UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE CIENCIAS SOCIALES

CARRERA DE DERECHO

“LOS DELITOS INFORMÁTICOS EN EL ECUADOR, ANÁLISIS COMPARATIVO CON LA LEGISLACIÓN DE COLOMBIA.”

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADO DE LOS TRIBUNALES DE JUSTICIA DE LA REPÚBLICA DEL ECUADOR.

AUTOR: JUAN CARLOS CADME ARCENTALES.

DIRECTOR: DR. EDWIN AREVALO VASQUEZ, MCS.

LA TRONCAL-ECUADOR

2020

REPÚBLICA DEL ECUADOR

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE CIENCIAS SOCIALES

CARRERA DE DERECHO

Título: Los delitos informáticos en el Ecuador, análisis comparativo con la Legislación de Colombia.

Trabajo de investigación previo a la obtención del Título de Abogado de los Tribunales de Justicia de la República.

AUTOR: JUAN CARLOS CADME ARCENTALES

Número de cédula 0301775052

TUTOR:

DR. EDWIN ARÉVALO MSC.

AÑO: 2020

Tabla de contenido

ACEPTACIÓN DEL TUTOR

CERTIFICÓ

Que, el presente Trabajo de Investigación realizado por el señor Cadme Arcentales Juan Carlos , de la carrera de Derecho Extensión La Troncal, ha sido orientado, corregido y revisado minuciosamente por lo que lo declaro APROBADO.

En calidad de tutor de grado, doy fe que dicho trabajo reúne todos los requisitos y méritos suficientes para ser sometido a presentación pública y evaluación por parte del jurado examinador que se designe, dando mi aprobación respectiva para que el señor Cadme Arcentales Juan Carlos pueda optar por el título de Abogado.

La Troncal, 21 de Septiembre de 2020

Ab. Edwin Arevalo Vazques, Mg.
DOCENTE TUTOR

DECLARACIÓN DE AUTORÍA

Yo, Juan Carlos Cadme Arcentales , declaro bajo juramento que, las ideas, conceptos, procedimientos y resultados del trabajo aquí descrito son de mi autoría, que no han sido previamente procesados para ningún grado ni calificación profesional y que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD CATÓLICA DE CUENCA EXTENSIÓN LA TRONCAL, según lo establecido por la ley de propiedad intelectual, por su reglamento y por la normativa institucional vigente.

Juan Carlos Cadme Arcentales .
AUTOR

Dedicatoria

Quiero empezar dedicando este trabajo, a Dios por ser el principal motor y guia durante la carrera, a mi madre que desde el cielo ha sido mi inspiración y fortaleza para prepararme profesionalmente, a mi padre por siempre darme el apoyo incondicional en cada momento que más lo necesitaba, a mis hermanos y familia que siempre me animarón a continuar hasta lograrlo.

También quiero dedicar este trabajo a un gran amigo y hermano que me apoyo, me apoya y me seguirá apoyando en todo, el es el Ing. Rómulo Alcívar Campoverde, quien me supo motivar cada vez que bajaba mis animos, como no decicar este esfuerzo tambien a mi ada madrina Angelita Arias que con su forma especial de animarme siempre hacía que no desmaye en en mis estudios.

A mi segunda familia, Don Germán, Sra. Esther Heras e hijas, que desde que inicie mis estudios siempre me diron su mano en todo, y me apoyaron para que no claudique en mi deseo de superación.

Agradecimiento

Mi agradecimiento principal a la Universidad Católica de Cuenca Extensión San Pablo La Troncal, por ser la casa de Estudio donde me he preparado profesionalmente para un ente activo en nuestra sociedad, a cada uno de los maestros que ciclo a ciclo impartieron su conocimiento conmigo, ya que, son sus enseñanzas y experiencia compartida lo que hoy me hace sentir un profesional preparado para ejercer con orgullo esta noble carrera que escogí sin lugar a duda la mejor.

Agradezco tambien de manera especial a mi tutor el Dr Edwin Arevalo por su constancia y motivación , quien con su experiencia permitió que culminara con éxito el presente trabajo de Titulación.

Resumen

El presente proyecto investigativo contiene un análisis comparativo de los delitos informáticos que han sobrevenido en los últimos años a través del desarrollo de las nuevas tecnologías. Recalcando la importancia de que las sociedades se acoplen a los nuevos delitos cibernéticos y de esta manera se pueda satisfacer las exigencias sociales de los ciudadanos, que diariamente se ven afectados por delincuentes que usan la tecnológica con el fin de cometer delitos y estos se dan en tiempo real, debido a que se utilizan equipos electrónicos manejados a través de la informática; es decir, no necesitan tener un acercamiento con la víctima para que estos se cristalicen.

La norma jurídica en el Ecuador especialmente en El Código Orgánico Integral Penal, determina los delitos en relación a la informática, bajo distintos artículos, destinados a cada delito, que en ocasiones y de acuerdo al tipo de delito se sanciona al autor hasta con dieciséis años de prisión. Particular que justamente sirve de mucha ayuda para que estos delitos de cierta forma sean cometidos en lo menor posible y lograr la paz social como fin primordial que tiene el Estado.

PALABRAS CLAVE.

Delitos, Informáticos, penal, víctima.

ABSTRACT

The purpose of this research project is to carry out a comparative analysis of computer crimes that have occurred in recent years through the development of new technologies. Emphasizing the importance of societies adapting to new cybercrimes and in this way satisfying the social demands of citizens, who are daily affected by criminals who use technology in order to commit crimes and these occur in real time, due to the use of electronic equipment managed through computers; that is, they do not need to have an approach with the victim for these to crystallize.

In Ecuadorian legislation, the Comprehensive Organic Penal Code, determines the crimes related to computing, under different articles, destined for each crime, which sometimes and according to the type of crime the author is punished with up to sixteen years in prison. Particular that precisely serves a lot of help so that these crimes in a certain way are committed as little as possible and achieve social peace as the primary purpose of the State.

KEY WORDS.

Crimes, Computer, criminal, victim.

1.INTRODUCCIÓN

El presente proyecto investigativo posee características sociales, académicas, doctrinarias, capaces de permitirnos comprender y desarrollar lo referente a los delitos informáticos, los mismos que son cometidos por personas que tienen conocimiento en esta área, que, en la mayoría de veces su único fin es afectar el patrimonio de sus víctimas.

Consideramos importante denotar que estos delitos tienen varias formas o modos para su cometimiento, por el mismo hecho los autores necesariamente deben tener estudios que pasan un bachillerato y muchas veces un pregrado, por lo que resulta de cierta manera abordar este tema con esa premisa, para clarificar la importancia de su estudio.

Los delitos informáticos se han convertido en una herramienta para vulnerar los derechos de las personas, tanto, naturales como jurídicas, puesto que con el avance tecnológico progresivo, se ha hecho cada vez más fácil evadir seguridades dentro de las plataformas informáticas o con el uso de las mismas conseguir datos de usuario que luego los emplearía en su propia contra, además de ciertas conductas que se han presentado con el libre acceso a redes sociales que no tienen un control estricto de creación de usuario, permitiendo con esto que cualquier persona pudiera con datos falsos crear un usuario y perjudica a terceros.

En la actualidad en nuestro país se reconocen varios delitos informáticos según el (COIP) Código Orgánico Integral Penal, pero cada vez siguen aumentando las conductas y se debe ir actualizando tanto como nuevos delitos como también especificado sus sanciones para cada uno de ellos.

En la vecina Colombia se considera es uno de los países de Latinoamérica que está más avanzado en el reconocimiento de este tipo de

conductas ilegales y que están debidamente sancionadas, por lo que es nuestro afán hacer un análisis comparativo para sugerir y recomendar que se considere también en nuestro país, siendo oportuno para que disminuya la vulneración de derechos con respecto al uso de la tecnología para no solamente delinquir sino, para usar de forma perjudicial a terceros.

De tal manera que, en la normativa penal de Ecuador, se realicen las debidas actualizaciones, evitando así mayor vulneración de derechos en las personas naturales y jurídicas, ya que en la actualidad por medio de redes sociales se puede, denigrar, ofender, calumniar sin medida ni control y no existe aún en nuestro país una debida forma de control y sanción para quienes tienen este tipo de conducta, así de esta manera poder convivir de manera pacífica en un entorno social y tecnológico amigable para todos.

2.METODOLOGÍA

El método a utilizarse es analítico–sintético, ya que con este método se podrá identificar y hacer un análisis comparativo de los delitos informáticos que se encuentran tipificados en la normativa jurídica de Colombia, que es pionera en este campo a nivel de Latinoamérica y los delitos informáticos que esán tipificados en nuestro paìs,asimismo se aplicará la técnica de revisión bibliográfica y base de datos científicos referentesal tema de la presente investigación.

CAPITULO I

1.1 Infracción penal.

Para abordar este importante tema, es necesario tener una concepción básica y, sobre todo, jurídica, de lo que es una infracción penal, para lo cual, recurrimos al Código Orgánico Integral Penal, concretamente al Art. 18, que señala: “Es la conducta típica, antijurídica y culpable cuya sanción se encuentra prevista en este código” (Código Orgánico Integral Penal, 2014), consecuentemente, la acción se refiere al acto que realiza una persona con respecto a un bien jurídico protegido, o a la humanidad de una persona; es decir, es la exteriorización de su conducta; por otra parte, la tipicidad hace referencia a que, cierto hecho debe estar determinado en una norma jurídica; o sea, en este caso, el C.O.I.P; sería antijurídica, en el caso que sea contraria a la norma pertinente y, por último, un sujeto será culpable, cuando adecuó su conducta al tipo penal, con perfecto conocimiento del hecho que realizó, sea penado o no.

