UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
SISTEMA DE POSGRADO
MAESTRÍA EN DERECHO MENCION DERECHO PROCESAL

TEMA:

La penalización de los delitos informáticos en el COIP

AUTOR:

Chávez Dávila Gonzalo Javier

Previo a la obtención del grado académico de:

MAGÍSTER EN DERECHO MENCIÓN DERECHO PROCESAL

TUTOR:

Msg. Vivar Álvarez Juan Carlos Esp.

ECUADOR

2022

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
SISTEMA DE POSGRADO

MAESTRÍA EN DERECHO MENCIÓN DERECHO PROCESAL

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por el **Abogado** Chávez Dávila Gonzalo, como requerimiento parcial para la obtención del Grado Académico de **Magister en Derecho Mención Derecho Procesal.**

DIRECTOR DEL PROYECTO DE INVESTIGACIÓN

_____
MSG. VIVAR ÁLVAREZ JUAN CARLOS ESP.

REVISOR

_____
DR. FRANCISCO DÁVILA

DIRECTOR DEL PROGRAMA

_____
Dr. Miguel Hernández Terán

Guayaquil, a los 28 días del mes de noviembre del año 2022

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
SISTEMA DE POSGRADO
MAESTRÍA EN DERECHO MENCIÓN DERECHO PROCESAL

DECLARACIÓN DE RESPONSABILIDAD

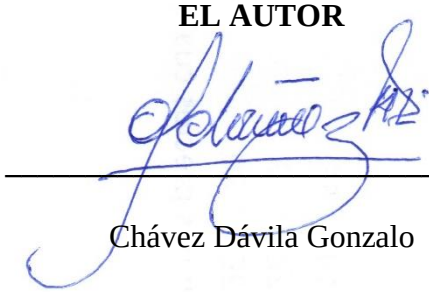
Yo, Chávez Dávila Gonzalo Javier

DECLARO QUE:

El Proyecto de Investigación **La penalización de los delitos informáticos en el COIP,** previa a la obtención del Grado Académico de **Magister en Derecho Mención Derecho Procesal**, ha sido desarrollado con base en una investigación exhaustiva, respetando derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía. Consecuentemente este trabajo es de mi total autoría. En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico de la tesis del Grado Académico en mención.

Guayaquil, a los 28 días del mes de noviembre del año 2022

EL AUTOR



Chávez Dávila Gonzalo

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN DERECHO MENCIÓN EN DERECHO PROCESAL

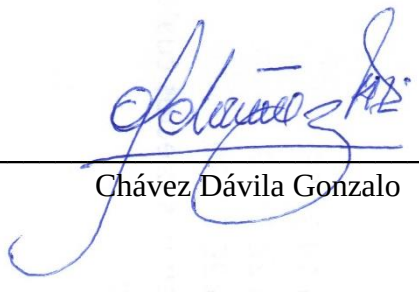
Yo, Chávez Dávila Gonzalo Javier

AUTORIZACIÓN

Autorizo a la Universidad Católica de Santiago de Guayaquil, la **publicación** en la biblioteca de la institución del **Proyecto de Investigación,** previo a la obtención del Grado Académico de Magister en Derecho Mención Derecho Procesal, titulada: **La penalización de los delitos informáticos en el COIP,** cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 28 días del mes de noviembre del año 2022

EL AUTOR:



Chávez Dávila Gonzalo

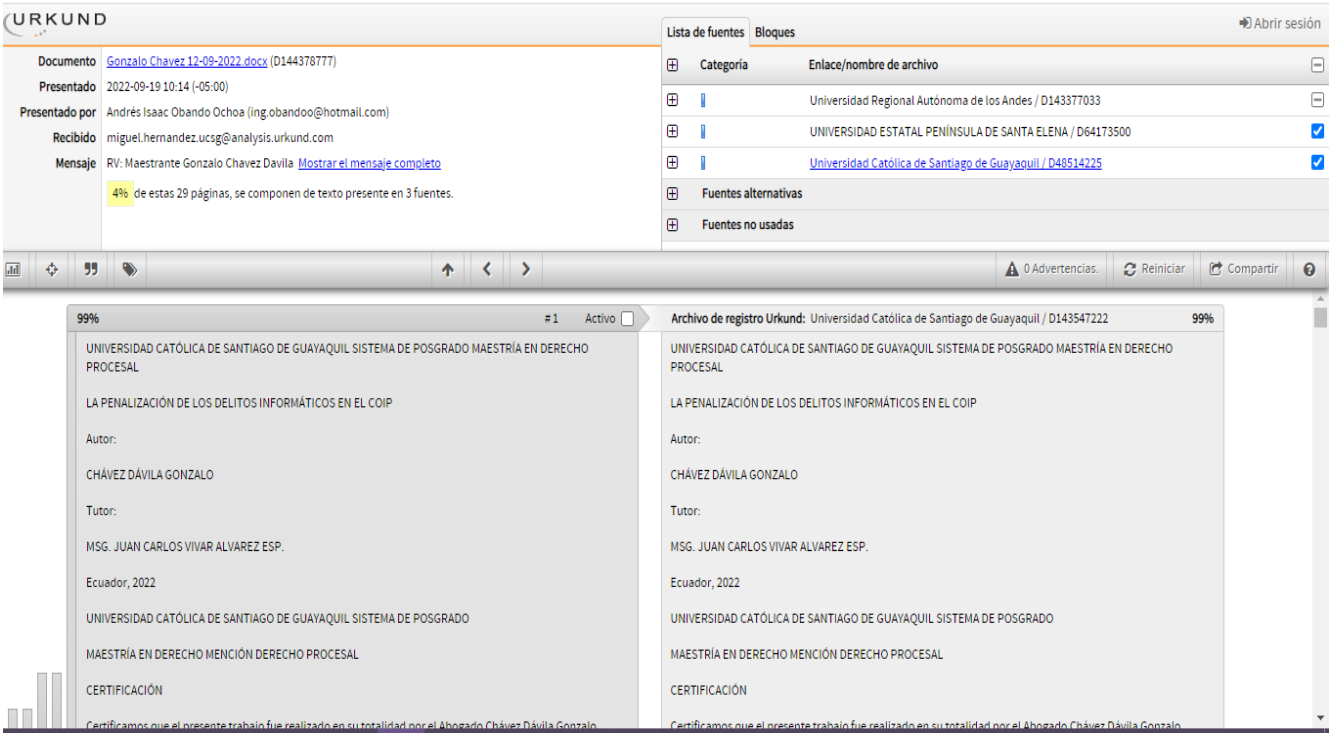
UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN DERECHO MENCIÓN DERECHO PROCESAL

INFORME DE URKUND



AGRADECIMIENTO

Quiero agradecer Dios mi guía espiritual que me ha permitido culminar este nuevo proyecto, gracias a Él inspiré mi vida, para salir adelante. Gracias Señor, por cada momento de mi vida, por cada sueño que me das y por cada bendición.

Dedicatoria

A **Dios** por guiarme por el camino correcto, porque nunca me ha abandonado, gracias por haberme dado una excelente familia, por permitirme conocer excelentes profesores y amigos y porque has llenado mi corazón con la luz de tu espíritu dejando que cumpla esta meta.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE GRAFICOS

RESUMEN

El objetivo general de la presente investigación fue determinar la penalización de los delitos informáticos en el Código Orgánico Integral Penal, como objetivos específicos se realizaron estudios de los delitos informáticos más comunes en la actualidad y sus sanciones, se revisaron las normativas jurídicas aplicadas en los casos de delitos informáticos y se estableció una propuesta de solución que mediante las sanciones eviten la impunidad de estos actos ilícitos como son los delitos informáticos. Estuvo basado en un análisis de carácter bibliográfico y documental que tuvo como centro del mismo el paradigma interpretativo, orientado al análisis de textos que tienen vinculación con el análisis de los delitos informáticos y su penalización según las leyes ecuatorianas tipificadas en el Código Orgánico Integral Penal. Los resultados demostraron que dentro de los delitos informáticos más cometidos en la República de Ecuador, destacan el delito de apropiación fraudulenta de por medios electrónicos, con la finalidad de apropiarse de un bien o valores ajenos, se encuentra también las trasferencias electrónicas de activo patrimonial, para causar un daño económico a la víctima y por último el acceso no consentido a un sistema informático en contra de la voluntad del titular de donde se determinó que la impunidad se debe a que son poco denunciados estos delitos. Por último, se instó a la Asamblea Nacional a los efectos de hacer una modificación al Código Orgánico Integral Penal, con el fin de elevar las penas a los delitos informáticos más cometidos con la finalidad de efectuar una sanción mayor a la comisión de los mismos.

Palabras Claves: Penalización, delitos, informáticos, código, pena.

ABSTRACT

The general objective of this research was to determine the criminalization of computer crimes in the Comprehensive Organic Penal Code, as specific objectives studies of the most common computer crimes today and their sanctions were carried out, the legal regulations applied in the cases were reviewed. of computer crimes and a proposed solution was established that through sanctions avoid impunity for these illicit acts, such as computer crimes. It was based on a bibliographic and documentary analysis that had as its center the interpretative paradigm, oriented to the analysis of texts that are linked to the analysis of computer crimes and their penalization according to the Ecuadorian laws typified in the Comprehensive Organic Penal Code. It was concluded that the computer crimes most committed in the Republic of Ecuador include the crime of fraudulent appropriation of by electronic means, with the purpose of appropriating a property or foreign values, there is also the electronic transfers of patrimonial assets, to cause damage economic to the victim and finally the non-consensual access to a computer system against the will of the owner from which it was determined that impunity is due to the fact that these crimes are little reported. Finally, the National Assembly was urged to make a modification to the General Organic Code of Processes, in order to increase the penalties for the most committed computer crimes in order to carry out a greater sanction than the commission of the themselves.

Key Words: Penalty, crimes, IT, code, penalty.

Introducción

1.1.Objeto de estudio: Delitos Informáticos

La tecnología ha invadido todos los espacios, un alto porcentaje de las actividades realizadas en la cotidianidad actual están altamente vinculadas al uso de dispositivos informáticos, incluso actividades que hasta hace unos años era casi imposible pensar realizar a través de la tecnología. A manera de historia, se hace referencia a una de las primeras definiciones sobre delitos informáticos, la cual fue establecida en el año 1983, cuando la Organización de Cooperación y desarrollo Económico lo definió como "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesamiento automático de datos y/o transmisiones de datos" (Meléndez, 2018, pág. 1). Para 1984, International Business Machine Corporation, de ahora en delante IBM PC se reporta un virus masivo denominado troyano, lo que conllevó a varios Estados de los Estados Unidos a crear una Ley específica con la finalidad de proteger los sistemas informáticos de las instituciones públicas.

En el Ecuador, para el año 2013 aproximadamente el 65% de los ciudadanos ecuatorianos ya contaba con acceso a servicios de internet. Para el año 2016 el porcentaje aumenta, un 86% de los ciudadanos ecuatorianos tiene acceso a las tecnologías de información, porcentaje que va en aumento cada vez más. La presencia de la tecnología no se limita solo al uso personal o en los hogares, sino que forman parte esencial de las actividades que se llevan a cabo en las empresas y organizaciones, facilitando los procesos y convirtiéndose en base primordial del éxito de las empresas. Sin embargo, unido a los avances tecnológicos se generan situaciones que empañan el buen uso de la tecnología pasando de ser una herramienta de suma importancia para las personas y empresas, a una herramienta con fines delictivos (Enriquez & Alvarado, 2015).

En virtud de los problemas cibernéticos que surgen con la aparición de los medios informáticos, se hace necesario dar respuesta legal a los casos delictivos relacionados con el mal manejo de recursos informáticos, por lo que desde el año 1999, comienza a discutirse en el Ecuador el proyecto de Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas (2002), posteriormente aprobado para el año 2002. Al principio la ley presentó falencias que poco a poco fueron corrigiéndose, sin embargo, en el mencionado Código no se consideraban los adelantos tecnológicos que para los años siguientes ya se daban en el país y el mundo.

