UNIVERSIDAD TÉCNICA DEL NORTE

INSTITUTO DE POSGRADO

MAESTRIA EN DERECHO: MENCIÓN DERECHO PENAL

"LA DEBILIDAD DEL PROCESO INVESTIGATIVO DE LOS DETILOS INFORMÁTICOS"

Trabajo de Investigación Previo a la Obtención del Título de Magister en Derecho Penal

DIRECTOR:

Hurtado Moreno Jhonny Iván

AUTOR:

Ana Belén Saraguro Olalla

IBARRA-ECUADOR

2021

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1721813895		
APELLIDOS Y NOMBRES:	SARAGURO OLALLA ANA BELEN		
DIRECCIÓN:	LOS GALEANOS Y MANUELA CAÑIZARES		
EMAIL:	absaraguroo@utn.edu.ec		
TELÉFONO FIJO:	062510009	**TELÉFONO MÓVIL:**	0983309201

DATOS DE LA OBRA	
TÍTULO:	LA DEBILIDAD DEL PROCESO INVESTIGATIVO DE LOS DETILOS INFORMÁTICOS
AUTOR (ES):	SARAGURO OLALLA ANA BELEN
FECHA: DD/MM/AAAA	11/11/2021
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	☐ **PREGRADO** ☒ **POSGRADO**
TITULO POR EL QUE OPTA:	**MAESTRIA EN DERECHO: MENCION DERECHO PENAL**
ASESOR /DIRECTOR:	**Hurtado Moreno Jhonny Iván**

2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 11 días del mes de noviembre de 2021

EL AUTOR:

.....

Nombre: Ana Belén Saraguro Olalla

A mis padres, Ramiro Saraguro y Cristina Olalla, por su amor, trabajo y sacrificio, en todas las etapas de mi vida, ha sido un orgullo y un privilegio ser su hija, son los mejores padres. A mi hermano, Francisco Saraguro, por estar siempre presente, acompañándome y por el apoyo que me ha brindado, para lograr cumplir esta meta. A mi hija, Camila Terán, por ser mi motivación y mi motor de vida, es gracias a ustedes la obtención de este grado académico.

A toda mi familia, especialmente, a Edgar Maya Olalla, Lucila Olalla, Diego Flores y Alexandra Martínez, quienes con sus consejos y palabras de aliento de una u otra forma me acompañan en todos mis sueños y metas.

Y a mis ángeles en el cielo, Beatriz Piarpuezán, María José Maya, Edgar Maya, Francisco Bolaños y en especial al Dr. Ivenn Raúl Bolaños, por su confianza, su apoyo, sus consejos, por tratarme como una hija en todo momento, un gran profesional y mi mentor, de quien me llevo su sabiduría y mi pasión por el Derecho.

Agradecimientos:

A mi Tutor el Dr. Hurtado Moreno Jhonny Iván, un gran profesional y amigo, gracias a su apoyo y dirección, ha sido posible la realización de este trabajo de titulación.

A mis docentes, quienes, con la enseñanza de sus valiosos conocimientos, hicieron que pueda crecer día a día como profesional, gracias a cada una de ustedes por su paciencia, dedicación.

A mis amigos, Sebastián Legarda, José Luis González, Juan Carlos Galarraga, Jenyfer Figueroa, Santiago Chimarro, César Lenin Rueda, Dennis Barreno por su apoyo incondicional y amistad.

ÍNDICE DE CONTENIDOS

Pág.

ÍNDICE DE FIGURAS

UNIVERSIDAD TÉCNICA DEL NORTE

INSTITUTO DE POSGRADO

PROGRAMA DE MAESTRÍA

"LA DEBILIDAD DEL PROCESO INVESTIGATIVO DE LOS DELITOS INFORMÁTICOS"

Autor: Ana Belén Saraguro Olalla

Tutor: Jhonny Iván Hurtado Moreno

Año: 2021

RESUMEN

Adecuado a la actualidad, realidad y normativa vigente, se identificó la necesidad de analizar la problemática respecto a los delitos informáticos y a la eficiencia de la investigación que se efectúa en el Ecuador, a fin de identificar el nexo causal y la materialidad de la infracción, acorde a las necesidades de los ilícitos, la naturaleza particular de cada uno de ellos y por ende la adecuada sanción que ameriten recibir. Se empleó el enfoque cuantitativo, tipo de investigación de carácter descriptivo, métodos descriptivo, inductivo y documental, como técnicas la entrevista, la encuesta y la muestra estadística, aplicadas que fueron a actores directos y profesionales estrechamente relacionados, conocedores, o referentes en la materia y el objeto de la investigación, mismos que procesados, y acorde al análisis de la normativa vigente, dieron como resultado la determinación de puntos críticos en torno a la deficiente investigación qué se da en los delitos informáticos en el Ecuador, arrojando que es imperante el invertir, adecuar, y reforzar en cuanto a la investigación, sus técnicas y procesos, para la determinación del nexo causal en los delitos informáticos, así mismo, la necesidad de capacitar y formar a los profesionales que intervienen cómo investigadores a fin de conseguir una mayor eficiencia y mejores resultados.

Palabras clave: informática, investigación, delitos, tecnología, pericia

UNIVERSIDAD TÉCNICA DEL NORTE

INSTITUTO DE POSGRADO

PROGRAMA DE MAESTRÍA

"LA DEBILIDAD DEL PROCESO INVESTIGATIVO DE LOS DELITOS INFORMÁTICOS"

Autor: Ana Belén Saraguro Olalla

Tutor: Jhonny Iván Hurtado Moreno

Año: 2021

ABSTRACT

Adequate to the current situation, reality and current regulations, the need to analyze the problem regarding computer crimes and the efficiency of the investigation carried out in Ecuador was identified, in order to identify the causal link and the materiality of the offense, according to the needs of the illicit, the particular nature of each one of them and therefore the appropriate sanction that they deserve to receive. The quantitative approach was used, a descriptive type of research, descriptive, inductive, and documentary methods, such as interview, survey and statistical sample techniques, applied to direct actors and closely related professionals, knowledgeable, or referents in the subject and the object of the investigation, the same as those processed, and according to the analysis of the current regulations, resulted in the determination of critical points around the deficient investigation that occurs in computer crimes in Ecuador, showing that it is The prevailing investment, adaptation and reinforcement in terms of investigation techniques and processes, for the determination of the causal link in computer crimes, likewise, the need to train and educate professionals who intervene as investigators in order to achieve greater efficiency and better results.

Keywords: informatics, investigation, crime, technology, expertise

INTRODUCCIÓN

En el presente capitulo se detallan los aspectos principales acerca del problema de investigación, que en este caso se refiere a la debilidad del proceso investigativo en los delitos informáticos, los objetivos desarrollados en el Trabajo de Titulación, así como, la justificación e importancia de su estudio.

En el Capítulo II se desarrolla el marco referencial, donde se contextualizan y describen los principales elementos de la problemática de investigación en el presente estudio, los delitos informáticos, definiciones, características, clases, normativa nacional e internacional al respecto y el proceso de investigación, nexo causal, técnicas y pericias especializadas, de tal manera que se presentan los referentes teóricos, normativos y doctrinarios básicos que permiten un análisis más técnico y amplio del objeto.

El Capítulo III contiene el marco metodológico, donde se describe el área de estudio, la modalidad, tipo, métodos, el procedimiento de investigación, la población, la aplicación de técnicas, el análisis estadístico, y se presentan los resultados de la aplicación de la encuesta y de la entrevista.

El Capítulo IV presenta los resultados, donde se analizan los indicadores y puntos críticos identificados en virtud de la contextualización del objeto de investigación, y el análisis de resultados obtenidos de la muestra estadística y la aplicación de la encuesta y entrevista, profundizando con atención a la norma y derechos, realizando un análisis crítico jurídico que permita identificar el origen de la problemática y establecer recomendaciones en torno a su solución.

Finalmente, se recoge las principales conclusiones y recomendaciones a las que se logró arribar, una vez culminado el trabajo investigativo y alcanzados que sean los objetivos planteados.

CAPITULO I

1.1 Problema de investigación

El ser humano es un ser social por naturaleza y en razón de aquello busca estar en constante conexión con los demás seres que habitan su entorno, es así que se crearon diversas formas de comunicación, las mismas que en sus orígenes se veían reflejadas por la pintura, en este caso la rupestre y en el caso de la escritura, la cuneiforme, con la evolución, se desarrolló la imprenta hasta llegar a lo que hoy tenemos como los medios electrónicos. Según una nota de la BBC Mundo denominada "Los 10 aparatos electrónicos más importantes de la historia, según la revista Time" los aparatos electrónicos que usamos constantemente en la actualidad, como los celulares, las cámaras de fotos o de video, los televisores y demás aparatos electrónicos, se deben a la forma en cómo vivimos y cada aparato influye en el desarrollo de la sociedad. (BBC , 2016)

Con este avance tecnológico fue necesario el reconocimiento del derecho de acceso a la información al cual la Corte Interamericana de Derechos Humanos (Corte IDH) ha dado:

> Dos dimensiones que deben estar garantizadas simultáneamente: una individual y una social. Estas requieren, por un lado, que nadie sea arbitrariamente menoscabado o impedido de manifestar su propio pensamiento y representa, por tanto, un derecho de cada individuo; pero implica también, por otro lado, un derecho colectivo a recibir cualquier información (entre ellas información pública) y a conocerla de forma directa y transparente. (INREDH, 2015, pág. 9)

Sin embargo, este derecho de acceso a la información se ve limitado por el derecho a la intimidad de las personas, y otros derechos conexos, en el tema patrimonial y la seguridad del Estado. Es así que, en el Comité de Derechos Humanos, conocido por sus siglas en inglés HRC (*Human Rights Committee*) Observación general N.º 16 (*General Comment*) de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos en un extracto nos menciona: "Como todas las personas viven en sociedad, la protección de la vida privada es por necesidad relativa. Sin embargo, las autoridades públicas competentes sólo deben pedir aquella información relativa a la vida privada de las personas cuyo conocimiento resulte indispensable para los intereses de la sociedad",

(Oficina del Alto Comisionado de las Naciones Unidas, 1988) haciendo que el derecho a la intimidad de las personas sea fundamental.

Es preciso establecer y situarnos en la realidad tecnológica de nuestro país, hoy en día, los sistemas informáticos se han convertido en la principal fuente de comunicación para las personas, además de que por medio de la informática realizan sus actividades cotidianas relacionadas con sus finanzas, relaciones de negocios e interpersonales, esto ya que indudablemente existe un acelerado avance tecnológico, el mismo que a la vez que representa un crecimiento para la humanidad, también conlleva diversas consecuencias y hace que la información reservada de las personas sea vulnerable, y que este progreso se vea empañado por quienes cometen actividades ilícitas relacionadas a este campo, que si bien son más sutiles y no transgreden de manera física a las personas si lo hacen a sus recursos patrimoniales y a su honra y personalidad. Estas actividades ilícitas se conocen como delitos informáticos, pues se los comete a través de medios y dispositivos tecnológicos.

Los delitos informáticos más frecuentes en Ecuador, son aquellos relacionados a las transferencias no autorizadas, cuyos sistemas informáticos de las Instituciones Bancarias son vulneradas, entre ellos el delito de estafa y el de apropiación fraudulenta por medios electrónicos, en los que ciberdelincuentes, obtienen las claves de acceso a los canales electrónicos financieros; o a través del uso de las tarjetas de débito y/o de crédito sin autorización del titular, esto en razón de que las personas no cultivan procedimientos de seguridad informática, la misma que debe ir acompañada de un correcto uso de las redes sociales, es así que se requiere una investigación digital eficaz, a fin llegar al convencimiento de la participación y responsabilidad de una persona dentro de estos delitos.

1.2 Objetivos de la investigación

1.2.1. Objetivo general

Identificar las debilidades del proceso investigativo de los delitos informáticos, para establecer el nexo causal entre la conducta del sujeto activo y el resultado material de la infracción.

1.2.2 Objetivos específicos

- Realizar una investigación bibliográfica, mediante el uso de herramientas informáticas; y a nivel de biblioteca, la elaboración del marco teórico.
- Realizar la investigación metodológica, mediante el uso de entrevistas y encuestas, para determinar la forma cómo se realiza la investigación digital de los delitos informáticos.
- Elaborar un análisis de la normativa nacional e internacional aplicable a la investigación de los delitos informáticos.

1.3 Justificación de la investigación

La presente investigación es necesaria, por cuanto existen vacíos y falta de recursos en la investigación de los delitos informáticos, y, es menester que se realice un análisis actual de la normativa nacional e internacional vigente, a fin de brindar a las personas una maximización en el respeto de sus derechos fundamentales, en especial que se proteja la intimidad, la confidencialidad e integridad de las personas y de los datos que se transfieran y que son almacenados en dispositivos electrónicos.

En razón de lo mencionado, es procedente realizar una investigación bibliográfica de la doctrina en cuanto a la investigación digital de los delitos informáticos, así como establecer la realidad de la problemática por medio del conocimiento que tienen los operadores de justicia.

Ya que, en la actualidad con el avance tecnológico, estas conductas delictivas se han incrementado, y refiriéndonos a los delitos informáticos, como un área no desarrollada, y como así lo menciona Melo en su artículo "El derecho informático y la gestión de la seguridad de la información":

> El desarrollo cada vez más acelerado de la tecnología, y el incremento de la penetración de Internet en la vida social, económica y cultural, además de los beneficios que reflejen para la sociedad, incrementarán los retos para los operadores jurídicos en materia de seguridad de la información y de regulación de estos fenómenos. (Velasco Melo, 2008, pág. 340)

Haciendo necesario desarrollar un análisis de la normativa aplicable y la forma en cómo se investigan estos delitos, a fin de identificar sus falencias, y necesidades en cuanto a la determinación ideal del delito y su autor o autores, a fin de que se logren procesos idóneos y sanciones en restitución de los derechos y garantías vulnerados por estos ilícitos.

La línea de investigación de la UTN a la que contribuye la presente investigación es la numero 8 “Desarrollo social y del comportamiento humano”.

CAPITULO II

MARCO REFERENCIAL

2.1. Antecedentes

La tecnología sin lugar a dudas es un factor que no solo ha cambiado a la sociedad, sus necesidades y comodidades, sino que a la vez ha ido facultando la aparición de nuevas conductas ilícitas y así mismo nuevos mecanismos para cometerlos, constantemente se perfeccionan sistemas, dispositivos, dominios, plataformas, entre otros medios electrónicos para acceder a cierta información o procesos, y el factor determinante en todo este conjunto de adelantos es el internet, pues la conectividad y acceso que permite es ilimitado en alcance y contenidos.

Pues bien, una vez planteada la introducción a la problemática, corresponde tratar la delincuencia o criminalidad informática, como el amplio espectro de cometer delitos a través de estos medios tecnológicos para lo cual corresponde mencionar a Mayer (2017), quien dice:

> El término criminalidad informática en sentido amplio o criminalidad cometida "mediante" sistemas informáticos, suele utilizarse para referir la comisión de delitos tradicionales a través de computadoras o de internet (v.gr. extorsión o difusión de pornografía infantil). En cambio, la expresión criminalidad informática en sentido estricto, (…) suele emplearse para aludir a comportamientos delictivos que inciden, directamente, en un sistema informático (v.gr. Sabotaje o espionaje informático). (p.237)

Sea el medio o el fin la informática, son estos los factores característicos de los delitos informáticos, precisamente consiste la delincuencia informática en la comisión de infracciones contra derechos y bienes protegidos a través de la web, sistemas o dispositivos electrónicos, pretendiendo por medio de ellos obtener lucro, satisfacción o beneficio propio o de ajenos, contraviniendo a la normativa vigente, muchas son las formas en las que se cometen estos perjuicios, así conciben Mayer y Oliver (2020):

> La idea de fraude informático evoca la producción de un perjuicio patrimonial mediante la manipulación o alteración de datos o programas de sistemas

> informáticos. Sin embargo, si se consideran las conductas que normalmente se califican de tales, podrá constatarse que el término fraude informático es entendido de forma bastante más amplia y que, en ese sentido, bajo dicha denominación suelen incluirse comportamientos muy diversos. (p.152)

La variedad de modos de infringir a través de la informática, representa un universo de posibilidades y por tanto es difícil catalogar o etiquetar con totalidad y precisión las formas de delincuencia digital o informática, lo cual permite que se mantenga su comisión y en muchos casos se vuelva imperceptible, alcanzando niveles alarmantes y perpetuándose como un riesgo latente para quienes requiere de estos medios, sistemas o dispositivos. Precisamente así lo ratifica Acurio (2015):

> El delito informático, más que una forma específica de delito, supone una pluralidad de modalidades delictivas vinculadas, de algún modo con los computadores, (…) el término Delito Informático debe usarse en su forma plural, en atención a que se utiliza para designar una multiplicidad de conductas ilícitas y no una sola de carácter general. (p. 12)

Así se tiene un contexto de la terminología dominante a ser empleada durante la investigación, ya que como se había expuesto, el delito informático es atribuido a cualquier conducta que por su naturaleza y para su configuración requiera y se perpetre a través de los medios electrónicos, informáticos, digitales o cibernéticos, la magnitud es de igual manera un factor distintivo, pero faculta de igual forma la perpetración de estas conductas, así, puede ser cometida por delincuentes comunes, o por grupos de delincuencia organizada y ser a nivel personal, nacional, o mundial, cabe acotar los señalamientos de Alcívar, Domenech y Ortiz (2015):

> Los delitos informáticos son aquellas actividades ilícitas que: (a) Se cometen mediante el uso de computadoras, sistemas informáticos u otros dispositivos de comunicación (la informática es el medio o instrumento para realizar un delito); o (b) Tienen por objeto causar daños, provocar pérdidas o impedir el uso de sistemas informáticos (delitos informáticos) (pág. 64).

