UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES
CARRERA DE DERECHO

TEMA:

LOS DELITOS INFORMÁTICOS Y LA VIOLACIÓN DE LOS DERECHOS CONSTITUCIONALES DEL OFENDIDO

Trabajo de Graduación, como requisito previo a la obtención del Título de Abogado de los Juzgados y Tribunales de la República del Ecuador.

Autor:

Diego Fernando Posso López

Tutor:

Ab. Jorge Sánchez Espín

AMBATO- ECUADOR

2014

TEMA:

LOS DELITOS INFORMÁTICOS Y LA VIOLACIÓN DE LOS DERECHOS CONSTITUCIONALES DEL OFENDIDO

APROBACIÓN DEL TUTOR

En calidad de Tutor del Trabajo de Investigación sobre el tema: "Los delitos informáticos y la violación de los derechos constitucionales del ofendido,", del señor Diego Fernando Posso López, Egresado de la Carrera de Trabajo Social, Comunicación Social o Derecho, de la Facultad de Jurisprudencia y Ciencias Sociales de la Universidad Técnica de Ambato, considero que dicho trabajo reúne los requisitos y méritos suficientes para ser sometido a la Evaluación del Tribunal de Grado, que el H. Consejo Directivo de la Facultad designe para su correspondiente estudio y calificación**.**

Ambato, 20 de Noviembre del 2013

…….

Dr. Jorge Sánchez Espín

TUTOR

APROBACIÓN DEL TRIBUNAL DE GRADO

Los miembros del Tribunal de Grado, APRUEBAN el Trabajo de Investigación sobre el tema: "Los delitos informáticos y la violación de los derechos constitucionales del ofendido", presentado por el señor Diego Fernando Posso López de conformidad con el Reglamento de Graduación para obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

Ambato……..

Para constancia firman:

f)…….

Presidente

f)……. f)…….

Dr. Klever Pazmiño **Dr. Rubén Guevara**

Miembro **Miembro**

AUTORÍA

Los criterios emitidos en el trabajo de investigación: "Los delitos informáticos y la violación de los derechos constitucionales del ofendido", como también los contenidos, ideas, análisis, conclusiones y propuestas son de responsabilidad del autor.

Ambato, 20 de Noviembre del 2013

EL AUTOR

……

Diego Fernando Posso López

C.C. 1003747068

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga de ésta tesis o parte de ella un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de la presente tesis, con fines de difusión pública, además apruebo la reproducción de esta tesis, dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor.

Ambato, 20 de Noviembre del 2013

EL AUTOR

……

Diego Fernando Posso López

C.C. 1003747068

DEDICATORIA

El presente trabajo investigativo lo dedico de manera especial a mi familia, quienes me han apoyado en las diversas situaciones de mi vida especialmente en mis estudios, gracias a su comprensión y apoyo incondicional han hecho posible que hoy logre culminar con éxito mi vida universitaria.

Diego Fernando Posso López

AGRADECIMIENTO

A mi familia por haber guiado mis pasos a lo largo de mi vida personal, familiar, social y universitaria; ya que, gracias a sus consejos sabios y sus bendiciones he logrado y seguiré logrando cristalizar con éxito cada una de mis metas.

A la Universidad Técnica de Ambato, por abrir sus puertas a la juventud estudiosa, y haberme brindado una superación intelectual y profesional.

A mis maestros, y en especial al Sr. Abogado Jorge Sánchez Espín, por dirigir acertadamente la ejecución de la presente investigación.

Diego Fernando Posso López

ÍNDICE GENERAL

CONTENIDO **Pág.**

CAPÍTULO
II. MARCO TEÓRICO

CAPÍTULO III.
METODOLOGIA

CAPÍTULO IV.
ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

CAPÍTULO V.
CONCLUSIONES Y RECOMENDACIÓN

CAPÍTULO VI.
PROPUESTA

ÍNDICE DE CUADROS

CONTENIDO **Pág.**

ÍNDICE DE GRÁFICOS

CONTENIDO **Pág.**

RESUMEN EJECUTIVO

La humanidad descubrió las ventajas que trae consigo la tecnología, el ser humano poco a poco, logró automatizar muchas de sus actividades, se ahorra tiempo y recursos con el empleo de lo que se denomina "inteligencia artificial".

Es difícil imaginar alguna actividad humana en la que no intervengan máquinas dotadas de gran poder de resolución, la informática, entendiéndola como el uso de computadoras y sistemas que ayudan a mejorar las condiciones de vida del hombre, la encontramos en todos los campos: en la medicina, en las finanzas, en el Derecho, en la industria, entre otras.

En la actualidad con la creación de la denominada "autopista de la información", el INTERNET, las posibilidades de comunicación e investigación se han acrecentado, se tiene acceso a un ilimitado número de fuentes de consulta y entretenimiento.

El problema radica en que, la conducta humana parece ser que está inclinada al delito, a conseguir satisfacción a sus deseos a toda costa.

Con el desarrollo de la informática, aparece también lo que se denomina como delito informático, por ende la investigación es la de evitar la violación de los derechos constitucionales del ofendido, en delitos informáticos en el cantón Ambato, provincia de Tungurahua.

INTRODUCCIÓN

El presente trabajo de grado tiene como tema: "Los delitos informáticos y la violación de los derechos constitucionales del ofendido**".**

La importancia de investigar el tema planteado radica básicamente en la necesidad de contribuir a la aplicación de una justicia equitativa e igualitaria, permitiendo que cada uno haga uso pleno de sus derechos.

Este trabajo investigativo está estructurado por capítulos.

El Capítulo I denominado EL PROBLEMA, contiene un análisis macro, meso y micro que hace relación al origen de la problemática con un panorama mundial, provincial y cantonal respectivamente, el árbol del problema, el análisis crítico, la prognosis, las interrogantes de la investigación, las delimitaciones, las unidades de observación, los objetivos tanto general como específicos.

El Capítulo II denominado MARCO TEÓRICO, se fundamenta en una visión filosófica, crítica, propositiva y legal del tema propuesto, además se plantea las hipótesis y el señalamiento de variables.

El Capítulo III denominado METODOLOGÍA, establece que la investigación se realizará desde un enfoque crítico propositivo, de carácter cuali-cuantitativo, y contiene la modalidad de la investigación, los niveles o tipos de la investigación, la población y muestra, la Operacionalización de variables, el plan de recolección de datos, el plan de procesamiento de información.

La modalidad de la investigación es bibliográfica, documental, de campo, de intervención social que nos permitirán estructurar predicciones llegando a modelos de comportamiento mayoritario.

El Capítulo IV denominado ANÁLISIS E INTERPRETACIÓN DE

RESULTADOS, incluye el análisis de los resultados obtenidos de la investigación mediante encuestas.

El Capítulo V contiene: CONCLUSIONES Y RECOMENDACIONES.

El Capítulo VI denominado PROPUESTA, contiene datos informativos, antecedentes de la propuesta, justificación, análisis de factibilidad, fundamentación, metodología, administración y prevención de la evaluación, todo esto con la finalidad de superar los problemas jurídicos y sociales, que se exteriorizan en la ejecución de delitos informáticos, así evitar la violación de los derechos constitucionales del ofendido.

Se concluye con la bibliografía, Linkografia y los anexos en los que se han incorporado los instrumentos que se aplicarán en la investigación de campo.

CAPÍTULO I

EL PROBLEMA

TEMA

Los delitos informáticos y la violación de los derechos constitucionales del ofendido.

PLANTEAMIENTO DEL PROBLEMA

CONTEXTUALIZACIÓN

Macro.

El uso de los ordenadores o computadores en el mundo jurídico comenzó en 1948, en la cibernética de Robert Wiener. El objeto de la Ley es la de regular los mensajes de datos, firmas electrónicas, servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos a través de redes de información, incluido el comercio electrónico (e-business) y lógicamente la protección a los usuarios de estos sistemas de cualquier mecanismo de distorsión.

Los efectos de la revolución digital se hacen sentir en los distintos sectores de la sociedad ecuatoriana como lo es en la economía, la política, la educación, el entretenimiento entre otras; así pues, éstos encontraron nuevas formas de interrelacionarse (compras on-line, chats, e-mail, educación a distancia, foros de discusión, etc.), y este fenómeno ha traído y traerá cambios profundos, por lo que es imprescindible estar preparados para enfrentar una evolución tecnológica acelerada, para que no se produzcan efectos negativos.