Posteriormente, para el año 2002, después de largas discusiones se aprueba la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, y en consecuencia se plantean las reformas al Código Penal, que originaban los llamados Delitos Informáticos. De esta manera, a la par con el progreso tecnológico que experimentan las sociedades y los países, se supone la creación de formas de delinquir y nuevos actos ilícitos, siendo necesario serios debates que conlleven a soluciones efectivas de estos delitos. Ahora bien, aun cuando se dan avances tecnológicos y manejo de equipos informáticos distintos cada vez, algunos analistas aportan que no es necesario hacer diferencia entre los delitos informáticos tradicionales y los actuales, resaltando que se trata de los mismos delitos pero que se cometen de manera diferente, y en conclusión se refieren a invadir la privacidad o confidencialidad de datos (Computer Forensic, 2019).

Para el año 2014, a través del Código Orgánico Integral Penal (2018) (en adelante COIP) se establece la Sección Tercera referida a Delitos contra la seguridad de los activos de los sistemas de información y comunicación; en los artículos 178, 179, 181, 190, 229, 230, 231, 232, 233, y 234, señalando las sanciones privativas de libertad. Según resumen presentado por la Policía Nacional del Ecuador (2017), actualmente Ecuador dispone de

Leyes que sancionan este tipo de delitos, reconocidos en el COIP, dentro de las cuales se mencionan las siguientes:

- Pornografía infantil: De 13 a 16 años de prisión.
- Violación del derecho a la intimidad: De uno a tres años de prisión
- Revelación ilegal de información de bases de datos: De uno a tres años de prisión
- Interceptación de comunicaciones: De tres a cinco años de prisión.
- Pharming y Phishing: De tres a cinco años de prisión
- Fraude informático: De tres a cinco años de prisión.
- Ataque a la integridad de sistemas informáticos: De tres a cinco años de prisión
- Delitos contra la información pública reservada legalmente: De tres a cinco años de prisión.
- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones: De tres a cinco años de prisión (Policía Nacional del Ecuador, 2017).

Los Delitos Informáticos son parte del apresurado cambio que sufren las Tecnologías de Información y Comunicación "TIC´s", dando paso a que el ser humano desarrolle métodos y prácticas maliciosas donde se utiliza la informática como medio u objeto para desarrollar acciones y posibles conductas que atentan contra el bien jurídico que es el daño económico que sufre la persona (Abogados Ecuador, 2019, p. 1). Generalmente, como resultado final son los ciudadanos los afectados en su patrimonio, privacidad e intimidad; a estas prácticas que lesionan el patrimonio de una persona mediante la utilización tecnológica se las denomina globalmente como delitos informáticos.

Los delitos informáticos se pueden definir como cualquier actividad delictiva en la que se utilizan como herramienta los computadores o redes, o éstos son las víctimas, o bien el medio desde donde se efectúa dicha actividad delictiva; se refieren a los actos dirigidos contra la confidencialidad, integridad y la disponibilidad de los datos y sistemas informáticos (APESPOL, 2015). De acuerdo a la definición señalada, los delitos informáticos son aquellos en los cuales se lesiona la confidencialidad de datos de sistemas informáticos con un fin económico.

Para María de Luz Lima, citada por Computer Forensic (2019), el delito electrónico en un sentido amplio es:

> Cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal, en el que las computadoras, sus técnicas y funciones desempeñan un papel esencial en el hecho punible (Computer Forensic, 2019, p. 1).

De igual manera, se define delitos informáticos como aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático (Huilcapi, 2011, p. 1). De acuerdo al autor, para que se constituya delito debe existir un sujeto activo y uno pasivo los cuales se caracterizan por:

- Sujeto Activo: Se refiere a personas que cometen el delito teniendo amplio conocimiento técnico de informática, con un nivel de instrucción alto que le permite manipular la información a través de los sistemas de computación.
- Sujeto Pasivo: Se refiere a individuos, instituciones de crédito, gobiernos, o entidades que usan sistemas automatizados de información (Huilcapi, 2011).

El delito informático ha sido tema de distintos análisis y se podría asegurar que a medida que avanza la tecnología, los temas continuarán surgiendo incluyendo nuevas alternativas de solución ante el problema delictivo informático. Nidia Calleara, citado por Huilcapi, define al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas" (Huilcapi, 2011). De este mismo modo, Carlos Sarzana, referido por Huilcapi (2011), los crímenes por computadora comprenden cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, como mero símbolo.

Por su parte, Meléndez (2018) comparte como concepto de delito informático:

> aquellos que afectan la información y al dato como bienes jurídicos protegidos, es decir, la información que un usuario tiene dentro de una cuenta de correo electrónico y el dato protegido de una cuenta bancaria, los datos que se contienen en un celular, los datos que se contienen en el sector público o privado, la identidad de ciertas personas que están protegidas por el Estado y la ley (p. 1).

Según información suministrada por la Fiscalía General del Estado ecuatoriano, a través del diario El Telégrafo (2016), en el país se registraron 530 delitos informáticos en los primeros cinco meses del año 2016, y durante el mismo período del año 2015 se presentaron 635 denuncias. En el Guayas hubo 18 casos; Pichincha, 145; Manabí, 24; El Oro, 22; en el resto de provincias se registró una cantidad menor. La mayoría de denuncias, puntualmente 368 casos, corresponden al delito de apropiación fraudulenta por medios electrónicos. De acuerdo a la información presentada por el diario, un 85%

de los delitos informáticos se originan porque los usuarios desconocen la manera de manejar correctamente los medios informáticos (El Telégrafo, 2016).

En este mismo orden de ideas, vale hacer referencia a lo que indica el Convenio de Ciberdelincuencia del Consejo de Europa, citado por Computer Forensic (2019) donde define delitos informáticos como: "los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos" (p. 1).

Ahora bien, parte de lo que es necesario indagar es de qué manera se socializan las penas o castigos por delitos informáticos en el país, es decir, muy poco se conoce al respecto; sin restar importancia al hecho de que desconocer la ley no exime de su cumplimiento, las personas deben estar enteradas de las sanciones que acarrean hacer un uso indebido de los medios informáticos, ya sea por uso personal o por formar parte de una institución o empresa, donde se manejen datos reservados. Sin embargo, en la realidad no existe un conocimiento pleno de lo que tipifica el COIP sobre delitos informáticos, unido al poco interés en conocer al respecto.

De esta manera, a través de la presente investigación se busca analizar todo lo concerniente a los delitos informáticos, considerando lo tipificado en el COIP en concordancia con lo que indica la Constitución de la República del Ecuador, la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas y otras normativas relacionadas, con la finalidad de conocer los delitos informáticos que se han dado en el Ecuador en mayor proporción, y las posibles soluciones a problemas que se detecten en el proceso.

1.2.Campo de estudio: Penalización del Delitos Informáticos según el COIP

En cuanto al campo de estudio del presente análisis, se toma en consideración lo dispuesto en la legislación ecuatoriana a través de la Constitución de la República, el

Código Orgánico Integral Penal, la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas y otras leyes y normativas relacionadas. Se hace necesario señalar que los delitos informáticos están tipificados en distintos artículos del COIP, puntualmente en los artículos 178, 179, 181, 190, 229, 230, 231, 232, 233, y 234 hacen referencia a este tipo de delitos, el cual puede darse en distintas formas, pero que de manera común y como resultado final, se vulnera la privacidad de las personas, instituciones o empresas, que manejan datos confidenciales o solo de importancia para el propietario de la información.

Es importante señalar que, si bien el delito informático es tipificado como un delito penal, es interesante conocer qué acciones toma la misma legislación ecuatoriana hacia las personas o instituciones que forman o entrenan a quienes cometen este tipo de delitos, abriendo paso al hecho de que quienes generalmente cometen este tipo de delitos, suelen estar altamente capacitados en el manejo de las redes y datos informáticos. Por otro lado, es importante conocer de qué manera el Estado enseña a los ciudadanos resguardar la información personal y la protección de los datos, en virtud del papel que desempeña el Estado como garante de la seguridad y protección de todos los ciudadanos de un país, por lo que deben existir mecanismos que alerten a las personas sobre posibles fraudes o actos delictivos a través de los medios informáticos.

En este orden de ideas, se presenta a continuación un resumen de los artículos que plantea el COIP que hacen referencia al delito informático y al acceso ilegal a datos de personas o empresas:

Tabla 1 Delitos Informáticos según el COIP

Artículo	Hecho	Pena
Art. 178. Violación a la intimidad	La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales,	Pena privativa de libertad de uno a tres años.

	información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio.	
Art. 179.- Revelación de secreto	La persona que teniendo conocimiento por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño a otra persona y lo revele.	Pena privativa de libertad de seis meses a un año
Art. 181.- Violación de propiedad privada .	La persona que, con engaños o de manera clandestina, ingrese o se mantenga en morada, casa, negocio, dependencia o recinto habitado por otra, en contra de la voluntad expresa o presunta de quien tenga derecho a excluirla.	Pena privativa de libertad de seis meses a un año
Art. 190.- Apropiación fraudulenta por medios electrónicos	La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones.	Pena privativa de libertad de uno a tres años
Art. 229.- Revelación ilegal de base de datos	La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas.	Pena privativa de libertad de uno a tres años.
Art. 230.- Interceptación ilegal de datos	Intercepción ilegal de datos señalados en el COIP	Pena privativa de libertad de tres a cinco años
Art. 231.- Transferencia electrónica de activo patrimonial	La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero.	Pena privativa de libertad de tres a cinco años.

Art. 232.- Ataque a la integridad de sistemas informáticos	La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen.	Pena privativa de libertad de tres a cinco años.
Art. 233.- Delitos contra la información pública reservada legalmente	La persona que destruya o inutilice información clasificada de conformidad con la Ley	Pena privativa de libertad de cinco a siete años
Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos.	Pena privativa de la libertad de tres a cinco años.

Fuente: (Código Orgánico Integral Penal, 2018)

1.3. Referentes empíricos del Campo de estudio

Dentro de los referentes empíricos que tienen pertinencia con la presente investigación hay que hacer referencia a Ycaza (2019) en su investigación titulada "Tratamiento Jurídico de los delitos informáticos en el Ecuador" para la Universidad Católica Santiago de Guayaquil, efectuó un estudio acerca de los delitos informáticos establecidos en el Código Orgánico Integral Penal, donde estableció las características de cada uno de ellos.

Dicha investigación arrojo como resultado de la misma, que producto de la evolución de la tecnología y de internet, han surgido nuevos delitos de carácter informáticos, los cuales son difíciles de detectar ya que los mismos operan en la clandestinidad, operan mediante software que son creados para tal fin, y que mediante correos electrónicos que son enviados a la víctima pueden sustraer información personal de cuentas bancarias y claves de acceso que se encuentran en la misma.

Por otra parte, Vivanco (2016) en su investigación que lleva por nombre "Reforma al Código Orgánico Integral Penal , de los delitos informáticos" para la Universidad de Loja, hizo referencia al aumento en el índice de este tipo de delitos en la actualidad, así como también estableció que existen nuevos delitos como el de apropiación fraudulenta de por medios electrónicos, la trasferencia electrónica de activo patrimonial y el acceso no consentido a un sistema informático, dicha investigación arrojo dentro de sus resultados, que se hace necesaria una modificación del Código Orgánico Integral penal ya que existen nuevas formas delictivas que no se encuentran en él reguladas, por lo que se hace necesario efectuar una modificación de este cuerpo normativo a los efectos de incluirlas como nuevos tipos penales con la finalidad que dentro de él se puedan incluir nuevas formas delictivas.

1.4.Pregunta de Investigación

¿Las penas bajas contempladas en el Código Orgánico Integral Penal influyen sobre la disminución de los delitos informáticos?