Como se ha podido concluir, los delitos informáticos en su definición son aquellas conductas ilícitas cometidas a través de medios electrónicos, digitales, cibernéticos o informáticos, en distintas modalidades y en distinta magnitud y alcance, la facilidad que

proporcionan es lo que genera su permanencia y perpetuidad, pues no requiere de mayores recursos o esfuerzos, como en otras conductas ilícitas que requiere una mayor intervención física.

Es pertinente exponer brevemente los antecedentes históricos de los delitos informáticos a fin de conocer su evolución y actualidad, corresponde así, mencionara a Riofrío (2012), quien indica:

> Históricamente los Delitos Informáticos tuvieron su origen, a finales de la segunda guerra mundial, en donde a través de las armas de guerra ya sean estas nucleares o químicas comenzaron a encontrar e investigar nuevas formas de poder vulnerar a los estados que se encontraban en conflicto unos con otros (…). Estos avances dieron lugar a la creación del primer satélite artificial llamado SPUNIK, creado por la EX UNION SOVIETICA (04 de octubre de 1957), quienes tomaron el liderazgo más pronto que los Estados Unidos de América, y ya habían anunciado al mundo sobre una carrera inter espacial. (pág. 8)

Continuando en la historia y dos años más tarde de lo antes citado, los Estados Unidos de América crean La Agencia de Proyectos de Investigación Avanzada o *ARPA* por sus siglas en inglés, marcando el comienzo del uso de comunicaciones globales, a cargo exclusivamente de intelectuales de elite. Más adelante y conforme indica Chauca (2014):

> La era de la revolución informática se empieza a desarrollar en la década de 1970 en sus años finales, y recoge campos tan distintos como el transporte, la inteligencia artificial, las comunicaciones, la exploración del espacio, entre otros campos; y hace que el computador sea un instrumento indispensable para el desarrollo de las actividades cotidianas de las personas sean naturales o jurídicas. (p.10)

Ya con adelantos significativos y proyectos de investigación avanzados, el nivel tecnológico se incrementa y es evidente la expansión y asimilación de tecnologías como necesarias y comunes, continúan los avances y como indica al respecto Sain (2015):

> A partir de los primeros años de la década de 1980, los delitos informáticos adquieren una importante notoriedad a partir de un aumento exponencial de fraudes y el tratamiento de la problemática por parte de organismos internacionales. Para el caso de los fraudes, los casos típicos se realizaban

> mediante la manipulación de uso de tarjetas de débito en cajeros automáticos, fundamentalmente a través de la vulneración de las bandas magnéticas. (p. 3)

Estos hechos motivaron a la utilización de chips por parte de las empresas emisores como medida de seguridad, y es que justamente durante esta época se empieza a considerar y llevar a cabo las adaptaciones normativas pertinentes para proteger a los ciudadanos de estos ilícitos, siendo para ello precursor el continente europeo, así mismo en Estados Unidos, es prioridad la protección y amparo sobre los datos y negocios, que sean considerados información comercial y faculten el intercambio económico.

> A fines de esa década comenzaron a aparecer contenidos ilícitos y nocivos en las redes tales como amenazas contra las personas, incitación al odio y el intercambio de material de pornografía infantil, tanto, así como actos de violencia y discriminación racista por parte de grupos extremistas. Nuevas técnicas de hacking manipulaban sistemas de vuelo o sistemas hospitalarios y de salud, definidos como "ataques contra la vida". (p. 3)

El acrecentamiento de estos hechos ilícitos, se da a la par del aumento de personas con acceso a la red, haciéndose evidente a finales de la década de los 80s, en cuanto a que, a nivel estatal, los encargados de la justicia alemana, identificaron a personas denominadas como hackers, quienes hacían uso de las redes de datos a nivel internacional, para el acceso a la información privilegiada de Gran Bretaña y Estados Unidos para negociarla al Comité para la Seguridad del Estado que en sus siglas en ruso es conocido comúnmente como KGB.

Con la apertura global de Internet a mediados de los 90s por parte de la administración norteamericana y el posterior desembarco de las Empresas y Bancos a la red para el desarrollo del comercio electrónico, la preocupación principal se centra en el desarrollo de estándares de encriptación seguros para la ejecución de operaciones financieras y la compraventa de productos en línea, siendo precisamente estas actividades financieras a través de la red las que permiten la obtención de datos y la perpetración de ilícitos por parte de quienes han llegado a obtener acceso a información y datos de la víctima, el internet brinda a los ciberdelincuentes un abismo de posibilidades.

La tecnología, al igual que promueve y facilita actividades licitas y económicamente relevantes, de igual manera ha sido empleada para fines ilícitos y el cometimiento de infracciones, como medio o como fin la tecnología genera una ola de

actividades que mínimas e ilegales, pueden llegar a afectar tanto al sitio, dispositivo o fuente empleado, como a otros sujetos y sus derechos, de allí deviene la importancia de estudiar y analizar a estos delitos y su investigación.

En América Latina, y de acuerdo a Temperini (2014) en países como:

Uruguay: Los delitos informáticos no son de tratamiento específico por la legislación uruguaya, puesto que no existe una ley de ilícitos informáticos, ni tampoco un título específico relativo a los mismos en el Código Penal uruguayo. No se establecen y definen de forma específica delitos electrónicos como conductas plenamente distinguidas y sanciones afines, lo cual faculta que se expandan y aumente el índice de estos ilícitos.

Colombia: Marcando una gran diferencia la normativa colombiana identifica no sólo las conductas a ser tipificadas como delitos y les atribuye sanciones, sino que, además, trata de forma específica al bien jurídico protegido afectado directamente como son los datos personales.

México: Los delitos de revelación de secretos y acceso ilícito a sistemas y equipos de informática ya sean que estén protegidos por algún mecanismo de seguridad, se consideren propiedad del Estado o de las instituciones que integran el sistema financiero son hechos sancionables por el Código Penal Federal, como por ejemplo el empleado que revele el manejo de productos y proceso de preparación de los mismos, que haya sido recomendado como secreto y se tenga la obligación de cuidado, así mismo, es el caso del empleado que borre, copie, transfiera o modifique una base de datos existente en tal o cual equipo sin autorización y que ha consecuencia de aquello causa perjuicio a la Institución. (Cámara de Diputados del H. Congreso de la Unión, 2009)

Venezuela: Concibe como bien jurídico la protección de los sistemas informáticos que contienen, procesan, resguardan y transmiten la información. Están contemplados en la Ley Especial contra los Delitos Informáticos, de 30 de octubre de 2001, en la que se identifican las infracciones de acuerdo al bien jurídico tutelado y se detalla el uso de medios electrónicos, cibernéticos u otros informáticos que sirvan de medio o sean el objeto de la comisión de un ilícito. (Asamblea Nacional de la República Bolivariana de Venezuela, 2001)

En **Ecuador** con la promulgación de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, el 17 de abril del 2002, al igual que su Reglamento,

que se expidió el 31 de octubre de 2002, se establecieron conductas delictivas relacionadas con los avances tecnológicos, puesto que con esta Ley se reconoció la importancia del uso de sistemas de información y de redes electrónicas, como un medio para el desarrollo del comercio, la cultura y la educación. Entre las infracciones informáticas que se incluyeron en la mencionada Ley a partir de su artículo 57 están, la destrucción o supresión de documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos, contenido en cualquier sistema de información o red electrónica; la falsificación electrónica; los daños informáticos y la utilización fraudulenta de sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno. (Congreso Nacional, 2002). Estas conductas estuvieron vigentes hasta la entrada en vigencia del Código Orgánico Integral Penal, el 10 de agosto de 2014.

2.2. Referentes teóricos

2.2.1. Clases de delitos informáticos

Consideradas que han sido las definiciones de estos delitos y una vez que se han analizado sus antecedentes y evolución histórica, corresponde conocer y definir las clases o tipos que existen de delitos informáticos, a fin de crear una distinción y su estudio amplio, es así que conforme la clasificación que realiza Riofrío (2012) se tienen dos tipos de delitos informáticos: Delitos computacionales y delitos informáticos:

> **Delitos computacionales:** son conductas delictivas que se cometen a través de máquinas conectadas a redes locales, nacionales y globales, con la finalidad de afectar al patrimonio de las personas como por ejemplo cuando tratan de sustraerse bienes, en este caso dinero de cuentas bancarias; o que quieran lesionar el derecho a la intimidad de las personas, el honor y el buen nombre la seguridad pública que nuestra Constitución de la República garantiza en el marco de los derechos y libertades. (p. 17)

> **Delitos informáticos:** A diferencia de los delitos computacionales estas conductas se atacan entre sí mismo, el daño es directamente al software, o sea el ataque es precisamente de forma lógica más no de forma física con el fin de hurtar objetos materializados, por ejemplo: la intromisión de virus, el acceso prohibido a un computador o a datos restringidos en una red. (p. 17)

Concluyendo, a partir de esta clasificación, podemos reiterar la enorme diferencia entre delito computacional e informático, siendo el delito informático la agresión a un sistema que procesa la información, y, el delito computacional, aquel en el que se usan sistemas informáticos para lesionar un bien jurídico protegido, inherentes a la persona, como el honor, la seguridad de datos públicos y privados, la libertad, entre otros.

Se tiene además y en forma más detallada, la clasificación según el "Convenio sobre la Ciberdelincuencia" de 1 de noviembre de 2001, suscrito en Budapest:

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

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

Como se aprecia de esta clasificación, el objeto de los ilícitos puede ser un sistema informático o la obtención ilícita de datos, como ejemplos de este grupo de delitos están: el robo o suplantación de identidad, la utilización de *keylogger*, es decir, que se usa un software de carácter malicioso para saltear información que es confidencial, como contraseñas o códigos de protección de información o información bancaria que después es enviadas a terceras personas con fines ilícitos, y, la conexión a sistemas de redes que no son autorizadas.

Delitos informáticos:

- Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.
- Falsificación informática mediante la introducción, borrado o supresión de datos informáticos.

Estos delitos implican el manejo ilícito de datos informáticos, ya sea a través de falsificación, o alteración de los mismos, incluso el borrado fraudulento de datos, estos ilícitos refieren la manipulación de datos y sistemas por medios irregulares y fines ilegales.

Delitos relacionados con el contenido:

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

Siendo el más claro ejemplo la pornografía infantil, la red permite la máxima difusión de este contenido ilícito, y refiere además su producción o almacenamiento en equipos, software, sistemas, plataformas u otro medio electrónico e informático ya sea para fines personales y almacenamiento propio o su comercialización y difusión.

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

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

Con el fin de criminalizar los actos de xenofobia y racismo cometidos mediante sistemas informáticos, en enero de 2008 se promulgó el "Protocolo Adicional al Convenio de Ciberdelincuencia del Consejo de Europa", donde se determinan medidas y acciones a tomar en caso de:

- Difusión de material xenófobo o racista.
- Insultos o amenazas con motivación racista o xenófoba.
- Negociación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad.

Una vez clara las definiciones de los tipos de delitos informáticos, se puede entonces afirmar que tanto los delitos computacionales como los informáticos tienen una relación directa con el uso de las TIC, y que éstas a su provocan un impacto delincuencial de alta magnitud, para lo cual la ciencia del derecho basándose en la conceptualización, deberá implementar leyes que sean capaz de combatir este tipo de actos delictivos.

2.2.2. Sujeto activo de los delitos informáticos, según el tipo de ataque

Descritos que han sido los delitos informáticos, sus elementos y clasificación principal, corresponde analizar las denominaciones o términos que se les ha atribuido a los autores de los delitos informáticos acorde a la conducta realizada, así como el modus operandi y los medios empleados para su ejecución. Y según Villalobos (2002):

Hackers: "es aquel que, por curiosidad, penetra a los sistemas informáticos, o a sus bases de datos, dichos actos los realiza a manera de reto para probar su capacidad intelectual, su intención no es causar daño a terceras personas. Estas personas son capaces de inventar su propio software para vulnerar las seguridades de la información. No buscan ganancias económicas" (p. 54).

Cracker: es quién a través de un sistema remoto pretenden destruir los datos, o restringir su uso, para generar malestar, es decir desestabilizar el sistema.

Trashing o Mercenarios y traficantes de la información: se relaciona con los delios informáticos, y se trata del uso ilegítimo de códigos, se busca lucro o coerción a través de actividades como el sabotaje o espionaje corporativo.

Terroristas y Grupos extremistas: aquellos que emplean la tecnología para actos contrarios al orden social y político, de forma ilegal, mostrando actividades de racismo, odio, homofobia, entre otros.

Phreaker: emplean la telefonía, aquel que tiene conocimientos profundos de telefonía móvil o terrestre, empleando este medio para vulnerar la seguridad de estas redes y alcanzar sus fines.

Lammers: podrían tenerse como similares a los hackers, sin embargo, no alcanzan esa denominación por no tener ese nivel de conocimientos.

Gurus: son en cambio mejores incluso que los hackers, con gran capacidad intelectual y amplia experiencia, comparten sus conocimientos con quienes pueden denominarse sus alumnos.

Bucaneros: a través del crackeo, y lo que se obtenga como producto de los productos obtenidos, comercian lo que otro sujeto activo logro obtener a través del uso de la tecnología, es así que no necesitan conocer y manejar un ámbito tecnológico.

Newbie: estos son novatos, el que empieza a partir de la WEB basada en hacking, aprende lentamente, que en su mayoría fracasa al intentarlo porque olvida ciertos parámetros.

Como se aprecia de los sujetos expuestos y conforme a la naturaleza de estos ilícitos, Huilcapi (2005), indica qué: "En este tipo de delitos, el sujeto activo debe tener conocimientos técnicos de informática, es decir, en cierto modo, una persona con nivel de instrucción elevado, para poder manipular información o sistemas de computación". (p. 18)

Así mismo, lo describe Acurio (2015), en cuanto a la formación, capacitación, conocimiento, dominio o alcance que tiene el sujeto activo para perpetrar un delito informático, así:

> Las personas que cometen los "Delitos Informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos. (p. 15)

Es innegable, e indispensable el conocer, dominar o manejar adecuadamente los sistemas, plataformas, redes, dispositivos u otros electrónicos, informáticos o digitales como elemento y requisito imprescindible para el cometimiento de delitos informáticos, precisamente en cuanto a aquellos expertos en la materia que se dedican a cometer estos ilícitos, radica la dificultad para su identificación y sanción, pues la tecnología faculta un sinnúmero de posibilidades y a la vez encubre su rastro y limita su investigación.

2.2.3. Bien jurídico tutelado

En relación al bien jurídico protegido, lo tenemos como aquello o aquel que recibe el perjuicio por el desarrollo o ejecución de la actividad ilícita, en el caso de los delitos informáticos, surge precisamente la interrogante en torno a definir al bien jurídico tutelado, al cual afecta directamente la perpetración de estos ilícitos, para iniciar puede referirse a la funcionalidad informática, y al respecto Mayer (2017), indica:

> El reconocimiento de la funcionalidad informática como bien jurídico específico, propiamente informático, se justifica si los delitos informáticos, junto con incidir en el soporte lógico de un sistema informático, implican el uso de redes computacionales. En ese contexto, la funcionalidad informática constituye, por una parte, un interés cuyo sentido y alcance debe precisarse dinámicamente, así como en atención a la forma en que opera el uso de redes computacionales, en tanto sistemas de interconexión (remota y masiva) entre los individuos. Ella constituye, por otra parte, un bien jurídico instrumental de carácter colectivo, cuya tutela penal debe verificarse en términos particularmente acotados. (pág.255)

Se podría tener además como bien jurídico tutelado la materialidad de equipos, dispositivos y maquinas, pues son medio pero también llegan a ser fin, la afectación a estos bienes refiere un daño físico, apreciable y cuantificable, así por ejemplo la infección con virus que inhabilite o inutilice por completo a un dispositivo representa un daño palpable, y así sucede incluso en otras afectaciones como daño colateral o consecuente, puede no ser el principal, pero viene a constituir un bien tutelado.

Se puede, sin necesidad de negar los otros bienes jurídicos afectados por los ilícitos electrónicos, referir que la información es el bien jurídico tutelado innegablemente afectado en los ilícitos informáticos sea cual fuere su naturaleza o consulta, así, según Suárez (2009):

> En conclusión, el delito informático está vinculado no sólo a la realización de 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. (p. 44)

La funcionalidad, constituye sin duda el bien más ligado a la tecnología, pues precisamente del adecuado funcionamiento de redes, sistemas y dispositivos depende la idoneidad y precisión de estos medios y mecanismos, lo que hace a la tecnología relevante y más útil que otras alternativas para desempeñar tal o cual actividad, presta facilidades y faculta una inmensa variedad de posibilidades de comunicación, desarrollo, prestación de servicios, atención y en definitiva la mayoría de actividades que puedan requerirse por las personas en sus distintas necesidades.

Es así que como bien jurídico protegido, en estos ilícitos informáticos, están la información personal y datos personales que forman parte de la identidad, pues una vez

que a causa del cometimiento de estos ilícitos se maneja estos datos e información de manera maliciosa y se los altera, desparece o comercia, se está transgrediendo además la privacidad e intimidad de esa persona, afectando su propiedad y restricción dejándole vulnerable y causando gran perjuicio económico y social.

Estrechamente ligado a lo antes manifestado está además, como bien jurídico protegido la confianza y necesidad que tienen las personas en su aplicación y ejecución, ya que la confianza refiere inversión de atención, tiempo, dinero, privacidad, integridad y en sí a través de medios informáticos se realizan actividades sustanciales para las personas y en la web se vierten datos personalísimos que pueden generar intereses no siempre legales y legítimos, causando grandes perjuicios a las víctimas de estas conductas.