1.2 Delitos informáticos.

Un delito informático, es considerado a la conducta de una persona, que, se aprovecha de los medios informáticos para provocar una vulneración del bien jurídico tutelado y, este acto lo puede realizar mediante operaciones que transgreden el software y hardware de una computadora, usando estos instrumentos o cualquier medio tecnológico para consumar un delito.

En este sentido, el tratadista Terragni, se refiere al delito informático como:

“Se podría definir el delito informático como toda acción (acción u omisión) culpable realizada por un ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor, aunque no perjudique de forma directo

o indirecta a la víctima, tipificado por la ley, que se realiza en el entorno informático y está sancionado con una pena.” (Verney, 2012)

Debemos considerar que, los delitos informáticos no tienen únicamente como objetivo que el actor se beneficie o no por algo, sino más bien, tenemos que enfocarnos en el hecho de causar daño; es decir, en la acción realizada por el presunto delincuente.

Bajo este orden de ideas, de la obra realizada por Julio Tellez, podemos apreciar que, los delitos informáticos, “son conductas criminales de cuello blanco o también denominadas, en inglés: “white collar crimes”, un determinado grupo de ciudadanas y ciudadanos con ciertos conocimientos en el ámbito de la informática, en este caso técnicos pueden llegar a cometerlas” (Tellez, 2001)

Como un dato adicional a la obra del mentado autor, señalamos que, los delitos de cuello blanco, los cometen sujetos que poseen un coeficiente intelectual más elevado, que ostentan un nivel de instrucción superior, así como un estatus social más alto, en contra de cualquier persona. Su objetivo no es una retribución económica, más bien, está destinado a causar daño a terceros simplemente por placer, por lo que, resulta un dato muy novedoso.

Con el paso del tiempo y, la llegada de las nuevas tecnologías, los delitos informáticos han pasado a ser un delito que se da cada vez con más frecuencias, pues, no puede ser de otra manera, si entramos a internet y tipeamos: “como cometer delitos informáticos”, nos vamos a encontrar con la grata sorpresa que, existe un sinnúmero de páginas que dan asesoramiento gratuito, lo que queremos denotar es que, cualquier persona puede cometer este delito y, más aun, con las múltiples facilidades que nos brinda la tecnología y las plataformas web. Por lo que, consideramos que se debe incorporar nuevas y más drásticas sanciones al respecto, en la normativa legal ecuatoriana.

De acuerdo a (Zambrano D. &., 2016) “La mayoría de los abogados y jueces, afirman que por sus características el delito informático no es fácil de probar, de ahí la necesidad de que el personal que garantiza esta actividad, tenga el suficiente conocimiento para detectar en cualquiera que fuera el caso, la existencia de una violación en la seguridad informática lo que incurriría en el delito informático.” Todo lo cual implica que se debe fomentar la preparación de personal especializado para investigar y detectar el cometimiento de delitos informáticos, pero asimismo se debe actualizar la normativa jurídica ya que a pesar de que en el Código Orgánico Integral Penal están tipificados ciertos delitos informáticos, actualmente han proliferado más delitos informáticos que lamentablemente no se encuentran tipificados y por tanto no pueden ser sancionados.

Según (Enríquez & Alvarado, 2015) “En conclusión, el delito informático está vinculado no sólo a la realización de una conducta delictiva a través de medios o elementos informáticos, o a los comportamientos ilícitos en los que aquellos sean su objeto, sino también a la afectación de la información”.

Las telecomunicaciones han evolucionado de manera impresionante que hoy en día todo se realiza a través de medios digitales y más si consideramos la situación que estamos pasando con la pandemia, toda nuestra vida se ha transformado y somos más dependientes de los medios informáticos para desarrollar nuestras actividades, pues bien un aspecto que ha tomado importante relevancia en la actualidad es la información, que se maneja a través de medios informáticos y por ende ésta se ha vuelto más vulnerable para el cometimiento de delitos informáticos y ahí radica la importancia de tener una normativa jurídica que sancione todos los delitos informáticos que actualmente se perpetran y quedan en la más absoluta impunidad.

Para (Zambrano, 2016) “El desconocimiento de las leyes que sancionan ciertas conductas informáticas, provoca que, no se exijan los derechos que por ley se adquieren al ser perjudicado con algunos de estos comportamientos,” Otro aspectos en el que se debe trabajar es el desconocimiento de las personas sobre qué actividades informáticas son consideradas delitos en nuestro Código Orgánico Integral Penal para que de esta manera dichos delitos sean denunciados y se protejan los bienes jurídicos vulnerados por los delitos informáticos.

A continuación, vamos a realizar una clasificación de los delitos informáticos:

1.3 Fraudes realizados a través de computadoras:

Estos delitos son frecuentes en los interiores de las Instituciones crediticias o bancarias, pues, las personas tienen facilidad de acceso a las bases de datos y registros de los usuarios.

1.4 Programación informática reproducida sin autorización:

Se trata de múltiples copias que se obtienen de programas que cuentan con licencia de uso, en nuestro medio, es comúnmente conocida como la piratería.

1.5 Manipulación de programas:

Esta modalidad se da a través de programas sustitutos que consienten y permiten manejar otros programas de mayor jerarquía y que cuentan con las licencias legales de cualquier organización o departamento estatal.

1.6 La manipulación de datos salientes:

Esta acción está destinada a adulterar los datos que son emitidos de una operación de computo, se realiza a través de otras computadoras.

1.7 Fraude por manipulación de la información:

Las personas que se dedican a esta modalidad, acceden a los programas que están en una base de datos informática, los manipulan con la finalidad de obtener una ganancia monetaria.

1.8 Falsificación informática:

Se da cuando una persona o grupos de personas, cambian la información que es emitida por una operación de consulta; es decir, manipulan los datos salientes de una base de datos.

1.9 Sabotaje informático:

Se trata de una interrupción de suministro de electrónica, telefonía e internet de manera intencional, para causar daño a los programas de cómputo.

1.10 Virus:

Se trata de la forma más peculiar de causar daño a los sistemas operativos, pues, son programas informáticos que se transfieren a las computadoras o equipos electrónicos y causan daño al perfecto funcionamiento de los mismos.

Los expuestos, son los delitos informáticos que se cometen día a día en nuestra legislación, por lo que consideramos que es muy importante, regular estas situaciones que causan malestar a los ecuatorianos y que, por la falta de ley, son cometidos con mayor frecuencia.

CAPITULO II

2.1 LEGISLACIÓN ECUATORIANA.

Como un dato interesante, para tener una mejor comprensión del tema, en el Ecuador, en el año 2019, durante los primeros diez meses, Fiscalía General del Estado, contabiliza alrededor de 1.254 denuncias que se refieren a delitos informáticos, de las cuales, 406 casos se dieron en la provincia del Guayas y 388 se ocasionaron en la provincia de Pichincha. (Diario El Universo, 2019)

Esto nos permite reflexionar que, existe una gran cantidad de delitos informáticos, que son ocasionados, en su mayoría, por el desconocimiento que tiene la ciudadanía al momento de entregar su información personal en distintas plataformas web. Además, debemos señalar que, varias empresas internacionales con domicilio en nuestro país, muy a menudo realizan llamadas telefónicas a los millones de usuarios ecuatorianos, solicitando información de carácter personal.

Todo esto, permite que más personas sean vulneradas en sus derechos, pues al no contar con una Ley penal, que tenga como objetivo, en primer lugar, prevenir que estos actos sean cometidos y, en segundo, en el caso del cometimiento del delito, sean sancionados con el máximo rigor de la ley.

Continuando con la investigación, acotamos que, el delito que más se comete respecto a los delitos informáticos, es la apropiación fraudulenta de dinero o información por medios electrónicos, éstos se encuentran regulados en el Código Orgánico Integral Penal, en el Art. 190 y, de acuerdo a la información obtenida por Diario el Universo, en el año 2019, se dieron 800 casos. (Diario El Universo, 2019).

Por otra parte, de acuerdo a los informes presentados por el

departamento contra la droga y el crimen, de las Naciones Unidas, el problema al que se enfrentan los investigadores de estos delitos es que “se buscan vestigios digitales, que suelen ser volátiles y de vida corta” (Naciones Unidas, Informes contra la droga y el crímen, 2012).

Resulta lógico pensar que estos vestigios digitales no van a estar permanentes en las plataformas web, pues como ya se mencionó, son delitos cometidos por profesionales en la informática, que por su experiencia y alto nivel de estudio no van a cometer errores de esa magnitud, esto nos lleva a deducir que, por lo expuesto, es casi imposible dar con la identidad y paradero del delincuente.

Cristian Mendoza, quien es magister en seguridad de la Informática, nos brinda varios consejos para de alguna manera cesar los delitos informáticos, tales como:

> “(…) al momento de tener enlaces sospechosos en nuestros dispositivos electrónicos, tenemos que evitar a toda costa, ingresar a ellos; si nos llega un correo de un remitente desconocido, tenemos que eliminarlo inmediatamente; disponer de varias contraseñas para las redes sociales y correos electrónicos; no ingresar claves o contraseñas cuando nos encontremos en redes wifi públicas y, actualizar el sistema operativo de los dispositivos, apenas esté disponible”. (Mendoza, 2015).