Sin lugar a duda en el Ecuador los delitos Informáticos implican actividades

criminales que en un primer momento se ha tratado de encuadrar en figuras típicas de carácter tradicional, tales como robo, hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, entre otros; sin embargo, debe destacarse que el uso indebido de las computadoras es lo que ha propiciado la necesidad de regulación por parte del derecho.

Por otro lado en el Ecuador en el año 2002 se expide la Ley de Comercio, Firmas Electrónicas y Mensajes de Datos, instrumento que da un marco jurídico a las innovaciones tecnológicas relacionadas con la transmisión de información utilizando medios electrónicos.

Con la expedición de esta Ley, aparecen otros delitos como es el sabotaje (SPAM) y los daños informáticos (CYBER CRIME), estas infracciones se incorporan al Código Penal Ecuatoriano, logrando así una protección concreta y específica a este tipo de actos, considerados desde abril de 2002 como delitos.

La Ley establece que los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Estos consisten en documentos que han sido enviados por un sistema electrónico, a los cuales se les da plena validez.

Meso.

En la Provincia de Tungurahua el avance tecnológico y el desconocimiento de la sociedad sobre su adecuado uso, hace necesario establecer mecanismos que permitan la persecución de actos ilícitos, cometidos utilizando medios tecnológicos (los denominados delitos informáticos); lamentablemente una de las grandes debilidades de nuestro sistema penal es no ir a la par con las necesidades actuales de nuestra sociedad, pese a ser éste uno de los temas de gran importancia, actualmente en el Código Penal se hace referencia al mismo únicamente en artículos agregados, lo que ha generado entre otras cosas, que vaya ascendiendo el porcentaje de víctimas del cometimiento de estos delitos.

El cometimiento de delitos informáticos, en la provincia de Tungurahua, ha

lesionado derechos constitucionales como son: el derecho a la intimidad personal y familiar que cada individuo posee, el derecho a conservar su patrimonio legalmente adquirido, entre otros, los mismos que serán materia de análisis a lo largo del presente trabajo investigativo crítico-propositivo.

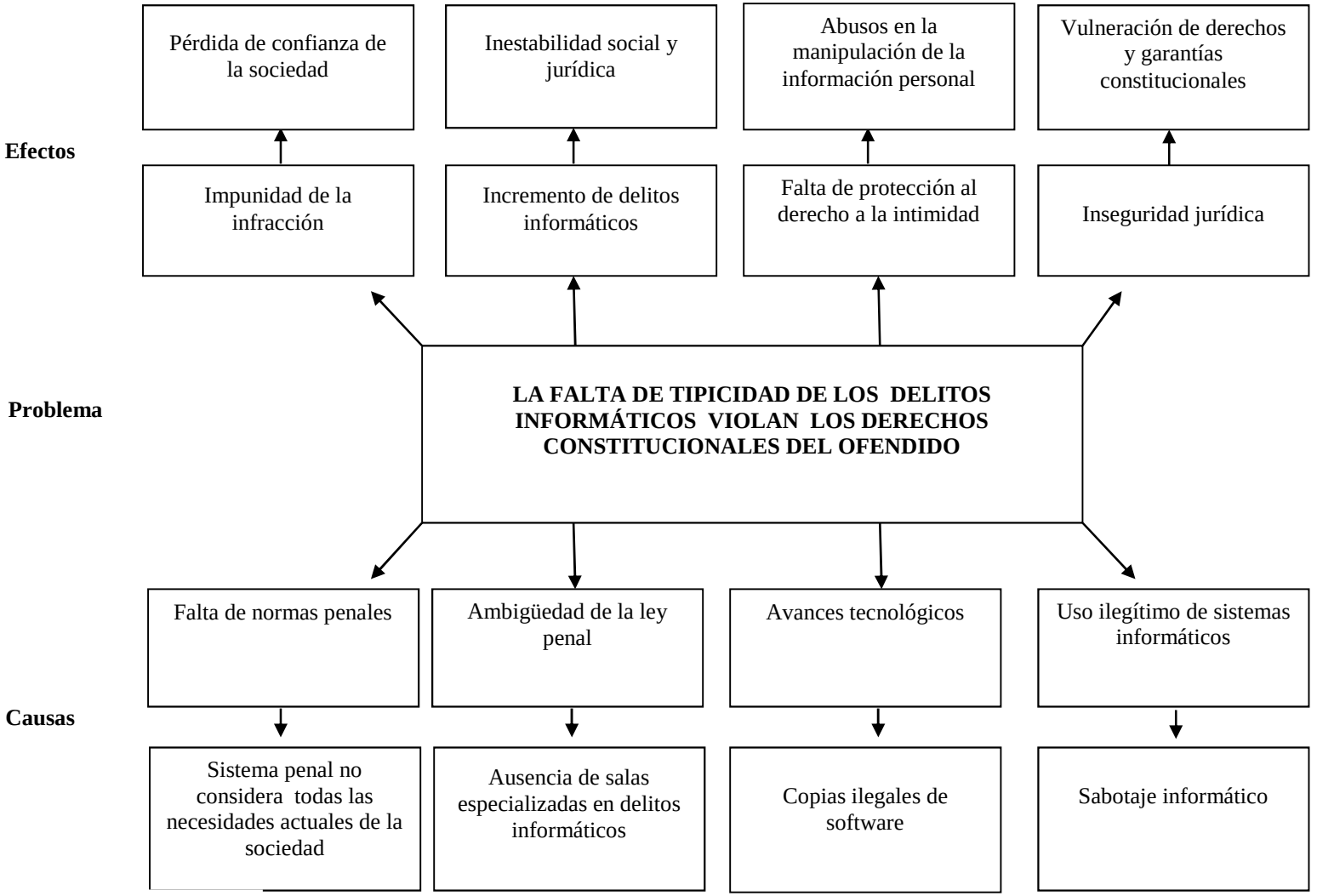
Micro.

Sin lugar a duda en la sociedad ambateña cada vez es más frecuente el uso fraudulento de sistemas, programas o redes informáticas, con el fin de causar un perjuicio económico; lo que, no solo afecta el patrimonio de los individuos sino también se vulnera su privacidad tanto personal como familiar.

Una de las razones por las que, el índice delincuencial en este tipo de delitos va en aumento es gracias a que la cuantía de los perjuicios así ocasionados no sólo es mayor que la obtenida por la delincuencia tradicional, sino que también es muy complicado llegar a descubrir a los autores intelectuales; hechos que se facilitan por la falta de ausencia de personal especializado en el tema, motivo por el que, este tipo de delitos en muchas ocasiones han quedado en la impunidad, generando progresivamente que la sociedad pierda la confianza en una justicia eficaz, eficiente y oportuna.

Gráfico Nº 1

ÁRBOL DEL PROBLEMA



Fuente: Investigador
Elaborado por: Investigador

ANÁLISIS CRÍTICO

En la sociedad de la información todos los ámbitos del quehacer cotidiano del ser humano se ven invadidos, manejados o al menos afectados por el hecho tecnológico. Esta "tecno dependencia" se observa con claridad en la industria, la banca, el comercio y más recientemente en casi toda actividad pública como en los sistemas tributarios y electorales. Las ventajas que ofrece el empleo de las nuevas tecnologías en la optimización de múltiples procesos, son incuestionables, pero como casi todo, tiene su lado oscuro han evolucionado también las formas de infringir la ley, dando lugar a la diversificación de delitos tradicionales como la aparición de nuevos actos ilícitos (Delitos Informáticos).

La dependencia humana por las computadoras como herramienta de trabajo en la más amplia diversidad de los campos, muchas de las actividades que solían efectuarse manualmente, ahora pueden realizarse a través de medios informáticos, lo cual es una gran ventaja, pues se ahorra tiempo y dinero en la mayoría de los casos, pero así como se puede aprovechar la tecnología para actos lícitos, también sirve para cometer delitos. Por lo tanto, es común ver que se presentan una gran cantidad de delitos en los que se ve involucrado algún sistema de cómputo ya sea como medio, o fin.

La investigación propuesta sirve para poder identificar un marco general sobre la conceptualización de las infracciones informáticas, con las regulaciones existentes (leyes) para el manejo de los delitos informáticos, mediante la comprensión de los lineamientos establecidos en nuestra legislación y tener un claro entendimiento de los criterios y medidas contempladas.