1.5.Premisa

De acuerdo a lo que indica la Constitución de la República y el Código Orgánico Integral Penal, los delitos acarrean consecuencias penales incluyendo la privación de libertad, sin embargo, es importante conocer que incidencia tiene lo establecido en la legislación ecuatoriana, sobre la minimización o efectividad en los casos penales relacionados con delitos informáticos.

1.6.Objetivos de la investigación

Objetivo General

- Analizar las penas de los delitos informáticos contempladas en el COIP

Objetivos Específicos:

- Realizar estudios de los delitos informáticos más comunes en la actualidad y sus sanciones.
- Revisar las normativas jurídicas aplicadas en los casos de delitos informáticos.
- Establecer propuestas de solución que eviten la impunidad de estos actos ilícitos como son los delitos informáticos.

1.7.Métodos teóricos

Según explica Hernández y otros (2018), el método teórico se aplica durante el proceso de explicación, interpretación y comprensión del tema estudiado, cumpliendo una función epistemológica. El método teórico permite la interpretación conceptual de los datos empíricos encontrados, así como también contribuye a revelar las relaciones que existen entre el objeto de investigación y aquellos elementos que pueden no ser observables o reflejarse sensorialmente. En este sentido, los métodos teóricos agregan valor a la investigación sirviendo de apoyo en el discernimiento y análisis requerido en el tema estudiado.

De igual manera, se realiza un análisis sintético, a través del cual se efectúa la descomposición del tema estudiado, en los elementos principales que lo conforman para determinar sus particularidades y mediante el análisis y la síntesis descubrir relaciones y características generales (Hernández, y otros, 2018)

Por otra parte, mediante el método histórico lógico, se puede realizar el análisis del presente tema y establecer los antecedentes del fenómeno en el devenir histórico al mismo tiempo se puede delimitar las leyes relacionadas al tema de estudio y conocer el desarrollo del problema estudiado (Hernández, y otros, 2018).

1.8.Métodos empíricos

Tabla 2 Método Empírico de Investigación

Categoría	Dimensiones	Instrumentos	Unidades de Análisis
Delitos Informáticos	Tipos de Delitos Informáticos Penalización Sanciones	Análisis documental	Código Orgánico Integral Penal Artículos 178, 179, 181, 190, 229, 230, 231, 232, 233, 234 Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas Artículos 21 y 22

Elaboración propia.

1.9.Novedad científica

Los delitos informáticos pueden ocurrir en cualquier momento, en virtud de la constante exposición a la manipulación de datos personales que circulan a través de las redes sociales y no sociales; la forma en que el Estado utilice los mecanismos para enfrentar este tipo de delitos, surtirá efecto en su minimización, sin embargo, es necesario realizar una revisión a la normativa establecida por la legislación ecuatoriana, con el fin de precisar alternativas de solución a delitos informáticos que cada vez suman más víctimas, muchas de las cuales no conocen cuál es el proceder legal ante situaciones de

vulneración de datos personales; del mismo modo, es importante indagar si los mecanismos hasta ahora utilizados son efectivos y si la justicia ecuatoriana ha dado respuesta legal oportuna en los casos denunciados.

2. Marco Teórico

2.1. Delitos informáticos

Los actos ilícitos que se realizan con la ayuda de las Tecnologías de la Información y Comunicación (TIC), se denominan delitos cibernéticos a los delitos informáticos como cualquier acto intencional o culpable, con o sin intención, que perjudica directa o indirectamente a la víctima mediante el uso de dispositivos que se utilizan en actividades informáticas (Enríquez & Alvarado, 2015, p. 9).

Las personas que violan la seguridad de los protocolos de comunicación y que tienen acceso no autorizado a un sistema de información a través de un usuario remoto se conocen como intrusos informáticos. Es importante tener en cuenta que las personas que cometen estos delitos están familiarizadas con las tecnologías y sistemas informáticos, así como con el comportamiento humano y organizacional (Brunet, 2018).

De acuerdo a lo manifestado por Enríquez & Alvarado, Cocero, Garcia, Jorda, & Lopez (2017) han manifestado: "Se entiende también como delito informático, al comportamiento antisocial que altera la calma de las personas o interfiere con el buen funcionamiento de una empresa pública o privada, que utiliza herramientas informáticas para alterar, eliminar o espiar información confidencial o violar derechos" (p. 22). Cada elemento de la computadora, ya sea hardware o software, debe ser sancionado de acuerdo con la ley aplicable.

2.2.Importancia de la informática en la sociedad de la información

La informática es una ciencia que se encarga del procesamiento automático de la información con el fin que una persona pueda tomar las decisiones adecuadas. Por lo tanto, la informática es la ciencia responsable de solicitar, organizar, almacenar y proteger la información (Cocero, Garcia, Jorda, & Lopez, 2017).

Por otra parte en relación con la importancia de la informática Baca (2016) manifiesta: "Así mismo, la importancia de la informática ha significado que se relaciona con otras áreas de conocimiento, como medicina, arquitectura, arqueología, educación, entre otras. El crecimiento de la informática hoy es muy notable" (p. 32). El uso de computadoras también se ha convertido en una herramienta indispensable para la sociedad actual, que, junto con las ventajas de Internet, hace que las personas sean usuarios de tecnologías de información y comunicación (TIC).

Como resultado, esta ciencia ha cruzado barreras y revolucionado dramáticamente la forma en que se hacen las cosas y ha cambiado radicalmente la forma en que las personas viven, trabajan y piensan. Como consecuencia, la evolución de la informática ha permitido la implementación y el uso de sistemas de información para realizar tareas que anteriormente se realizaban manualmente. Por esta razón, el trabajo, los negocios, la administración y el ocio son algunas de las facetas que están cambiando a pasos agigantados, creando una sociedad cada vez más global que se caracteriza por el uso y acceso a la información y la bautiza como: la sociedad de la información (Viega, 2020).

Por lo tanto, las computadoras e internet juegan un papel muy importante en la sociedad de la información, ya que, permiten la transferencia e intercambio de información sincrónica, asincrónica y streaming, y el diseño de nuevos escenarios socioeconómicos, por ejemplo, a través del comercio electrónico, bancos virtuales y gestión electrónica de recursos corporativos, computación en la nube, educación en línea, videoconferencia y teletrabajo. Este es el trabajo que se realiza de forma remota utilizando tecnologías de información y comunicación (Clotet, 2006).

Como resultado, de lo manifestado anteriormente por Cloted hay que señalar que (Acurio, 2015) estableció lo siguiente:

por los avances tecnológicos de la información y el impacto de internet en la sociedad han dado lugar a ciertos comportamientos ilegales que han desencadenado una serie de comportamientos que comprometen la seguridad de la información digital. Este conjunto de comportamientos se ha definido ampliamente como: delitos informáticos, criminalidad mediante computadoras, delincuencia informática y criminalidad informática. Por esta razón, la necesidad de mitigar y castigar este delito cibernético conduce a la unificación de dos áreas de estudio, como la Tecnología Informática y el Jurídico (p. 42).

2.3. Tipos de delitos informáticos

Hay varias formas de cometer cibercrimen. Los mismos se dividieron en cuatro categorías importantes:

1) Los fraudes Informáticos;
2) El sabotaje Informático;
3) El espionaje informático; y
4) Los accesos no autorizados a sistemas de información.

Es importante afirmar que el orden en que se describen no indica el alcance del peligro que representan (Acurio, 2015). En la categoría de fraude informático, los siguientes métodos de delitos penales son notables:

a) Los datos incorrectos o engañosos son la introducción para lograr movimientos artificiales en las transacciones de una empresa.
b) La manipulación del programa o caballo de Troya consiste en ocultar un programa informático en una computadora extranjera para llevar a cabo acciones no autorizadas.
c) La falsificación informática, tiene como objetivo falsificar documentos comerciales con una fotocopiadora.

d) Pishing, tiene como objetivo robar la identidad de la víctima mediante el uso de trucos para obtener información personal, abrir cuentas bancarias, solicitar crédito y tarjetas de crédito en nombre de la víctima.

La segunda agrupación es el sabotaje informático, entre los métodos de mayor incidencia están:

a) Bombas Lógicas, consiste en una especie de bomba de tiempo que daña el sistema informático.
a) Gusanos, es un tipo de virus que se infiltra en programas legítimos de procesamiento de datos con el objetivo de cambiar o destruir información.
b) Los virus informáticos y malware, son programas maliciosos que tienden a reproducirse y extenderse dentro del sistema. (Ferro, 2020)
c) Ciberterrorismo o terrorismo informático, está tomando medidas que desestabilizan a un país o ejercen presión sobre un gobierno.
d) Ataques de denegación de servicio, apuntan a la computadora objetivo que consume recursos de memoria hasta que ocurre una falla del sistema que tiene consecuencias catastróficas.

El tercer grupo es el espionaje informático y el robo o hurto de software. En esta categoría están los siguientes métodos:

a) Fuga de datos, consiste en la divulgación o publicación de información confidencial de una empresa.
b) Reproducción no autorizada de programas informáticos de protección legal, este delito tiene que ver con los piratas informáticos, es decir, el uso ilegal de software privativo.

La cuarta agrupación es el acceso no autorizado a servicios informáticos, los principales métodos son:

a) Las puertas falsas, tiene como objetivo verificar procesos complejos mediante interrupciones para garantizar que sean correctos.
b) La llave maestra, es un programa informático que puede usar para abrir cualquier archivo para este propósito.

2.4. Penalización de los delitos informáticos

En Ecuador, el delito informático que utiliza el Código Penal Orgánico Integral (COIP) (2014) en la tercera sección, desde la sección 178 hasta la sección 234 del COIP, se castiga por intentar, entre otras cosas, obtener información confidencial, la divulgación ilegal de datos, pérdidas financieras y acceso no autorizado, entre otros.

Los ataques informáticos a las agencias gubernamentales se castigan con penas de prisión. Vale la pena señalar que las víctimas de un ciberataque, tienen derechos de reclamar mediante una denuncia oficial ante las autoridades pertinentes (Philco & Rosero, 2014).

Cabe destacar que el artículo 190 del COIP señala, cualquier persona que utilice fraudulentamente un sistema informático o una red electrónica y de telecomunicaciones para facilitar la apropiación de la propiedad de otra persona, o que intente vender bienes, activos o derechos sin su consentimiento en detrimento de esa persona o un tercero alterando, manipulando o modificando el funcionamiento de las redes electrónicas, programas, sistemas informáticos, terminales telemáticos y de telecomunicaciones se castiga con una pena privativa de libertad de uno a tres años (Asamblea Nacional, 2014).

Esto también incluye descifrar claves secretas o cifradas, cambiar la información de inicio de sesión en programas de computadora, clonar páginas electrónicas o tarjetas de crédito, débito, pago o similares. Estas violaciones se castigan con una pena de prisión de tres a cinco años.

2.5. Delitos Informáticos en Latinoamérica.

Según Temperini (2013) ha manifestado lo siguiente:

> La actividad criminal en las computadoras está aumentando en todo el mundo, incluso en América Latina. Según una de las encuestas más relevantes sobre cibercrimen en el mundo, que involucró a más de 13,000 adultos en 24 países, el costo directo del cibercrimen para los consumidores de todo el mundo en 2012 fue de $ 110,000 mil millones en doce meses. El mismo estudio muestra que 18 adultos por segundo son víctimas de delitos informáticos, lo que lleva a más de un millón y medio de víctimas de delitos informáticos en todo el mundo todos los días (p. 33).

Concluyó que los países latinoamericanos presentan una falta de homogeneización en el ámbito sustantivo de la normativa penal aplicable a los delitos informáticos, se destaca la necesidad de mejorar los niveles de armonización y actualización legislativa en la materia, a fin de mitigar la existencia de paraísos legales en la región que favorezcan la ciberdelincuencia (Temperini, 2013).