Sin lugar a dudas, acatar estos sencillos, pero importantes consejos, nos van a permitir en gran medida evitar ser víctima de los delitos informáticos, pues, en el transcurso de esta investigación, señalaremos que, mediante estas técnicas, los delincuentes informáticos realizan sus crímenes en la actualidad.

Por su parte las autoridades estatales, recomiendan asimismo que los ciudadanos apliquen estos consejos en su diario vivir. Hay que tener claro que,

la mayoría de los ecuatorianos cuentan con dispositivos electrónicos, tales como tabletas, celulares, computadoras, etc., dispositivos que permiten que se den estos delitos. Esta modalidad es muy común en nuestra legislación, a pesar de que las entidades bancarias y crediticias manifiestan que: “han aumentado su seguridad”, pero los datos emitidos por Fiscalía General del Estado, dicen otras cosas.

Para conocer un poco más de la realidad y los hechos que acontecen en nuestro País, citamos nuevamente a diario El Universo, con una noticia muy peculiar que justamente se ajusta a nuestro proyecto investigativo.

El ciudadano Eduardo Arellano, narra que, en el mes de noviembre de 2018, mientras se encontraba en su domicilio en la zona céntrica de Guayaquil, recibió una llamada telefónica, así como un mensaje de texto, en las cuales le indicaban que, se realizó un retiro en la cuenta de su banco, por la cantidad de 100.00 dólares americanos. Lógicamente su reacción inmediata fue intentar bloquear su cuenta bancaria para intentar cesar el robo, pues comenta que no autorizo a ningún familiar, ni persona el retiro del mismo. A renglón seguido, le llegó nuevamente un mensaje de texto indicándole, de la misma manera que había sido retirado 100.00 dólares adicionales, mediante un cajero que estaba ubicado en el Cantón Milagro, provincia del Guayas. Sin poder hacer más, se dirigió rápidamente al banco más cercano para recibir información al respecto, cuando llegó, una de las encargadas le indicó que, nada se podía hacer al respecto, pues la tarjeta con la que se hicieron los retiros, estaba legalmente autorizada. Luego de las investigaciones realizadas por Fiscalía, pudieron identificar que se trataba de una clonación realizada a su tarjeta de débito, esto permitió a los delincuentes realizar los múltiples retiros y perjudicar de esta forma a un ciudadano ecuatoriano. (Diario El Universo, 2019).

Esto nos permite apreciar de forma clara la realidad en la que vivimos en nuestro país, pues según los bancos, cuentan con varios sistemas de

seguridad capaces de evitar estos crímenes, pero, como ya se señaló, es muy distinto lo que pasamos los ecuatorianos.

Los delitos informáticos en nuestra legislación, se encuentran tipificados en el Art. 168, numeral 2, que se refiere a la Estafa, que se conceptualiza a continuación:

> **"Art. 186.2. Estafa.** -La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años. Defraude mediante el uso de dispositivos electrónicos que alteren o modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copiar o reproducir información de tarjetas de crédito, débito, pago o similares**"**. (Código Organico Integral Penal, 2014)

Entonces, si una persona, adecua su conducta a lo dispuesto en el artículo precedente, el máximo de la pena que recibiría, seria siete años. Hemos considerado que debería existir una sanción más drástica, pues, como en varias ocasiones se señaló, es un delito de difícil investigación, pues el actor seguramente va a tener un avanzado conocimiento en esta área de la informática y, sin menospreciar, hay cantones en nuestra legislación, que ni siquiera cuentan con departamentos técnicos y especializados en el área de la informática, por lo que resulta muy difícil investigar y dar con el responsable.

En esta virtud, agregamos que, se deben incluir en cada cantón de nuestro país, en donde se cuente lógicamente con Fiscalía, unidades de investigación con un amplio conocimiento en este tema, para que, de alguna

manera, se ponga un alto a estos delitos que diariamente causan malestar y afectan al patrimonio de las víctimas.

Por otra parte, debemos hacer notar que, a diferencia de los delitos informáticos, existen los delitos cibernéticos, que estos son concatenados al ciberterrorismo, por citar un ejemplo: una persona puede utilizar un aparato electrónico para armar una bomba, capaz de producir una explosión, entonces, esta bomba está guiada por el aparato electrónico que, mediante pulsaciones electromagnéticas, crea la detonación, causando daño a gente inocente. El común denominador de estos delitos es la informática como el arma de ataque, que en su mayoría tienen un carácter o fin económico.

Denotamos que la informática, resulta una herramienta muy cómoda para causar daño a terceros y, esto se debe a que, las bases de datos o plataformas web, cuentan con grandes cantidades de datos personales, lo que permite la manipulación con gran facilidad de aquellos y sus resultados son devastadores en virtud de que se pueden acceder a sus cuentas bancarias y, en el caso que soliciten información de carácter personal, estas puedan ser introducidas fácilmente.

Justamente a este hecho hace referencia el tratadista Ríos, al manifestar que: “Debemos tener conciencia que esta clase de ilícitos son devastadores debido a que permiten entregar datos e informaciones, de carácter importante o confidencial, sobre millones de personas naturales y jurídicas, inclusive el propio Estado ecuatoriano, en este caso, que son fundamentales para el funcionamiento de sus actividades de todo tipo” (Ríos, 2011).

Es lógico pensar y deducir que el desarrollo tecnológico ayuda de sobremanera a las sociedades, pues, esto nos permite desde adquirir productos simples, así como realizar transferencias bancarias, comunicarnos

con las personas en cualquier parte del mundo, saber lo que ocurre alrededor del planeta, en todo momento y, en todo lugar, pero de la misma manera si esos desarrollos tecnológicos no son debidamente regulados, pueden ocasionar daños con grandes consecuencias, tanto para los individuos, así como las sociedades en general; es por ello que, consideramos que las sanciones para las personas que cometen delitos informáticos deben ser drásticas, porque las consecuencias pueden llegar a ser mortales en un gran número de personas y, expresamos esto porque una bomba nuclear puede tranquilamente terminar con la vida de países enteros, tomando en consideración que esas bombas son manipuladas gracias a la tecnología y la informática.

Continuando con la normativa legal ecuatoriana, debemos considerar que, los tipos penales que se encuentran regulados son sancionadores; es decir, el acto se tiene que realizar, mas no son preventivos, comprendido que son identificados bajo verbos rectores de la acción, tales como: introducir, manipulación, borrar, interferir, entre otros, comúnmente poseen esta denominación y son conocidos como esta manera para clasificar a los delitos. El legislador, mediante aquellos, brinda al Juzgador, la opción de no solo sancionar el acto de diseñar, vender, fabricar y otros establecidos en el cuerpo penal. Con esto se evita que los actores de estos delitos, burlen las disposiciones normativas.

Para ampliar un poco más este controvertido tema, nos permitimos ejemplificar lo expuesto: **A** obtiene de forma fraudulenta, datos personales de **B,** esos datos son traficados con el fin de cometer fraudes informáticos.

Aquí evidenciamos que **A,** comete dos delitos, el primero, la obtención de datos de forma fraudulenta y, el segundo, el tráfico de esos datos. Pero el C.O.I.P, establece una sola sanción por esos dos delitos, lo podemos verificar en el Art. 186 del mentado cuerpo legal. Entonces podemos observar que, es

necesario que se incorporen nuevas medidas, con base en un estudio minucioso de cada caso y acorde a las estadísticas y datos que posee el Consejo de la Judicatura y la Fiscalía, para poder cumplir y satisfacer las necesidades sociales que son cambiantes por el mismo desarrollo de las tecnologías.

Es así que además de lo expuesto anteriormente tenemos también que considerar los siguientes artículos que, si están debidamente tipificados en el código orgánico integral penal, COIP, y son los siguientes:

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, será sancionada con pena privativa de libertad de uno a tres años. (COIP, 2018)

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.

Art. 230.- Interceptación ilegal de datos. - Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvié, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.

2. La persona que diseñe, desarrolle, venda, ejecute, programe o envié mensajes, certificados de seguridad o páginas electrónicas, enlaces o

ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.

3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.

4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior. (COIP, 2018)

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 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. (COIP, 2018)

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, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.

2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.

Art. 233.- Delitos contra la información pública reservada legalmente. - La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años.

La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años. (COIP, 2018)

Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor publico encargado de la custodia o utilización legitima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad.

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 tres a cinco años. (COIP, 2018)

Como una nota adicional, señalamos que no solo es necesario que una persona cometa este tipo de delitos, sino más bien, en la mayoría de veces se trata de organizaciones perfectamente establecidas. Mientras un miembro de la organización se dedica a la recopilación de datos de sus víctimas, otras personas o colegas de crimen están especializados en manipular esos datos para sacar algún beneficio económico. Pero debemos entender que ambos, son sujetos activos del delito, pues no se puede concebir el hecho de que uno es autor y, otro es cómplice, para nuestro pensamiento, las dos personas son sujetos activos del delito.

CAPITULO III

3.1 DELITOS INFORMATICOS Y EL DERECHO COMPARADO.

Pocos son los países que actualmente cuentan con disposiciones legales aptas para sancionar a las personas que cometen delitos informáticos y, justamente es el caso de Colombia, Uruguay y la república de Argentina, los modelos exitosos de América Latina.

Dentro del presente trabajo investigativo, se ha considerado realizar un análisis comparativo entre las legislaciones ecuatoriana y colombiana, debido al aporte significativo que brindan a los países latinoamericanos con la normativa penal en cuanto a los delitos informáticos.