PROGNOSIS

Si no se toma alternativas para la prevención de la ejecución de delitos informáticos se seguirá vulnerando los Derechos Constitucionales del ofendido, así como el incremento de delitos informáticos, inestabilidad social, inseguridad

jurídica, falta de protección al derecho de intimidad, abusos en la manipulación de la información personal, uso ilegítimo de sistemas informáticos y falta de control por parte de la autoridad pública, por lo que, la situación jurídica del país estaría expuestas a constantes transgresiones.

FORMULACIÓN DEL PROBLEMA

¿Cómo los delitos informáticos violentan los derechos constitucionales del ofendido?

INTERROGANTES DE LA INVESTIGACIÓN

1.- ¿Cuáles son los tipos de delitos informáticos?

2.- ¿Cuáles son los derechos Constitucionales del ofendido?

3.- ¿Cómo plantear una alternativa para evitar que los delitos informáticos genera la violación de los Derechos Constitucionales del ofendido?

DELIMITACIÓN DEL OBJETO DE LA INVESTIGACIÓN

Delimitación de contenido

CAMPO: Jurídico – social

ÁREA: Código Penal

ASPECTO: Violación de los derechos constitucionales de la personas ofendidas por delitos informáticos.

Delimitación Espacial

La investigación se realizará en la ciudad de Ambato, provincia de Tungurahua.

Delimitación Temporal

El trabajo de investigación se lo desarrollará durante el periodo comprendido del de Enero a Diciembre del año 2012

Unidades de Observación

- Funcionarios de la Fiscalía Provincial de Tungurahua.
- Jueces de Garantías Penales del cantón Ambato.
- Jueces de Tribunales de Garantías Penales de Tungurahua.
- Abogados en libre ejercicio profesional en el cantón Ambato.
- Víctimas de delitos informáticos del cantón Ambato.

JUSTIFICACIÓN

El uso fraudulento de las computadoras con el fin de obtener ganancias, la destrucción de programas, el acceso y el uso inadecuado de la información, repercute en la violación a la privacidad.

La investigación propuesta sirve para poder identificar un marco general sobre la conceptualización de las infracciones informáticas, con las regulaciones existentes (leyes) para el manejo de los delitos informáticos, mediante la comprensión de los lineamientos establecidos en nuestra legislación y tener un claro entendimiento de los criterios y medidas contempladas.

Por la falta de personal investigativo especializado en delitos informáticos se tiene como consecuencia que las personas que cometen estos ilícitos, los delincuentes informáticos, quedan en total impunidad. De tal forma que los perjuicios que se

ocasionan a las personas naturales y personas jurídicas de derecho público y privado son de gran magnitud en el Ecuador, por lo que la investigación determina cuáles delitos son sancionados en nuestra legislación y qué ilícitos deben agregarse a la misma. Necesidad manifestada por los requerimientos de los Tribunales de Justicia.

Así mismo, la presente investigación pretende canalizar la búsqueda e incorporación de nuevos delitos informáticos y en especial los que se dan en ciudad de Ambato, Provincia de Tungurahua; definir cuáles se enmarcan en procesos judiciales actuales; cuáles son los que penalizan en nuestra legislación Ecuatoriana y hechos delictivos que deberían agregarse en el futuro como delitos penales constituye una exigencia del entorno jurídico, técnico y social de la actualidad.

OBJETIVOS

Objetivo General

Conocer la realidad de los Delitos Informáticos en el cantón Ambato en cuanto a su regulación y formación de los profesionales que investigan dichos delitos, así como también identificar los retos y brechas que deben ser superadas por el Ecuador para el tratamiento de los mismos.

Objetivos Específicos

1. Conceptualizar la naturaleza de las Infracciones Informáticas y tipificar de acuerdo a sus características principales.

2. Analizar los derechos constitucionales que tiene el ofendido en los delitos informáticos.

3. Establecer alternativas de soluciones para sancionar los delitos informáticos y evitar la vulneración de los derechos constitucionales del ofendido.

CAPÍTULO II

MARCO TEÓRICO

ANTECEDENTES INVESTIGATIVOS

Realizado un recorrido por la biblioteca de la Universidad Técnica de Ambato; se encuentra que en la Facultad de Jurisprudencia y Ciencias Sociales de la Universidad Técnica de Ambato no existe ningún trabajo con el tema que se está desarrollando, por consiguiente; esto significa que este trabajo es original y se lo está realizando con el soporte de libros, códigos, internet y demás fuentes que aporten con la ayuda a este tema.

Además se ha realizado un recorrido por las principales Bibliotecas del cantón Ambato donde se encontraron libros de mucho apoyo a la investigación como es en los libros de filosofía, Manual de Manejo de Evidencias Digitales y Entornos Informáticos, de derechos humanos, como también se apoya la investigación en leyes conexas al Código Penal.

Son libros de mucha importancia que me ayudaron a identificar por que se violentan los derechos constitucionales del ofendido en los delitos informáticos, en mi estudio de investigación, se va a analizar las causas y los efectos jurídicos y sociales que ocasionan los delitos informáticos y como crear medidas de amparo para proteger los derechos constitucionales de los individuos, ya que la inexistencia de una unidad especializada en la Fiscalía Provincial de Tungurahua en delitos informáticos no permite una adecuada investigación vulnerando así éstos derechos.

FUNDAMENTACIÓN FILOSÓFICA

El presente trabajo se fundamenta en el paradigma critico - propositivo de Ausbel, Vigotski y Brunner, “todo proceso del individuo está en el desarrollo próximo”, y en la teoría de Luís Legaz Lacambra “ el derecho constituye un punto de vista sobre la justicia existe en tanto que nace con la mira de realizar la justicia”; por cuanto es transcendental elaborar una ley para regular las actuaciones de las personas dentro de la sociedad, teniendo como objetivo primordial la realización de la justicia.

La presente investigación no solo está encaminada a establecer qué derechos constitucionales del ofendido son violentados, sino a través de una reforma legal acceder sin restricciones a dichos derechos.

El paradigma de la investigación Crítico –Propositivo, es la base principal para la presente investigación, por el constante cambio de esquemas sociales y tecnológicos. Es crítico porque cuestiona los esquemas jurídicos y sociales; y, es propositivo porque la investigación no se detiene en la observación de hechos, sino plantea alternativas de solución.

FUNDAMENTACIÓN LEGAL

Antes de conocer las regulaciones que se han establecido en el Ecuador y que están relacionadas con las tecnologías de la información, se indicará cual es la estructura general de dichas regulaciones, para ello, se toma como referencia la Pirámide Kelseniana, que es un recurso que permite ilustrar, la jerarquía de las normas jurídicas.

En la legislación del Ecuador bajo el contexto de que la información es un bien jurídico a proteger, se mantienen leyes y decretos que establecen apartados y especificaciones acorde con la importancia de las tecnologías.

Constitución de la República del Ecuador – 2008:

Es la ley suprema del Estado, es el conjunto de normas y principios fundamentales que constituyen la base de todo el sistema jurídico ecuatoriano y cuya finalidad es organizar la vida social, ninguna ley o norma secundaria puede contradecir o violar ningún precepto contemplado en ella, la ley debe someterse a la Constitución.

Artículo 1.- "El Ecuador es un Estado constitucional de derechos y justicia, democrático, soberano, independiente, unitario, intercultural, plurinacional y laico. Se organiza en forma de república y se gobierna de manera descentralizada…"

Comentario: Al determinar el Estado como constitucional de derechos y justicia, pretende no sólo que se aplique la ley, sino que prevalezca por sobre todo la justicia y los derechos de los ciudadanos

Artículo 10.- "Las personas, comunidades, pueblos, nacionalidades y colectivos son titulares y gozaran de los derechos garantizados en la Constitución y en los instrumentos internacionales…."

Comentario: Todos los ciudadanos ecuatorianos tenemos derecho a que se nos reconozca en cualquier situación jurídica o social nuestros derechos y garantías contempladas en la Constitución y en los tratados internacionales sin ninguna clase de discriminación.

Artículo 52.- "Las personas tienen derecho a disponer de bienes y servicios de óptima calidad y a elegirlos con libertad, así como a una información precisa y no engañosa sobre su contenido y características.

La ley establecerá los mecanismos de control de calidad y los procedimientos de defensa de las consumidoras y consumidores; y las sanciones por vulneración de

estos derechos, la reparación e indemnización por deficiencias, daños o mala calidad de bienes y servicios, y por la interrupción de los servicios públicos que no fuera ocasionada por caso fortuito o fuerza mayor".