Es así que, el delito informático, debido a que se manifiesta de múltiples maneras, se lesionan varios bienes jurídicos protegidos, de acuerdo a la modalidad o en la forma en que se ejecuta, y es por ello que el legislador los ha ubicado en el Código Orgánico Integral Penal, según el bien jurídico que se protege.

2.2.4. Delitos informáticos en Ecuador

Ecuador ha llevado a cabo una evolución significativa en materia penal, pues los códigos penales y de procedimiento penal que antecedieron al código vigente, no incluían tipos penales, sanciones, diligencias o procesos penales que hoy se recogen en el denominado Código Orgánico Integral Penal, que innova en materia de delitos, pues incorpora nuevos tipos y sanciones afines, como los son precisamente los delitos informáticos, que en su articulado se tipifica como:

Revelación ilegal de base de datos: tipificado en el artículo 229 del Código Orgánico Integral Penal, se refiere a la violación de información confidencial que se encuentra en una base de datos u otro similar, la pena es de uno a tres años. Sin embargo, es un agravante que el delito sea cometido por un servidor público o colaboradores de instituciones bancarias que realicen intermediación financiera o contratistas, en estos casos el delito se sanciona con pena privativa de libertad de tres a cinco años. (Asamblea Nacional del Ecuador, 2014)

Interceptación ilegal de datos: tipificado en el artículo 230, cuando sin orden judicial previa, se intercepta, un dato informático, una señal o una transmisión de datos o señales con el fin de obtener esta información registrada. Este delito se sanciona con pena privativa de libertad de tres a cinco años. (Asamblea Nacional del Ecuador, 2014)

Este artículo permite también sancionar la clonación de tarjetas de débito y crédito, así como también el desarrollo de software malicioso, envío de mensajes o realización de llamadas que induzcan a ingresar a una dirección o sitio de web diferente a la que quiere acceder ya sea este un servicio financiero, pago electrónico o cualquier otro sitio personal o de confianza.

Transferencia electrónica de activo patrimonial: tipificado en el artículo 231, con pena privativa de libertad de tres a cinco años se sanciona la alteración o manipulación de un activo patrimonial de manera no consentida.

Ataque a la integridad de sistemas informáticos: tipificado en el artículo 232, se refiere a la acción que ocasione destrucción, alteración o mal funcionamiento de sistemas de tratamiento de información, telemático o de telecomunicaciones. En cuanto a este delito se habla de "sanciones con penas privativas de tres a cinco años, y para casos donde se realice este delito a bienes informáticos como parte de una prestación de servicio público o con vínculo con la sociedad sería un total de cinco a siete años de privación de libertad" (Asamblea Nacional del Ecuador, 2014)

Esta situación se hace evidente a medida que se han implementado nuevas penas y sanciones para limitar a quienes hacen de la información un negocio ilegal.

Delitos contra la información pública reservada legalmente: tipificado en el artículo 233, se habla de "quien destruya o inutilice información pública clasificada de conformidad con la Ley será sancionado con pena de tres a cinco años" (Asamblea Nacional del Ecuador, 2014), en el país hay información que también es pública la cual está autorizada para ser divulgada, en base a los principios de publicidad, la misma que no se tipifica como delito alguno por tener el derecho a su divulgación.

Acceso no consentido a un sistema informático, telemático o de telecomunicaciones: tipificado en el artículo 234, este delito sanciona a la persona o conjunto de personas que accedan ilegítimamente, es decir sin autorización, a un portal web, o que redireccionen el tráfico de datos o voz a fin de lucrarse ilícitamente de esta acción u ofrecer servicios que estos sistemas provean a terceros.

Además de los delitos antes detallados, en el Código Orgánico Integral Penal, se encuentran también tipificados los siguientes delitos:

- Art. 190.- Apropiación fraudulenta por medios electrónicos.
- Art. 211.- Supresión, alteración o suposición de la identidad y estado civil.
- Art. 229.- Revelación ilegal de bases de datos.
- Art. 231.- Transferencia electrónica de activo patrimonial.
- Art. 232.- Ataque a la integridad de sistemas informáticos.
- Art. 234 Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.

Existen artículos en el Código Orgánico Integral Penal que, si bien es cierto, contemplan el uso de tecnologías informáticas, no son considerados como tal, delitos informáticos, pero implican el uso de la tecnología como medio. Estos son los siguientes:

- Art. 103.- Pornografía con utilización de niñas, niños o adolescentes.
- Art. 178.- Violación a la intimidad
- Art. 233.- Delitos contra la información pública reservada legalmente
- Art. 186.- Estafa

Como diagnóstico referente e inicial la Fiscalía General del Estado en el año 2015 ante la reciente vigencia del Código Orgánico Integra Penal, refiere el siguiente gráfico y datos estadísticos:

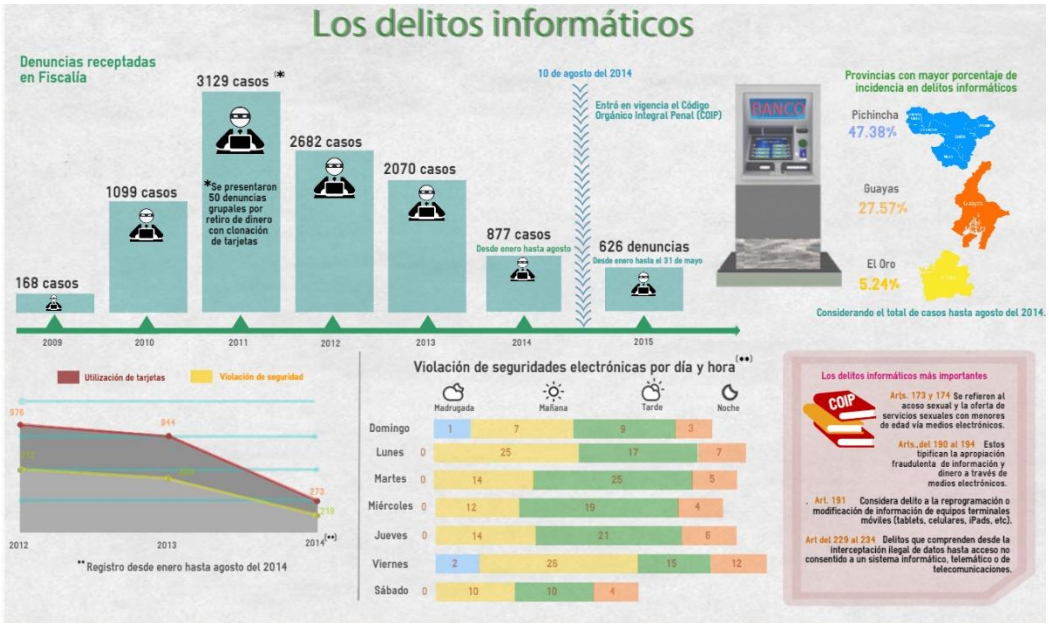


Figura1. Los Delitos Informáticos
Nota: Tomado de Fiscalía General del Estado (2015).

Como se aprecia los delitos informáticos como tal encuentran sus conductas tipificadas y para ellas una sanción afín, establecida en la normativa expuesta, así también se tienen conductas donde no necesariamente se habla del perjuicio a la informática, sino que más bien, refiere un medio, mecanismo o vía que permite la ejecución de un ilícito cuya conducta constituyen acciones ilegales más prácticas.

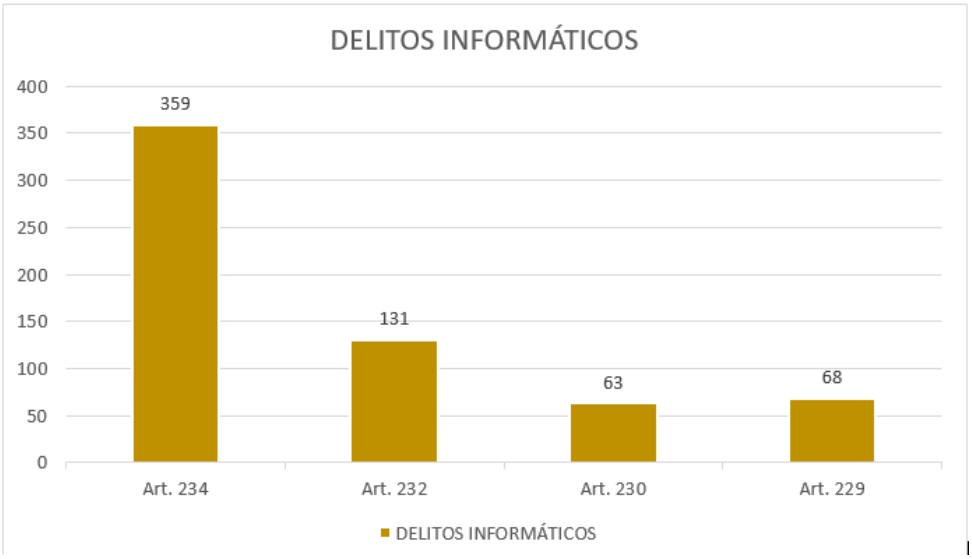


Figura 2. *Delitos Informáticos*
Nota: Tomado de Fiscalía General del Estado (2019)

Como se observa en el año 2019, en relación a las denuncias realizadas, se destacan como los delitos informáticos más frecuentes en el Ecuador los de carácter económico, a través del manejo, alteración, comercialización y desaparición de información y datos personales, muchos de ellos obtenidos de forma fraudulenta en la red, o través del uso de dispositivos, sistemas o software que permitan captar dicha información, y con estos datos realizar transacciones, transferencias, o inversiones sin el consentimiento del titular, en favor propio del delincuente o terceros.

2.2.5. Delitos informáticos económicos

De los delitos reconocidos en la normativa vigente a nivel nacional e internacional son de frecuente reincidencia y de alto perjuicio aquellos que atentan contra la economía y recursos de las víctimas, cometidos a través de medios electrónicos tienen igual o mayor perjuicio que aquellos delitos cometidos de forma física, a fin de referir una definición de estos, Barroso (2015) indica:

> Es, toda agresión, prohibida o no por el ordenamiento jurídico, que ponga en grave peligro los esquemas fundamentales de producción, distribución y consumo de los bienes de la comunidad como tal, o de un número apreciable de sus miembros, o que afecte, de igual forma, sus sistemas de financiación y de cambio. Todo ello, provocando el nacimiento de un daño directo y real; acudiendo al uso de métodos y formas atentatorios al equilibrio y fiabilidad de aquéllos, o a través de la comisión de otros delitos, ejecutados por puro móvil de enriquecimiento. (pág.100)

La afectación económica pese a ser cometido el ilícito por mecanismos tecnológicos o electrónicos es grave, y representa en muchos casos perjuicios millonarios y perdidas incalculables, casi siempre imposibles de recuperar, a lo cual se suma la dificultad de su investigación e identificación de un responsable, tal como lo manifiesta Casabona (2006):

> Aparte de los diversos problemas que presenta la manifestación de esta nueva delincuencia (entre los que se encuentra, en primer lugar, la difícil detección de esta clase de atentados, al ampararse sus autores precisamente en las características tecnológicas de los medios informáticos), están otros de índole

> técnico-jurídica, concretamente en que en ocasiones resulta problemático encuadrar estas conductas en los delitos tradicionales contra el patrimonio, si no se quieren vulnerar las garantías que se derivan de la vigencia del principio de legalidad. (p. 413)

La dificultad en su seguimiento y la obtención de indicios de responsables, magnifica el daño, y adicional se tiene la escasa normativa vigente con tipos penales específicos a las conductas ilícitas electrónicas, y por lo tanto resulta insuficiente cualquier analogía o intento por encuadrar la conducta muy exclusiva a otras similares, constituyéndose además en una ilegalidad, ahondando en la problemática, de forma particular en el Ecuador, si bien se tipifican delitos electrónicos que afectan al patrimonio, no se reconocen muchos de los que en la realidad se cometen con más frecuencia a través de medios electrónicos y afectan a la economía de las víctimas, por lo que si no encajan en los ilícitos tipificados se corre el riesgo de la impunidad de esos hechos.

Cabe referir como ejemplo del ilícito informático económico, el fraude informático, sobre lo cual Mayer y Calderón (2020), mencionan:

> La idea de fraude informático evoca la producción de un perjuicio patrimonial mediante la manipulación o alteración de datos o programas de sistemas informáticos. Sin embargo, si se consideran las conductas que normalmente se califican de tales, podrá constatarse que el término fraude informático es entendido de forma bastante más amplia y que, en ese sentido, bajo dicha denominación suelen incluirse comportamientos muy diversos. (pág. 152)

La información vertida en la red, implica la circulación de datos personales de alta relevancia y facultan así a la delincuencia el ingreso a cuentas, dominios y servicios bancarios, adquisición de servicios, manipulación de datos, uso de claves, tarjetas, cuentas y emplear esos recursos para su beneficio, ya sea en consumos, pagos, transferencias o desvíos de dineros u otros recursos a través del uso de medios electrónicos, lo cual es imperceptible en su comisión, y difícil de detener sino solo detectable ya el perjuicio consumado.

2.2.6. Características de los delitos informáticos económicos

Conforme se ha descrito tanto la naturaleza de los delitos informáticos en general, como los delitos informáticos de carácter económico, se puede caracterizar e identificar a estos últimos en base a estos presupuestos concluidos del análisis de la normativa vigente y teniendo como referente a Ron (2019):

Obtener un resultado. – Ya sea con la falsificación de datos, o con el manejo de las tecnologías en general, el resultado es obtener un lucro económico;

Datos. – a través del empleo de datos se busca afectar directamente al patrimonio del titular de los datos o de terceros, ya sea con datos verdaderos o falsos, siendo los más comunes los delitos de phishing;

TICS. – se debe usar como medio o mecanismo para su ejecución las Tecnologías de la Información y Comunicación, lo cual puede ser usado como inicio, medio y final;

Lucro. – Como móvil o fin del ilícito electrónico económico, debe estar precisamente el lucro, siendo el objetivo del delincuente obtener ganancias económicas, con lo cual se configura en efecto esta clase de delitos; y,

Bien jurídico. – Que además de lo ya mencionado, en lo referente a los delitos informáticos económicos, el patrimonio se aprecia como el bien jurídico tutelado, los medios electrónicos son precisamente eso un canal, un mecanismo, que facilita su ejecución. (Ron, 2019)

A lo cual acotan como métodos para delinquir Enríquez & Alvarado (2015):

a) Los datos falsos o engañosos, consiste en la introducción de datos falsos con el fin de producir o lograr movimientos artificiales en las transacciones de una empresa.
b) Manipulación de programas o Caballo de Troya, consiste en ocultar un programa informática en un computador ajeno, para ejecutar acciones no autorizadas.
c) Falsificaciones informáticas, tiene por objeto la falsificación de documentos empresariales haciendo uso de una fotocopiadora.

> d) Pishing, tiene con objetivo robarle la identidad a la víctima, utilizando engaños obtienen los datos personales, lo que les permite abrir cuentas bancarias, solicitar préstamos y tarjetas de créditos a nombre de la víctima. (p. 173, 174)

Es precisamente, la finalidad, la que identifica a los delitos informáticos económicos puesto que a diferencia de otros ilícitos de esta clase electrónica, no solo pretenden la afectación de sistemas, dispositivos o dominios, o el solo hecho de desviar información, u obtenerla para comerciarla, así tampoco el mal funcionamiento de tal o cual sistema, sino que, directamente pretenden conseguir un beneficio económico para sí o para terceros, a través de los recursos e intereses de los titulares de datos, cuentas o dominios.

2.2.7. Las TICS y los delitos informáticos

En virtud de la importancia, que tiene como medio o fin las tecnologías de la información y la comunicación o TICS, en el cometimiento de los delitos informáticos, cabe hacer un análisis particular de estas tecnologías y para ello en su definición genérica, y conforme Pineda (2008), las TICS son:

> [...] la unión de las telecomunicaciones y la informática. Comprenden todas las formas de tecnología empleadas para crear, almacenar, intercambiar y usar información en sus más variadas formas (datos, conversaciones de voz, imágenes, etc.). En términos generales, se puede afirmar que la industria de TICS crea un nivel significativo de empleos altamente capacitados y promueve industrias de apoyo y distribución. Asimismo, contribuye de forma substancial a los ingresos fiscales del Estado, por el pago de impuestos directos e indirectos; mejora sustancialmente la competitividad de las empresas y las industrias, en entornos locales y globales, ya que este sector proporciona un gran número de las herramientas que el sector productivo necesita para desarrollar las empresas y formar a los profesionales necesarios para competir de forma eficaz en una economía global. (p. 138)

Como se aprecia la tecnología, y comunicaciones a través de sus distintos medios, es de gran trascendencia para la interacción y desarrollo de la sociedad por los espacios que ocupa y los avances que facultan, y, agrega, además, Rosario (2011), que:

> Las Tecnologías de la Información y la Comunicación TIC, se constituyen en el conjunto de tecnologías que permiten la adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de informaciones, en forma de voz, imágenes y datos contenidos en señales de naturaleza acústica, óptica o electromagnética. Las TIC incluyen a la electrónica como tecnología base que soporta el desarrollo de las telecomunicaciones, la informática y el audiovisual.