2.6.Legislación en otros Países

Estados Unidos

Se considera importante mencionar la adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030) que modificó al Acta de Fraude y Abuso Computacional de 1986. Para eliminar los argumentos hipertónicos sobre qué es un virus, un gusano, un caballo de Troya y qué no lo es, y cómo se diferencian de los virus, la nueva ley prohíbe la transmisión de un programa, información, código o comandos que le causen daño a computadoras, en el sistema, en redes, información, datos o programas.

En este sentido Martinez (2017) señaló lo siguiente: “Llama la atención que el Acta de 1994 deja en claro que el creador de un virus no puede esconderse detrás de él, que no

sabía que su acto dañaría a alguien, o que solo quería enviar un mensaje" (p. 42). Según los legisladores estadounidenses, la nueva ley representa un enfoque más responsable ante el creciente problema de los virus informáticos, que pretende tener en cuenta la nueva era de los ataques tecnológicos en los sistemas informáticos en el futuro en cualquier forma que se hagan.

Al diferenciar los niveles de delincuencia, la nueva ley crea una visión de lo que constituye un delito. En California, la Ley de Protección de Datos se aprobó en 1992, que incluye el delito cibernético, pero en menor medida que los delitos relacionados con la protección de datos que son el propósito principal de esta ley.

Chile

En junio de 1993, la Ley N ° 19.223 sobre cibercrimen entró en vigencia en Chile. La Ley 19.223 tiene como objetivo proteger un nuevo bien legal, como: "La calidad, pureza y adecuación de la información contenida en un sistema automatizado para su manejo y los productos en los que opera". El articulo Nº 1 de la La Ley 19.223 (1993) establece lo siguiente:

> Cualquier persona que destruya un sistema de procesamiento de información o sus partes o componentes o los haga inútiles o malintencionados o que impida, obstaculice o modifique su operación es, en promedio, menos arrestado. Si, como resultado de estos comportamientos, los datos contenidos en el sistema se ven afectados, la penalización especificada en el párrafo anterior se aplica al máximo" (p. 1).

España

El tratamiento de este asunto se trata en el nuevo Código Penal de 1995, aprobado por la Ley Orgánica 10/1995 de 23 de noviembre, y publicado el 24 de noviembre de 1995 en el BOE No. 281. Este código penal contenía la realidad aritmética mundial limitada a

los tipos criminales clásicos, no solo la regulación del delito cibernético con un mejor conocimiento de la doctrina y otras leyes (Nava, 2017).

A pesar de las críticas a esta normativa, su intento de lograr la armonía legal entre los delincuentes clásicos y el fenómeno informático es innegable, lo que requiere mucho esfuerzo, no tanto la solución que tienen. Se han adoptado instrumentos legales que se limitan a abordar el problema a través de leyes específicas que tienen en cuenta el fenómeno informático aislado del resto de la legislación y se alejan de las buenas prácticas legales, como en el caso de Chile.

2.7. Delitos informáticos en el Ecuador y su realidad procesal en el Ecuador

El delito cibernético se comete en Ecuador como en todos los países, y en 2013 aumentó el número de denuncias cibernéticas tal como lo evidencia un informe del año 2014 de la Fiscalía General del Estado. Los ciudadanos denunciaron incidentes de ataques ilegales a la interceptación de integridad de la información, sistemas de uso indebido de dispositivos, fraude cibernético, fraude informático, pornografía infantil y delitos contra la propiedad intelectual. Desde la entrada en vigencia del Código Penal Orgánico Integral el 10 de agosto hasta el 31 de mayo de 2015, se han presentado 626 quejas sobre delitos informáticos ante el Departamento de Política Criminal de la Oficina del Fiscal General (Lopez, 2017).

Según el entonces Fiscal General, en un boletín publicado el 13 de junio de 2015, los delitos más comunes son: transferencia ilegal de dinero, divulgación fraudulenta de datos personales, interceptación ilegal de datos, acoso sexual. El Departamento de Criminalística se creó como un departamento criminal y, en particular, sexual, que también interfiere con la evidencia basada en datos de la computadora (Fiscalia General Del Estado, 2015).

Por ejemplo, COIP fue aprobado el 10 de agosto de 2014, y se sabe que el Fiscal General solo registró 626 denuncias sobre delitos informáticos hasta mayo de 2015. En los primeros cinco meses de 2016, se registraron 530 delitos cibernéticos con la FGE, una disminución significativa. Aunque se sabe que el 80% de los delitos cibernéticos no se denuncian, existe lo que podemos llamar la falta de una cultura de denuncias (Fiscalia General Del Estado, 2015).

De acuerdo a lo anterior el autor Chiluiza (2017) señala que: "a pesar de la existencia de regulaciones para castigar los delitos informáticos, existe una falta de comprensión de la ley sobre delitos relacionados con herramientas electrónicas e informáticas" (p. 3). Las nuevas reglas son inútiles y creen que una de las principales desventajas del delito cibernético es pasar la prueba debido a la falta de conocimiento y herramientas para transferirlo al proceso.

Todos los delitos informáticos cometidos en diferentes partes del mundo deben clasificarse por consenso para que puedan ser tratados internacionalmente con la participación de la mayoría de los Estados situación que permita tomar medidas efectivas, es decir, el desarrollo de un sistema legal internacional que garantice la correcta aplicación de las regulaciones existentes en cada país.

2.8 Investigación criminal tecnológica de los delitos económicos cometidos por medio de las tic

Las tecnologías de la información (TIC) en la actualidad juegan un papel fundamental en el desarrollo de cualquier país, a tal punto que si un Estado no hace uso de ellas se encontrará en desventaja a los demás, ya que, ellas brindan una gran cantidad de plataformas que permiten efectuar trámites y actividades que anteriormente, no era posible realizar y si se efectuaba tardaba mucho más tiempo, por tal razón en la actualidad es uno de los principales activos que puede poseer un país (Berenger, 2015).

Continuando, las TIC han hecho que se cambien los parámetros para efectuar actividades comerciales, cuando con anterioridad era preciso la presencia física de una persona para efectuar una determinada negociación, ahora en la era digital ya no es necesario, existen las firmas electrónicas, las trasferencias, los pagos virtuales y una gran cantidad de variables que han hecho que las TIC se conviertan en un aliado de la sociedad actual (Velasco, 2017).

Ahora bien, así como se han señalado los beneficios que prestan las TIC también hay que señalar que muchas personas se han valido de estas plataformas con la finalidad de cometer delitos en contra de terceros y en beneficio propio, se ha observado que, así como han evolucionado las TIC también han evolucionado las formas de cometer delitos mediante ellas. Se observa de manera habitual como son enviados gusanos o a los correos electrónicos de distintas personas con la finalidad de obtener información confidencial de sus tarjetas de crédito, así como también de sus cuentas bancarias y poder de esta manera efectuar operaciones bancarias con la finalidad de sustraer dinero de la cuenta bancaria del afectado o efectuar compras lesionando de igual manera el patrimonio de la víctima (García , 2016).

Los delitos informáticos en su alta mayoría, son delitos de índole económico que buscan lesionar el patrimonio de la víctima, logrando de esta manera un beneficio para el delincuente, en la actualidad se venden en los mercados negros kits de piching, en los cuales se les brinda una asesoría al comprador, con la finalidad que pueda robar información bien sea financiera o de interés a terceras personas. Con este tipo de kits, el comprador puede tener una herramienta para robar información de una persona determinada, el precio promedio de este tipo de kits en la web dark, es de aproximadamente $50, con los que se le asegura al comprador que podrá obtener información electrónica de un tercero. Ejemplos de estos delitos se pueden citar

corrupción, fraude corporativo, fraude público, evasión de impuestos, contrabando de bienes, manipulación de acciones, falsificación de monedas (Ruiz & González, 2015).

Las personas que de manera habitual cometen este tipo de delitos roban grandes cantidades dinero y para ello se valen de las TIC, que les brindan una plataforma rápida para efectuar cada uno de sus delitos. La mayoría de este tipo de delitos se producen por el desconocimiento y exceso de confianza de las víctimas, quienes desconocen este tipo de procedimientos y no tomar las precauciones necesarias caen en este tipo de delitos. Las víctimas de este tipo de fraudes en la mayoría de los casos desconocen el hecho de que han sido engañadas, porque inclusive en muchas oportunidades los delincuentes son personas que conocen muy bien a la víctima. Muchas veces este tipo de delitos no son denunciados porque las victimas desconocen a que autoridades acudir, o en otras oportunidades porque el delincuente siempre le promete a la víctima que pronto le devolverá su dinero y como el interés de la víctima es ese, o no lo denuncia, o tarda mucho tiempo en hacerlo (Gomez, 2016).

Cuando este tipo de crímenes se vuelve global, no solo afecta a un grupo seleccionado de instituciones financieras o áreas regionales, más bien afecta las redes financieras internacionales y las economías a nivel nacional. El rápido crecimiento de la tecnología, especialmente el crecimiento ilimitado que posee internet, ha cambiado la manera como operaban los delincuentes tradicionales, cuando en el siglo pasado robaban un banco de manera presencial o mediante distintos programas lo pueden hacer sin necesidad de que acuda una pandilla a la sede física del mismo (Palomino, 2016).

El avance de la tecnología en este sentido, ha traído como consecuencia que sea más difícil detener a este tipo de delincuentes, los cuales cada vez se logran ocultar en el I.P por cuanto se desconoce su identidad y siempre operan desde distintas pc ubicadas en sitios diferentes, perjudicando a una gran cantidad de personas a nivel mundial regional

y local. Se evidencia, como el crimen ha mutado en muchas circunstancias los delincuentes han abandonado las calles para refugiarse en centros tecnológicos, anteriormente existían las guaridas de delincuentes, ahora se han formado los cibercentros de la delincuencia organizada, en los cuales mediante herramientas que brinda la web se perpetran delitos en contra de terceras personas (Cruz, 2017).

Los ciber delincuentes se valen de herramientas como el correo electrónico, para infiltrarse en el computador de sus víctimas y obtener datos personales de la víctima y luego estafarlos o extorsionarlos, los servicios de anonimato en línea se prestan para este tipo de conductas delictuosas, ahora bien todo esto constituye un desafío para cada Estado porque mientras exista internet, también será posible la comisión de este tipo de delitos, ahora bien el remedio no es eliminar el internet, que del Estado cree mecanismos de seguridad para evitar este tipo de delitos y que si bien es cierto el crimen ha evolucionado se hace necesario que la justicia y los órganos de persecución penal, también evolucionen y posean las técnicas y maneras para poder detener el avance de este tipo de delitos.

En este tipo de delitos, es bastante dificultoso determinar quién ha sido el autor del hecho punible, ya que cuando se ubica en oportunidades donde está localizado el computador del cual se ha efectuado el hecho punible, surge la incertidumbre de cuantas personas manejan ese PC, si es un lugar público como por ejemplo un laboratorio de internet de carácter gubernamental, o por el contrario es una oficina privada (Aboso, 2006).

Este tipo de situaciones hacen en muchas oportunidades cuesta arriba la labor de los cuerpos de investigación penal, por lo que se hace necesario mayor investigación por parte de los cuerpos de seguridad del Estado a los efectos de poder capturar y sancionar a estas bandas delictivas, de igual forma es importante instar a la población a utilizar

software de seguridad en sus computadores, alertarlos a no abrir correos electrónicos de destinatarios desconocidos así como también a denunciar estos delitos que en muchas oportunidades quedan impunes por la falta de denuncia de sus víctimas (Coderata, 2016).

La situación descrita anteriormente es bastante preocupante ya que se observa como la ciberdelincuencia, ha aventajado a la justicia por un trecho bastante amplio al punto que en oportunidades es imposible detener a los responsables de este tipo de delitos, porque técnicamente es bastante complejo determinar quién fue el autor del hecho punible por lo que se recomienda a los Estados, instar de manera continua a sus cuerpos de seguridad a mantenerse al día con las nuevas tecnologías y el manejo de ellas.