Comentario: De acuerdo a esta disposición legal todos los ciudadanos tenemos derecho a disponer de bienes y servicios de óptima calidad y las personas naturales o jurídicas están en la obligación de prestar el servicio con responsabilidad so pena de incurrir en acciones de carácter civil de indemnización de daños y perjuicios, en el caso que se hayan retirado de una cuenta bancaria dinero perteneciente a un cuentacorrentista o ahorrista, la institución financiera está obligada a devolver el dinero que se sustrajeron personas inescrupulosas y por ningún motivo podría perder el cliente.

Artículo 53.- "Las empresas, instituciones y organismos que presten servicios públicos deberán incorporar sistemas de medición de satisfacción de las personas usuarias y consumidoras, y poner en práctica sistemas de atención y reparación.
El Estado responderá civilmente por los daños y perjuicios causados a las personas por negligencia y descuido en la atención de los servicios públicos que estén a su cargo, y por la carencia de servicios que hayan sido pagados".

Comentario: De acuerdo a esta norma legal las entidades que presten servicios públicos deberán entregar a los usuarios y consumidores seguridad y confianza en el servicio que prestan al ciudadano, caso contrario el Estado responderá civilmente por la defectuosa atención hacia la persona, y a su vez el ente estatal podrá iniciar el derecho de repetición en contra de la entidad que incurrió en la mala prestación del servicio.

Artículo 54.- "Las personas o entidades que presten servicios públicos o que produzcan o comercialicen bienes de consumo, serán responsables civil y penalmente por la deficiente prestación del servicio, por la calidad defectuosa del producto, o cuando sus condiciones no estén de acuerdo con la publicidad efectuada o con la descripción que incorpore.

Las personas serán responsables por la mala práctica en el ejercicio de su profesión, arte u oficio, en especial aquella que ponga en riesgo la integridad o la vida de las personas".

Comentario: De acuerdo a esta norma constitucional las personas naturales o jurídicas que presten servicios públicos o que vendan productos al usuario y que sean de mala calidad serán responsables civil y penalmente por los daños ocasionados al consumidor por la mala calidad y deficiencia en los bienes ofertados a las personas, además se sanciona la mala práctica en la profesión en la que se ponga en peligro inminente la vida de un ciudadano.

Artículo55.- **"**Las personas usuarias y consumidoras podrán constituir asociaciones que promuevan la información y educación sobre sus derechos, y las representen y defiendan ante las autoridades judiciales o administrativas.
Para el ejercicio de este u otros derechos, nadie será obligado a asociarse".

Comentario: Todas las personas tienen derecho a asociarse y el Estado está en la obligación de estimular la creación y organizaciones en especial de trabajadores, a fin de que ejerzan sus legítimos derechos ante las autoridades de la Función Judicial o ante las autoridades de tipo administrativo como son Gobiernos Autónomos Descentralizados, Gobiernos Provinciales, entidades bancarias y otros.

Artículo 66.- "Se reconoce y garantizará a las personas:
Numeral 19.- El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.
Numeral 20.- El derecho a la intimidad personal y familiar…"

Comentario: En esta carta constitucional se reconoce a los ciudadanos su derecho

a la protección de sus datos, es decir nadie puede invadir la vida privada de los individuos.

Ley Orgánica de Transparencia y Acceso a la Información Pública

La Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP), publicada en el Registro Oficial Suplemento # 337 del 18 de mayo del 2004, fue expedida con la finalidad de llevar a la práctica la disposición contenida en el Art. # 81 de la Constitución Política de 1998, en la que disponía qué "la información es un derecho de las personas que garantiza el Estado".

Artículo 1.- **"**El acceso a la información pública es un derecho de las personas que garantiza el Estado.

Toda la información que emane o que esté en poder de las instituciones, organismos y entidades, personas jurídicas de derecho público o privado que, para el tema materia de la información tengan participación del Estado o sean concesionarios de éste, en cualquiera de sus modalidades, conforme lo dispone la Ley Orgánica de la Contraloría General del Estado; las organizaciones de trabajadores y servidores de las instituciones del Estado, instituciones de educación superior que perciban rentas del Estado, las denominadas organizaciones no gubernamentales (ONG's), están sometidas al principio de publicidad; por lo tanto, toda información que posean es pública, salvo las excepciones establecidas en esta Ley".

Comentario: La ley establece que todas las instituciones del sector público pongan a disposición de la ciudadanía, el libre acceso a la información institucional (estructura orgánica, bases legales, regulaciones, metas, objetivos, presupuestos, resultados de auditorías, etc.), a través de sus sitios web, bajo este mismo contexto las disposiciones contenidas en la Constitución de la República del Ecuador, en su capítulo tercero de las Garantías Jurisdiccionales de sus secciones cuarta y quinta de los Art. 91 y 92 sobre la acción de acceso a la información pública y acción de

Habeas Data, también se establece dichas garantías.

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

La Ley de Comercio Electrónico, Firmas Digitales y Mensaje de Datos fue publicada en el Registro Oficial N° 557 del 17 de Abril del 2002 en el que se dispone que los mensajes de datos tendrán, igual valor jurídico que los documentos escritos.

Artículo 1.- "Esta Ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas".

Artículo 57.- "Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley".

Comentario: La Ley contiene los principios jurídicos que regirán las transmisiones de los mensajes de datos, se le concede pleno valor y eficacia jurídica a los mensajes de datos, tanto a su información como a su contenido general. Se protege la confidencialidad de los mensajes de datos en sus diversas formas, señalando lo que se entenderá por tal concepto y su violación. Se equipara el documento escrito con el documento electrónico para el caso en que se requiera la presentación de un documento escrito, procediendo de igual manera con el documento original y la información contenida en él, siempre y cuando exista garantía de su conservación inalterable.

Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional

Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, fue publicada en el Registro Oficial N° 52 del 22 de Octubre del 2009.

Artículo 49.- “La acción de habeas data tiene objeto garantizar judicialmente a toda persona el acceso a los documentos, datos genéticos, bancos o archivos de datos personales e informe que por sí misma, o sobre sus bienes, estén en poder de entidades públicas o de personas naturales o jurídicas privadas en soporte material o electrónico. Asimismo, toda persona tiene derecho a conocer el uso que se haga de dicha información, su finalidad, el origen y destino, y el tiempo de vigencia del archivo o banco de datos”.

Comentario: En la Constitución de la República del Ecuador, en su capítulo tercero de las Garantías Jurisdiccionales de su sección quinta Art. 92, también se establece el recurso jurídico de Habeas Data.

Código Penal

Es aquel que contiene disposiciones generales sobre los delitos y faltas, las personas responsables y las penas, en lo referente a mi tema tengo a bien transcribir los artículos que han sido incorporados en el Código, Registro Oficial Suplemento 147 de 22-Ene-1971. Contiene hasta la reforma del 15-Feb-2012:

(A continuación del Artículo 202) Artículo innumerado 1.- “El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica…”

(A continuación del Artículo 202) Artículo innumerado 2.- “La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica”.

Artículo 262.- “Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados sin razón de su cargo”.

(A continuación del Artículo 353) Artículo innumerado 1.- “Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio; alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:

1.- Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;
2.- Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;
3.- Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.

El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este Capítulo”.

(A continuación del Artículo 415) Artículo innumerado 1.- “El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica…”.

(A continuación del Artículo 520) Artículo innumerado 7.- “Quien produjere, publicare o comercializare imágenes pornográficas, materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato, u organizare espectáculos en vivo, con escenas pornográficas en que participen los mayores de catorce y menores de dieciocho años, será reprimido con la pena de seis a nueve años de reclusión menor ordinaria, el comiso de los objetos y de los bienes producto del delito, la inhabilidad para el empleo, profesión u oficio…”.

(A continuación del Artículo 553) Artículo innumerado 1.- “Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes el electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos”.

