ¿cambian los paradigmas existentes? *Revista IUS*. doi:http://orcid.org/0000-0003-2572-2804

Salcedo, O., Fernández, C., & Castellanos , L. (2012). HACKERS EN LA SOCIEDAD DE LA INFORMACIÓN: ANÁLISIS DE SU DINÁMICA DESDE UNA PERSPECTIVA SOCIAL. *Visión Electrónica*, 115-123.

Suarez-Sánchez, A. (2009). *La estafa informática.* Bogotá: Ibáñez.

Téllez-Valdéz, J. (2008). *Derecho informático.* México: Mc-GrawHill.

Tello Leal, E., Sosa Reyna, C. M., Lucio Castillo, M., & Flores Morelos, M. M. (22 de noviembre de 2010). *www.nosolousabilidad.com.* Obtenido de http://www.nosolousabilidad.com/articulos/tecnologia_educacion.htm

Torres Moreno, J. M. (1998). INTERNET 2 : Las nuevas redes del futuro. *Laboratorio Nacional de Informática Avanzada*, 25-29.

Zambrano-Mendieta, J. E., Dueñas-Zambrano, K., & Macías-Ordoñez, L. (2016). Delíto informático. Procedimiento Penal en Ecuador. *Dominio de las ciencias, 2*, 204-215.