2.9 Prevención de delitos informáticos por medios de las TIC.

Producto del aumento de la ciencia y la tecnología el uso de las TIC a nivel mundial regional y local ha aumentado de una manera vertiginosa, y paralelamente a este aumento también lo ha hecho la delincuencia informática, razón por la cual resulta pertinente el conocimiento de este tipo de delitos ya que si bien es cierto su aparición no es algo nuevo ni novedoso, es bastante difícil su sanción penal de hecho, si se observa las sanciones a este tipo de delitos son bastante bajas y no es porque no se cometan sino que es bastante complejo determinar el autor del hecho punible (Ricardo , 2017).

En estos delitos informáticos, el más común es el financiero que consiste en la sustracción de sumas de dinero de las cuentas de las víctimas, quienes acuden muchas veces a instituciones financieras a realizar los respectivos reclamos y no reciben una respuesta satisfactoria al problema causado. Este tipo de delitos son bastantes complejos desde el punto de vista procesal y por tal razón muy pocos culminan con una sentencia condenatoria, ya que a la representación fiscal se le hace muy difícil ubicar a un delincuente que no deja ningún tipo de evidencias. (Romero, 2017).

Por tal razón se hace necesario, la utilización de nuevas tecnologías de información ya que, con el paso del tiempo, se posee un mayor avance en lo que respecta a los certificados de búsqueda, para de esta manera poder rastrear a este tipo de delincuentes y evitar las pérdidas millonarias que sufren las personas a nivel global por este tipo de delitos. En tal sentido se hace necesario la adquisición de software avanzado y medidas preventivas para proteger a las víctimas, en este caso las instituciones bancarias deben mejorar sus sistemas de seguridad con la finalidad de proteger al usuario (Rodríguez, 2015).

2.10 Problemática para la persecución los delitos informáticos

Las capacidades de las instituciones de seguridad del Estado están formadas por un conjunto de variables como lo son las capacidades de carácter estratégicas y operativas, las aptitudes técnicas que poseen los integrantes de los cuerpos de seguridad del Estado, así como también contar con un número apropiado de oficiales que ayuden en esta labor. Otro elemento de vital importancia, se encuentra formado por el grado de especialización que poseen estos funcionarios, ya que este tipo de delitos por ser cometidos por personas de un alto nivel de conocimientos en la materia informática, se hace necesario combatirlo con cuerpos de seguridad que tengan un alto nivel de conocimientos en la materia.

Continuando, con lo anterior se hace necesario que para determinados delitos existan peritos o una unidad especializada que posea esta competencia, ya que, los funcionarios ordinarios no tienen el entendimientos de cómo se materializa este tipo de delitos, que implican programación de software, como combatir o rechazar un malware y otros aspectos que solo manejan funcionarios especializados, ya que, este tipo de delitos no deja los rastros o huellas de un delito común como un robo, un asesinato o una violación.

2.11. Especialización organizacional

En este sentido se hace necesario que para combatir este tipo de delitos existan peritos en el área cibernética, que sirvan como cuerpos auxiliares de la investigación penal ya

que si bien es cierto no todos los jueces, fiscales del Ministerio Público secretarios y asistentes de un tribunal, tienen los conocimientos necesarios en este tipo de delitos ellos se pueden valer de este tipo de unidades, que en el cumplimiento de sus obligaciones prestan los conocimientos necesarios para que las autoridades competentes puedan sancionar a este tipo de delitos.

Por otra parte también vale la pena resaltar que para la detección de este tipo de delitos, va a depender mucho del nivel de desarrollo donde se cometa el hecho punible, ya que, se ha evidenciado que la mayoría de los países europeos han puesto en prácticas legislaciones continentales para armonizar los sistemas legales en cada uno de esos Estados, en tal sentido en la mayoría de las naciones europeas el Ministerio Público cuenta con unidades especializadas en materia de delitos cibernéticos, ahora bien esta realidad no es la misma en Latinoamérica donde solo pocos países avanzados tienen este tipo de unidades para combatir los delitos cibernéticos .

Se hace necesario que la Fiscalía cuente con este tipo de unidades, y que las mismas sean dotadas de software y el hardware necesario y que, así como los delincuentes tienen su ciberguaridas de donde operan sus mafias los fiscales cuenten con estas unidades, esta es una opción que en el continente europeo ha dado resultados lo cual debería implementarse en Latinoamérica donde este tipo de delitos ha llegado a niveles insostenibles(Rodríguez, 2015).

2.12. Delitos informáticos en el Código Orgánico Integral Penal (2018)

En este sentido el artículo 190 del Código Orgánico Integral Penal (2018) establece lo siguiente:

> Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure

> la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes (p. 68).

En este sentido el artículo 178 del Código Orgánico Integral Penal (2018) establece lo siguiente:

> Violación a la intimidad.- La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años. No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley (p. 61).

De igual forma En este sentido el artículo 229 del Código Orgánico Integral Penal (2018) establece lo siguiente:

> Revelación ilegal de base de datos.- La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años (p. 79).

De igual forma En este sentido el artículo 231 del Código Orgánico Integral Penal (2018) establece lo siguiente:

> Transferencia electrónica de activo patrimonial.- La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona.

3. Metodología

3.1. Metodología de la investigación

La metodología que fue empleada en el presente estudio, está constituida por métodos y técnicas que evidencian la manera como fue realizado el presente estudio, la presente investigación, con el fin de poder obtener el cumplimiento del objetivo general y los objetivos específicos que fueron planteados al comienzo de la presente investigación. La metodología de la investigación está formada por todas aquellas situaciones que se obtienen en la experiencia de los seres humanos, con el vivir de forma cotidiana los distintos elementos a través del tiempo, fundamentales para poder obtener resultados en los cuales se sustente la investigación (Villalón, 2015).

3.2. Diseño de la investigación

El diseño de la presente investigación, estuvo basado en un análisis de carácter bibliográfico y documental que tuvo como centro el paradigma interpretativo, orientado al análisis de textos que tienen vinculación con el análisis de los delitos informáticos y su penalización según las leyes ecuatorianas tipificadas en el Código Orgánico Integral Penal. De esta manera fue planteado el presente estudio bajo un nivel descriptivo, que para desarrollarlo fue necesaria la utilización de los métodos deductivo, inductivo, analítico y sintético, lo que facilitó la formación de las opiniones y conclusiones.

3.3. Métodos de investigación

Los métodos de investigación, son aquellos que establecen y señalan la vía que debe seguir el investigador con la finalidad de lograr los objetivos que se ha planteado en el inicio de la investigación, por tal motivo, él debe apoyarse en los conocimientos del método científico que es aquel que toma las técnicas empleadas como la observación, demostración e interpretación para determinar el comportamiento de un fenómeno de estudio (Pulido, 2015).

Estos pasos son esenciales para el logro de cualquier tipo de investigación y que de esta manera se pueda lograr el procesamiento de la información que se necesita para obtener un análisis acerca de las distintas teorías relativas al tema de estudio. Se admite que los métodos son fundamentales para poder ir avanzando en cada fase o etapa del desarrollo de la investigación.

Esta investigación fue concebida tomando en cuenta distintos métodos para tomar lo más importante de cada uno de ellos y poder realizar una investigación completa, con el fin que mediante la utilización de cada uno de ellos se pueda tener un conocimiento profundo análisis de los delitos informáticos y su penalización según las leyes ecuatorianas tipificadas en el Código Orgánico Integral Penal. Por tal motivo, en el proceso del presente estudio fue utilizado el método analítico y sintético para de esta manera poder efectuar la interpretación de la información obtenida, mediante la revisión documental y bibliográfica relacionada con las variables de estudio.

3.3.1. Método descriptivo

Este método es aquel que se encuentra formado por la disposición de un primer plano del conocimiento que se tiene de la realidad, y tiene por objeto demostrar cómo es la situación o el problema que se está investigando, el investigador actúa de una manera directa y observa el problema en primera persona lo que le otorga un conocimiento directo del problema. De esta forma, el método descriptivo tiene como fin primordial interpretar y presentar con la mayor claridad y exactitud posible, los datos obtenidos de acuerdo a la verificación realizada (Calduch, 2015).

Desde este panorama, se ha elegido el método descriptivo con la finalidad de estudiar todos los elementos análisis de los delitos informáticos y su penalización según las leyes ecuatorianas tipificadas en el Código Orgánico Integral Penal. Este método se aplicó en

el presente estudio, cuando fueron descritos los delitos informáticos la importancia de ellos, su penalización, como son el Latinoamérica, cuáles son los más cometidos en Ecuador que se encuentran establecidos en el COIP.

3.3.3. Analítico

Este método parte del conocimiento que se tiene de un problema o tema concreto de manera general y en el cual se pretende extraer conclusiones individuales de una de las partes o sectores del problema o tema investigado. Por tal razón este método está formado por la descomposición del todo en sus partes. En tal sentido, este método comprende la descomposición de las partes de un problema para estudiarlas bien sea de una manera aislada o de forma complementaria (Calduch, 2015).

Se eligió este método en la presente investigación, ya que permite análisis de los delitos informáticos y su penalización según las leyes ecuatorianas tipificadas en el código orgánico integral penal. Este método fue aplicado cuando se efectuó el análisis de cada uno de los delitos informáticos establecidos en el Código Orgánico Integral Penal.

3.3. Sintético

Este método tiene como característica fundamental que parte de una realidad completa la cual ya es conocida de una manera previa por el investigador, ello con la finalidad de obtener una información reducida y concreta del problema investigado, es decir, que se conozca la esencia del problema, el no busca la profundidad del conocimiento, sino obtenerlo de una manera más reducida. (Calduch, 2015)

Este método se utilizó, cuando se obtuvo la totalidad de las leyes y del material documental que sirvió de base para este estudio y de ella se seleccionaron los autores más relevantes, con en relación al análisis de los delitos informáticos y su penalización según las leyes ecuatorianas tipificadas en el Código Orgánico Integral Penal.

.4. Deductivo

De acuerdo a la utilización de este método, parte de la construcción de un análisis que se tiene acerca del problema, pero desde un punto de vista general con la finalidad de posteriormente llegar a un conocimiento completo del problema o tema de estudio (Calduch, 2015).

Fue seleccionado este método por cuanto permite partir de unos conocimientos bastante amplios análisis de los delitos informáticos y su penalización según el ordenamiento penal vigente. Este método se utilizó en la presente investigación cuando se analizaron las normas establecidas en el Código Orgánico Integral Penal relativas a los delitos informáticos y su penalización.

3.5. Métodos comparativos

Es un método que tiene como fin plantear tanto las similitudes como las divergencias que se presentan en relación al objeto de estudio (Calduch, 2015).

Este método fue seleccionado para realizar análisis de los delitos informáticos y su penalización según las leyes de otros países. Este método se utilizó cuando se hizo una comparación de la manera como Estados Unidos, Chile y España acerca de los delitos informáticos en esos países por cuanto se ha evidenciado que en los mismos existe un mayor desarrollo normativo.

3.6. Técnicas de investigación

Las técnicas para el logro de los objetivos establecidos en el presente estudio, se consideró en primer lugar la observación, la entrevista y la encuesta.

3.6.1. La entrevista

Este instrumento que resulta esencial para cualquier tipo de investigación y ella consiste en un diálogo entre el entrevistador y una o más personas que tienen conocimiento acerca de la problemática investigada (Sampieri, T, 2015).

3.6.2. Encuesta

La encuesta estuvo dirigida a 375 fiscales de la provincia del Guayas.