(A continuación del Artículo 553) Artículo innumerado 2.- “La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios:
1. Inutilización de sistemas de alarma o guarda;
2. Descubrimiento o descifrado de claves secretas o encriptados;
3. Utilización de tarjetas magnéticas o perforadas;
4. Utilización de controles o instrumentos de apertura a distancia; y,
5. Violación de seguridades electrónicas, informáticas u otras semejantes”.
Artículo 563.- “… Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizado medios electrónicos o telemáticos…”
Artículo 606.- “Serán reprimidos con multa de siete a catorce dólares de los

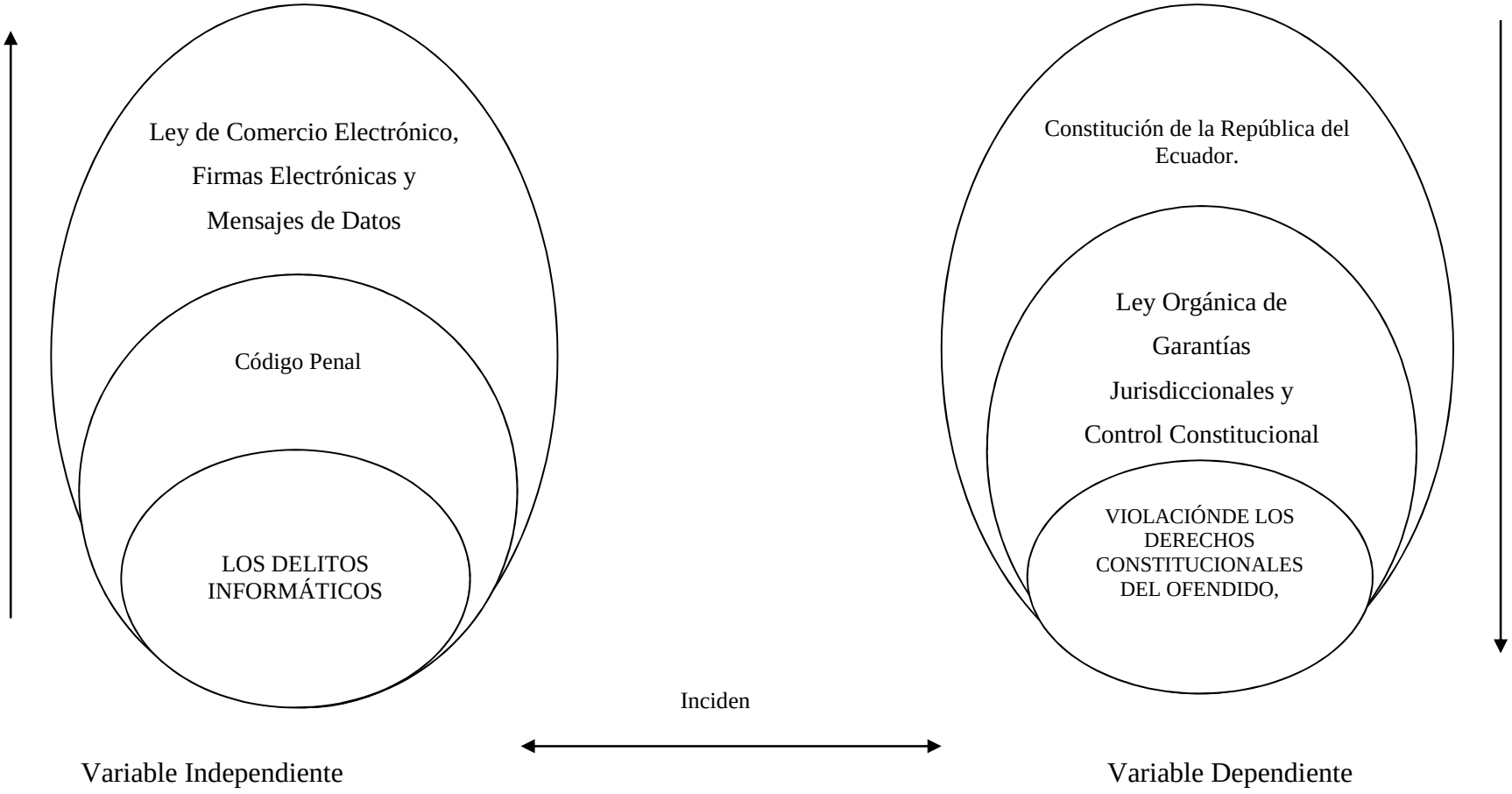
Estados Unidos de Norte América y con prisión de dos a cuatro días, o con una de estas penas solamente:

(A continuación del numeral 19)... Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos".

Comentario: El Ecuador ha dado sus primeros pasos con respecto a las leyes existentes, en las que se contemplan especificaciones de la información y la informática, lo que se considera un avance importante ante el desarrollo tecnológico que se ha tenido en los últimos años en el país, pero es evidente que aún falta mucho por legislar, para asegurar que no queden en la impunidad los actos que se cometan relacionados con las tecnologías; lamentablemente en los artículos señalados anteriormente se puede evidenciar que la Ley Penal no considera a los delitos informáticos como tales, sino ha tratado de encuadrar a través de artículos innumerados, en figuras típicas de carácter tradicional, tales como robo, estafas y otras defraudaciones, falsificaciones, perjuicios, inviolabilidad del secreto, usurpación de atribuciones y abuso de autoridad, explotación sexual, entre otros; lo que ha ocasionado la violación de los derechos constitucionales de las personas víctimas de estos delitos.