3.2 NORMATIVA PENAL INTERNACIONAL

Chile, fue el pionero dentro de Latinoamérica en instituir la normativa legal penal a su ordenamiento jurídico, tipificando lo referente a los delitos informáticos y estableciendo como mínimo, tres años de prisión para las personas que cometen estas acciones.

Justamente fue en el año 1993, que Chile, mediante la Ley No. 19223, estableció normas que permitieron sancionar los delitos cibernéticos o informáticos que se cometían a diario en este país, tomando en consideración que el desarrollo de la tecnología estaba en auge y que era necesario establecer la normativa.

A continuación, realizamos una reseña de los delitos informáticos tipificados en la Ley No. 19223, el Art. 1 de la mentada Ley, establece que"El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo

Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en

su grado máximo.” (Insights about Cyberspace Law and Cybercultures :A salvador millaleo's blog, 2012)

El mentado articulo guarda relación con lo señalado en el C.O.I.P, que precisamente sanciona hasta con tres años de prisión la persona que emplee conductas dañinas sobre la información delicada

Acerca del Art. 2, de la misma Ley, que señala:

> El que, con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo o medio. (Insights about Cyberspace Law and Cybercultures :A salvador millaleo's blog, 2012)

Agregamos que, en esta legislación desde los años 90, se determinó que divulgar, interceptar e interferir cierta información, se considera un delito menor y se sanciona en su grado mínimo o medio.

Mientras que, el tercer artículo de la Ley relativa a los delitos informáticos, determina: “El que maliciosamente altere, dañe o destruya los datos

contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio” (Insights about Cyberspace Law and Cybercultures :A salvador millaleo's blog, 2012)

Dañar un sistema informático a través de un virus, es sancionado en Chile hasta con tres años; es decir, este país se toma muy en serio el tema de los delitos informáticos que, a diferencia de nuestro país, que ni siquiera contempla el hecho que sea un delito, insertar un virus, en un sistema informático.

El cuarto artículo, especifica que:

> El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado. (Insights about Cyberspace Law and Cybercultures :A salvador millaleo's blog, 2012).

Efectivamente de esta forma, se resalta en la Legislación Chilena que, revelar o difundir datos que causan agravio a terceras personas, será sancionada como una pena menor, mientras que, si esta acción la comete la persona responsable de tutelar y almacenar la información, la pena será aumentada de grado medio a grave.

A manera de síntesis, especificamos que los Arts. 1 y 3 de la mentada Ley No. 19223, están direccionados a sancionar el tema del "sabotaje informático" y, por otro lado, los Arts. 2 y 4, tienen como propósito sancionar el "espionaje de la información". En todos los casos, la legislación chilena, mediante esta Ley, se presenta como un ejemplo para que el resto de países repliquen esta normativa, que permite que sus ciudadanos gocen de seguridad jurídica, gracias a una ley protectora, que, de cierta manera, abarca casi todo lo referente a los delitos que se pueden cometer mediante cualquier medio informático y electrónico.

Para el tratadista Chileno González, resulta elemental señalar que:

Para estos delitos, la Ley establece penas de presidio menor diferentes grados que van de mínimo, medio o máximo, por lo que, dependiendo de la gravedad del delito cometido, el Juzgador podrá aplicar penas privativas de libertad que van desde los sesenta y un días hasta los cinco años (González, 2015)

Como observamos, esta deducción deviene de la lógica de que una persona debe ser sancionada de acuerdo a la infracción o delito que cometa, pues, a decir de los delitos cibernéticos, existen varios tipos y que presentan daños más fuertes a las personas, ya que no se puede concebir el hecho de que una persona ingrese a la base de datos de una Institución después de varios intentos y que cause daño a terceros, a que una persona que labora en una Institución ya sea esta de carácter público o privado y, tenga libre acceso a la información de la misma, provocando daño. La primera debe ser sancionada con una pena inferior a la segunda, debido a que la segunda tuvo en su poder toda la información y era la responsable de almacenar y proteger la misma.

Debido a que las sociedades se encuentran en constante transformación y consecuente los desarrollos tecnológicos se dan con el paso de los días, La Ley, 19223, con el fin de ajustarse a las necesidades sociales actuales, sufrió una reforma en cuando a las políticas de seguridad informática, pues se debatió sobre la existencia de nuevos y varios delitos que debían ser considerados para garantizar que sus ciudadanos sean protegidos contra la delincuencia cibernética e informática.

Es así que, en el año 2017, a la Ley 19223 se incorporó los siguientes delitos:

-Captación visual y sonora de la información sin consentimiento.

-Difusión de ese material.

-Producción de programas o dispositivos para cometer delitos.

-Difusión de información de un sistema informático.

-Manipulación de claves confidenciales y de datos codificados en una tarjeta.

-Uso de programas o dispositivos para vulnerar la integridad de los datos.

-Alteración o daño de sistemas informáticos.

-Alteración de datos para acceder a un sistema informático. (Insights about Cyberspace Law and Cybercultures :A salvador millaleo's blog, 2012) .

3.3 LEGISLACIÓN PENAL COLOMBIANA SOBRE DELITOS INFORMÁTICOS

Según (Ojeda, 2010) La Ley 1273 del 5 de enero de 2009, reconocida en Colombia como la *Ley de Delitos Informáticos*, tuvo sus propios antecedentes jurídicos, además de las condiciones de contexto analiza- das en el numeral anterior. El primero de ellos se remite veinte años atrás, cuando mediante el Decreto 1360 de 1989 se reglamenta la inscripción del soporte lógico (software) en el Registro Nacional de Derecho de Autor, que sirvió como fundamento normativo para resolver aquellas reclamaciones por violación de tales derechos, propios de los desarrolladores de software. A partir de esa fecha, se comenzó a tener asidero jurídico para proteger la producción intelectual de estos nuevos creadores de aplicativos y soluciones informáticas.

En este mismo sentido y en el entendido de que el soporte lógico o software es un elemento informático, las conductas delictivas descritas en los Artículos 51 y 52 del Capítulo IV de la Ley 44 de 1993 sobre Derechos de Autor, y el mismo Decreto 1360 de 1989, Reglamentario de la inscripción del soporte lógico (software) en el Registro Nacional del Derecho de Autor, se constituyeron en las primeras normas penal- mente sancionatorias de las violaciones a los citados Derechos de Autor. Al mismo tiempo, se tomaron como base para la reforma del año 2000 al Código Penal Colombiano:

3.4 Capítulo Único del Título VII que determina los Delitos contra los Derechos de Autor:

Artículo 270: Violación a los derechos morales de autor.

Incurrirá en prisión de dos (2) a cinco (5) años y multa de veinte (20) a

doscientos (200) salarios mínimos legales mensuales vigentes quien:

1. Publique, total o parcialmente, sin autorización previa y expresa del titular del derecho, una obra inédita de carácter literario, artístico, científico, cinematográfico, audiovisual o fonograma, programa de ordenador o soporte lógico.

2. Inscriba en el registro de autor con nombre de persona distinta del autor verdadero, o con título cambiado o suprimido, o con el texto alterado, deformado, modificado o mutilado, o mencionando falsamente el nombre del editor o productor de una obra de carácter literario, artístico, científico, audiovisual o fonograma, programa de ordenador o soporte lógico.

3. Por cualquier medio o procedimiento compendie, mutile o transforme, sin autorización previa o expresa de su titular, una obra de carácter literario, artístico, científico, audiovisual o fonograma, programa de ordenador o soporte lógico.

Parágrafo. Si en el soporte material, carátula o presentación de una obra de carácter literario, artístico, científico, fonograma, videograma, programa de ordenador o soporte lógico, u obra cinematográfica se emplea el nombre, razón social, logotipo o distintivo del titular legítimo del derecho, en los casos de cambio, supresión, alteración, modificación o mutilación del título o del texto de la obra, las penas anteriores se aumentarán hasta en la mitad. (Colombia, 2000)

Artículo 271: Defraudación a los derechos patrimoniales de autor.

Incurrirá en prisión de dos (2) a cinco (5) años y multa de veinte (20) a mil (1.000) salarios mínimos legales mensuales vigentes quien, salvo las excepciones previstas en la ley:

1. Por cualquier medio o procedimiento, sin autorización previa y expresa del titular, reproduzca obra de carácter literario, científico, artístico o cinematográfico, fonograma, video-grama, soporte

lógico o programa de ordenador, o transporte, almacene, conserve, distribuya, importe, venda, ofrezca, adquiera para la venta o distribución, o suministre a cualquier título dichas reproducciones.

2. Represente, ejecute o exhiba públicamente obras teatrales, musicales, fonogramas, video-gramas, obras cinematográficas, o cualquier otra obra de carácter literario o artístico sin autorización previa y expresa del titular de los derechos correspondientes.

3. Alquile o de cualquier otro modo comercialice fonogramas, video-gramas, programas de ordenador o soportes lógicos u obras cinematográficas, sin autorización previa y expresa del titular de los derechos correspondientes.

4. Fije, reproduzca o comercialice las representaciones públicas de obras teatrales o musicales, sin autorización previa y expresa del titular de los derechos correspondientes.

5. Disponga, realice o utilice, por cualquier medio o procedimiento, la comunicación, fijación, ejecución, exhibición, comercialización, difusión o distribución y representación de una obra de las protegidas en este título, sin autorización previa y expresa de su titular.

6. Retransmita, fije, reproduzca o por cualquier medio sonoro o audiovisual divulgue, sin autorización previa y expresa del titular, las emisiones de los organismos de radiodifusión.

7. Recepcione, difunda o distribuya por cualquier medio, sin autorización previa y expresa del titular, las emisiones de la televisión por suscripción.