Un sistema completo faculta la comunicación y las tecnologías, incluyen operaciones, sistemas, y códigos que van a devenir en el producto de insumos tecnológicos, este complejo, pero útil proceso y concepción facilitan una serie de actividades y resultados, para comprender lo práctico y útil de estas tecnológicas Berumen & Ariaza (2009), indican:

> La implementación de las nuevas tecnologías para el manejo y manipulación de datos es posible gracias a las facilidades de su almacenamiento y localización en pequeños espacios electrónicos y a un relativo bajo costo; todo ello ha permitido que los flujos de información sean más rápidos y tengan una aplicación prácticamente inmediata. (p. 20)

Estos factores les dan a dichas tecnologías la relevancia y alcance a las personas para usarlas y median entre una serie de actividades, relaciones y acciones, pero conforme indica Igarza (2007): “Las TIC no son autónomas, no adquieren significación sino por el tipo de recepción y adaptación que les confiere la sociedad, la que le ofrecerán entonces las prácticas sociales, la cultura y la política”. Por lo tanto, se pueden constituir en un medio o como se había ya afirmado como un fin, el cual emplea la persona o persigue para su beneficio o el de terceros (p. 8)

2.2.8. Investigación en delitos informáticos

El Código Orgánico Integral Penal, es la norma que establece, los principios y las garantías sobre las cuales se rige el sistema judicial penal, en el que a Fiscalía le corresponde el impulso de la investigación pre procesal y procesal penal, los delitos en

general y salvo los caso del delitos flagrantes, tienen como inicio una indagación o investigación previa, cuyo concepto se encuentra en el artículo 580 del Código Orgánico Integral Penal y cuyas características principales se detallan a continuación:

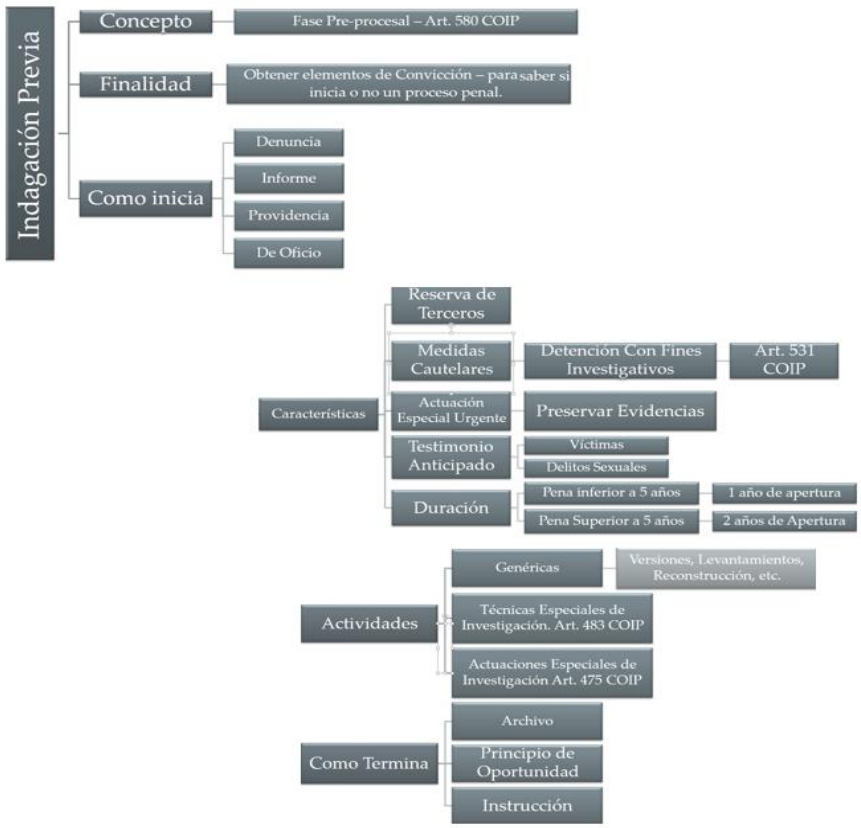


Figura 3. ***Indagación previa***
Nota: Tomado de Código Orgánico Integral Penal (2014)

En esta etapa se recopilan los elementos de cargo y descargo que sirven de base para iniciar o no un proceso penal, el cual se desarrolla en las etapas de Instrucción, Evaluación y preparatoria de Juicio y Juicio, como se detalla a continuación:

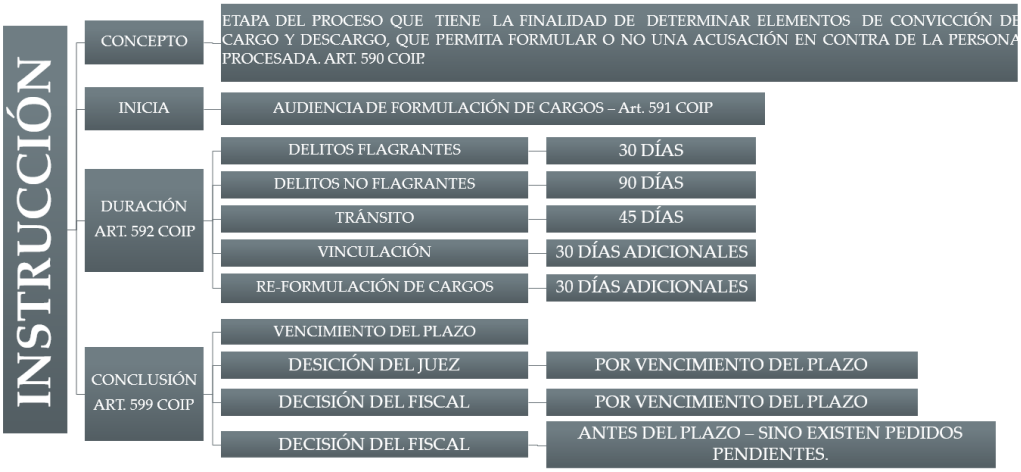


Figura 4. ***Instrucción***
Nota: Tomado de Código Orgánico Integral Penal (2014)

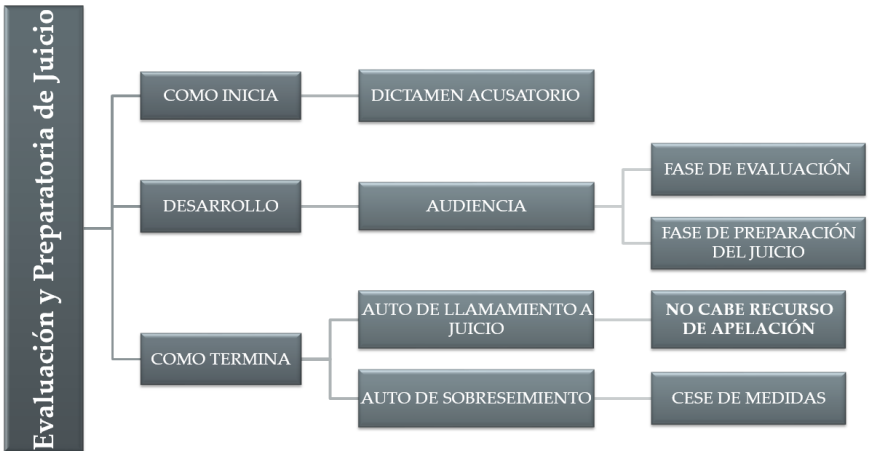


Figura 5. ***Evaluación y preparatoria de Juicio***
Nota: Tomado de Código Orgánico Integral Penal (2014)

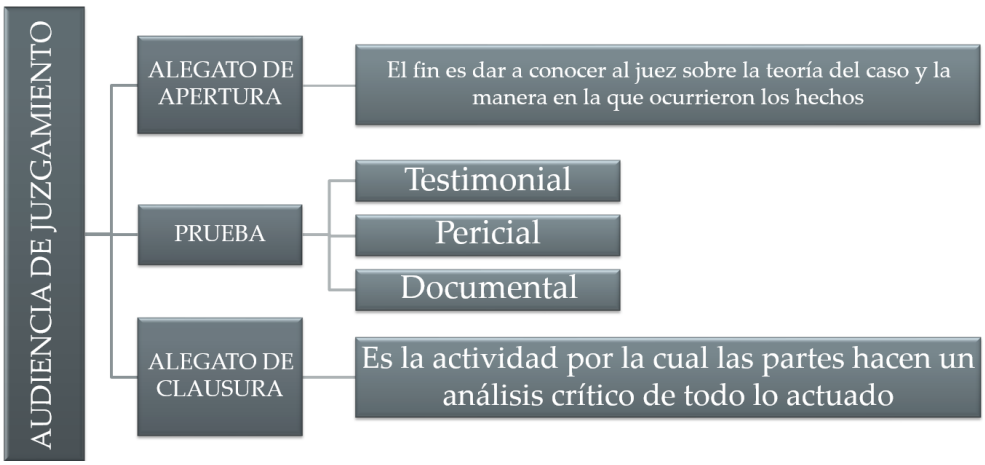


Figura 6. ***Juicio***
Nota: Tomado de Código Orgánico Integral Penal (2014)

De acuerdo al Informe de Rendición de Cuentas de la Fiscalía General del Estado del año 2021, esta dependencia ha tenido un total de 268.398 noticias del delito recibidas a nivel Nacional en el año 2020, conforme se observa:

Etapa Procesal	2020
Investigación previa	239.802
Instrucción fiscal	9.434
Preparatoria de juicio	10.350
Etapa de juicio	8.804
Impugnación	8
Total	**268.398**

Figura 7. ***Noticias del delito clasificadas por etapa procesal 2020***
Nota: Tomado de Sistema Integrado de Actuaciones Fiscales (SIAF). Informe de Rendición de cuentas de la Fiscalía General del Estado del año 2021.

En la investigación de delitos y a fin de determinar la materialidad de la infracción en delitos, cuya naturaleza así lo amerite, corresponde y como evidencia determinante, la intervención de un profesional especialista, y acciones técnicas específicas de cuya aplicación se aprecien verificaciones y vestigios contundentes de la materialidad y responsabilidad en virtud de la cual se inicie un proceso judicial y se llegue a ordenar una sanción, así cabe analizar la investigación en el caso de los delitos informáticos, para lo cual es preciso tomar en cuenta los datos que establece el Observatorio de Ciberseguridad del año 2017, ya que con estos datos se verifica la importancia de un manejo adecuado de la investigación informática forense, en los cuales se refleja que de los 16.785.361 habitantes de Ecuador, 14.651.404 poseen una línea celular y 9.613.353 tiene acceso a internet (Banco Interamericano de Desarrollo,2020).

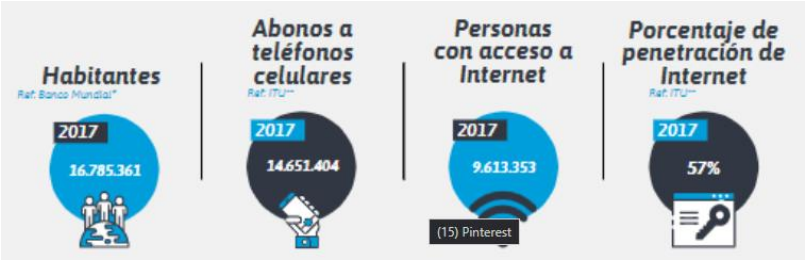


Figura 8. ***Observatorio de Ciberseguridad del año 2017***
Nota: Tomado de Banco Interamericano de Desarrollo (2020)

De acuerdo al criterio de Ferruzola, 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. (Ferruzola, 2014).

Vizueta (2011) indica que la falencia principal de la pericia informática en el Ecuador es la carencia de peritos 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.

En el país, se han detectado como falencias la falta de capacitación y la falta de procedimientos registrados de los delitos informáticos por parte de las entidades (Ureta, 2015), lo que ha producido que la pericia informática no tenga la fortaleza suficiente generando malos procesos los cuales se convierten en casos impunes (López, 2014).

En el boletín de la Fiscalía General del Estado, se indica lo siguiente:

> Según el fiscal provincial de Pichincha, Wilson Toainga, las investigaciones referentes a los delitos informáticos se realizan de forma técnica y demanda tiempo para establecer la responsabilidad de aquellos que quebrantan la ley sentados frente a un monitor. (Boletín Fiscalía General del Estado, 2020)

La cuestión de tiempo, en efecto es un atributo que genera dificultad a la hora de esclarecer los hechos aludidos y la protección de los bienes jurídicos tutelados, sin embargo, los requerimientos técnicos así lo justifican pues de ello depende el éxito de las investigaciones y los indicios concluyentes.

Se presenta a continuación un gráfico donde se evidencia el procedimiento de investigación correspondiente a los delitos informáticos, tomado de Bogen & Dampier,

quienes realizan un detalle de este proceso en relación a la computación forense, a fin de obtener un informe técnico:

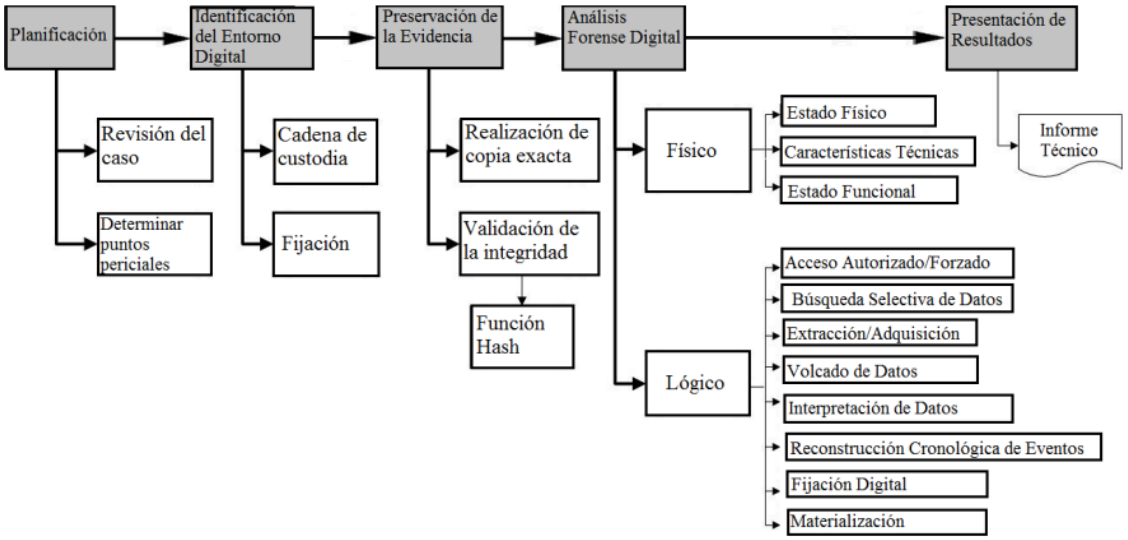


Figura 9. ***Procesos de Computación Forense***
Nota: Tomado de Bogen & Dampier (2005)

Teniendo en cuenta la importancia de la cadena de custodia de los medios probatorios, conforme lo reconoce el Código Orgánico Integral Penal, principio con el que deben cumplir así mismo los medios electrónicos esto es que, los elementos de convicción que luego en juicio toman el valor de prueba deben cumplir con estándares de credibilidad, probidad, idoneidad esto es: Ser auténticos (no manipulados), deben ser identificados (fijados y o reconocidos en estado original), ser recolectados técnica y adecuadamente, ser manejados y remitidos debidamente para su análisis posterior respectivo registrando las personas que tienen contacto con la evidencia a fin de que el juez, confíe que es la misma durante todo el proceso.

Así, lo adecuado es que el perito o técnico identifique en primer lugar el soporte técnico, es decir el dispositivo donde se halle la información, la extraiga y materialice en otro dispositivo, lo relevante para el caso, manteniendo así la cadena de custodia hasta que esta llegue al juez.

Sucede, además, que, los denunciantes suelen adjuntar su propio soporte con copia de la información, y esto no excluye la práctica de la pericia y la extracción técnica de la información, a lo provisto por las partes de le puede dar el tratamiento establecido en el Código Orgánico Integral Penal esto es, pericia de análisis, valoración y originalidad, así como transcribir su contenido.

En cuanto a la pericia electrónica al tratarse de información cruzada entre las partes, o la extracción de datos relacionados al caso, lo principal es identificar la fuente si es de red social o mensaje de correo, y la dirección objeto de pericia, a lo cual se procederá oficiando a criminalística directamente si se trata de una red social, para materializar la información e identificar su titular; mientras que si se trata de correo electrónico, se solicita la autorización del juez para posteriormente continuar como en el caso anterior.

> El señor fiscal Edwin Pérez, especialista en delitos informáticos, indicó que en Ecuador existen dificultades durante la investigación de delitos propiciados por el uso de la tecnología, por cuanto la información cruzada a nivel de redes sociales o cuentas de correos electrónicos no se encuentra en el país. (Boletín Fiscalía General del Estado, 2020)

Es también la cooperación imprescindible en estos casos, y más aún cuando los proveedores de redes sociales y generadores de sistemas informáticos como Facebook, Yahoo, Google, entre otros, tienen sus bancos de datos en Estados Unidos, y aspirar a obtener información de estas fuentes toma incluso meses, de allí se hace necesario que se suscriban los convenios internacionales pertinentes, mismos que no existen con tales sistemas y limitan el accionar.

Constituye un inconveniente para la investigación precisamente el hecho de que no existe un instrumento de carácter Internacional, que regule las relaciones entre Estados, a fin de realizar la investigación penal, sin embargo, esta el principio de

reciprocidad internacional, con el cual se maneja la Asistencia penal Internacional (API), la cual tiene como base:

- Convención de las Naciones Unidas contra la Corrupción.
- Convención de las Naciones Unidas contra el Tráfico Ilícito de Estupefacientes y Sustancias Sicotrópicas.
- Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional.
- Convención Interamericana sobre asistencia mutua en Materia Penal.