CATEGORÍAS FUNDAMENTALES

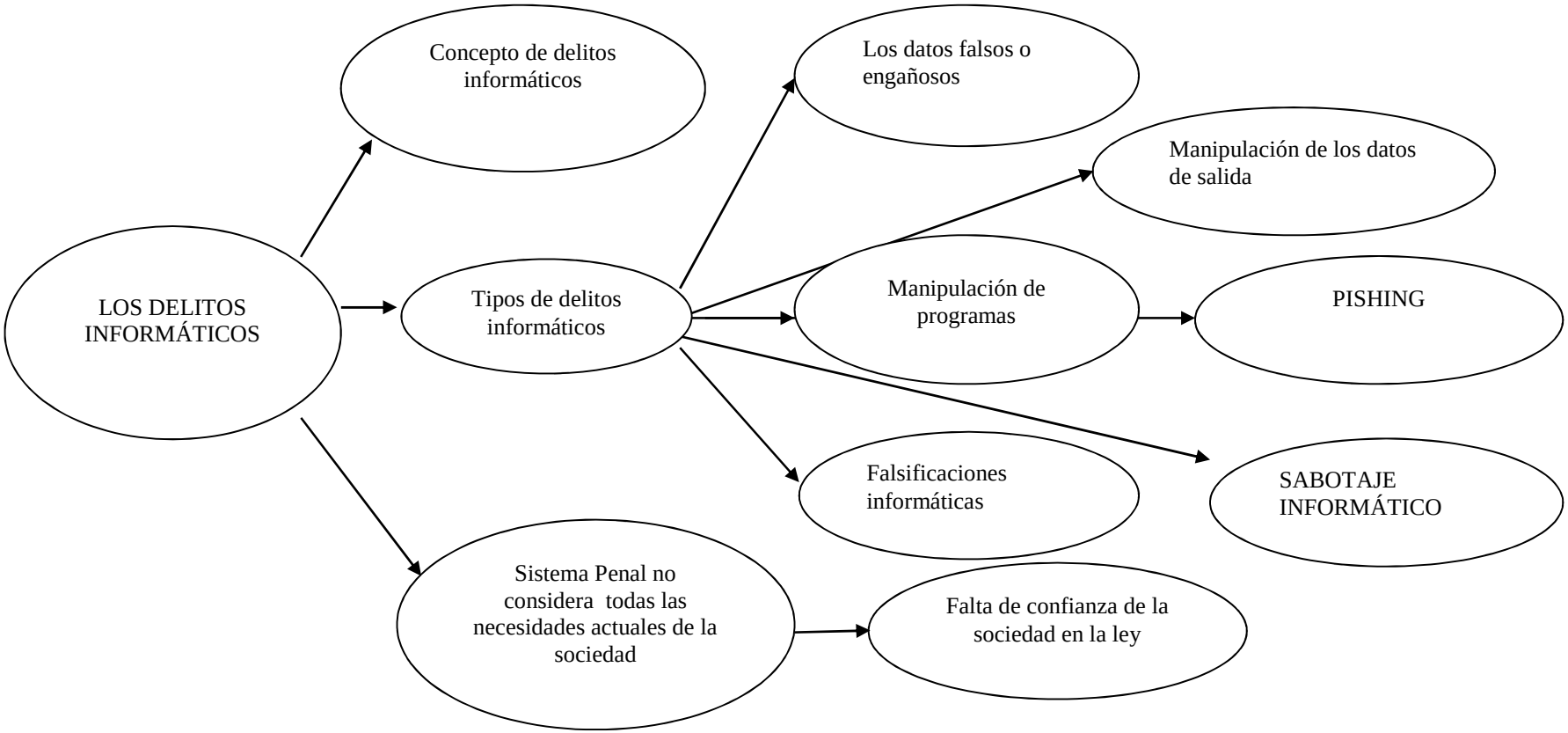
Gráfico Nº 2



Elaborado por: Diego Fernando Posso López
Fuente: Diego Fernando Posso López

CONSTELACIÓN DE IDEAS DE LA VARIABLE INDEPENDIENTE

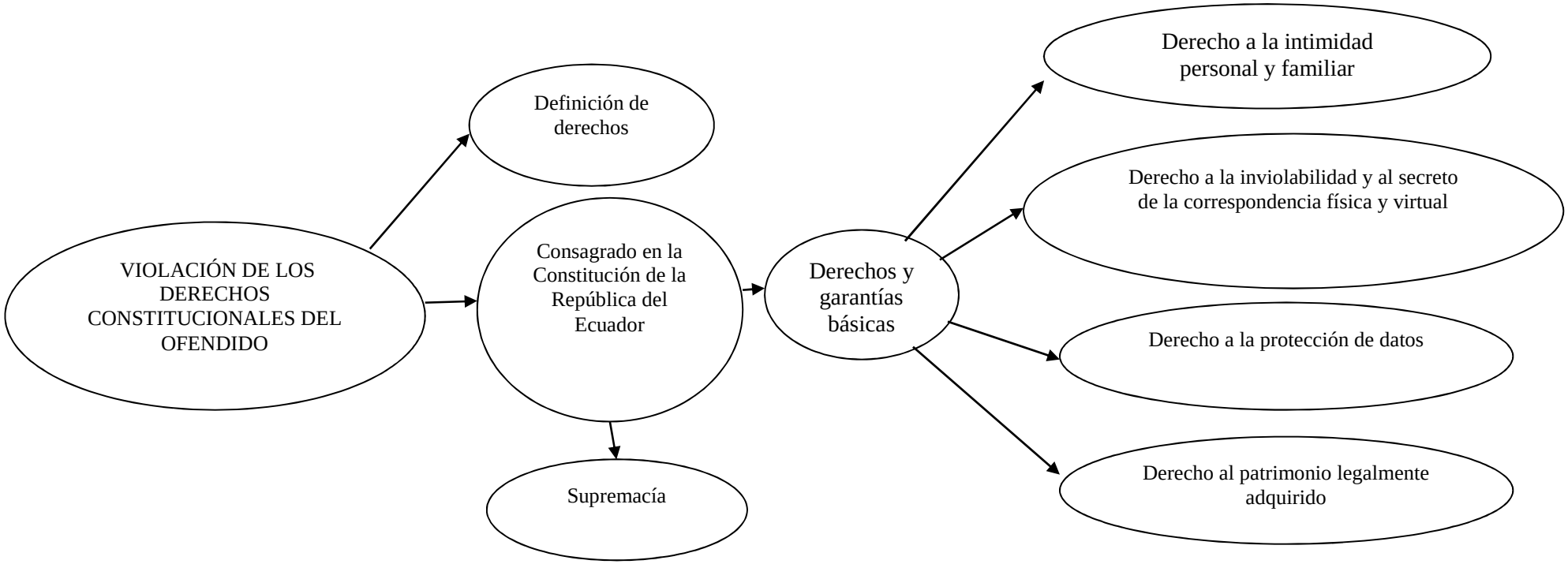
Gráfico Nº 3



Fuente: Diego Fernando Posso López
Elaborado por: Diego Fernando Posso López

CONSTELACIÓN DE IDEAS DE LA VARIABLE DEPENDIENTE

Gráfico Nº 4



Fuente: Diego Fernando Posso López
Elaborado por: Diego Fernando Posso López

Generalidades de los Delitos Informáticos

En la sociedad de la información todos los ámbitos del quehacer cotidiano del ser humano se ven invadidos, manejados o al menos afectados por el hecho tecnológico. Esta "tecno dependencia" se observa con claridad en la industria, la banca, el comercio y más recientemente en casi toda actividad pública como en los sistemas tributarios y electorales. Las ventajas que ofrece el empleo de las nuevas tecnologías en la optimización de múltiples procesos, son incuestionables, pero como casi todo, tiene su lado oscuro.

ANTECEDENTES DE LOS DELITOS INFORMÁTICOS

Con el creciente desarrollo y popularización de la tecnología en los años setenta, empiezan los problemas de seguridad en los sistemas. En efecto, con la creación de aplicaciones interactivas de sistemas online y de tratamientos en tiempo real, comienzan a verse casos de uso fraudulento del aparato o del software sobre datos comunes. De aquí la necesidad de las contraseñas identificativas de usuarios para controlar y restringir el acceso a los datos. Desde los años ochenta a la presente, se determina que los ataques informáticos se han triplicado en lo que tiene que ver con la seguridad dado el avance de la tecnología, el aumento de número de usuarios conectados a través de redes de comunicación y de ordenadores personales trabajando como terminales del computador central o en procesos locales online.

Todo eso hizo que los factores de riesgo de las empresas se incrementaran por pérdida de un activo tan importante como es la información. Lo cierto es que la realidad del fenómeno fraudulento por medio de, o con ocasión de la informática es preocupante, pese a la dificultad para obtener cifras reales lo que ha llevado a algunos a mitificar la criminalidad informática. No obstante, hay algo cierto: el fraude informático lesiona cualquier sector de la economía.

Las víctimas del fraude informático son de preferencia del sector bancario y le

siguen las grandes empresas. En piratería a los distribuidores, editores o autores del mismo.

El descubrimiento de la infracción es difícil porque a veces se programa la destrucción de datos para que ocurra meses más tarde. Casi siempre el fraude se descubre por azar, falta de previsión, negligencia o imprudencia del delincuente.

La prueba del hecho es con frecuencia difícil, porque casi nunca se dejan huellas (la informática se caracteriza por su "inmaterialidad"). El número de indagaciones previas es mínimo, tal vez por el temor de tener que pagar las costas del juicio.

La informatización de la sociedad contemporánea ha incidido en muchos comportamientos sociales: ha creado nuevos valores económicos (los bienes informacionales), ha cambiado las estrategias y escenarios de varias relaciones comerciales y profesionales, públicas y privadas.

DEFINICIÓN DE LOS DELITOS INFORMÁTICOS

Delitos Informáticos son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático.

El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha provocado nuevas posibilidades del uso indebido de las computadoras lo que ha creado la necesidad de regulación por parte del derecho.

Se considera que no existe una definición formal y universal de delito informático pero se han formulado conceptos respondiendo a realidades, "no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación

alude a una situación muy especial, ya que para hablar de “delitos” en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión “delitos informáticos” esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no han sido objeto de tipificación aún.

En 1983, la Organización y Cooperación y Desarrollo Económico (OCDE) inició un estudio de las posibilidades de aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas computacionales.

Se entiende Delito como: “acción penada por las leyes por realizarse en perjuicio de algo o alguien, o por ser contraria a lo establecido por aquéllas”.

Los delitos informáticos se realizan necesariamente con la ayuda de sistemas informáticos o tecnologías similares, atentando contra su integridad, confidencialidad o disponibilidad, como la propiedad común, intimidad, propiedad intelectual, seguridad pública, confianza en el correcto funcionamiento de los sistemas informáticos.

CLASIFICACIÓN DE DELITOS INFORMÁTICOS.

Existen muchos tipos de delitos informáticos, la diversidad de comportamientos constitutivos de esta clase de ilícitos es muy amplia según Camacho Losa, el único límite existente viene dado por la conjugación de tres factores: la imaginación del autor, su capacidad técnica y las deficiencias de control existentes en las instalaciones informáticas, por tal razón y siguiendo la clasificación dada por el estadounidense Don B. Parker más la lista mínima de ilícitos informáticos señalados por las Naciones Unidas, se ha tratado de lograr una clasificación que desde el punto de vista objetivo sea lo más didáctica posible al momento de tratar esta clase de conductas delictivas. A continuación se citan los delitos informáticos más conocidos:

ÁMBITO DE APLICACIÓN DELITO INFORMATICO

Como el campo de la informática es muy amplio, considero que el ámbito de aplicación del tema tratado se encuentra en las tecnologías de la información; datos, programas, documentos electrónicos, dinero electrónico.

Es importante indicar que también se aplica esta denominación a las infracciones que cometen los usuarios del INTERNET, con el envío de programas piratas, o la intromisión en sistemas gubernamentales de seguridad o en programas bancarios.