Parágrafo. Si como consecuencia de las conductas contempladas en los numerales 1, 3 y 4 de este artículo resulta un número no mayor de cien (100) unidades, la pena se rebajará hasta en la mitad.

Artículo 272: Violación a los mecanismos de protección de los derechos patrimoniales de autor y otras defraudaciones.

Incurrirá en multa quien:

1. Supere o eluda las medidas tecnológicas adoptadas para restringir los usos no autorizados.
2. Suprima o altere la información esencial para la gestión electrónica de derechos, o importe, distribuya o comunique ejemplares con la información suprimida o alterada.
3. Fabrique, importe, venda, arriende o de cualquier forma distribuya al público un dispositivo o sistema que permita descifrar una señal de satélite cifrada portadora de programas, sin autorización del distribuidor legítimo de esa señal, o de cualquier forma de eludir, evadir, inutilizar o suprimir un dispositivo o sistema que permita a los titulares del derecho controlar la utilización de sus obras o producciones, o impedir o restringir cualquier uso no autorizado de éstos.
4. Presente declaraciones o informaciones destinadas directa o indirectamente al pago, recaudación, liquidación o distribución de derechos económicos de autor o derechos conexos, alterando o falseando, por cualquier medio o procedimiento, los datos necesarios para estos efectos. (Colombia, 2000)

El Código Penal colombiano (Ley 599 de 2000) en su Capítulo séptimo del Libro segundo, del Título III: Delitos contra la libertad individual y otras garantías, trata sobre la violación a la intimidad, reserva e interceptación de comunicaciones:

Artículo 192: Violación ilícita de comunicaciones.

El que ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida una comunicación privada dirigida a otra persona, o se entere indebidamente de su contenido, incurrirá en prisión de uno (1) a tres (3) años, siempre que la conducta no constituya delito sancionado con pena

mayor.

Si el autor de la conducta revela el contenido de la comunicación, o la emplea en provecho propio o ajeno o con perjuicio de otro, la pena será prisión de dos (2) a cuatro (4) años.

Artículo 193: Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas.

El que, sin permiso de autoridad competente, ofrezca, venda o compre instrumentos aptos para interceptar la comunicación privada entre personas, incurrirá en multa, siempre que la conducta no constituya delito sancionado con pena mayor.

Artículo 194: Divulgación y empleo de documentos reservados.

Modificado por el art. 25, Ley 1288 de 2009. El que en provecho propio o ajeno o con perjuicio de otro divulgue o emplee el contenido de un documento que deba permanecer en reserva, incurrirá en multa, siempre que la conducta no constituya delito sancionado con pena mayor.

Artículo 195: Acceso abusivo a un sistema informático.

Modificado por el art. 25, Ley 1288 de 2009, Derogado por el art. 4, Ley 1273 de 2009. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa.

Artículo 196: Violación ilícita de comunicaciones o correspondencia de carácter oficial.

El que ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida comunicación o correspondencia de carácter oficial, incurrirá en prisión de tres (3) a seis (6) años.

La pena descrita en el inciso anterior se aumentará hasta en una tercera parte cuando la comunicación o la correspondencia esté destinada o remitida

a la Rama Judicial o a los organismos de control o de seguridad del Estado.

Artículo 197: Utilización ilícita de equipos transmisores o receptores**.**

Estos artículos son concordantes con el artículo 357: Daño en obras o elementos de los servicios de comunicaciones, energía y combustibles.

El que con fines ilícitos posea o haga uso de aparatos de radiofonía o televisión, o de cualquier medio electrónico diseñado o adaptado para emitir o recibir señales, incurrirá, por esta sola conducta, en prisión de uno (1) a tres (3) años.

La pena se aumentará de una tercera parte a la mitad cuando la conducta descrita en el inciso anterior se realice con fines terroristas. (Colombia, 2000)

Una norma posterior relacionada fue la Ley 679 de 2001, que estableció el Estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con niños menores de edad. De igual manera, consagra prohibiciones para los proveedores o servidores, administradores o usuarios de redes globales de información, respecto a alojar imágenes, textos, documentos o archivos audiovisuales que exploten a los menores en actitudes sexuales o pornográficas. Sin embargo, la norma no contiene sanciones penales, sino administrativas (Artículo 10), pues siendo simple prohibición, deja un vacío que quita eficacia a la Ley, cuando se trata de verdaderos delitos informáticos. (Departametno Administrativo de la Funciòn Pública, 2001)

Para subsanar lo anterior, el 21 de julio de 2009, se sancionó la Ley 1336, “por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual, con niños, niñas y adolescentes”. En forma específica, en su Capítulo VI, sanciona los “Tipos penales de turismo sexual y almacenamiento e intercambio de pornografía infantil” con penas de prisión de diez (10) a veinte (20) años y multas de ciento cincuenta (150) a mil quinientos (1.500) salarios mínimos legales mensuales vigentes .

La Ley 1273 de 2009 complementa el Código Penal y crea un nuevo bien jurídico tute- lado a partir del concepto de la *protección de la información y de los datos*, con el cual se preserva integralmente a los sistemas que utilicen las tecnologías de la información y las comunicaciones. El primer capítulo de los dos en que está dividida la Ley, trata de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. El segundo Capítulo se refiere a los atentados informáticos y otras infracciones.

A partir de la Ley 1273 de 2009, se tipificaron los delitos informáticos en Colombia en los siguientes términos: acceso abusivo a un sistema informático (modificado del Código Penal); obstaculización ilegítima del sistema informático o red de telecomunicación; interceptación de datos informáticos; daño informático; uso de software malicioso; hurto por medios informáticos y semejantes; violación de datos personales; suplantación de sitios *web* para capturar datos personales y transferencia no consentida de activos. (Daccach, 2009)

Este marco jurídico se ha convertido en una importante contribución y un instrumento efectivo para que las entidades públicas y privadas puedan enfrentar los “delitos informáticos”, con definiciones de procedimientos y políticas de seguridad de la información; y, en consecuencia, con las acciones penales que pueden adelantar contra las personas que incurran en las conductas tipificadas en la norma. Con ella, Colombia se ubica al mismo nivel de los países miembros de la Comunidad Económica Euro- pea (CEE), los cuales ampliaron al nivel internacional los acuerdos jurídicos relacionados con la protección de la información y los recursos informáticos de los países, mediante el Convenio ‘Ciber-criminalidad’, suscrito en Budapest, Hungría, en 2001 y vigente desde julio de 2004. Con los desarrollos jurídicos hasta ahora logrados acerca de “la protección de la información y de los datos y la preservación integral de los sistemas que utilicen las tecnologías de in- formación y comunicaciones”, las organizaciones pueden amparar gran parte

de sus sistemas integrados de información: datos, procesos, políticas, personal, entradas, salidas, estrategias, cultura corporativa, recursos de las TIC y el entorno externo (Davenport, 1999), de manera que, además de contribuir a asegurar las características de calidad de la información, se incorpora la administración y el control, en el concepto de protección integral.

Retomando la estructura de la Ley 1273 de 2009, el capítulo I está orientado especialmente a apoyar la labor de los grupos de Auditoría de Sistemas, al apuntar al propósito de aseguramiento de las condiciones de calidad y seguridad de la información en la organización, cuando se refiere a los "atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos". Corrobora la importancia de la información como activo de valor para las organizaciones (ISO/IEC 17799/2005), que es necesario proteger adecuadamente para garantizar la continuidad del negocio, la maximización del retorno de la inversión y el aprovechamiento de las oportunidades del en- torno, así como para disminuir y contrarrestar los riesgos y delitos que la amenazan.

La gestión confiable de la seguridad de la información en las organizaciones parte del establecimiento de políticas, estándares, procedimiento y controles eficientes, en natural concordancia con las características del negocio y, en ese sentido, el capítulo I de la Ley 1273 de 2009 contribuye a tal propósito, de la misma manera que los estándares nacionales e inter- nacionales sobre administración eficiente de la información.

En las siguientes figuras se presenta un detalle del contenido de la Ley y sus características aplicables a este análisis. La figura 2 identifica las actuaciones con las cuales se tipifica el delito y la punibilidad aplicable (en su mayoría, penas de prisión entre 48 y 96 meses y multas de 100 a 1.000 SMLMV).

El artículo 1 de la Ley 1273 de 2009 incorpora al Código Penal el Artículo 269A y complementa el tema relacionado con el "acceso abusivo a un sistema informático", que se manifiesta cuando el pirata informático o *hacker*

aprovecha la vulnerabilidad en el acceso a los sistemas de información, o las deficiencias en los procedimientos de seguridad informática establecidos por las organizaciones, para ex- traer beneficios económicos o para indagar o demostrar la capacidad y recursos que ofrece la tecnología de la información. Cuando se presenta este abuso, en muchos casos, se observa que proviene de los mismos usuarios del sistema, tal como se evidencia en los informes anuales de la Pricewater houseCoopers, *The global state information security* y en estudios realizados por Cisco (2008), en los cuales se señala que el 42% de los tres casos de abuso más frecuentes corresponde a los detectados entre los empleados.

El artículo 269B contempla como delito la “obstaculización ilegítima del sistema informático o red de telecomunicación”, y se origina cuando el *hacker* informático bloquea en forma ilegal un sistema o impide su ingreso por un tiempo, hasta cuando obtiene un beneficio por lo general económico. Aquí también se enmarca el acceso a cuentas de correo electrónico sin el debido consentimiento de sus propietarios y el manejo o bloqueo de las claves obtenidas de distinta forma.