Para contar con esta asistencia, se realiza una solicitud de asistencia penal internacional que es "la petición y/o rogatoria internacional generada por la autoridad operativa judicial, en materia penal, del país requirente para ser diligenciada y cumplida por la autoridad judicial penal del país requerido" (Fiscalía General del Estado, 2021). Esta asistencia puede ser activa: la que la realiza un fiscal ecuatoriano a fin de obtener información o realizar diligencias en materia penal en otro Estado; o pasiva: la que realiza una autoridad en materia penal de un estado extranjero para solicitar información o la práctica de diligencias en Ecuador, cuyo trámite se observa en el siguiente gráfico:

Figura 10. ***Asistencia Penal Internacional***
Nota: Tomado de la Fiscalía General del Estado. Manual de Procesos de Asistencia Penal Internacional (2021)

Gracias a esta asistencia, para el caso de los delitos informáticos en los que se use las plataformas de Facebook o Whatsapp, la solicitud de información se la puede realizar

directamente sin la formalidad de una solicitud de asistencia penal internacional, a través de los siguientes (URL) Localizador Uniforme de Recursos:

- https//:www.facebook.com/records/login/
- https//:www.whatsapp.com/records/login/

Sin embargo, para las demás plataformas es necesario que la solicitud de asistencia penal internacional cumpla con los requisitos de:

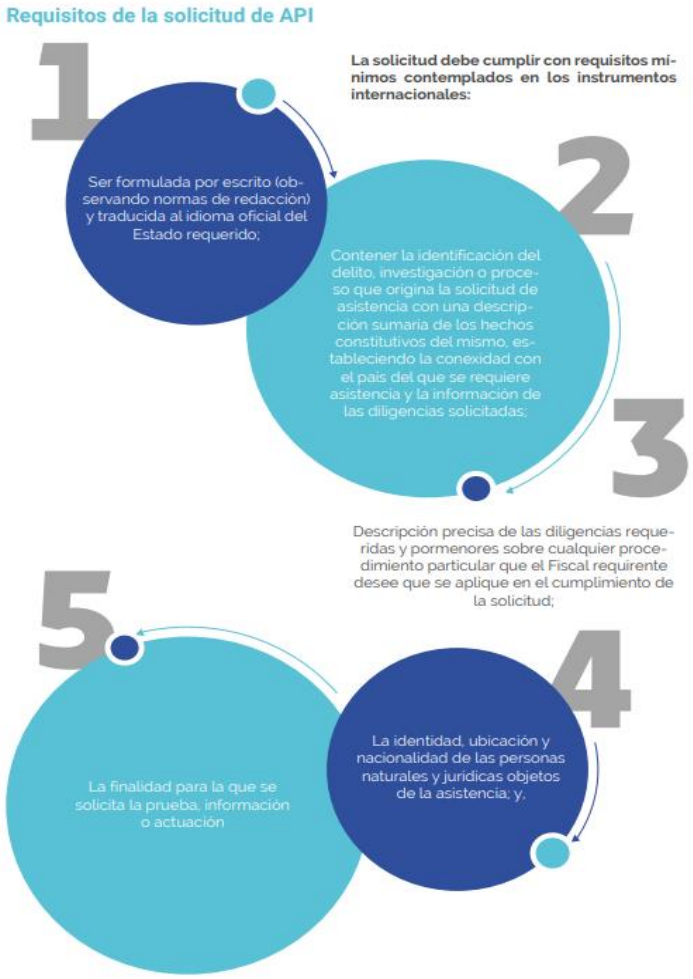


Figura 11. ***Requisitos de la solicitud (API)***
Nota: Tomado de la Fiscalía General del Estado. Manual de Procesos de Asistencia Penal Internacional (2021)

Se puede concluir que, para la investigación de los delitos informáticos, existe una complejidad en cuanto a la obtención de información ya sea por medios físicos constantes en elementos computacionales o en dispositivos electrónicos, así como de los que se obtienen de sistemas informáticos o plataformas de redes, la tarea de fiscalía para determinar el nexo causal es ardua y requiere de capacitación y conocimientos en informática forense.

2.2.9. Peritajes, y procedimientos de extracción de información

De lo antes expuesto es importante, además, considerar las principales técnicas empleadas para investigar los delitos informáticos, acorde a su naturaleza, al respecto cabe indicar algunos puntos enunciados por Quevedo (2017):

Obtención de una IP

> Es el primer paso para desarrollar cualquier investigación de este tipo. La dirección IP es una etiqueta numérica que identifica a una interfaz (elemento de comunicación/conexión) de un dispositivo (ordenador, móvil, pda, ipad, televión, ebook, consola de videojuegos) dentro de una red que utiliza el protocolo IP (Internet Protocol). Las direcciones IP son asignadas por los ISP (Internet service provider), compañías proveedoras de acceso a Internet (Telefónica, Jazztel, Orange). (p.169)

> Identificación de IMEI, IMSI y MAC. Con el término IMSI se hace referencia a un código de identificación único para cada línea de telefonía móvil integrada en la tarjeta SIM (*Subscriber Identy Module*) que permite la identificación del abonado a través de las redes GSM y UMTS. (p.176)

Como identificaciones únicas de los dispositivos y sistemas informáticos, estos códigos son los principales indicios a ser definidos dentro de una investigación en cuanto a delitos informáticos, así, en el caso del IMEI, que es un código pregrabado en teléfonos móviles, identifica de forma singular a nivel mundial al equipo, mientras que el numero MAC responde a la serie del equipo, constituye un avance significativo el definir estos números para posteriormente definir su propietario y ubicación.

Obtención de datos desvinculados de los procesos de comunicación

Una vez que se han procedido definir los principales indicios más evidentes en cuánto a equipos e identificación sistemática, corresponde se proceda a:

A) Identificación de titulares o terminales o dispositivos de conectividad.

a) rastrear e identificar el origen de una comunicación.

b) Identificar el destino de una comunicación.

c) Determinar la fecha, hora y duración de una comunicación.

d) Identificar el tipo de comunicación.

e) Identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación.

B) Acceso a datos no integrados en un proceso de comunicación (agenda de un teléfono móvil)

En virtud del registro que se mantiene de usuarios y propietarios de redes, equipos y cuentas de sistemas y equipos, se puede convalidar y en base a lo ya determinado inicialmente sobre la identificación del equipo o serie, determinar el propietario o titular del mismo, y de esta manera continuar con la investigación favorablemente.

Captación de Conversaciones Públicas

Como otro mecanismo de intervención ya más directa y oportuna en la investigación de los ilícitos informáticos, se encuentra la interceptación y captación de conversaciones, como fuente primordial de información, al tanto Quevedo (2017), menciona:

> Existen medios en internet, como los chats o foros, que permiten comunicarse a varias personas simultánea y públicamente en tiempo real. Obviamente, cuando las comunicaciones son accesibles para cualquier usuario de internet, no pueden tener la consideración de conversaciones privadas, pues es el propio usuario de la red quien se introduce en la misma y asume que muchos de los datos se convierten en públicos para todos los usuarios. (p. 193)

Es así que teniendo en cuenta la naturaleza de estas comunicaciones, no pueden considerarse amparadas por el derecho fundamental, el secreto de las comunicaciones, y responden a una excepcionalidad a los derechos constitucionales, bajo la investigación que se prosigue.

Pues si bien la protección y amparo normativo es amplio y general en lo que a tutela de derechos se refiere, la practicidad y fácil acceso a las tecnologías deja inoperante la prevención y salvaguarda en base a legislación, cuando el control supera las capacidades del órgano estatal encargado y se someten a la voluntad, ignorancia, necesidad, uso y abuso de quien como titular de los mismos derechos, es libre de emplear

como considere las tecnologías, dispositivos, sistemas, plataformas y redes, en las que invierte tiempo, confianza y dinero.

Interceptación de las comunicaciones telemáticas

Al igual que en el caso anterior, pero con otra fuente, es imperante en los casos de investigación de delitos informáticos el intervenir y captar información de medios o dispositivos telemáticos, como son:

a) Correo Electrónico
b) SMS y MMS
c) Mensajería Instantánea y las comunicaciones VoIP
d) Redes Sociales

En virtud de la trascendencia de la información, para extraerla u obtenerla, se interceptan bajo un procedimiento legítimo, y autorizado dentro del proceso investigativo, los mensajes de correo, mensajes de texto, mensajes multimedia, mensajería instantánea y de redes sociales, de igual manera con la excepcionalidad de la investigación y sanción de un delito, que faculta la intervención y exposición de estas fuentes.

Como se aprecian los principales mecanismos y técnicas de obtención de la información dentro de un proceso de investigación de ilícitos informáticos, responde a actividades meramente técnicas, tecnológicas y de capacidad pericial, formación y capacitación, así como de ética y profesionalismo afín de mantener los derechos de protección y no vulnerar derecho alguno durante su transcurso.

2.2.10. Nexo causal en delitos informáticos

El principal reto en torno a la investigación, juzgamiento y sanción efectiva de los delitos informáticos, está el establecer el nexo causal y poder definir satisfactoriamente el vínculo entre el acto, el daño y su responsable, para ello cabe mencionar a Patiño (2008), quien manifiesta: “Este elemento de la responsabilidad va ligado a la vinculación entre la causa y el efecto. De esta manera, “se entiende como la relación necesaria y eficiente entre el hecho generador del daño y el daño probado”. (p.193)

Por su parte el Código Orgánico Integral Penal, en su artículo 455, define al nexo causal y establece:

> La prueba y los elementos de prueba deberán tener un nexo causal entre la infracción y la persona procesada, el fundamento tendrá que basarse en hechos reales introducidos o que puedan ser introducidos a través de un medio de prueba y nunca, en presunciones. (Asamblea Nacional del Ecuador, 2014)

Precisamente para sancionar y llegar al resultado final del proceso judicial en el caso de delitos informáticos, se requiere definir la causalidad en el tipo penal, a lo cual indica Peláez (2018):

> La existencia de causalidad o nexo causal entre la conducta ejecutada por una persona y el ulterior resultado producido es un elemento imprescindible de la responsabilidad penal en los delitos de resultado, y aunque está claro que su comprobación es un requisito necesario para considerar a un sujeto como responsable.

Con una adecuada investigación llevada a cabo con la técnica y tecnología pertinentes es posible llegar a vislumbrar la relación entre la infracción electrónica y sus responsables, así como determinar las circunstancias y atributos del delito, que permitan en efecto motivar y conducir una resolución legitima.

En los delitos informáticos más que en otros ilícitos, se dificulta quizá la determinación de este nexo, sin embargo, impera la tecnificación y los recursos humanos y económicos pertinentes que faculten la cooperación internacional, la capacitación del personal interviniente, y finalmente la aplicación de prácticas técnicas y tecnológicas en apego al fin de la investigación, al debido proceso y sin transgredir derechos o garantía alguna.

2.3. Marco legal

Dentro de la normativa nacional vigente, existe normativa general y especifica en relación a la investigación, juzgamiento y sanción de delitos informáticos, desde la vialidad para el inicio de su investigación, hasta la conclusión del proceso, así desde la Constitución de la República del Ecuador, se dan los principales preceptos:

> Art. 16.- Todas las personas, en forma individual o colectiva, tienen derecho a:
> (…)

2. El acceso universal a las tecnologías de información y comunicación.

Art. 66.- Se reconoce y garantizará a las personas: (…)

19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.

20. El derecho a la intimidad personal y familiar.

21. El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación. (Asamblea Constituyente de Montecristi, 2008)

Con fundamento en los derechos y garantías antes expuestos, se tipifica en el Ecuador, delitos informáticos, así como otras infracciones cometidas a través de medios informáticos, digitales o cibernéticos, en el Código Orgánico Integral Penal, tal y como se ha especificado en el apartado correspondiente.

Existen cuerpos normativos que de forma general sirven de apoyo en la protección, prevención e investigación de delitos informáticos, mismos que proveen de indicaciones, preceptos y valores referenciales y bases para identificar conductas ilícitas, evitar el ser víctimas de tales infracciones o promover el adecuado uso de las tecnologías y medios electrónicos.

Cabe citar principalmente, al Reglamento para el Subsistema de Interceptación de Comunicaciones o Datos Informáticos, que establece como su objetivo en el artículo 2:

El Subsistema realizará la interceptación de las comunicaciones o datos informáticos, previa coordinación con el fiscal requirente a efectos de dar prioridad a la investigación de los delitos considerados como graves por la Convención de Las Naciones Unidas Contra la Delincuencia Organizada Transnacional, publicada en el Registro Oficial 197 del 24 de octubre de 2003,

con especial énfasis, en aquellos tipificados y sancionados en el Código Orgánico Integral Penal (...). (Fiscalía General del Estado, 2015)

Se tiene además a la Regulación No. DIR-103-2020 que contiene el Manual de Procedimientos para la verificación en listas nacionales e Internacionales para Prevenir el Lavado de Activos y el Financiamiento de Delitos.

Se halla vigente también, el Reglamento para el Procedimiento de Obtención, Registro, Análisis y Cotejamiento de Muestras Biométricas y Datos de la Fiscalía General del Estado, que tiene como objetivo y determinado en su artículo 1:

> El presente reglamento se aplicará para el proceso de obtención, registro, análisis y cotejamiento de muestras biométricas y datos, tales como: voz, imagen facial, huellas e impresiones papiloscópicas y otras que permitan descubrir la identidad de una persona procesada penalmente y privada de la libertad por delitos de acción pública determinados en el COIP; de los cadáveres identificados, no identificados; personas desaparecidas; y, las demás personas procesadas penalmente por delitos de acción pública sin medidas cautelares personales de privación de la libertad, que hayan autorizado por escrito el registro y toma de muestras biométricas. (Fiscalía General del Estado, 2015)

En cuanto a Convenios cooperación internacional, se tiene a la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, que es un tratado multilateral patrocinado por Naciones Unidas, cuyo objetivo es promover la cooperación para prevenir y combatir más eficazmente la delincuencia organizada transnacional., y en su artículo 14, respecto a capacitación y cooperación técnica, indica:

> 3. Los Estados Parte que tengan conocimientos especializados pertinentes considerarán la posibilidad de prestar asistencia técnica a los Estados que sean frecuentemente países de origen o de tránsito de personas que hayan sido objeto de las conductas enunciadas en el artículo 6 del presente Protocolo. Los Estados Parte harán todo lo posible por suministrar los recursos necesarios, como vehículos, sistemas de informática y lectores de documentos, para combatir las conductas enunciadas en el artículo 6. (Oficina de las Naciones Unidas contra la Droga y el Delito, 2004)

Se tiene, además, como una organización intergubernamental que cuenta con 194 países miembros, a la INTERPOL, quien es la encargada de ayudar a la policía de estos países a colaborar entre sí para hacer del mundo un lugar más seguro, para ello, le facilita el intercambio y acceso a información sobre delitos y delincuentes, y también les ofrece apoyo técnico y operativo de diversa índole.

Cabe citar finalmente que, en el marco de la VII Reunión de Ministros en Materia de Seguridad Pública de las Américas, la ministra de Gobierno, María Paula Romo; el ministro de Justicia y Seguridad Pública de Brasil, Sérgio Fernando Moro; el comandante General de la Policía Nacional, Gral. Nelson Villegas; y el director General de la Policía Federal, Maurício Leite Valeixo, suscribieron un Convenio de Cooperación Interinstitucional, y reafirmaron su misión de fortalecer la seguridad pública, a través de acciones conjuntas y estrategias coordinadas entre ambos países, el objetivo de este convenio es mejorar y ampliar la cooperación en la prevención y lucha contra la delincuencia organizada transnacional y los delitos conexos, económicos y cibernéticos, así como otras formas delincuenciales de dimensión internacional.

CAPITULO III

MARCO METODOLÓGICO

La presente investigación se desarrolló bajo el siguiente esquema metodológico.

3.1. Descripción del área de estudio

El área de estudio en donde se desarrolló esta investigación es en la Provincia de Imbabura, bajo la observación de los casos de delitos informáticos, que han sido denunciados en las unidades fiscales de esta Provincia.

3.2. Diseño y tipo de investigación

El enfoque bajo el cual se desarrolló la investigación es el cuantitativo pues se utilizaron las encuestas y cualitativo al realizar entrevistas, como medio para obtener la

información necesaria para el desarrollo del tema de investigación, además del bibliográfico, al emplear referentes doctrinarios, y expertos, así como teóricos, en torno al tema de investigación.

En cuanto al tipo de investigación, se desarrolló una investigación de carácter descriptivo, por cuando se detalló el problema planteado en relación con los datos obtenidos con la utilización de los instrumentos. La investigación histórico-lógica debido a que se realizó una construcción de la forma en cómo se investigan los delitos informáticos.

3.3. Procedimiento de investigación

Para el desarrollo de la investigación se utilizó una investigación bibliográfica, se recopiló el material escrito sobre los delitos informáticos para conocer la realidad actual sobre la investigación de los delitos informáticos. En la presente investigación no se tomaron en cuenta variables por lo que no corresponde a un tipo experimental de investigación.

Se utilizó el método descriptivo para determinar y analizar la situación actual de la investigación de los delitos informáticos, como el estudio refiere un fenómeno socio económico detrás, latente correspondió analizar su interacción, efectos y determinar su origen, conforme a los elementos que lo integran y a la idea de problemática aquí planteada.

Método Inductivo, a fin de establecer los elementos particulares del problema de investigación hacia la generalidad, es decir a través del análisis doctrinario, normativo, teórico, histórico, casos prácticos y demás evidencias, concluir en la existencia de una problemática esto es la investigación de los delitos informáticos, como idea central y objeto de investigación.

Método Documental. - pues se utilizaron diferentes tipos de documentos, sean teóricos, doctrinarios, cuerpos normativos, entre otros textos, en forma física, o digital, de los cuales se pudo extraer referentes, atributos, citas que contribuyeron al desarrollo de la presente investigación, de sus argumentos y sustento referencial y crítico.