Se aplica con exactitud a la conceptualización del delito informático. Encontramos tantos conceptos del mismo, cuantos investigadores del tema existen. Citaré algunos de ellos

ELEMENTOS DEL DELITO INFORMÁTICO

- La computadora como medio o fin de la infracción; y,
- El uso de la informática para el cometimiento de la conducta delictiva

SUJETOS DEL DELITO INFORMÁTICO

- Sujeto activo
- Sujeto pasivo

SUJETO ACTIVO

En este tipo de delitos, el sujeto activo debe tener conocimientos técnicos de informática, es decir, en cierto modo, una persona con nivel de instrucción elevado, para poder manipular información o sistemas de computación.

SUJETO PASIVO

En el caso del delito informático pueden ser: individuos, instituciones de crédito, gobiernos, en fin entidades que usan sistemas automatizados de información.

Las Naciones Unidas reconocen como delitos informáticos los siguientes

Fraudes cometidos mediante manipulación de computadoras:

- Manipulación de datos de entrada.
- Manipulación de programas.
- Manipulación de los datos de salida.

Falsificaciones informáticas: Cuando se alteran datos de los documentos almacenados en forma computarizada, cuando se usan las computadoras para efectuar falsificaciones de documentos de uso comercial

LEGISLACIONES INTERNACIONALES

- Alemania
- Austria
- Francia y
- Estados Unidos

Si necesitamos hacer una consulta sobre Derecho Civil, Derecho Penal, Derecho Administrativo, y demás ramas jurídicas, podemos remitirnos a obras de tratadistas en estos temas. Al referirnos al Delito Informático, la única fuente de consulta, por el momento, constituye las legislaciones de los países desarrollados en tecnología.

ALEMANIA: A partir del 1 de Agosto de 1986, se adoptó la Segunda Ley contra la Criminalidad Económica del 15 de Mayo de 1986, en la que se contempla los siguientes delitos: espionaje de datos, estafa informática, falsificación de datos probatorios, alteración de datos, sabotaje informático, utilización abusiva de cheques o tarjetas de crédito.

AUSTRIA: Ley de reforma del Código Penal de 22 de Diciembre de 1987, que contempla los siguientes delitos: destrucción de datos, estafa informática.

FRANCIA: Ley Nº 88-19 de 5 de enero de 1988 sobre el fraude informático, así como también: acceso fraudulento a un sistema de elaboración de datos, sabotaje informático, destrucción de datos, falsificación de datos informatizados, uso de documentos informatizados falsos

ESTADOS UNIDOS: En 1994, adoptó el Acta Federal de Abuso Computacional (18U.S.C.Sec.1030) que modificó el Acta de Fraude y Abuso Computacional de 1986, con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y qué no es un virus, un gusano, un Caballo de Troya, y en que difieren de los virus…

La nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, al sistema informático, a las redes, información, datos o programas.

CONVENIOS INTERNACIONALES

TRATADO DE LIBRE COMERCIO DE AMÉRICA DEL NORTE (TLC), firmado por México, Estados Unidos, Canadá en 1993, con un apartado sobre propiedad intelectual, la sexta parte del capítulo XVII, en el que se contemplan los derechos de autor, patentes, otros derechos de propiedad intelectual y procedimientos de ejecución.

El Acuerdo General de Aranceles Aduaneros y Comercio (GATT), en su ronda uruguaya, en este acuerdo en el artículo 10, relativo a los programas de ordenador y compilaciones de datos, se establece que este tipo de programas, ya sean fuente u objeto, será protegido como creaciones de carácter intelectual.

En Europa se ha constituido la BUSINESSSO FTWAREA LLIANCE (BSA), que es una asociación que actúa legalmente contra la piratería informática en Europa, Asia y Latinoamérica

En la actualidad la legislación en el Ecuador lo único que se reprime como delito informático es la utilización del hardware y el software pirata, campaña lanzada con el auspicio de MICROSOFT, empresa transnacional interesada en recaudar mayores divisas por el uso de sus programas.

El delito informático es difícil de perseguir por cuanto, por las cualidades del sujeto activo de este nuevo tipo de infracciones, las huellas del mismo son borradas con cierta facilidad.

El Derecho tiene como finalidad normar la conducta humana. Los actos del hombre cambian de acuerdo a la época, en la actualidad no existe institución, incluso hogar en el que no se encuentre un ordenador o un sistema informático.

Seguridad y tecnología en el desarrollo del comercio electrónico, la mayoría de las tecnologías de información actual se basan en su seguridad en la identificación de un nombre y una contraseña, sistema útil en una red cerrada, pero todo lo contrario en una red abierta como la de Internet, Dicho problema ha ocasionado la limitación en la oferta de productos y servicios que las entidades financieras o económicas pueden ofrecer a sus clientes por estos canales.

El problema parte del hecho que nuestra legislación se basa en el principio del Derecho Romano: "nulliun crimen nullium pena sinelege", precepto que se consagra en la ley del Ecuador, de que no existe delito si previamente no se encuentra determinada la conducta típica antijurídica en la ley, por tanto, en nuestro país no existe delito informático propiamente dicho.

FRAUDE:

El Fraude es una sustracción hecha maliciosamente a las normas de la ley o del contrato en perjuicio de alguien, es una de las causas de nulidad de los actos jurídicos.

Fraude en derecho su pone un ataque oblicuo a la ley, pues quien lo comete se ampara en una norma lícita equivale a engaño, que consiste en cualquier falta de verdad de vida simulación entre lo que se piensa o se dice o se hace creer, instigando o induciendo a otra persona a actuar en la forma que interesa, o en la falta de verdad en lo que se dice o se hace.

Fraude, es un acto cumplido intencionalmente, con la finalidad de herir los derechos o intereses ajenos. Ejemplo, ocultación o malversación; fraude del deudor contra sus acreedores; ventaja indirecta con sentida por el de sujetos.

Debemos advertir que los diferentes tipos de fraude que vamos a tratar a continuación, no se encuentran tipificados en nuestro Código Penal, sino que los hemos extraídos de las legislaciones de otros países.

Sin embargo, estos fraudes se dan en nuestro país, pero al no estar tipificados en nuestro ordenamiento jurídico y al tener la misma apariencia que la estafa, los jueces y tribunales de garantías penales se ven en la necesidad de asimilarlos a la misma, para poder sancionarlos.

Los que se asemejan a la estafa, y son los que queremos que se sancionen separadamente de la estafa por poseer sus características propias, son los siguientes:

- Fraude procesal.
- Fraude informático.
- Fraude en los cajeros automáticos.
- Fraude bancario.

El artículo 374 del Código Penal Italiano define al fraude procesal de la siguiente manera: “El perito que, en la ejecución de un dictamen pericial, o el que, en el curso de un proceso civil, administrativo o penal, o anterior a este último, cambien artificiosamente el estado de lugares, de cosas o de personas, con el fin de engañar al juez en una diligencia de inspección o de reconstrucción judiciales, serán

castigados, si el hecho no estuviere previsto como infracción por alguna disposición legal especial, con reclusión de seis meses a tres años".

El artículo 182 del Código Penal Colombiano define al fraude procesal así: "El que por cualquier medio fraudulento induzca en error a un empleado oficial para obtener sentencia, resolución o acto administrativo contrarios a la ley, incurrirá en prisión de uno a cinco años".

Es decir, que el fraude procesal es realizado por cualquier persona, que interesada en resolver un asunto jurídico que se está conociendo en alguna institución judicial, provoque un engaño a través de informaciones falsas para obtener un beneficio en consecuencia de esa información, la cual no habría sido obtenida si la información brindada hubiera sido la verídica.

Los elementos objetivos del fraude procesal son:

A) El empleo de medios fraudulentos en procesos judiciales o administrativos
B) Provocar error en un empleado oficial.

El empleo de medios fraudulentos en una actuación judicial se caracteriza por presentar al oficial respectivo, las cosas o hechos, diferentes de cómo pasaron realmente, es decir, contrarios a la verdad.

El empleo de medios fraudulentos puede consistir en la manifestación de testimonios falsos, peritajes carentes de veracidad, alteración de registros contables entre otros.
El fraude procesal se considera hecho desde el instante en que el sujeto en una actuación procesal, utiliza medios fraudulentos, aunque el error que comete el funcionario se produzca con posterioridad.

La falta o error, debe materializarse a través de una resolución judicial, no basta con que se mantenga en la cabeza del empleado público.