El artículo 269C plantea la infracción relacionada con la “interceptación ilícita de datos informáticos”, también considerada en el Artículo 3 del Título 1 de la Convención de Buda- pest de 2001. Se presenta cuando una persona, valiéndose de los recursos tecnológicos, obstruye datos sin autorización legal, en su sitio de origen, en el destino o en el interior de un sistema informático, o de emisiones electromagnéticas de un sistema electromagnético que los transporte.

El delito relacionado con los “daños informáticos” está contemplado en el Artículo 269D y se comete cuando una persona que, sin estar autorizada, modifica, altera, daña, borra, destruye o suprime datos del programa o de documentos electrónicos, en los recursos de las TIC.

El artículo 269E contempla el delito vinculado con el “uso de software malicioso” técnicamente denominado *malware*, ya generalizado en internet. Se

presenta cuando se producen, adquieren, venden, distribuyen, envían, introducen o extraen del país software o programas de computador que producen daños en los re- cursos de las TIC.

El delito sobre "violación de datos personales" (*hacking*) lo trata el artículo 269F y está orientado a proteger los derechos fundamentales de la persona (como dignidad humana y libertad ideológica). Se da cuando un individuo sin estar facultado, sustrae, vende, envía, compra, divulga o emplea datos personales alma- cenados en ficheros, archivos, bases de datos o medios similares con el fin de lograr utilidad personal o para otros.

El artículo 269G trata de la "suplantación de sitios *web* para capturar datos personales". Sucede cuando el suplantador (*phisher*) o delincuente informático crea una página y un dominio similar al de la entidad a la cual de- sea abordar, lo ubica en un *hosting* (espacio en un servidor) desde donde envía correos *spam* o engañosos (por ejemplo, empleos). Al no distinguir la página original de la falsa, las personas inocentemente suministran información personal y claves bancarias que el suplantador almacena en una base de datos y luego ordena la transferencia del dinero de la víctima a cuentas de terceros quienes prestan sus cuentas o servicios (testaferros), que luego reclama o distribuye.

Estas condiciones se dan cuando el delito se comete en redes, sistemas informáticos y de comunicaciones del Estado o del sector financie- ro nacional o extranjero; o cuando se origina o promueve por un funcionario público; o cuan- do se da a conocer información confidencial en perjuicio de otro para obtener provecho propio o de terceros; o cuando se actúa con fines terroristas para atentar contra la seguridad o defensa nacional, o cuando se usa como instrumento a un tercero de buena fe.

CONCLUSIONES

Una vez realizado la investigación conforme un análisis jurídico de comparación de las normas de Colombia y Ecuador con respecto de los delitos informáticos y su incidencia y efectividad en las normas aplicables según estos estados, es claramente evidente el (COIP Código Orgánico Integral Penal) que rige en Ecuador aun cuando existe el reconocimiento de ciertas conductas como delitos informáticos, es menester reconocer también que la norma carece de efectividad comparada con la ley colombiana.

Al concluir este trabajo es importante recalcar las debilidades actuales de nuestro Código Orgánico Integral Penal reconociendo las diversas conductas delictivas que aplican ciertas personas para vulnerar los derechos de otras, lo que hace de cierta manera fácil el cometimiento de conductas plenamente delictivas y que no están tipificadas ni sancionadas en dicha norma legal.

Bibliografía

Código Orgánico Integral Penal. (2014). *Código Orgánico Integral Penal.* Quito: DESAYP.

Terragni, A. (2007). *Bioética y Derecho Penal.* Santa Fe: Editoriales Penales.

Tellez, J. (2001). *Derecho Informático.* México: Instituto de investigaciones Jurídicas.

Campos, S. (2016). *Delitos de la Informática.* Buenos Aires: Antonifa.

Diario El Universo. (30 de octubre de 2019). *Delitos Informáticos en nuestro País*, pág. 7.

Naciones Unidas. (2012). *Informes contra la droga y el crímen.*

Mendoza, C. (2015). *Daños provocados por delitos informáticos.* Quito: DESAYP.

Ríos, P. (2011). *Los Delitos Cibernéticos y su impacto en las sociedades.* Buenos Aires: Nuevos Horizontes.

Scheineir, C. (2015). *Problemas causados por los avances tecnológicos.* Madrid: Antofagasta.

Naciones Unidas. (1948). *Declaración Universal de los Derechos Humanos.*

Ley Relativa a Delitos Informáticos. (1993). *Ley N.19223.* . Santiago de Chile: Norton.

González, A. (2015). *Presidio Menor en Chile*. Obtenido de https://chile.leyderecho.org/presidio-menor/

Zambrano, D. &. (Agosto de 2016). Delito Informatico .Procedimiento Penal en Ecuador. *Revista Cientifica Dominio de las Ciencias , 2*, 204-215.

Ojeda, A. R. (Enero de 2010). Delitos Informáticos y entorno jurídico en Colombia. *11*(28).

Colombia, C. d. (2000). *www.derechocolombiano.com.co*. (P. d. Autor, Editor) Recuperado el 2020 de 2020, de Ley 599 de 2000: https://www.derechocolombiano.com.co/derecho-penal/codigo-penal/

Verney, S. (2012). *https://www.terragnijurista.com.ar*. Obtenido de DELITOS INFORMATICOS : https://www.terragnijurista.com.ar/doctrina/informaticos.htm

Código Organico Integral Penal, C. (2014). *Delitos* (Vol. 1). Quito.

Insights about Cyberspace Law and Cybercultures :A salvador millaleo's blog, I. (24 de Enero de 2012). *https://smillaleo.wordpress.com/*. Obtenido de Ley Chilena Sobre Delitos Informàicos 1993: https://smillaleo.wordpress.com/2012/01/24/ley-chilena-sobre-delitos-informaticos-1993/

Departametno Administrativo de la Funciòn Pública. (03 de Agosto de 2001). *https://www.funcionpublica.gov.co*. Obtenido de Departamento Administrativo de la Función Pública: https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=18309

Daccach, J. C. (05 de Enero de 2009). *Ley de delitos Informáticos en Colombia* . Obtenido de Delta Asesores : https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

Campos, N. O. (2019). Normativa Legal sobre delitos informáticos en el Ecuador. *Hallazgos*, 100-110.

Zambrano, J., Dueñas, K., & Macías, L. (2016). Obtenido de Dialnet: file:///C:/Users/uf/Downloads/Dialnet-DelitoInformaticoProcedimientoPenalEnEcuador-5761561.pdf

Enríquez, J., & Alvarado, Y. (2015). *Sathiri*. Obtenido de file:///C:/Users/uf/Downloads/404-25-1393-1-10-20180712.pdf

Universidad Católica de Cuenca

PERFIL DE TESIS

Universidad Católica de Cuenca

Universidad Católica de Cuenca

UNIVERSIDAD CATÓLICA DE CUENCA

COMUNIDAD EDUCATIVA AL SERVICIO DEL PUEBLO

UNIDAD ACADÉMICA DE CIENCIAS SOCIALES

CARRERA DE DERECHO EXTENSIÓN LA TRONCAL

Tema: Delitos informáticos en las legislaciones de Ecuador y Colombia.

Título: Los delitos informáticos en el Ecuador, análisis comparativo con la Legislación Colombiana.

Alumno: Juan Carlos Cadme Arcentales.

Tutor: Dr. Edwin Arevalo Msc.

LA TRONCAL
2020

1. Estructura del diseño del proyecto de investigación

1.1. Tema

Delitos informáticos en las legislaciones de Ecuador y Colombia.

1.2. Título

Los delitos informáticos en el Ecuador, análisis comparativo con la legislación Colombiana.

1.3. Justificación

Los delitos informáticos se han convertido en una herramienta para vulnerar derechos de las personas, tanto, naturales como jurídicas, puesto que con el avance tecnológico progresivo, se ha hecho cada vez más fácil evadir seguridades dentro de las plataformas informáticas o con el uso de las mismas conseguir datos de usuario que luego los emplearía en su propia contra, además de ciertas conductas que se han presentado con el libre acceso a redes sociales que no tienen un control estricto de creación de usuario, permitiendo con esto que cualquier persona pudiera con datos falsos crear un usuario y perjudica a terceros.

En la actualidad en nuestro país se reconocen varios delitos informáticos según el (COIP) Código Orgánico Integral Penal, pero cada vez siguen aumentando las conductas y se debe ir actualizando tanto como nuevos delitos como también especificado sus sanciones para cada uno de ellos.

En la vecina Colombia se considera es uno de los países de Latinoamérica que esta más avanzado en el reconocimiento de este tipo de conductas ilegales y que están debidamente sancionadas, por lo que es nuestro afán hacer un análisis comparativo para sugerir y recomendar que se considere también en nuestro país, siendo oportuno para que disminuya la vulneración de derechos con respecto al uso de la tecnología para no solamente delinquir sino, para usar de forma perjudicial a terceros.

De tal manera que en la normativa penal de Ecuador se realicen las debidas actualizaciones, evitando así mayor vulneración de derechos en las personas naturales y jurídicas, ya que en la actualidad por medio de redes

sociales se puede, denigrar, ofender, calumniar sin medida ni control y no existe aún en nuestro país una debida forma de control y sanción para quienes tienen este tipo de conducta, así de esta manera poder convivir de manera pacífica en un entorno social y tecnológico amigable para todos.

1.4. Formulación del Problema

¿ Como incide la deficiente tipificación de los delitos informáticos, en el incremento de estas conductas delictivas, mediante el uso de herramientas tecnológicas?