Como Técnicas, está la Encuesta con la cual se procedió a recolectar la información necesaria y la realidad del problema de investigación. Se la realizó por medio de cuestionarios a profesionales Abogados. Y la Entrevista realizada en base a una guía dirigida a Fiscales de la Provincia de Imbabura.

3.3.1 Población

En esta investigación se aplicaron entrevistas a 8 señores Fiscales de la Provincia de Imbabura y encuestas a 90 profesionales del derecho de la Provincia de Imbabura, en un número de noventa, a los cuales se les remitió un cuestionario a ser contestado, a través de la herramienta web de Google forms, en el siguiente link: https://docs.google.com/forms/d/1qnciU_Uj3k-e6aEk0oWUIFB1KmOt2zdCD1i02PWp4Ro/edit

3.3.2. Muestra

Para la aplicación de entrevistas se recurrió a 8 fiscales de la provincia de Imbabura priorizando aquellos relacionados y con vinculación directa al objeto de investigación es decir los delitos informáticos de tal manera que puedan aportar con información de primera mano y con fundamento práctico.

Para la aplicación de la encuesta, se encuestó a 90 personas, teniendo en cuenta que fue aplicada a Profesionales del Derecho de Imbabura y qué para el año 2020, se encuentran registrados en el Foro de Abogados de Imbabura 2055 profesionales, y en virtud de la aplicación de esta técnica a través de la plataforma Google Forms, al encontrarse latente la pandemia por COVID-19 y siendo un mecanismo de investigación confiable y oficial, se aplicó el método de muestreo aleatorio, que, de acuerdo a CACES (2020):

MUESTREO ALEATORIO: es aquel procedimiento de selección de la muestra en el que todos y cada uno de los elementos de la población tiene una cierta probabilidad de resultar elegidos. De esta forma, si tenemos una población de N elementos y estamos interesados en obtener una muestra de n elementos (muestra de tamaño n), cada subconjunto de n elementos de la población tendrá también una cierta probabilidad de resultar la muestra elegida.

Si designamos por M_i a cada uno de estos subconjuntos, con i= 1,2,3, ...N;

cada M_i tendrá una cierta probabilidad P(Mi) de resultar elegido.

A través de la fórmula que aquí se ha planteado la característica aleatoria de selección dela muestra permite la probabilidad de qué dentro de la población establecida pueda obtenerse la participación de cuántos quieren participar o cómo es el caso de la presente investigación los resultados en tiempo real que se hayan podido obtener hasta el corte y análisis de resultados qué a continuación se plantea, al ser un método probabilístico no necesariamente precisa un cálculo matemático exacto qué refiere a un número de encuestados, considerando qué el universo de profesionales del derecho es muy amplio se puntualizó y conforme la localización de la investigación y de la investigadora, esto es la provincia de Imbabura y particularmente cómo eje de acción la ciudad de Ibarra.

3.4. Aplicación de técnicas

3.4.1. Análisis estadístico

Corresponde analizar los datos estadísticos en relación a los delitos informáticos en el Ecuador, a fin de identificar la cronología y evolución de estos ilícitos y su incidencia en cifras, tal es así que a continuación se presenta un gráfico en el que se detallan los indicadores correspondientes a cada delito tipificado en el Ecuador, así:

NÚMERO DE DENUNCIAS SOBRE DELITOS INFORMÁTICOS EN ECUADOR

Tipos de delitos	2014*	2015	2016	2017	2018	2019	2020**	
Suplantación de identidad	1355	3920	4152	3676	4180	4607	2162	24 052
Falsificación y uso de documento falso	1048	2594	3117	3183	3292	3231	1448	17 913
Apropiación fraudulenta por medios electrónicos	507	1280	1045	960	1451	1746	1033	8022
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	54	141	145	218	236	246	175	1215
Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	21	80	108	159	202	166	85	821
Ataque a la integridad de sistemas informáticos	49	77	76	86	87	113	51	539
Interceptación ilegal de datos	38	55	82	63	41	87	45	411
Transferencia electrónica de activo patrimonial	17	59	47	54	38	49	31	295
Revelación ilegal de base de datos	29	24	24	22	44	34	18	195
Total	**3118**	**8230**	**8796**	**8421**	**9571**	**10 279**	**5048**	**53 463**

*Desde agosto - **Hasta agosto

Fuente: Fiscalía General del Estado

EL UNIVERSO

Figura 12. ***Número de denuncias sobre delitos informáticos en Ecuador***
Nota: Fuente: Fiscalia General del Estado. Tomado de El Universo (2020)

Los delitos informáticos van en aumento en Ecuador, según las denuncias presentadas en la Fiscalía, desde antes de la pandemia del Covid-19. En el 2017 se registraron 8421 casos; subieron a 9571 y 10 279 en 2018 y 2019. La tendencia se mantiene. Desde enero hasta agosto del 2020 ya se registran 5048 delitos informáticos. Si la tendencia sigue casi se igualará a los casos del 2019.

Los más frecuentes son las estafas digitales con modalidades como la suplantación de la identidad y la apropiación fraudulenta a través de medios electrónicos. Sin embargo, es un riesgo constante el ser víctima de cualquiera de estas conductas ilícitas y se cometen a diario estas infracciones contra la seguridad informática, integridad y más derechos de las personas usuarias o no de estas plataformas, sistemas y dispositivos.

Contándose además que en Ecuador existen tan solo 19 peritos acreditados al Consejo de la Judicatura, especializados en Informática y Telecomunicaciones e Informática Forense.

PERITOS ACREDITADOS AL CONSEJO DE LA JUDICATURA		
INFORMÁTICA Y TELECOMUNICACIONES	QUITO	5
	GUAYAQUIL	3
	CUENCA	1
INFORMÁTICA FORENSE	QUITO	5
	GUAYAQUIL	3
	CUENCA	1
	RUMIÑAHUI-SANGOLQUÍ	1

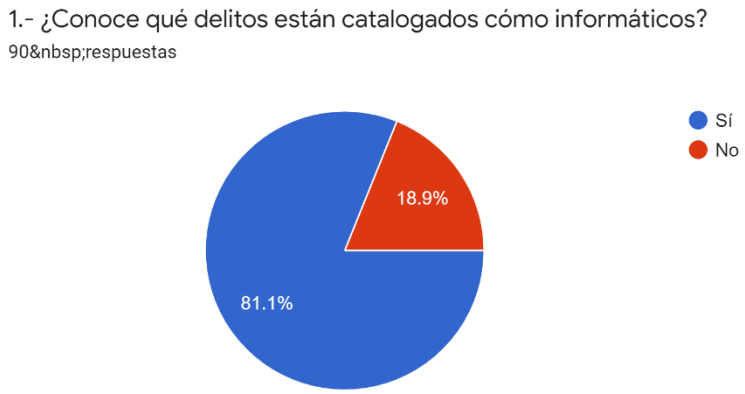
Figura 13. ***Peritos Acreditados al Consejo de la Judicatura (2021)***
Nota: Fuente Sistema Pericial- Consulta de Peritos Acreditados

Con estos resultados se valida la problemática identificada como objeto de la presente investigación, en tonto a los delitos informáticos y la deficiente investigación que existe, lo cual faculta su incremento desmedido y el alto índice de cometimiento de estas infracciones, sirviendo de respaldo y referente para la consecución del presente estudio, siendo pertinente por tanto realizar un análisis profundo que determine los factores detonantes de esta problemática, a lo cual es posible plantear recomendaciones estratégicas de solución.

3.4.2. Resultados de la aplicación de la encuesta

El objetivo de la encuesta fue, obtener información, opiniones, criterios y consideraciones profesionales y técnicas respecto a los principales indicadores identificados como elementos de la problemática objeto de investigación, es decir la investigación de los delitos informáticos y de esta manera sustentar y validad este estudio y su conclusión.

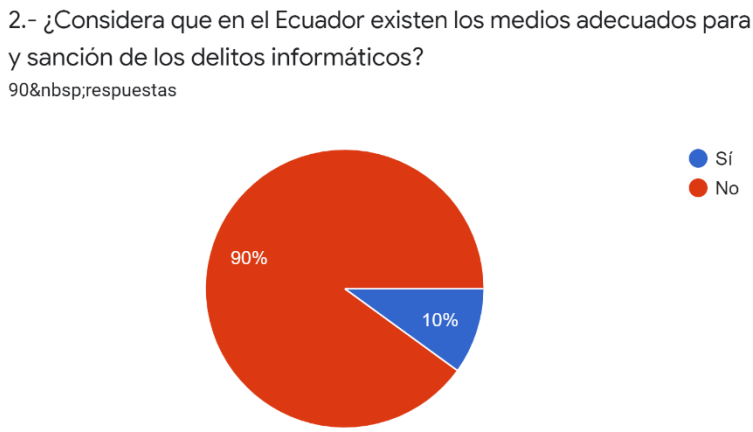
PREGUNTA 1



Elaborado por: Ana Saraguro

Interpretación: De los profesionales encuestados, se puede apreciar que, en torno a los delitos que están catalogados de forma específica como informáticos, en un 81.1% constituyendo la mayoría, afirman conocerlos e identificarlos, mientras que un porcentaje mínimo restante de 18.9% no los conoce, delimitando así el ámbito y manejo del tema por parte de los profesionales referidos, con lo cual se prosigue la presente investigación y su conclusión.

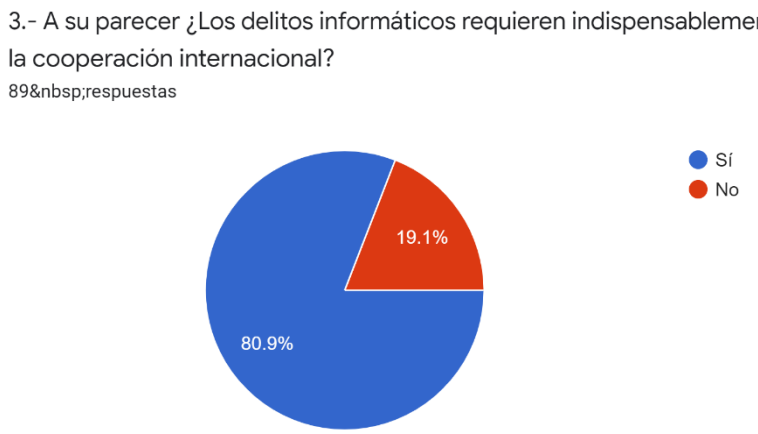
PREGUNTA 2



Elaborado por: Ana Saraguro

Interpretación: Respecto a la interrogante aquí planteada, los encuestados en una mayoría absoluta con el 90% consideran que en el Ecuador no existen los medios adecuados para la investigación, juzgamiento y sanción de los delitos informáticos, no así un mínimo porcentaje del 10% consideran que si existen tales medios, con estos resultados se valida un indicador en torno a la problemática objeto de estudio esto es, la falta de recursos para la investigación de los delitos informáticos con lo cual se respalda además el estudio y propuesta a realizar.

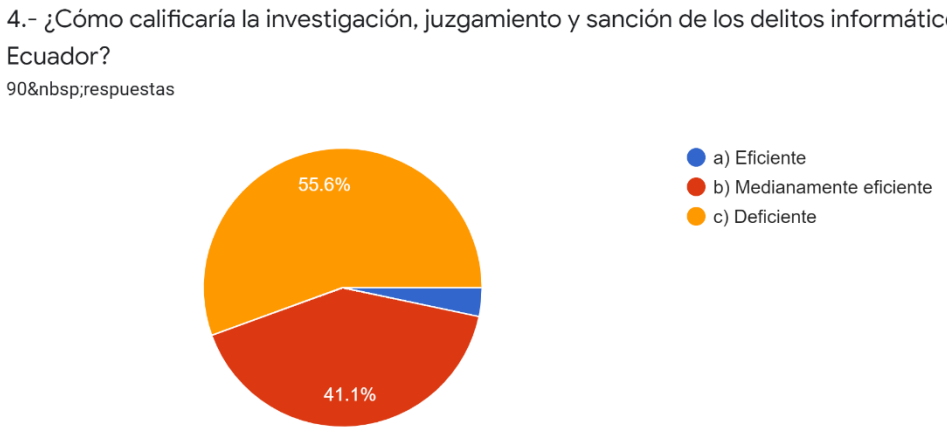
PREGUNTA 3



Elaborado por: Ana Saraguro

Interpretación: Con un 80.9% constituyendo la mayoría los encuestados consideran que en indispensable la cooperación internacional para la adecuada investigación y sanción de los delitos informáticos, y, en un porcentaje mínimo del 19.1% consideran que no es indispensable, de esta manera se valida el indicador de la problemática respecto a la falencia identificada por falta de convenios internacionales que faculten una adecuada investigación, de los delitos informáticos que por su naturaleza transcienden fronteras.

PREGUNTA 4



Elaborado por: Ana Saraguro

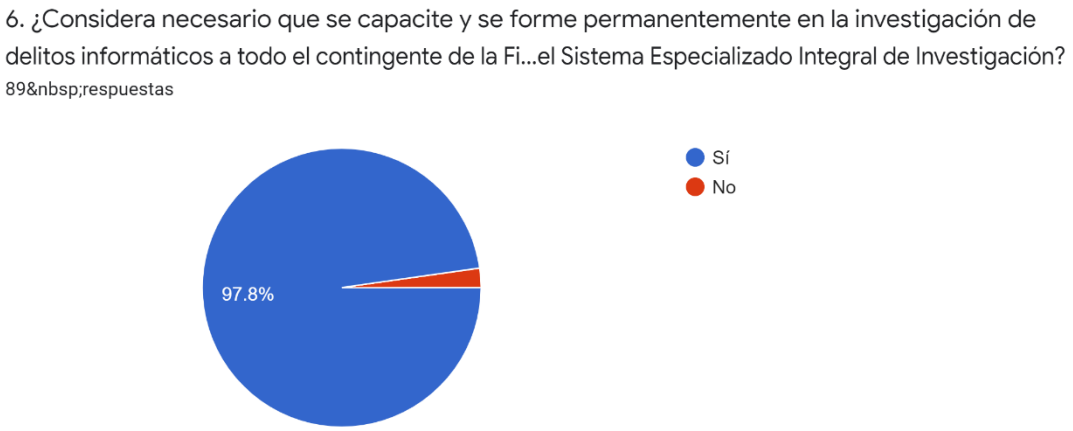
Interpretación: Entre los encuestados, se tiene que la mayoría de profesionales en un 55.6% consideran que la investigación, juzgamiento y sanción de los delitos informáticos en el Ecuador es deficiente, un porcentaje considerable cercano al anterior del 41.1% lo considera medianamente eficiente, y un mínimo restante del 3.3% lo ven como eficiente, de tal manera que los resultados apuntan a que la problemática identificada en realidad es validad y vista así por los encuestados, en su experiencia, con la idea que se continúa el presente análisis.

PREGUNTA 5

Elaborado por: Ana Saraguro

Interpretación: Plantadas que han sido algunas alternativas, respecto a la interrogante sobre las deficiencias que existen en torno a la investigación y sanción de los delitos informáticos, el 43.3% consideran que es el sistema especializado de investigación, un 30% afirma que radica en el personal especializado, un 18.9% considera que la problemática gira en torno a los recursos asignados para investigación, y; un 7.8.% considera que se debe a la normativa vigente, con estos resultados se valida la problemática objeto de investigación y los indicadores principales de la idea principal respecto a la deficiente investigación en delitos informáticos.

PREGUNTA 6



Elaborado por: Ana Saraguro

Interpretación: Los encuestados respecto a la necesidad de capacitar y formar permanentemente al personal de la Fiscalía y Sistema Especializado Integral de Investigación, sobre la investigación de delitos informáticos, consideran en su mayoría con un 97.8% que si es necesario, y en un mínimo de 2.2% consideran que no, de tal manera que en efecto se valida un factor determinante en torno al origen de la problemática que representa la deficiente investigación de delitos informáticos y la factibilidad del análisis aquí desarrollado.

PREGUNTA 7

Elaborado por: Ana Saraguro

Interpretación: Conforme las interrogantes que se han presentado y respecto a la pertinencia de reformar la normativa vigente en relación a la tipificación y procedimiento para el juzgamiento de los delitos informáticos, el 86.5% considera que si es pertinente y el porcentaje restante de 13.5% considera que no, de tal manera se obtiene un indicador respecto a la conformidad y satisfacción con la normativa vigente y una tendiente recomendación estratégica de solución, con la que se sustenta además el presente estudio.

3.4.3. Resultados obtenidos de la aplicación de la entrevista a los señores Fiscales de la provincia de Imbabura

La entrevista tuvo como objetivo, el conocer la percepción existente respecto a la investigación de los delitos informáticos en el Ecuador y la normativa vigente para ese fin. En la entrevista realizada a los señores fiscales de la provincia de Imbabura, se pudo obtener la siguiente información en relación a las preguntas realizadas:

Análisis Pregunta 1: En su experiencia, ¿Los delitos informáticos presentan gran dificultad para su investigación? ¿Por qué?

Para los señores Fiscales de las Fiscalías Especializadas en Delincuencia Organizada Transnacional e Internacional, presentan gran dificultad para su investigación, ya que, en nuestro medio, es decir la provincia de Imbabura, no existen peritos especializados, sumado al hecho de que el autor de los delitos informáticos, por lo general no se lo puede identificar, o se encuentra fuera del país.

Para los señores Fiscales de las Fiscalías Especializadas en Violencia de Genero, la investigación de los delitos informáticos es una tarea compleja, pues resulta difícil el aplicar un método científico de investigación tanto en estos delitos como en aquellos relacionados a la delincuencia organizada, tanto como a la delincuencia transnacional.