3.6.3. Población

Este aspecto investigativo, es considerado como los elementos que el investigador necesita conocer y determinar las características esenciales del mismo. De esta manera se afirma que una investigación puede tener como fin de ella el obtener un conocimiento acerca de muchos objetos cosas, temas específicos o generales. A todo ese conjunto se le denomina población (Arias, 2012)

Por tal motivo, se observa que la población es considerada como el conjunto objeto de estudio, que puede ser presentado de una forma finita o infinita con características usuales definida por el problema y los objetivos del estudio. En relación al tema aquí descrito, esta investigación se desarrolla en una población aproximada de 375 fiscales de la Provincia de Guayas, Ecuador.

3.6.4. Muestra

La muestra es definida como un elemento que se encuentra del problema o del universo que se necesita estudiar, los cuales se concentran en uno o pocos elementos que se observan, no partiendo de un conjunto sino de aspectos específicos (Arias, 2012). Por tal razón, cuando resulta complejo tomar en cuenta un problema en su totalidad se busca determinar una muestra significativa que arroje unos resultados similares a las que arrojaría la totalidad de la población.

tamaño de muestra	N	16.840
probabilidad de que ocurra un evento	p	0,5
probabilidad de que no ocurra un evento	q	0,5
error de la estimación	E	0,05
nivel de confianza	Z	1,96

Resultado = 375

3.3. Encuestas

1.- ¿Considera usted que en Ecuador son penados los delitos informáticos?

Tabla 3
¿Considera usted que en Ecuador son penados los delitos informáticos?

	Frecuencia	Porcentaje
Si	95	25%
No	280	75%
TOTAL	375	100%

Fuente: encuesta aplicada
Elaborado por: Chávez 2020

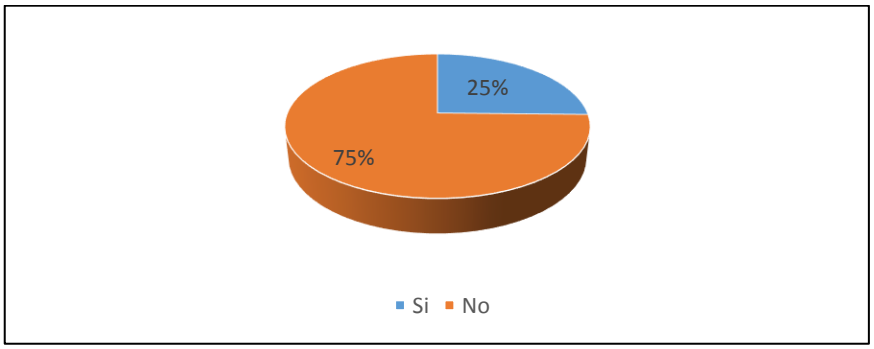


Grafico 1 ***¿Considera usted que en Ecuador son penados los delitos informáticos?***
Fuente: encuesta aplicada
Elaborado por: Chávez 2020

Análisis: De las respuestas señaladas en el presente ítem se evidencia que una amplia mayoría considera que no son penados los delitos informáticos en Ecuador mientras que una minoría considera que si son penados los delitos informáticos en Ecuador.

2.- ¿Considera usted que los criterios aplicables a los delitos informáticos son justas?

Tabla 4
¿las sanciones aplicables a los delitos informáticos son justas?

	Frecuencia	Porcentaje
Si	70	19%
No	305	81%
TOTAL	375	100%

Fuente: encuesta aplicada
Elaborado por: Chávez 2020

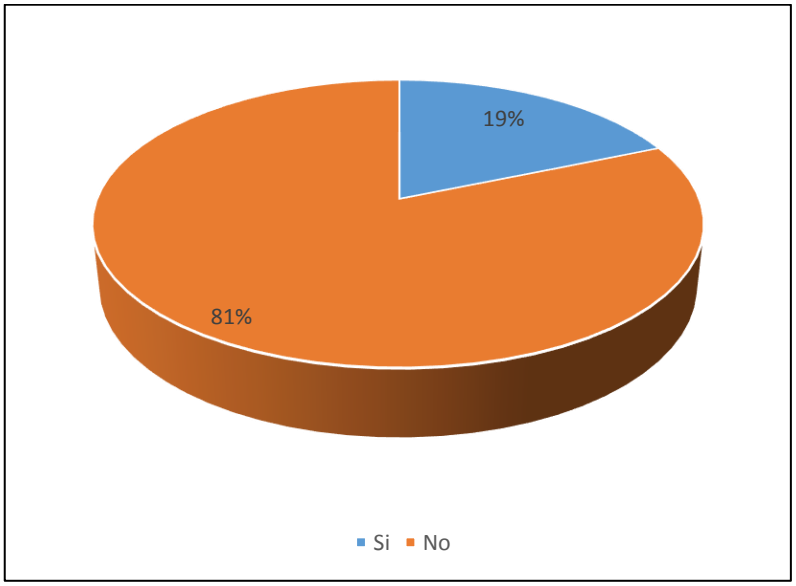


Grafico 2 ***¿las sanciones aplicables a los delitos informáticos son justas?***
Fuente: encuesta aplicada
Elaborado por: Chávez 2020

Análisis: De las respuestas señaladas en el presente ítem se evidencia que una gran mayoría es del criterio que las sanciones aplicables a los delitos informáticos no son justas mientras que una minoría considera que si son justas las sanciones aplicables a estos delitos son penados los delitos informáticos en Ecuador.

3.- ¿Considera usted que son sancionados la todos los delitos informáticos cometidos en la República del Ecuador?

Tabla 5
¿son sancionados la totalidad de los delitos informáticos en Ecuador?

	Frecuencia	Porcentaje
Si	64	17%
No	311	83%
TOTAL	375	100%

Fuente: encuesta aplicada
Elaborado por: Chávez 2020

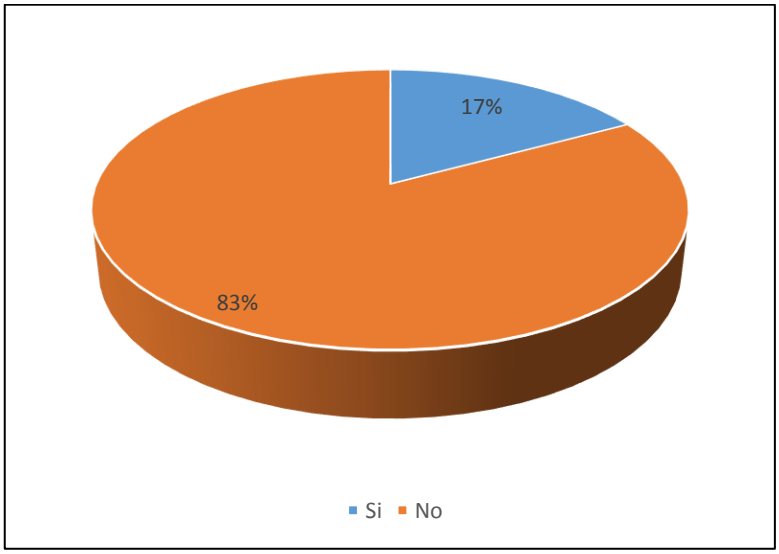


Grafico 3 ***¿son sancionados la totalidad de los delitos informáticos en Ecuador?***
Fuente: encuesta aplicada
Elaborado por: Chávez 2020

Análisis: De las respuestas señaladas en el presente ítem se evidencia que una gran mayoría es del criterio que no son sancionados la totalidad de los delitos informáticos cometidos en Ecuador mientras que una minoría bastante pequeña es del criterio que si son sancionados los delitos informáticos en Ecuador.

4.- ¿a su criterio la mayoría de los delitos informáticos son procesados en Ecuador?

Tabla 6
¿la mayoría de los delitos informáticos son procesados en Ecuador?

	Frecuencia	Porcentaje
Si	64	17%
No	311	83%
TOTAL	375	100%

Fuente: encuesta aplicada
Elaborado por: Chávez 2020

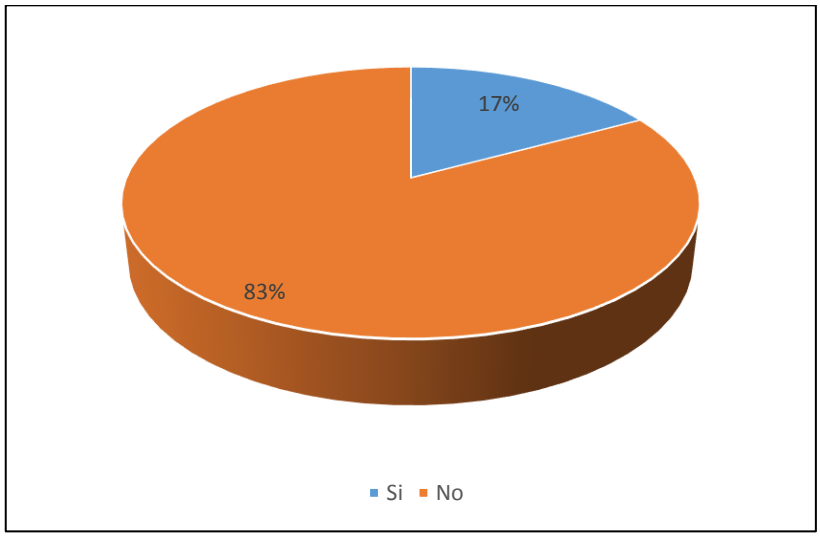


Grafico 4 ***¿ la mayoría de los delitos informáticos son procesados en Ecuador?***
Fuente: encuesta aplicada
Elaborado por: Chávez 2020

Análisis: De las respuestas señaladas en el presente ítem se evidencia que una gran mayoría es del criterio que no son procesados la mayoría de los delitos informáticos cometidos en Ecuador mientras que una minoría bastante pequeña es del criterio que si son sancionados los delitos informáticos en Ecuador.

5.- ¿Considera usted que se deberían agregar nuevos tipos penales informáticos en el Código Orgánico Integral penal?

Tabla 7
¿se deberían agregar nuevos tipos penales informáticos en el COIP?

	Frecuencia	Porcentaje
Si	292	78%
No	83	22%
TOTAL	375	100%

Fuente: encuesta aplicada
Elaborado por: Chávez 2020

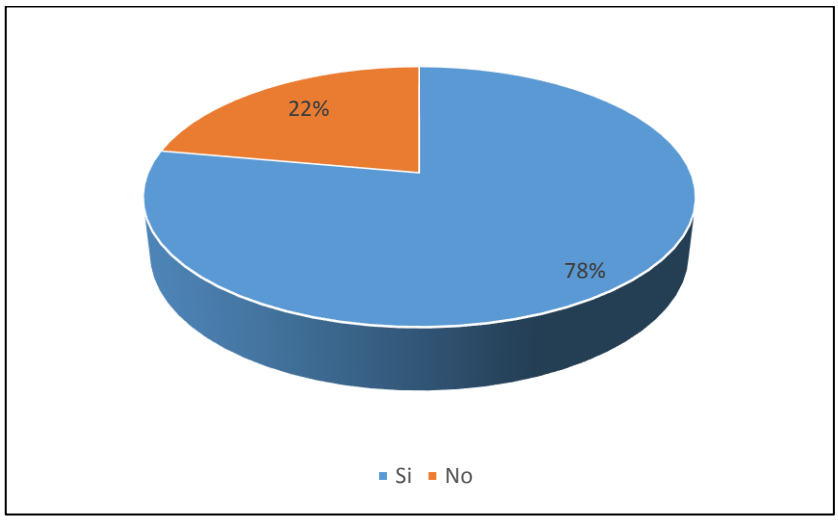


Grafico 5 ***¿se deberían agregar nuevos tipos penales informáticos en el COIP?***
Fuente: encuesta aplicada
Elaborado por: Chávez 2020

Análisis: De las respuestas señaladas en el presente ítem se evidencia que una gran mayoría es del criterio que, si se deberían agregar nuevos tipos penales informáticos al COIP, mientras que la minoría es del Criterio que deberían agregarse nuevos tipos penales al COIP.