1.5. Objeto de Estudio

Derecho penal

1.6. Campo de Acción de la Investigación

Conductas ilegales que se deberían regular tal como lo hacen otros países hermanos y han reducido notablemente la vulneración de derechos y formas de delinquir, usando herramientas informáticas.

1.7. Líneas de Investigación de la Carrera

Derecho Penal y Política Criminal

1.8. Objetivos de la Investigación

1.9. General

Determinar mediante revisión bibliográfica si es efectivo actualizar y reconocer nuevas conductas ilegales en nuestro país, comparando con la legislación

colombiana que es reconocida como una de las legislaciones más rígidas con respecto a los delitos informáticos, con el fin de evidenciar incidencia la falta de una actualizada normativa sobre la temática.

1.10.Específicos

- Determinar cuáles son los delitos informáticos que no están reconocidos en nuestro país como tal y que en Colombia sí.
- Describir cuales son las nuevas conductas que se deberían estipular en la legislación de nuestro país.
- Comprobar s que es necesario una actualización de nuestra normativa legal para reducir el tamaño de actos ilegales con el uso de herramientas tecnológicas.

1.11 Tipo De Investigaciónn

La investigaciónn teórica bibliográfica es el tipo de investigación aplicada a este tema, ya que por motivos de la restricción de movilidad por la pandemia del CORONAVIRUS o también llamado Covid19, no se puede realizar otro tipo de investigación, por esta razón se ha optado por realizar una investigación netamente bibliográfica, sin dejar de lado que será muy útil para llegar a cumplir todos los objetivos planteados.

1.12. Marco teórico

Según (Campos N. O., 2019) “Los delitos informáticos son conductas típicas, antijurídicas y culpables que tienen a las computadoras como instrumento o fin ” Podemos determinar que los delitos informáticos son una forma de infringir la ley que conforme pasa el tiempo esa aplicada con más frecuencia, y que está en constante innovación ya que la tecnología en sí evoluciona constantemente, asimismo pasa con los delitos informáticos, por ello es

importante que el derecho evolucione a la par con la tecnología y tipifique ciertas conductas que perjudican al bien jurídico protegido por la normativa jurídica.

De acuerdo a (Zambrano, Dueñas, & Macías, 2016) “La mayoría de los abogados y jueces, afirman que por sus características el delito informático no es fácil de probar, de ahí la necesidad de que el personal que garantiza esta actividad, tenga el suficiente conocimiento para detectar en cualquiera que fuera el caso, la existencia de una violación en la seguridad informática lo que incurriría en el delito informático.” Todo lo cual implica que se debe fomentar la preparación de personal especializado para investigar y detectar el cometimiento de delitos informáticos, pero asimismo se debe actualizar la normativa jurídica ya que a pesar de que en el Código Orgánico Integral Penal están tipificados ciertos delitos informáticos, actualmente han proliferado más delitos informáticos que lamentablemente no se encuentran tipificados y por tanto no pueden ser sancionados.

Según (Enríquez & Alvarado, 2015) “En conclusión, el delito informático está vinculado no sólo a la realización de una conducta delictiva a través de medios o elementos informáticos, o a los comportamientos ilícitos en los que aquellos sean su objeto, sino también a la afectación de la información”. Las telecomunicaciones han evolucionado de manera impresionante que hoy en día todo se realiza a través de medios digitales y más si consideramos la situación que estamos pasando con la pandemia, toda nuestra vida se ha transformado y somos más dependientes de los medios informáticos para desarrollar nuestras actividades, pues bien un aspecto que ha tomado importante relevancia en la actualidad es la información, que se maneja a través de medios informáticos y por ende ésta se ha vuelto más vulnerable para el cometimiento de delitos informáticos y ahí radica la importancia de

tener una normativa jurídica que sancione todos los delitos informáticos que actualmente se perpetran y quedan en la más absoluta impunidad.

Para (Zambrano, Dueñas, & Macías, 2016) “El desconocimiento de las leyes que sancionan ciertas conductas informáticas, provoca que, no se exijan los derechos que por ley se adquieren al ser perjudicado con algunos de estos comportamientos,” Otro aspectos en el que se debe trabajar es el desconocimiento de las personas sobre qué actividades informáticas son consideradas delitos en nuestro Código Orgánico Integral Penal para que de esta manera dichos delitos sean denunciados y se protejan los bienes jurídicos vulnerados por los delitos informáticos.

1.13. Hipótesis o ideas a defender en la Investigación

La hipótesis a defender con la presente investigación es que el incumplimiento del mandato constitucional de la creación de las regiones autónomas en el Ecuador ha tenido impacto en la planificación y por ende el desarrollo equitativo y descentralizado del país, principalmente de los sectores más desfavorecidos del país que con las regiones buscaba equilibrar el desarrollo con la unión de provincias fuertes con provincias con poco desarrollo.

1.14 Método A Utilizarse En La Investigación

El método a utilizarse es el analítico-sintético, ya que con este método se podrá identificar y hacer una análisis comparativo de los delitos informáticos que se encuentran tipificados en la normativa jurídica de Colombia, que es

pionera en este campo a nivel de Latinoamérica y los delitos informáticos que están tipificados en nuestro país, asimismo se aplicará la técnica de revisión bibliográfica y base de datos científicos referentes al tema de la presente investigación.

Cuenca: Av. de las Américas y Tarqui. *Telf: 2830751, 2824365, 2826563* **Azogues:** Campus Universitario "Luis Cordero El Grande", (Frente al Terminal Terrestre). *Telf: 593 (7) 2241 - 613, 2243-444, 2245-205, 2241-587* **Cañar:** Calle Antonio Ávila Clavijo. *Telf: 072235268, 072235870* **San Pablo de la Troncal:** Cdla. Universitaria km.72 Quinceava Este y Primera Sur *Telf: 2424110* **Macas:** Av. Cap. José Villanueva s/n *Telf: 2700393, 2700392*

1.15 Cronograma De Tareas

CRONOGRAMA DE ACTIVIDADES

ETAPAS	ACTIVIDADES	MES 1				MES 2				MES 3				MES 4				MES 5				MES 6			
		S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4
ANTEPROYECTO	Revisión bilbiográfica para elección del tema, titulo y justificación	x																							
	Formulación del problema, Campo de acción y líneas de investig., y Objetivos		x																						
	Tipo de Investi, Investigación de artículos para Estado del arte			x																					
	Método a utilizar, Cronograma			x																					
MARCO TEÓRICO	Revisión bibliográfica del tema de investigación				x	x	x																		
	Elaboración de la fundamentación teórica,							x	x																
	Desarrollo de las bases legales y definición de términos									x	x														
	Procesamiento y análisis de la información											x	x												
MARCO SITUACIONAL	Búsqueda de información sobre el marco situacional													x	x										
	Análisis del marco situacional															x	x								
PROPUESTA O SOLLUCIÓN	Comparación de las teorías,																	x	x						
	Análisis del marco teórico y situacional y la elaboración de propuestas																			x	x				
CONCLUSIONES	elaboración de conclusiones.																					x	x		
RECOMENDACIONES	Elaboración de recomendaciones																							x	
	Revisión final de la investigación																								x
	entrega de la tesis																								x

BIBLIOGRAFIA

Código Orgánico Integral Penal. (2014). *Código Orgánico Integral Penal.* Quito: DESAYP.

Terragni, A. (2007). *Bioética y Derecho Penal.* Santa Fe: Editoriales Penales.

Tellez, J. (2001). *Derecho Informático.* México: Instituto de investigaciones Jurídicas.

Campos, S. (2016). *Delitos de la Informática.* Buenos Aires: Antonifa.

Diario El Universo. (2019, octubre 30). *Delitos Informáticos en nuestro País*, p. 7.

Naciones Unidas. (2012). *Informes contra la droga y el crímen.*

Mendoza, C. (2015). *Daños provocados por delitos informáticos.* Quito: DESAYP.

Ríos, P. (2011). *Los Delitos Cibernéticos y su impacto en las sociedades.* Buenos Aires: Nuevos Horizontes.

Scheineir, C. (2015). *Problemas causados por los avances tecnológicos.* Madrid: Antofagasta.

Naciones Unidas. (1948). *Declaración Universal de los Derechos Humanos.*

Ley Relativa a Delitos Informáticos. (1993). *Ley N.19223.* . Santiago de Chile: Norton.

González, A. (2015). *Presidio Menor en Chile*. Tratto da https://chile.leyderecho.org/presidio-menor/

Zambrano, D. &. (2016, Agosto). Delito Informatico .Procedimiento Penal en Ecuador. *Revista Cientifica Dominio de las Ciencias , 2*, 204-215.

Ojeda, A. R. (2010, Enero). Delitos Informáticos y entorno jurídico en Colombia. *11*(28).

Colombia, C. d. (2000). *www.derechocolombiano.com.co*. (P. d. Autor, A cura di) Tratto il giorno 2020 2020 da Ley 599 de 2000: https://www.derechocolombiano.com.co/derecho-penal/codigo-penal/

Verney, S. (2012). *https://www.terragnijurista.com.ar*. Tratto da DELITOS INFORMATICOS : https://www.terragnijurista.com.ar/doctrina/informaticos.htm

Código Organico Integral Penal, C. (2014). *Delitos* (Vol. 1). Quito.