Para los señores Fiscales de las Fiscalías Multicompetentes y de Soluciones Rápidas, no existen peritos especializados, ni capacitados para determinar cuál es el lugar desde donde se realiza el cometimiento de estos delitos.

Análisis Pregunta 2: ¿Cuál es su criterio respecto a los recursos con los que cuenta Fiscalía General del Estado y el Sistema Especializado Integral de Investigación, para la determinación de los delitos informáticos? ¿Son suficientes o existen necesidades por cubrir?

Para los señores Fiscales de las Fiscalías Especializadas en Delincuencia Organizada Transnacional e Internacional, los recursos con los que cuenta Fiscalía General del Estado y el Sistema Especializado Integral de Investigación, para la determinación de los delitos informáticos, no son suficientes, puesto que quienes realizan las pericias para la determinación de estos delitos son escasas e inclusive sus conocimientos no están actualizados.

Para los señores Fiscales de las Fiscalías Especializadas en Violencia de Genero, en cuanto a los recursos con los que cuenta Fiscalía General del Estado y el Sistema Especializado Integral de Investigación, no son suficientes, por cuanto se debe solicitar apoyo a otras Instituciones a fin de cumplir con la tarea investigativa.

Para los señores Fiscales de las Fiscalías Multicompetentes y de Soluciones Rápidas, no son suficientes los recursos con los que cuenta Fiscalía General del Estado y el Sistema Especializado Integral de Investigación, es necesaria la capacitación del personal en todas las Provincias.

Análisis Pregunta 3: A su criterio ¿Por el alcance y ámbito de cometimiento de los delitos informáticos es indispensable la cooperación internacional? ¿El Ecuador cuenta en efecto con tal cooperación?

Para los señores Fiscales de las Fiscalías Especializadas en Delincuencia Organizada Transnacional e Internacional, por el alcance y ámbito de cometimiento de los delitos informáticos es indispensable la cooperación internacional, debido a que las sedes de las plataformas digitales se encuentran en el extranjero, y el acceso a la información contenida en estas plataformas es de vital importancia.

Para los señores Fiscales de las Fiscalías Especializadas en Violencia de Genero, nuestro país si cuenta con Cooperación Internacional, sin embargo, es proceso lento, y el acceso a la información es limitado.

Para los señores Fiscales de las Fiscalías Multicompetentes y de Soluciones Rápidas, si se cuenta con cooperación internacional, sin embargo, sus trámites son muy complejos.

Análisis Pregunta 4: ¿Cuál podría identificar como la mayor dificultad para establecer el nexo causal entre la conducta del sujeto activo y el resultado material de la infracción, en los delitos informáticos?

Para los señores Fiscales de las Fiscalías Especializadas en Delincuencia Organizada Transnacional e Internacional, la mayor dificultad para establecer el nexo causal entre la conducta del sujeto activo y el resultado material de la infracción, en los delitos informáticos, es el establecer la autoría, el tiempo, el lugar en donde se comete el

delito, pues existe gran dificultad para ubicar los IP usados para el cometimiento de estos delitos.

Para los señores Fiscales de las Fiscalías Especializadas en Violencia de Genero, existen muchos elementos de prueba, con los que se puede llegar a establecer el nexo causal, entre estos esta la identificación de la dirección IP, para de esta manera determinar el lugar en donde se encuentran los dispositivos, sin embargo, para ello se requiere mejor los recursos digitales.

Para los señores Fiscales de las Fiscalías Multicompetentes y de Soluciones Rápidas, la dificultad para identificar a los posibles autores de estos delitos, está en que existe un gran porcentaje de casos en los que los autores usan documentos e identidades falsas, para encubrir estos ilícitos.

Análisis Pregunta 5: De acuerdo a su experiencia ¿En qué porcentaje, aproximadamente, se llega a juzgar y sentenciar el cometimiento de delitos informáticos?

Para los señores Fiscales de las Fiscalías Especializadas en Delincuencia Organizada Transnacional e Internacional, en la Provincia de Imbabura, de su conocimiento aún no se ha llegado a juzgar y sentenciar el cometimiento de delitos informáticos.

Para los señores Fiscales de las Fiscalías Especializadas en Violencia de Genero, existe un porcentaje muy bajo de delitos informáticos que se ha llegado a juzgar y sentenciar.

Para los señores Fiscales de las Fiscalías Multicompetentes y de Soluciones Rápidas, existen muy pocos delitos informáticos que se han llegado a juzgar y sentenciar.

Análisis Pregunta 6: ¿Considera necesario reformar alguno de los tipos penales que tratan acerca de los delitos informáticos? ¿Qué modificaciones deberían realizarse?

Para los señores Fiscales de las Fiscalías Especializadas en Delincuencia Organizada Transnacional e Internacional, no se considera necesario reformar alguno de los tipos penales que tratan acerca de los delitos informáticos, pues a su parecer los tipos penales están bien definidos, lo que, si es necesario, es actualizar los conocimientos de

los señores peritos y gestionar mayor equipamiento de instrumentos tecnológicos que permitan establecer la autoría de estos delitos.

Para los señores Fiscales de las Fiscalías Especializadas en Violencia de Genero, se podría agravar las penas para evitar el cometimiento de estos delitos.

Para los señores Fiscales de las Fiscalías Multicompetentes y de Soluciones Rápidas, existe disposición legal, pero esta la falta de peritos y capacitación para especializar en este campo al personal de la Fiscalía General del Estado y el Sistema Especializado Integral de Investigación.

CAPITULO IV

RESULTADOS

La tecnología es sin duda un adelanto y factor de evolución significativo, de gran utilidad para todos los fines que se puedan requerir en la sociedad, cada avance, innovación, implementación, dispositivo, aplicación, sistema o plataforma han representado pasos agigantados hacia lo que hoy en día se aprecia como es la vida llena de facilidades, la sustitución de manufactura por la implementación de máquinas y sistemas, la creación de conexiones, la simplificación en general de procesos y actividades han ido convirtiendo a la tecnología y electrónica como necesidades ineludibles y hasta impositivas.

El amplio mundo de posibilidades que se abren en base a los adelantos tecnológicos y su acceso ilimitado y sin restricción, han hecho que cualquier persona pueda emplear este medio para los fines que considere más adecuados, y conforme ha ido evolucionando la sociedad y sus atributos lo han hecho a la par, las conductas ilícitas, mismas que se resumen a la facilidad de su uso y a encontrar debilidades, fallas o espacios que se han identificado en tal o cual medio o dispositivo informático o tecnológico, utilizando eso para la comisión de una inmensa variedad de delitos.

Las conductas ilícitas cometidas a través de los medios cibernéticos, tecnológicos o electrónicos, pueden verse como inimputables, puesto que se ve con dificultad el llegar a identificar el origen de la infracción y su responsable, por mucho que se analicen ciertas cuestiones físicas, internas de dispositivos y se analice la web, redes, plataformas y sistemas la limitante surge y de forma irónica al momento de encontrarse con restricciones de privacidad, acceso y uso, de lo cual son titulares y custodios quienes poseen y administran los dominios donde se almacenan los datos de sus usuarios y se sostienen plataformas, sitios y redes, de los distintos proveedores de servicios, la obtención de permisos, accesos e información además de ser muy difíciles de obtener, pueden tardar meses en ser obtenidos, cuestiones que se escapan de las manos de los investigadores, pero que sin embargo, representan la incertidumbre en el proceso de investigación y vulneran los derechos afectados ya por el ilícito electrónico.

Los delitos tipificados son varios y pese a ello surge un universo de posibilidades de conductas que pueden ser cometidas empleando a la informática y tecnología como

fin, medio o consecuencia, y es que la web es un abismo que hace que casi todo sea posible y cualquier conducta sea alcanzada, sean lícitas o ilícitas, si a ello se suma que el Internet facilita conexiones a nivel mundial y en tiempo real, se hace aún más extenso el espectro dónde acciona la delincuencia electrónica, y su persecución, investigación y sanción se convierten en un reto por un lado por la dificultad en identificar al responsable de la conducta ilícita y por otra parte el identificar y configurar cierto o ciertos hechos en los ilícitos tipificados en la normativa vigente y así sancionarlos.

Para que un delito pueda ser juzgado y sancionado adecuadamente se requiere de una investigación adecuada que arroje indicios convincentes respecto a la infracción, su materialidad y responsabilidad, para ello principalmente se requieren recursos, pues la investigación y contingente necesario para ese fin es costoso y el tiempo que se requiere lo incrementa pues no es un trabajo fácil y se indagan aristas que su vez se ramifican en nuevos indicios, la investigación no sólo es infructuosa de no hacerse adecuadamente sino que deviene en gastos desperdiciados y recursos mal empleados.

Conforme a la naturaleza de los delitos informáticos económicos, su investigación implica el uso así mismo de tecnologías, técnicas y procedimientos precisos y profundos, correspondiendo la necesidad de contar con profesionales especializados en investigación pericial, criminalística o forense de ilícitos informáticos, electrónicos o cibernéticos, que no sólo sean afines a ello, puesto que a partir de su intervención se conseguirá el adecuado manejo de equipos, información e indicios, salvaguardando su validez y cadena de custodia que los conviertan en medios probatorios válidos, así como eficientes en conducir al investigador a una conclusión.

El alcance de este tipo de infracciones se proyecta a nivel mundial, por lo tanto, las fronteras no son restricción para el paso de la tecnología y es que a través de la web el acceso es ilimitado, por lo que es necesario que se establezcan y suscriban convenios que faciliten la prosecución de esta clase de ilícitos a través del mundo, hasta descubrir su origen, determinar responsables y de esta manera reparar los daños o vulneraciones a los bienes jurídicos protegidos, o a su vez prevenir la expansión y aumento del índice de estos delitos, siendo así posible contactar a aquellos servidores donde reposan los datos de redes, sistemas y plataformas, obteniendo no solo una respuesta favorables sino que en el menor tiempo, la cooperación es sin duda vital en este ámbito, y lamentablemente

el Ecuador no cuenta con tales contactos y convenios, en forma suficiente para que se faculte una investigación de delitos electrónicos internacional y llegar a un fin exitoso.

En el Ecuador se aprecian deficiencias estructurales evidentes, partiendo de los recurso limitados que se destinan para la investigación, administración de justicia y sanciones de ilícitos, los delitos informáticos se ven lejanos de obtener la atención económica necesaria para su efectiva investigación, juzgamiento y sanción, otra falencia es la deficiente cooperación internacional, y falta de sustento en convenios que faciliten la investigación de delitos informáticos a niveles internacionales, así como la falta de especialización, capacitación y formación de profesionales exclusivamente preparados para el fin investigativo de estos ilícitos y su conclusión.

Si se parte de una falencia en la investigación, no se puede augurar la conclusión idónea del proceso, y la impunidad se deja ver como consecuencia, lamentablemente y como se había antes manifestado esta situación penosa se ahonda cuando los resultados no son exitosos y se invierten y desperdician prácticamente recursos, ante las limitantes ya establecidas para la investigación de los delitos informáticos, si se habla de una investigación con falencias, carencias y limitantes, no se puede hablar de una verdadera investigación, pues no alcanzarían los fines que esta etapa persigue.

Ante estas circunstancias se ven vulnerados preceptos constitucionales al no precautelarse derechos, intereses y garantías comprometidos con la ejecución de conductas electrónicas ilícitas, su secuencia y perpetuidad, la deficiente e infructuosa investigación y la falta de sanciones adecuadas, mientras se mantenga esta problemática en torno a la investigación de delitos informáticos, la vulneración se mantiene y agrava, dejando en la indefensión a los bienes tutelados y promoviendo el incremento de comisión de estas conductas.

El principio de progresividad a la par con los derechos a la seguridad jurídica y la tutela judicial efectiva, evidencian la necesidad de adaptar la normativa vigente a la realidad actual de la sociedad y las nuevas conductas ilícitas y formas nuevas de cometer los delitos ya tipificados con anterioridad, esto es una reforma al Código Orgánico Integral Penal en la cual se incluyan de forma específica conductas que no encajan en los delitos ya tipificados pero que son cometidos con frecuencia a través de medios informáticos, incremento de las sanciones establecidas para los delitos informáticos, así

como la definición de un sistema especializado para la investigación de delitos informáticos, que cuente con el ámbito, objeto y preceptos específicos que faculten una investigación especializada, exclusiva, específica y eficiente.

El ámbito internacional es quizá la mayor debilidad del Ecuador en la investigación de delitos informáticos, pues ante la falta de una adecuada cooperación internacional se ve limitado este proceso, por lo que corresponde se suscriban los convenios pertinentes con otros países, sobre todo con aquellos donde se encuentran los servidores de almacenamiento de datos de redes, plataformas y sistemas, así como, se hagan los acercamientos necesarios con organismos de investigación, justicia e intervención especializados en delitos informáticos, a fin de obtener comunicación, capacitación, formación y apoyo en la investigación y persecución de delitos informáticos y sus responsables.

El perjuicio es claro a la eficiencia de la tecnología y por ende a la confianza que depositan las personas en sus servicios, siendo en su mayoría delitos contra la propiedad, el patrimonio y los ingresos económicos de la persona, vulneran principalmente los derechos a la integridad, a la libertad, intimidad, y en consecuencia muchos otros derechos, inclusive colectivos y la soberanía misma del Estado, de allí deviene la urgencia de atender estas falencias y necesidades de forma amplia y suficiente.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

Como conclusiones de la investigación fue posible determinar que:

- Realizada que ha sido la investigación bibliográfica, fundamentados los elementos principales del objeto de investigación y contextualizados tanto con el apoyo de fuentes doctrinarias, como jurídicas se ha establecido un ámbito en el que, se va a desarrollar la investigación conforme el análisis de la problemática aquí planteada, una vez que se conoce más detalladamente lo referente a los delitos informáticos y las implicaciones jurídicas que acarrea, esto ha sido en efecto plasmado en el marco teórico del presente estudio.

- Realizada que ha sido la investigación metodológica, se han empleado principalmente las técnicas de la encuesta y entrevista, validadas que fueron, además, con la muestra estadística en cuanto a la investigación de los delitos informáticos, precisamente, con estos datos se ha podido validar la idea objeto de investigación, y así identificar los puntos críticos a ser resueltos con el análisis y sentar así conclusiones y recomendaciones en cuanto al estado actual del objeto de investigación y las necesidades qué se evidencia en el ámbito jurídico ecuatoriano.

- Como parte de la investigación, además, se ha contrastado la normativa nacional con la normativa vigente en otros países, buscando través de ello establecer la forma en la que se lleva la investigación de los delitos informáticos en el Ecuador y conocer a breves rasgos la situación de estos países en la materia, para de esta manera proyectar ventajas y desventajas así como las necesidades y posibles alternativas que al respecto muestran otros países, en tal razón ha sido posible apreciar que la problemática se refiere a la localización y organización así como la economía del Ecuador, puesto que son limitantes precisamente para que se de un adecuado proceso investigativo, en torno a la disponibilidad de recursos..

- La magnitud de la web y medios informáticos, permite que así mismo se expanda la delincuencia informática al mundo, pudiendo ser cometida en un país y afectando a su víctima o victimas en otro país distinto y del otro lado del planeta sin dificultad alguna, las facilidades le han dado al infractor carta abierta para hacer y deshacer sin problema, con una infinidad de posibilidades en distintos ámbitos y con distintos objetivos a afectar, limitando a la justicia de tal forma que ha quedado relegada y a pasos agigantados la delincuencia le ha dejado atrás.

- Una adecuada investigación y sanción de los delitos informáticos es la clave para su sanción, combate y reducción de su índice, para lo cual los recursos deben ser proporcionales, justos y suficientes, se debe contar con personas capacitadas en el área que se encarguen de llevar la investigación, y así mismo se cuente con normativa y juzgadores capacitados para configurar, juzgar y sancionar adecuadamente a estas conductas ilícitas, caso contrario no tiene mayor sentido si se lleva a cabo de forma parcial o incompleta.

- Las necesidades en el Ecuador respecto a la investigación de los delitos informáticos son latentes, y se pueden identificar en torno a la falta de recursos, falta de profesionales capacitados y peritos, y un sistema de administración de justicia debilitado para atender de manera eficiente estas necesidades.

- La Fiscalía como órgano encargado de la investigación en causas penales, y pese a sus mejores esfuerzos poco o nada puede lograr ante las limitantes referidas para la adecuada investigación de los delitos informáticos, sus peritos, agentes e investigadores no son suficientes en número, y requieren mayor especialización, la carga laboral y numero de causas que ingresan hacen que su tiempo sea limitado y por ende requieran de mayor tiempo en la investigación que de por sí, lleva ya mucho tiempo por el alcance y magnitud.

RECOMENDACIONES

En atención a lo expuesto es pertinente recomendar:

- Que, el Estado destine los recursos necesarios para implementar un mejor servicio, adecuar procesos, efectuar pericias, trabajo de campo, dotación de equipos, contingente adecuado para la investigación de delitos informáticos, de tal manera que pueda llegarse a una conclusión favorable en protección y tutela de los derechos constitucionales, y los bienes jurídicos protegidos, así como se promueva la formación, capacitación y difusión en prevención de los delitos informáticos, y el conocimiento del marco legal vigente.

- Que, se refuerce la capacitación y formación continua del personal de la Fiscalía General del Estado, en especial de agentes de investigación, peritos y, de funcionarios y administradores de justicia en la materia, a fin de alcanzar una intervención eficiente e idónea, que verdaderamente consiga el objeto de tutela judicial efectiva que como derecho reconoce la Constitución de la República.

- Que, se prosigan las causas e investigaciones de delitos informáticos con responsabilidad y empeño hasta que se concluyan en indicios o acusaciones sustentadas en argumentos, fundamentos y evidencias validas, y que mejor hasta sancionar a los responsables y reparar integralmente a la víctima, o víctimas.