6.- ¿Considera usted que las normativas jurídicas que contempla el COIP en los casos de delitos informáticos son acertadas?

Tabla 8
¿las normativas jurídicas que contempla el COIP en los casos de delitos informáticos son acertadas?

	Frecuencia	Porcentaje
Si	87	23%
No	288	77%
TOTAL	375	100%

Fuente: encuesta aplicada
Elaborado por: Chávez 2020

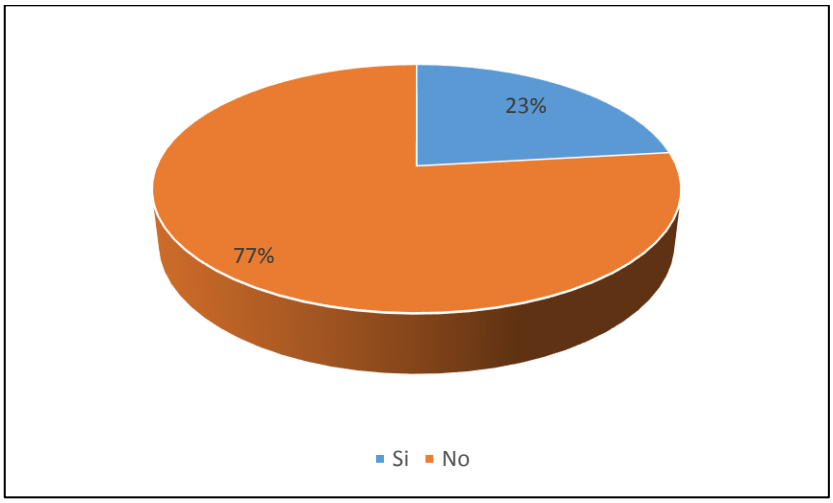


Grafico 6 ***¿las normativas que contempla el COIP en los casos de delitos informáticos son acertadas?***
Fuente: encuesta aplicada
Elaborado por: Chávez 2020

Análisis: De las respuestas señaladas en el presente ítem se evidencia que una gran mayoría es del criterio que, las normativas aplicadas en los casos si se deberían agregar nuevos tipos penales informáticos al COIP, mientras que la minoría es del Criterio que deberían agregarse nuevos tipos penales al COIP.

3.4. Entrevista Nº 1

1.- ¿Considera usted que en Ecuador son penados los delitos informáticos?

Si son penados los delitos informáticos en Ecuador lo que sucede que también hay que hacer referencia que no hay una tasa alta de denuncias de este tipo de delitos por lo que esta circunstancia influye en la sanción de los mismos.

2.- ¿Considera usted que en Ecuador son conocidos los delitos informáticos?

De acuerdo a mi opinión la sociedad en general no conoce la totalidad de cuáles son los delitos económicos que se encuentran contemplados en el Código Orgánico Integral Penal por lo que se recomienda a las autoridades que tienen la competencia en materia de seguridad coordinar conversatorios a los fines de divulgar este tipo de delitos.

3.- ¿Considera usted que las sanciones aplicables a los delitos informáticos son justas?

A mi criterio las sanciones que se encuentran establecidas en el COIP deberían ser aumentadas a los efectos que los delincuentes eviten este tipo de delitos, ya que al tener sanciones que no son tan fuertes, reinciden en dichos delitos.

4.- ¿Considera usted que son sancionados la totalidad de los delitos informáticos cometidos en la República del Ecuador?

No, por cuanto la mayoría de esos delitos no son denunciados.

5.- ¿Considera usted que la mayoría de los delitos informáticos quedan impunes en Ecuador?

Quedan impunes por lo que he venido sosteniendo que no hay una cultura para denunciar este tipo de delitos, pero de los que son denunciados y se efectua el procedimiento penal si son sancionados.

6. ¿Cuáles son los delitos informáticos más cometidos en Ecuador?

La apropiación fraudulenta de por medios electrónicos, la trasferencia electrónica de activo patrimonial y el acceso no consentido a un sistema informático de acuerdo a las cifras que yo conozco ellos son los más comunes.

3.5. Entrevista Nº 2

1.- ¿Considera usted que en Ecuador son penados los delitos informáticos?

Si, todo delito que es denunciado sigue su tramite penal y de darse las circunstancias y de demuestra la culpabilidad del denunciado son penados este tipo de delitos.

2.- ¿Considera usted que en Ecuador son conocidos los delitos informáticos?

No, para la sociedad en general y la mayoría de las personas desconocen cuáles son los delitos informáticos, es más me atrevo a decir que las personas que conocen este tipo de delitos es debido a que han sido víctimas de este tipo de delitos.

3.- ¿Considera usted que las sanciones aplicables a los delitos informáticos son justas?

De acuerdo a las sanciones establecidas en el COIP me parecen que deberían ser más duras a los efectos de evitar este tipo de delitos.

4.- ¿Considera usted que son sancionados la totalidad de los delitos informáticos cometidos en la República del Ecuador?

El problema que yo observo en relación a los delitos informáticos es que por no ser conocidos no son denunciados considero que muchas personas son víctimas de este tipo de delitos y desconocen que han sido víctimas de ellos.

5.- ¿Considera usted que la mayoría de los delitos informáticos quedan impunes en Ecuador?

El problema de la impunidad de este tipo de delitos va de la mano de la falta de conocimientos que se tiene de ellos es más considero que las autoridades que tienen competencia en esta materia deberían difundir las características de estos delitos y la manera como se cometen a efectos de evitarlos.

6. ¿Cuáles son los delitos informáticos más cometidos en Ecuador?

De acuerdo a la información que se maneja al respecto puedo indicarte que dentro de ellos los más comunes son la apropiación fraudulenta de por medios electrónicos, el acceso no consentido a un sistema informático y la trasferencia electrónica de activo patrimonial.

3.6. Análisis de las entrevistas

De acuerdo al criterio de los entrevistados se observó que en Ecuador los delitos informáticos son poco conocidos por los fiscales encuestados colectividad, y a pesar de ser muy comunes no hay un conocimiento acerca de ellos, hace falta una divulgación por parte de los órganos del Estado como el Ministerio de Gobierno a los efectos de informar cuáles son estos delitos, como se cometen, cual es el fin perseguido, a que órganos deben acudir las personas que han sido víctimas de estos delitos.

Por otra parte, destacan los entrevistados que el índice de denuncias de este tipo de delitos es bastante bajo por lo que la gran mayoría de ellos quedan impunes y esto se encuentra relacionado con lo afirmado en el párrafo anterior en relación al desconocimiento de este tipo de delitos. Se hace necesario que las víctimas de estos delitos efectúen las denuncias a los fines que los órganos de seguridad puedan efectuar las sanciones aplicables a este tipo de delitos. En este sentido las penas establecidas en el COIP ambos entrevistaron fueron del criterio que las sanciones deben ser mayores a los efectos que los delincuentes cometan este tipo de delitos o reincidan en los mimos.

Por último de acuerdo a los criterios señalados por ambos entrevistados concluyeron que los delitos informáticos que más se cometen en la actualidad en Ecuador, son la apropiación fraudulenta de por medios electrónicos, el acceso no consentido a un sistema informático y la trasferencia electrónica de activo patrimonial. Analizando lo señalado por los entrevistados y relacionándolos de manera directa con las encuestas realizadas se puede señalar que se hace necesaria una modificación a las penas contempladas en los delitos establecidos en los artículos 190,231 y 234 del Código Orgánico Integral Penal

CAPITULO IV PROPUESTA

Exposición de motivos

Los delitos cibernéticos han aumentado de manera progresiva en el Ecuador sobre todo a partir del año 2013 lo que ha causado preocupación en la población, así como también en las autoridades competentes como el Ministerio Público y demás cuerpos de seguridad del Estado. Dentro de los delitos más denunciados se encuentran la apropiación fraudulenta de medios electrónicos, la transferencia, electrónica de activo patrimonial, así como también el acceso no consentido a un sistema informático o de telecomunicaciones por lo cual se hace necesario que se eleven las penas en este tipo de delitos a los fines de lograr una disminución en su comisión.

Tomando en consideración:

Que el artículo 190 del Código Orgánico Integral Penal (2014) establece: "Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de

telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años" (p. 68).

Que artículo 231 del Código Orgánico Integral Penal (2014) señala: " Transferencia electrónica de activo patrimonial.- La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona (p. 80)".

Que artículo 234 del Código Orgánico Integral Penal (2014) señala: "Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años (p. 80).

RESUELVE LA MODIFICACIÓN DE LAS PENAS DE LOS DELITOS ESTABLECIDOS EN LOS ARTICULOS 190, 231 Y 234 DEL CODIGO ORGANICO INTEGRAL PENAL LOS CUALES QUEDARAN DE LA SIGUIENTE MANERA

Art. 190.- Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de cinco a ocho años.

Art. 231.- Transferencia electrónica de activo patrimonial. - La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de seis a nueve años.

Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de siete a diez años.

CONCLUSIONES

Luego de culminar la presente investigación que tuvo como objetivo general la penalización de los delitos informáticos en el Código Orgánico Integral Penal se han llegado a las siguientes conclusiones:

Se efectuó un estudio acerca de los delitos informáticos que más se han cometido en Ecuador, dentro de los cuales destaca el delito de apropiación fraudulenta de por medios electrónicos para apropiarse de un bien o valores ajenos, se encuentra también la trasferencia electrónica de activo patrimonial con el fin de causar un daño económico a la víctima y el acceso no consentido a un sistema informático en contra de la voluntad del titular de donde se determinó que la impunidad se debe a que son poco denunciados estos delitos.

Se efectuó un estudio acerca de las penas de cada uno de los delitos informáticos que dio como resultado que dichas sanciones no son aplicables a la mayoría de los delitos cometidos, ya que este tipo de delitos no son denunciados por las víctimas, lo que trae como consecuencia una alta tasa de impunidad en ellos

Por último, se hace necesario que las penas de los delitos informáticos sean aumentadas a los efectos que los delincuentes se abstengan a cometer este tipo de delitos, así como también evitar su reincidencia, los entrevistados consultados manifestaron que se hacía necesario elevar las sanciones a este tipo de delitos.

RECOMENDACIONES

Luego de culminar la presente investigación que tuvo como objetivo general la penalización de los delitos informáticos en el Código Orgánico Integral Penal se han llegado a las siguientes recomendaciones:

Se insta a las víctimas de los delitos informáticos a efectuar las denuncias pertinentes antes las autoridades respectivas a los fines de reducir la impunidad en este tipo de delitos efectuó un estudio acerca de los delitos económicos que más se han cometido en Ecuador dentro de los cuales destaca el delito de apropiación fraudulenta de por medios electrónicos para apropiarse de un bien o valores ajenos, se encuentra también la trasferencia electrónica de activo patrimonial con el fin de causar un daño económico a la víctima y el acceso no consentido a un sistema informático en contra de la voluntad del titular de donde se determinó que la impunidad se debe a que son poco denunciados estos delitos.

Se insta a los órganos con competencia penal a efectuar charlas y conversatorios a los fines de hacer una divulgación de los delitos informáticos a los efectos que las personas que en general tenga conocimiento de ellos, como se comenten, quienes los realizan, de qué manera son cometidos a los efectos de conocerlos y evitar ser víctima de ellos.

Se insta a la Asamblea Nacional a los efectos de hacer una modificación al Código Orgánico General de Procesos, con el fin de elevar las penas a los delitos informáticos más cometidos como la apropiación fraudulenta por medios electrónicos para apropiarse de un bien o valores ajenos y el acceso no consentido a un sistema informático en contra de la voluntad del titular.

Bibliografía

Abogados Ecuador. (08 de Julio de 2019). *Abogados Ecuador.* Recuperado el 05 de abril de 2020, de https://abogadosecuador.com.ec/post/delitos-informaticos-en-crecimiento

Aboso, G. (2006). *Cibercriminalidad y Derecho Penal.* Buenos Aires: B de F.