Insights about Cyberspace Law and Cybercultures :A salvador millaleo's blog, I. (2012, Enero 24). *https://smillaleo.wordpress.com/*. Tratto da Ley Chilena Sobre Delitos Informàicos 1993: https://smillaleo.wordpress.com/2012/01/24/ley-chilena-sobre-delitos-informaticos-1993/

Departametno Administrativo de la Funciòn Pública. (2001, Agosto 03). *https://www.funcionpublica.gov.co*. Tratto da Departamento Administrativo de la Función Pública: https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=18309

Daccach, J. C. (2009, Enero 05). *Ley de delitos Informáticos en Colombia* . Tratto da Delta Asesores : https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

Campos, N. O. (2019). Normativa Legal sobre delitos informáticos en el Ecuador. *Hallazgos*, 100-110.

Zambrano, J., Dueñas, K., & Macías, L. (2016). Tratto da Dialnet: file:///C:/Users/uf/Downloads/Dialnet-DelitoInformaticoProcedimientoPenalEnEcuador-5761561.pdf

Enríquez, J., & Alvarado, Y. (2015). *Sathiri*. Tratto da file:///C:/Users/uf/Downloads/404-25-1393-1-10-20180712.pdf

1.17. Firmas del tutor y del responsable de investigación que aprueba el diseño

La Troncal 27 de mayo de 2020

Juan Carlos Cadme Arcentales

_____	_____
Dr. Edwin Arévalo	Dr. Julio Garate Amoroso
TUTOR	RESPONSABLE DE INVESTIGACIÓN

Fecha: _____

Aprobado en sesión del H. Consejo Directivo de fecha: _____

_____

Asesor Jurídico

Unidad Académica de Ciencias Sociales

Universidad Católica de Cuenca

ANEXOS

Universidad
Católica
de Cuenca

La Troncal 06 de mayo 2020

Dr. Héctor Tapia Mgtr.
DIRECTOR DE LA CARRERA DE DERECHO EXTENSIÓN LA TRONCAL

Presente

De mi consideración:

Yo, CADME ARCENTALES JUAN CARLOS con C.I 0301775052, alumno de la carrera de Derecho, llego con un afectuoso saludo y al mismo tiempo comunicarle que, una vez cumplido con los requisitos académicos establecidos por la Universidad Católica de Cuenca Sede San Pablo de la Troncal, solicito a usted que se me inscriba en la Unidad de Titulación para optar por la modalidad de graduación: TRABAJO DE TITULACION.
Para cuyo efecto reconozco y acepto las disposiciones establecidas en el Reglamento de Titulación

Atentamente,

JUAN CARLOS CADME ARCENTALES
ESTUDIANTE DE DECIMO CICLO PERIODO MARZO 2020-AGOSTO 2020
C.I. 0301775052
Mail: juancadme@hotmail.com, jccadmea52@est.ucacue.edu.ec

Universidad Católica de Cuenca

turnitin

Recibo digital

Este recibo confirma quesu trabajo ha sido recibido por Turnitin. A continuación podrá ver la información del recibo con respecto a su entrega.

La primera página de tus entregas se muestra abajo.

Autor de la entrega:	Juan Carlos Cadme Arcentales
Título del ejercicio:	TRABAJOS
Título de la entrega:	Los delitos informáticos en el Ecuad…
Nombre del archivo:	Tesis_Juan_Cadme_Final.pdf
Tamaño del archivo:	265.79K
Total páginas:	39
Total de palabras:	9,094
Total de caracteres:	51,679
Fecha de entrega:	29-sep-2020 11:27p.m. (UTC-0500)
Identificador de la entrega:	1401026337

Universidad Católica de Cuenca

REPÚBLICA DEL ECUADOR

UNIVERSIDAD CATÓLICA DE CUENCA
Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE CIENCIAS SOCIALES

CARRERA DE DERECHO

Título: Los delitos informáticos en el Ecuador, análisis comparativo con la Legislación de Colombia.

Trabajo de investigación previo a la obtención del Título de Abogado de los Tribunales de Justicia de la República.

AUTOR: JUAN CARLOS CADME ARCENTALES
Número de cédula 0301775052

TUTOR:
DR. EDWIN ARÉVALO MSC.

AÑO: 2020

Página 1 | 39

Los delitos informáticos en el Ecuador, análisis comparativo con la Legislación de Colombia

INFORME DE ORIGINALIDAD

6%	6%	1%	1%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	anahuanca.blogspot.com Fuente de Internet	1%
2	www.derautor.gov.co Fuente de Internet	<1%
3	www.nocheyniebla.org Fuente de Internet	<1%
4	www.aadat.org Fuente de Internet	<1%
5	www.refworld.org Fuente de Internet	<1%
6	www.dspace.uce.edu.ec Fuente de Internet	<1%

CENTRO DE IDIOMAS

ABSTRACT

This bibliographical research is interested in knowing the evolution of the different children and adolescents' rights, determining them through a historical analysis of society and States, since for this it has been essential to go back to the middle, ancient and contemporary age until reaching our days, in order to be able to specify and examine the broad evolution that has been achieved in the development of society, children and adolescents' rights; due to their importance, even States like ours give prevalence and application to any other right or guarantee enshrined, as well as the state responsibility to ensure its application, and the creation of public policies that fulfill this obligation in their favor, so they are even guaranteed in the Ecuadorian legal system.

It is necessary to determine the evolution and background of children and adolescents' rights that inspired a constant battle to create legal bodies to protect and guarantee the life quality of them.

Keywords: rights, protective measures, infringement, children, State.

La Troncal, 6 de octubre de 2020

EL CENTRO DE IDIOMAS DE LA UNIVERSIDAD CATÓLICA DE CUENCA, CERTIFICA QUE EL DOCUMENTO QUE ANTECEDE FUE TRADUCIDO POR PERSONAL DEL CENTRO PARA LO CUAL DOY FE Y SUSCRIBO

LIC. NANCY PAOLA ORELLANA PARRA
Documento certificado digitalmente por Emergencia Sanitaria en Ecuador por COVID-19
La Troncal - Ecuador
2020-10-06 15:06-05:00

Lic. Nancy Orellana P., MSc.
COORDINADORA CENTRO DE IDIOMAS LA TRONCAL

www.ucacue.edu.ec

Cuenca: Av. de las Américas y Tarqui. *Telf: 2830751, 2824365, 2826563* **Azogues:** Campus Universitario "Luis Cordero El Grande", (Frente al Terminal Terrestre). *Telf: 593 (7) 2241 - 613, 2243-444, 2245-205, 2241-587* **Cañar:** Calle Antonio Ávila Clavijo. *Telf: 072235268, 072235870* **San Pablo de la Troncal:** Cdla. Universitaria km.72 Quinceava Este y Primera Sur *Telf: 2424110* **Macas:** Av. Cap. José Villanueva s/n *Telf: 2700393, 2700392*

Universidad Católica de Cuenca

Universidad Católica de Cuenca

La Bibliotecaria de la extensión La Troncal

CERTIFICA:

Que, **Juan Carlos Cadme Arcentales** portador(a) de la cédula de ciudadanía Nº 0301775052 de la Carrera de **Derecho** no adeuda libros, a esta fecha.

La Troncal, 05 de octubre de 2020

F: .....
Ing. Thalia Alvarado Ortega

UNIDAD ACADÉMICA "SAN PABLO" DE LA TRONCAL
ucacue
COMUNIDAD EDUCATIVA AL SERVICIO DEL PUEBLO
BIBLIOTECA

www.ucacue.edu.ec
Cuenca: Av. de las Américas y Tarqui. *Telf: 2830751, 2824365, 2826563* **Azogues:** Campus Universitario "Luis Cordero El Grande", (Frente al Terminal Terrestre). *Telf: 593 (7) 2241 - 613, 2243-444, 2245-205, 2241-587* **Cañar:** Calle Antonio Ávila Clavijo. *Telf: 072235268, 072235870* **San Pablo de la Troncal:** Cdla. Universitaria km.72 Quinceava Este y Primera Sur *Telf: 2424110* **Macas:** Av. Cap. José Villanueva s/n *Telf: 2700393, 2700392*

DR. EDWIN AREVALO VASQUEZ, MCS.
DOCENTE DE LA CARRERA DE DERECHO DE LA UNIVERSIDAD CATÓLICA DE CUENCA
SEDE LA TRONCAL

INFORMA:

Que el señor estudiante **JUAN CARLOS CADME ARCENTALES**, ha realizado su trabajo de investigación "**LOS DELITOS INFORMÁTICOS EN EL ECUADOR, ANÁLISIS COMPARATIVO CON LA LEGISLACIÓN COLOMBIANA**", previo a la obtención del título de Abogado de los tribunales de justicia.

En virtud de lo expuesto, se aprueba el trabajo de investigación con la calificación de 50/50, con lo cual, solicito se proceda con el trámite pertinente.

Atentamente,

DR. EDWIN AREVALO VASQUEZ, MCS.
DOCENTE-TUTOR

Universidad Católica de Cuenca

PERMISO DEL AUTOR DE TESIS PARA SUBIR AL REPOSITORIO INSTITUCIONAL

Yo **JUAN CARLOS CADME ARCENTALES** portadora de la cédula de ciudadanía Nro. 030177505-2 en calidad de autor y titular de los derechos patrimoniales del trabajo de titulación: **"LOS DELITOS INFORMÁTICOS EN EL ECUADOR,ANÁLISIS COMPARATIVO CON LA LEGISLACIÓN COLOMBIANA",** de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de Los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos, Así mismo; autorizo a la Universidad para que realice la publicación de éste trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

La Troncal, a 30 de Octubre del 2020

SR. JUAN CARLOS CADME A.