- Que, se asuma con responsabilidad el uso de tecnologías y la informática, para ello cada persona sea consciente y responsable de la magnitud e importancia que tiene el uso que se le dé a tal o cual dispositivos, sistema, plataforma, aplicación o red, y los datos que se proporcionen, es siempre importante informarse al respecto y tomar medidas de prevención y cuidado adecuadas al amplio mundo de la informática y sus servicios.

- Que, por parte de las empresas a cargo de los servicios web, tecnológicos e informáticos, se fortalezcan los controles, precaución, restricciones y permisos en sus espacios, sistemas o dispositivos, en cuanto al acceso y manejo a fin de que se promueva el uso adecuado de los mismos, y se prevenga el perjuicio como consecuencia de las conductas ilícitas informáticas, y así mismo se controle la intervención de personas miembros de grupos de atención prioritaria en estos medios, de tal manera que se evite también el que sean víctimas de esos delitos.

- Qué, se habilite una oficina para pericias informáticas en la provincia de Imbabura a fin de evitar que los procesos investigativos dependan del trasladarse a la ciudad de Quito ya que esto representa actualmente la inversión de tiempo y recursos, y la habilitación de la oficina representaría un apoyo relevante para el pronto y adecuado despacho.

REFERENCIAS BIBLIOGRÁFICAS

Acurio, S. (2015). *Delitos Informáticos: Generalidades.* Quito: PUCE. Obtenido de: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Alcívar, c., Domenech, G., & Ortiz, K. (2015). La Seguridad Jurídica frente a los delitos informáticos. *Avances*, 10-12. obtenido de: https://libros.ecotec.edu.ec/index.php/editorial/catalog/download/32/29/243-2?inline=1

Barroso, J. (01 de 06 de 2015). *Scielo*. Obtenido de Los delitos económicos desde una perspectiva criminológica: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472015000100095

BBC . (4 de mayo de 2016). *BBC Mundo, redacción.* Obtenido de BBC: https://www.bbc.com/mundo/noticias/2016/05/160504_tecnologia_aparatos_mas_influyentes_historia_yv

Berumen, S., & Ariaza, K. (2009). *Evolución y desarrollo de las TIC en la economía del.* Madrid: Ecobook.

Cano M., J. J. (2016). *Computación forense: Descubriendo los rastros informáticos.* Bogotá : Alfaomega.

Cano, D. (2011). *Contra el fraude: Prevención e investigación en América Latina.* Barcelona: Granica.

Casabona, C. (2006). *Delitos Informáticos de carácter patrimonial* . La Laguna: Universidad de la Laguna.

Chauca, G. (2014). *EL PRINCIPIO DE PROPORCIONALIDAD EN LA PREVENCION DE LOS DELITOS INFORMATICOS.* Ibarra: UNIANDES.

Código Orgánico Integral Penal [COIP] (2014). *Código Orgánico Integral Penal.* Asamblea Nacional. Registro Oficial, Suplemento 180.

Código Penal Federal (2009). Código Penal Federal. Cámara de Diputados del H. Congreso de la Unión. Última reforma publicada el 24 de

junio de 2009.

Consejo de Europa. (23 de noviembre de 2001). *Ministerio de Asuntos Exteriores.* Obtenido de Convenio sobre la ciberdelincuencia: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Corporación de Estudios y Publicaciones. (2016). *Constitución de la República del Ecuador, comentarios, legislación conexa, concordancias.* Quito: Corporación de Estudios y Publicaciones.

Constitución de la Republica del Ecuador (2008). *Constitución de la Republica del Ecuador.* Asamblea Constituyente de Montecristi. Registro Oficial 449.

Donnelly, J. (2017). *Derechos humanos internacionales.* México, D.F: Trillas.

Enríquez, J., & Alvarado, Y. (2015). *LOS DELITOS INFORMÁTICOS Y SU PENALIZACIÓN EN EL CÓDIGO ORGÁNICO INTEGRAL PENAL ECUATORIANO.* Tulcán: UPEC.

FGE. (13 de 06 de 2015). *Fiscalía General del Estado*. Obtenido de Los delitos informáticos van desde el fraude hasta el espionaje: https://www.fiscalia.gob.ec/los-delitos-informaticos-van-desde-el-fraude-hasta-el-espionaje/

Fiscalía General del Estado (2021). *Instructivo de Cooperación Penal Internacional*. Quito: Asuntos Internacionales de la Fiscalía General del Estado.

Fiscalía General del Estado (2015). *Reglamento para el Procedimiento de Obtención, Registro, Análisis y Cotejamiento de Muestras Biométricas y Datos*. Resoluciones 2015

Fiscalía General del Estado (2015). *Reglamento para el* Subsistema de Interceptación de Comunicaciones o Datos Informáticos *Subsistema de Interceptación de Comunicaciones o Datos Informáticos*. Resoluciones 2015

García Falconí, J. (2011). *Los nuevos paradigmas en materia constitucional en el ordenamiento jurídico ecuatoriano: Nuestros derechos constitucionales. Tomo 2.* Quito: Rodin.

Gómez Vieites, Á. (2013). *Auditoría de seguridad informática.* Bogotá: Ediciones de la U.

Huilcapi, A. (24 de 11 de 2005). *Derecho Ecuador.* Obtenido de El Delito Informático: https://www.derechoecuador.com/el-delito-informatico

Igarza, R. (2009). *Burbujas de ocio, Nuevas formas de consumo cultural.* Buenos Aires: La Crugía.

INREDH. (mayo de 2015). *Fundación Regional de Asesoría en Derechos Humanos.* Obtenido de INREDH: https://www.inredh.org/archivos/pdf/derecho_a_la_informacion_publica.pdf

Lázaro Domínguez, F. (2013). *Informática forense: Introducción.* Bogotá: Ediciones de la U.

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (2002). *Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos*. Congreso Nacional. Registro Oficial, Suplemento 557.

Ley Especial contra los Delitos Informaticos (2001). *Ley Especial contra los Delitos Informaticos*. Asamblea Nacional de la República Bolivariana de Venezuela. Gaceta Oficial Nro. 37.313.

Martos Rubio, A. (2015). *Redes sociales.* Madrid: Anaya Multimedia.

Mata y Martín, R. M. (2001). *Delincuencia informática y derecho penal.* Madrid: Edifoser.

Mayer, L. (01 de 04 de 2017). *Scielo.* Obtenido de El bien jurídico protegido en los delitos informáticos: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-34372017000100011&lng=pt&nrm=i.p&tlng=es

Mayer, L., & Oliver, G. (01 de 06 de 2020). *Scielo.* Obtenido de El delito de fraude informático: Concepto y delimitación: https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0719-25842020000100151&lng=es&nrm=iso#aff1

Muñoz Conde, F. (2017). *Derecho penal: Parte especial.* Valencia: Tirant lo Blanch.

OFICINA DEL ALTO COMISIONADO DE LAS NACIONES. (1988). *ACNUR.* Obtenido de ACNUR: https://www.acnur.org/fileadmin/Documentos/BDL/2005/3584.pdf

Oficina de las Naciones Unidas contra la Droga y el Delito (2004). *Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional*. Nueva York.

Pineda, L. (20 de 01 de 2014). *Universidad & Empresa.* Obtenido de Las tecnologías de información y comunicaciones: https://www.redalyc.org/articulo.oa?id=187214457006

Quevedo, J. (2017). *Investigación y prueba del ciberdelito.* Barcelona: Universitat de Barcelona.

Riofrío, J. (2012). *Los Delitos Informáticos y su Tipificación en la Legislación Ecuatoriana.* Loja: UNIVERSIDAD NACIONAL DE LOJA . Obtenido de: https://dspace.unl.edu.ec/jspui/bitstream/123456789/9329/1/Jaime%20Francisco%20Riofr%C3%ADo%20.pdf

Rivera, L. d. (2013). *El maltrato psicológico: Cómo defenderse del bullying, el mobbing y otras formas de acoso.* Bogotá: Ediciones de la U.

Ron, M. (21 de 10 de 2019). *Estafa informática.* Obtenido de Derechoecuador.com: https://www.derechoecuador.com/estafa-informatica

Rosario, J. (01 de 08 de 2011). *Cibersociedad.* Obtenido de Cibersociedad: http://www.cibersociedad.net/archivo/articulo.php?art=218

Sain, G. (2015). Evolución histórica de los delitos informáticos. *Revista Pensamiento Penal*, 4. Obtenido de: http://www.pensamientopenal.com.ar/system/files/2015/04/doctrina40877.pdf

Suárez, A. (2009). *La estafa informática.* Bogotá: Grupo Ibáñez.

Temperini, M. (2014). *Delitos Informáticos en Latinoamerica: un estudio de Derecho Comparado.* Buenos Aires: SOCIEDAD ARGENTINA DE INFORMÁTICA E INVESTIGACIÓN OPERATIVA

Vallejo Delgado, V. E. (2010). *El delito informático en la legislación ecuatoriana.* Quito: Corporación de Estudios y Publicaciones.

Velasco Melo, A. H. (29 de junio de 2008). *Sistema de Información Científica Redalyc.* Obtenido de Revista de Derecho: https://www.redalyc.org/articulo.oa?id=85102913

Vizueta Ronquillo, J. (2011). *Delitos informáticos en el Ecuador.* Guayaquil: Edino.

ANEXOS

A) ENCUESTA DIRIGIDA A PROFESIONALES DEL DERECHO DE LA CIUDAD DE IBARRA

Objetivo: Conocer la percepción existente respecto a la investigación de los delitos informáticos en el Ecuador y la normativa vigente para ese fin.

1.- ¿Conoce qué delitos están catalogados cómo informáticos?

Sí

No

2.- ¿Considera que en el Ecuador existen los medios adecuados para la investigación, juzgamiento y sanción de los delitos informáticos?

Sí

No

3.- A su parecer ¿Los delitos informáticos requieren indispensablemente, para su investigación, de la cooperación internacional?

Sí

No

4.- ¿Cómo calificaría la investigación, juzgamiento y sanción de los delitos informáticos en el Ecuador?

a) Eficiente

b) Medianamente eficiente

c) Deficiente

5.- De haber seleccionado las opciones b o c en la pregunta anterior. ¿Cuál es, a su parecer, la deficiencia más fuerte en cuanto a la investigación, juzgamiento y sanción de los delitos informáticos en el Ecuador?

a) Normativa vigente

b) Sistema especializado de investigación

c) Recursos asignados para investigación

d) Personal especializado

6. ¿Considera necesario que se capacite y se forme permanentemente en la investigación de delitos informáticos a todo el contingente de la Fiscalía General del Estado y del Sistema Especializado Integral de Investigación?

Sí

No

7. ¿Es a su criterio pertinente reformar la normativa vigente en cuanto a la tipificación, y procedimiento para el juzgamiento de los delitos informáticos?

Sí

No

B) ENTREVISTA DIRIGIDA A FISCALES DE LA PROVINCIA DE IMBABURA

Objetivo: Conocer la percepción existente respecto a la investigación de los delitos informáticos en el Ecuador y la normativa vigente para ese fin.

1) En su experiencia, ¿Los delitos informáticos presentan gran dificultad para su investigación? ¿Por qué?

2) ¿Cuál es su criterio respecto a los recursos con los que cuenta Fiscalía General del Estado y el Sistema Especializado Integral de Investigación, para la determinación de los delitos informáticos? ¿Son suficientes o existen necesidades por cubrir?

3) A su criterio ¿Por el alcance y ámbito de cometimiento de los delitos informáticos es indispensable la cooperación internacional? ¿El Ecuador cuenta en efecto con tal cooperación?

4) ¿Cuál podría identificar como la mayor dificultad para establecer el nexo causal entre la conducta del sujeto activo y el resultado material de la infracción, en los delitos informáticos?

5) De acuerdo a su experiencia ¿En qué porcentaje, aproximadamente, se llega a juzgar y sentenciar el cometimiento de delitos informáticos?

6) ¿Considera necesario reformar alguno de los tipos penales que tratan acerca de los delitos informáticos? ¿Qué modificaciones deberían realizarse?

C) SOLICITUD (API) FISCALÍA GENERAL DEL ESTADO

FGE
Fiscalía General del Estado
ECUADOR

1701018894123 44

SOLICITUD DE ASISTENCIA PENAL INTERNACIONAL

1. ÓRGANO REQUIRENTE:

Nombre de la institución:	Fiscalía General del Estado. Fiscalía Provincial de……
Autoridad solicitante:	Fiscal de la Unidad Especializada de……..
Dirección:	……..
Teléfono:	(593)……
Fax:	(593)……..
Correo electrónico:	……...
Punto de Contacto:	DIRECCION DE ASUNTOS INTERNACIONALES FISCALÍA GENERAL DEL ESTADO.
Dirección: Quito – Ecuador.	Av. Juan León Mera N1936 y Av. Patria. (593) 2 3985800, extensión 173193/173023
Correo Electrónico:	asistenciaspenales@fiscalia.gob.ec

2. AUTORIDAD CENTRAL:

Institución:	FISCALÍA GENERAL DEL ESTADO
Autoridad Central:	Dra. Diana Salazar Méndez FISCAL GENERAL DEL ESTADO
País:	Ecuador
Dirección:	Av. Juan León Mera N1936 y Av. Patria.
Teléfonos:	(593) 2 3985800 despacho@fiscalia.gob.ec

3. AUTORIDAD CENTRAL DEL PAÍS REQUERIDO:

Autoridades competentes de ……

4. IDENTIFICACIÓN DEL CASO:

Expediente Nº: ……

Año: ……

Ofendidos (s): .....

Investigado(s) o Procesado(s): .....

Delito / Acto Administrativo: .....

5. PROVISIONES LEGALES PARA SOLICITAR LA ASISTENCIA:

5.1. Constitución de la República del Ecuador

Art. 195.- La Fiscalía dirigirá, de oficio o a petición de parte, la investigación pre procesal y procesal penal; durante el proceso ejercerá la acción pública con sujeción a los principios de oportunidad y mínima intervención penal, con especial atención al interés público y a los derechos de las víctimas.

De hallar mérito acusará a los presuntos infractores ante el juez competente, e impulsará la acusación en la sustanciación del juicio penal.

Para cumplir sus funciones, la Fiscalía organizará y dirigirá un sistema especializado integral de investigación, de medicina legal y ciencias forenses, que incluirá un personal de investigación civil y policial; dirigirá el sistema de protección y asistencia a víctimas, testigos y participantes en el proceso penal; y, cumplirá con las demás atribuciones establecidas en la ley.

5.2. Código Orgánico Integral Penal (COIP)

Art 442.- Fiscalía.- La Fiscalía dirige la investigación pre procesal y procesal penal e interviene hasta la finalización del proceso.

La víctima deberá ser instruida por parte de la o el fiscal sobre sus derechos y en especial, sobre su intervención en la causa.

Artículo 497.- Asistencia judicial recíproca.- Las o los fiscales podrán solicitar asistencia (…) para la práctica de diligencias procesales, pericias e investigación de los delitos previstos en este Código.

(…) Asimismo, la o el fiscal podrá efectuar actuaciones en el extranjero dirigidas a recoger antecedentes acerca de hechos constitutivos de alguna infracción, a través de la asistencia penal internacional.

Las diligencias señaladas serán incorporadas al proceso, presentadas y valoradas en la etapa del juicio.

Informe de Cumplimiento de Asistencia Penal Internacional
(API N° ...)

1. Antecedente:

Mediante memorando No..... de....(fecha) ...., la Dirección de Cooperación y Asuntos Internacionales remitió la solicitud de asistencia penal internacional librada por las autoridades de ...(nombre del país)...., dentro del caso No. ....., que se sigue por el presunto delito de....., en contra de.....

2. Diligencias requeridas:

Una vez revisada la solicitud de asistencia penal, se advirtió que lo peticionado por el Estado requirente consistió en:

(LISTAR LAS DILIGENCIAS REQUERIDAS)

1. *(Ejemplo: Información migratoria de NN;*
2. *Antecedente penales de NN*)
3.

3. Actuaciones fiscales:

Para dar cumplimiento a lo requerido, la Fiscalía de ....., mediante impulso fiscal del ....(fecha)..., dispuso dar cumplimiento a la rogatoria internacional, para lo cual se procedió a oficiar a las entidades correspondientes: *Ejemplo: Registro Civil, Policía Judicial, Superintendencia de Compañías, Dirección Nacional de Migración, etc.*

4. Resultados obtenidos:

(Detallar los resultados concretos, obtenidos de cada diligencia solicitada, indicando el número de foja en la que se encuentra el documento)

1. *Ejemplo: De la información migratoria solicitada, se adjunta el certificado migratorio en el que consta que NN salió del país el 2 de febrero de 2016. (foja 20)*

2. *Se adjunta el documento remitido por el Consejo de la Judicatura con resultados negativos. (foja 22)*
3.

5. Conclusión:

La solicitud de Asistencia Penal Internacional librada por las autoridades de…(nombre del país)…, dentro del caso No. ……., que se sigue por el presunto delito de……., en contra de……., ha sido cumplida en su totalidad (y/o parcialmente -según corresponda-, por cuanto……)

Es de relieve indicar que las diligencias, cuyos respaldos se adjuntan, fueron ordenadas y cumplidas conforme lo establece la Constitución de la República y demás leyes pertinentes ecuatorianas.

Por consiguiente, se dispone la devolución de la solicitud de asistencia penal internacional a la Dirección de Cooperación y Asuntos Internacionales, para que por su intermedio se remita al Estado requirente.

Lugar y Fecha……..

Atentamente,

Firma del Fiscal delegado
Nombre del Fiscal delegado

Anexo: …..fojas