Acurio, S. (8 de Abril de 2015). Una visión general del Derecho Informático en el Ecuador con énfasis en las infracciones informáticas, la informática forense y la evidencia digital. *Derecho Penal Informático*. Obtenido de https://www.academia.edu/19803737/Derecho_Penal_Inform%C3%A1tico

APESPOL. (01 de Noviembre de 2015). *APESPOL*. Recuperado el 05 de Abril de 2020, de http://www.apespol.ec/articulo.php?id=11

Asamblea Nacional. (2014). *Código Orgánico Integral Penal.* ecuador. Recuperado el 19 de 06 de 2020, de https://biblioteca.defensoria.gob.ec/handle/37000/497

Baca, G. (2016). *Introducción a la seguridad informática.* Grupo editorial PATRIA. Obtenido de https://books.google.com.ec/books?hl=es&lr=&id=IhUhDgAAQBAJ&oi=fnd&pg=PP1&dq=la+inform%C3%A1tica&ots=0WTw7DzeGu&sig=nyFivQMuMP7Fc7kpX_aP85rSclY&redir_esc=y#v=onepage&q=la%20inform%C3%A1tica&f=false

Berenger, O. (2015). *Delitos informaticos.* Madrid: Tirant lo Blanch.

Brunet, L. (2018). *Manual de Derecho Informatico.* Madrid: Causa.

Chiluiza, E. (10 de 11 de 2017). Delitos y Abusos en redes Sociales en Ecuador. *El Universo*. Recuperado el 19 de 06 de 2020, de https://www.eluniverso.com/opinion/2017/11/10/nota/6472012/delitos-abusos-redes-sociales-ecuador

Clotet, J. (2006). *Delito informático y su investigación.* Obtenido de http://portal.uned.es/pls/portal/docs/PAGE/UNED_MAIN/LAUNIVERSIDAD/UBICACIONES/06/DUQUE_AHUMADA/PONENCIAS%20XX%20SEMINARIO%20DUQUE%20DE%20AHUMADA/4.PDF

Cocero, D., Garcia, M., Jorda, J., & Lopez, J. (2017). *Informática Aplicada. Herramientas Digitales Para La Investigación Y El Tratamiento De La Informacion En Humanidades.* Madrid. Obtenido de https://books.google.com.ec/books?hl=es&lr=&id=o4I9DwAAQBAJ&oi=fnd&pg=PP1&dq=La+inform%C3%A1tica+es+una+ciencia+que+se+encarga+del+tratamiento+autom%C3%A1tico+de+la+informaci%C3%B3n+&ots=n7KJ-MqKgW&sig=rmzlI8jCJXl34yUvaVrkda4sgl4&redir_esc=y#v=onepage&q&f

Coderata, P. (2016). *Delitos por las nuevas tecnologias.* Madrid: Consejo General del Poder Judicial.

Código Orgánico Integral Penal. (2018). *Código Orgánico Integral Penal.* Quito: Asamblea Nacional.

Código Penal del Ecuador. (1971). *Código Penal del Ecuador.* Quito: Asamblea Nacional. Recuperado el 05 de Abril de 2020, de http://www.pucesi.edu.ec/webs/wp-content/uploads/2018/03/C%C3%B3digo-Penal-2014.pdf

Computer Forensic. (2019). *Delitos Informáticos*. Recuperado el 05 de abril de 2020, de https://www.delitosinformaticos.info/delitos_informaticos/definicion.html

Constitución de la República del Ecuador. (2008). Constitución de la República del Ecuador. *Constitución de la República del Ecuador*. Quito, Pichincha, Ecuador: Decreto Legislativo.

Cruz, J. (2017). *Derecho penal y nuevas tecnologias.* Barcelona: Difusion Juridica.

El Telégrafo. (16 de Agosto de 2016). Recuperado el 05 de Abril de 2020, de https://www.eltelegrafo.com.ec/noticias/judicial/12/en-ecuador-el-85-de-los-delitos-informaticos-ocurre-por-descuido-del-usuario

Enriquez, J., & Alvarado, Y. (2015). LOS DELITOS INFORMÁTICOS Y SU PENALIZACIÓN EN EL CÓDIGO ORGÁNICO INTEGRAL PENAL ECUATORIANO. *CITT UPEC*, 171-194. Recuperado el 05 de Abril de 2020, de file:///C:/Users/USER/Downloads/404-25-1393-1-10-20180712%20(1).pdf

Enríquez, J., & Alvarado, Y. (2015). Los delitos informáticos y su penalización en el código orgánico integral penal ecuatoriano. *SATHIRI Sembrador*(8). doi:https://doi.org/10.32645/13906925.404

Ferro, J. (2020). *Ciencias Policiales.* Obtenido de https://books.google.com.ec/books?id=5FfRDwAAQBAJ&pg=PT2321&lpg=PT2321&dq=Los+virus+inform%C3%A1ticos+y+malware,+son+programas+maliciosos+que+tienden+a+reproducirse+y+extenderse+dentro+del+sistema&source=bl&ots=QsAkLrUtf0&sig=ACfU3U13fNUqsjIjJEvA9huZ5lRI8

Fiscalia General Del Estado. (06 de 2015). *Fiscalia 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/

García , O. (2016). *Fraude y estafa mediante sistemas informaticos.* Valencia: Purrua.

Gomez, M. (2016). *Responsabilidad por delitos cometidos mediante internet.* Pamplona: Aranzadi.

Hernández, A., Ramos, M., Placencia, B., Indacochea, B., Quimis, A., & Moreno, A. (2018). *Metodología de la Investigación Científica.* Alicante: Editorial Area de Innovación y Desarrollo. Recuperado el 06 de Abril de 2020

Huilcapi, A. (23 de 11 de 2011). *Derecho Ecuador*. Recuperado el 05 de Abril de 2020, de https://www.derechoecuador.com/el-delito-informatico

LawHelp.org. (04 de 03 de 2019). ¿Hay diferencias entre la patria potestad y la custodia? *Guía rápida sobre la patria potestad y la custodia*, 01. Obtenido de https://ayudalegalpr.org/resource/gua-rpida-sobre-la-patria-potestad-y-la-custo?ref=1Ibeh

Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas. (2002). *Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas.* Quito: Congreso Nacional. Recuperado el 05 de Abril de 2020, de https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf

Lopez, M. (2017). Hacking Etico. Vulnerabilidad de Sistemas Operativos en el acceso por contraseñas. *Revista Publicando, 4*(10(1)). Obtenido de https://revistapublicando.org/revista/index.php/crv/article/view/407

Martinez, J. (2017). *Delitos Informaticos* . Mexico: Mexiplus.

Meléndez, J. (2018). *Derecho Ecuador.com*. Recuperado el 05 de Abril de 2020, de https://www.derechoecuador.com/delitos-informaticos-o-ciberdelitos

Nava, A. (2017). *Delitos Informaticos.* Madrid: Mata.

Palomino, J. (2016). *Derecho Penal y Nuevas Tecnologias.* Valencia: Tirant lo Blanch.

Philco, O., & Rosero, L. (2014). Los Riesgos en Transacciones Electrónicas en Línea y la Criptografía como Modelo de Seguridad Informática. *1*. Recuperado el 19 de 06 de 2020, de http://publicaciones.usm.edu.ec/index.php/GS/article/view/44

Policía Nacional del Ecuador. (27 de Diciembre de 2017). *Policía Nacional del Ecuador*. Recuperado el 05 de Abril de 2020, de https://www.policiaecuador.gob.ec/delitos-informaticos-establecidos-en-el-coip-y-como-prevenirlos/

Quimbita, J. (2017). Obtenido de http://www.dspace.uce.edu.ec/bitstream/25000/10540/1/T-UCE-0013-Ab-85.pdf

Ricardo , M. (2017). *Estafa convencional y estafa informatica.* Madrid: Aranzadi.

Temperini, M. (2013). *Delitos Informáticos en Latinoamérica: un estudio de derecho comparado. 1ra. Parte.* Recuperado el 19 de 06 de 2020, de http://elderechoinformatico.com/publicaciones/mtemperini/CONAIISI_Temperini_Camera_Ready.pdf

Viega, M. (2020). *Derecho Informatico.* Montevideo: CADE.

Vivanco, I. (2016). *Reforma al Codigo Orgánico Integral Penal , de los delitos informaticos.* Loja: Universidad de Loja.

Ycaza, A. (2019). *Tratamiento Jurídico de los delitos informaticos en el Ecuador.* Guayaquil: Universidad Catolica Santiago de Guayaquil.

DECLARACIÓN Y AUTORIZACIÓN

Yo, Chávez Dávila Gonzalo Javier, con C.C: 070370271-2 autor(a) del trabajo de titulación: *La Penalización de los Delitos Informáticos en el COIP* previo a la obtención del grado de **MAGÍSTER EN DERECHO MENCIÓN DERECHO PROCESAL** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de graduación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 28 de noviembre del 2022

f. _____

Nombre: Chávez Dávila Gonzalo Javier

C.C: 0703702712

REPOSITORIO NACIONAL E CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE GRADUACIÓN			
TÍTULO Y SUBTÍTULO:	La penalización de los delitos informáticos en el COIP		
AUTOR(ES) (apellidos/nombres):	Chávez Dávila Gonzalo Javier		
REVISOR(ES)/TUTOR(ES) (apellidos/nombres):	Msg. Vivar Álvarez Juan Carlos Esp.		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
UNIDAD/FACULTAD:	Sistema de Posgrado		
MAESTRÍA/ESPECIALIDAD:	Maestría en Derecho Mención Derecho Procesal		
GRADO OBTENIDO:	Magíster en Derecho Mención Derecho Procesal		
FECHA DE PUBLICACIÓN:	28 de noviembre del 2022	**No. DE PÁGINAS:**	55
ÁREAS TEMÁTICAS:	Protección de datos, Derecho a la privacidad		
PALABRAS CLAVES/ KEYWORDS:	Penalización, delitos, informáticos, código, pena.		
RESUMEN/ABSTRACT El objetivo general de la presente investigación fue ddeterminar la penalización de los delitos informáticos en el Código Orgánico Integral Penal, como objetivos específicos se realizaron estudios de los delitos informáticos más comunes en la actualidad y sus sanciones, se revisaron las normativas jurídicas aplicadas en los casos de delitos informáticos y se estableció una propuestas de solución que mediante las sanciones eviten la impunidad de estos actos ilícitos como son los delitos informáticos. estuvo basado en un análisis de carácter bibliográfico y documental que tuvo como centro del mismo el paradigma interpretativo, orientado al análisis de textos que tienen vinculación con el análisis de los delitos informáticos y su penalización según las leyes ecuatorianas tipificadas en el Código Orgánico Integral Penal. Se concluyó que los delitos informáticos más cometidos en la República de Ecuador destacan el delito de apropiación fraudulenta de por medios electrónicos, con la finalidad de apropiarse de un bien o valores ajenos, se encuentra también las trasferencias electrónicas de activo patrimonial, para causar un daño económico a la víctima y por último el acceso no consentido a un sistema informático en contra de la voluntad del titular de donde se determinó que la impunidad se debe a que son poco denunciados estos delitos. Por último, se instó insta a la Asamblea Nacional a los efectos de hacer una modificación al Código Orgánico General de Procesos, con el fin de elevar las penas a los delitos informáticos más cometidos con la finalidad de efectuar una sanción mayor a la comisión de los mismos.			
ADJUNTO PDF:	☒ Si	☐ NO	
CONTACTO CON AUTOR/ES:	**Teléfono:** 0998008835	E-mail: gojacha@hotmail.com	
CONTACTO CON LA INSTITUCIÓN:	**Nombre:** Andrés Obando Ochoa		
	Teléfono: +593-992854967		
	E-mail: ing.obandoo@hotmail.com		

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	