La clasificación que a mi juicio considero la más adecuada y acertada es la del norteamericano Parker, ya que es una de las que ha tenido más difusión y aceptación a escala mundial. Esta clasificación es la siguiente:

CLASIFICACIÓN DEL NORTEAMERICANO PARKER

a) Introducción de datos falsos (data diddling).
b) El Caballo de Troya (Troyan Horse).
c) La técnica del salami (rounding down).
d) Puertas falsas (trap doors).
e) Bombas lógicas.
f) Ataques asíncronos (asynchronous attacks).
g) Recogida de información residual.
h) Divulgación no autorizada de datos no reservados (data eakage).
i) Toma no autorizada de información (Piggybacking and Imperonation)
j) Pinchado de líneas (wiretapping).
k) Simulación y modelado (Simulation and Modeling).

INTRODUCCIÓN DE DATOS FALSOS (DATA DIDDLING): Es el método más sencillo y más utilizado habitualmente, consiste en manipular las transacciones de entrada al ordenador con el fin de introducir movimientos falsos en todo o en parte, o en eliminar transacciones verdaderas que deberían haberse introducido.

Para realizar este tipo de delito no se necesita tener conocimientos técnicos especiales, es decir que basta con conocer las deficiencias de control del sistema informatizado de datos. Para evitar estas conductas delictivas será necesario establecer medidas de prevención y determinación que aseguren controles internos eficientes.

EL CABALLO DE TROYA (TROYAN HORSE): Este método consiste en introducir dentro de un programa de uso habitual una rutina o conjunto de

instrucciones, por supuesto no autorizadas, para que dicho programa actúe en ciertos casos de una forma distinta a como estaban previsto.

Ejemplo de esta técnica seria aquel en el cual en una entidad bancaria se introduce una modificación en el programa de tratamiento de cuentas corrientes, para que siempre que se consulte el saldo de alguna cuenta determinada, lo multiplique por mil, o cualquier cantidad, autorizándose pagos o transferencias por montos muy superiores al saldo real.

LA TÉCNICA DEL SALAMI (ROUNDING DOWN): Método usado en instituciones donde se producen movimientos de dinero (transferencia electrónica de fondos), y que consiste en la sustracción de pequeñas cantidades de activos de distintas procedencias haciendo un redondeo de las respectivas cuentas, y depositando luego en otras cuentas específicas.

SUPERZAPPING: Se denomina así al uso no autorizado de un programa de utilidad para alterar, borrar, copiar, insertar, o utilizar en cualquier forma no permitida los datos almacenados en el ordenador o en los soportes magnéticos.

Este método se asimila a una llave no autorizada que abre cualquier archivo de la computadora por más protegida que este.

PUERTAS FALSAS (TRAP DOORS): Es una práctica acostumbrada en el desarrollo de aplicaciones complejas que los programadores introduzcan interrupciones en la lógica de los programas con objeto de chequear en medio de los procesos si los resultados intermedios son correctos, producir salidas de control con el mismo fin o guarda resultados intermedios en ciertas áreas para comprobarlos más tarde.

BOMBAS LÓGICAS: El método consiste en introducir en un programa un conjunto de instrucciones no autorizadas, para que en una fecha o circunstancia predeterminadas ejecuten desencadenando la destrucción de información

almacenada en el ordenador, distorsionando el funcionamiento del sistema, provocando paralizaciones intermitentes, etc.

Según algunos autores, este es el método más utilizado por empleados informáticos descontentos, que antes de abandonar el lugar donde trabajan introducen "bombas de tiempo", para que éstas produzcan daños en un período posterior a su retiro de la empresa.

Se asemeja a la técnica del Caballo de Troya, pero, según Camacho Losa, la diferencia fundamental radica en que el método del Caballo de Troya se utiliza generalmente para cometer un fraude, mientras, las llamadas bombas lógicas se emplean con fines de sabotaje, venganza, con el afán de hacer daño, sin otro beneficio que el placer de perjudicar.

ATAQUES ASÍNCRONOS (ASYNCHRONOUS ATTACKS): Basados en la forma de funcionar los sistemas operativos y sus conexiones con los programas de aplicación a los que sirven y soportan en su ejecución. Es un fraude de alto conocimiento técnico, muy difícil de detectar.

RECOGIDA DE INFORMACIÓN RESIDUAL: Este procedimiento se basa en aprovechar los descuidos de los usuarios o los técnicos informáticos para obtener información que ha sido abandonada sin ninguna protección como residuo de un trabajo real efectuado con autorización

TOMA NO AUTORIZADA DE INFORMACIÓN (PIGGYBACKING AND IMPERONATION): Consiste en acceder a áreas restringidas para sustraer información de una empresa, aprovechando que el empleado encargado del equipo no está presente.

PINCHADO DE LÍNEAS (WIRETAPPING): Esta modalidad consiste en "pinchar líneas de transmisión de datos y recuperar la información que circula por ellas", todo lo que se necesita es un pequeño cassette como grabador, un radio

portátil AM\FM, un módem para demodular las señales telefónicas analógicas y convertirla en digitales, y una pequeña impresora para listar la información que se ha captado.

SIMULACIÓN Y MODELADO (SIMULATION AND MODELING): En esta técnica se utiliza la computadora como instrumento para planificar y controlar un delito, mediante técnicas de simulación de situaciones y modelos de las mismas.

Es decir que este método consiste en la planificación y simulación de un delito informático antes de realizarlo, para ver que repercusión va a tener los asientos contables de una empresa. Existen otras clasificaciones como la de Klaus, que distingue cuatro grupos como son:

a) Manipulaciones.
b) Espionaje.
c) Sabotaje.
d) Hurto de tiempo.

MANIPULACIONES: Resultan poco importantes las manipulaciones en el hardware, al cual pertenecen los elementos mecánicos del equipo de procesamiento de datos

ESPIONAJE: En el ámbito del procesamiento de datos, el espionaje económico se ve favorecido por el hecho de que las informaciones se encuentran archivadas en un espacio mínimo y pueden ser transferidas sin ningún problema a otro soporte.

El espionaje mediante computadoras, según el autor, no es utilizado únicamente con propósitos económicos por empresas rivales, sino también con finalidades políticas por Estados extranjeros

SABOTAJE: Incluyen las formas de destrucción y alteración de datos, así como los programas virus. Borran, suprimen o modifican sin autorización función eso

datos de computadoras con intención de obstaculizar el funcionamiento normal del sistema.

HURTO DE TIEMPO: Lo que debe corregirse en este caso no consiste tanto en el escaso consumo de energía eléctrica, ni en el mínimo desgaste del equipo de cómputos, sino en el notable enriquecimiento del autor proveniente del uso indebido de la computadora.

CARACTERÍSTICAS DE LOS DELITOS

- Son "delitos de cuello blanco", pues solo un limitado número de personas con conocimientos informáticos puede cometerlos. Generan grandes pérdidas de dinero, ya que se realizan en contra de personas o instituciones pudientes.

- Se realizan en poco tiempo y no es necesaria la presencia física para que pueda llegar a consumarse el delito.

- Son pocas las denuncias debido a la falta de reglamentación por parte del derecho sobre esta materia.

- Su comprobación es muy difícil.

- No siempre se cometen con la intención de perjudicar a otro.

- Últimamente se ha incrementado, por lo que creemos que es necesario que se regule para poder sancionarlo penalmente

- Lo que caracteriza al fraude informático es el medio a través del cual se comete, la computadora.

LOS ELEMENTOS CONSTITUTIVOS DEL FRAUDE INFORMÁTICO, según Camacho Losa, son:

a) Un sujeto, que es quien comete el fraude.
b) Un medio, que es el sistema informático.
c) Un objeto, que es el bien que produce el beneficio ilícito.

CASOS MÁS FRECUENTES DE FRAUDE INFORMÁTICO son los siguientes:

EL FRAUDE EN LOS CAJEROS AUTOMÁTICOS: Los cajeros automáticos son máquinas electrónicas que controlan y programan una información de las que comúnmente realiza un cajero bancario La principal función de los cajeros automáticos es la de transferencia electrónica de fondos.

TRANSFERENCIA ELECTRÓNICA: La transferencia electrónica de fondos se configura con el traslado de una suma de dinero de una cuenta bancaria a otra a través de un sistema informático, mediante el uso de órdenes de crédito y débito, es decir, que la misma debe ser realizada con la intervención de un banco o de cualquier otra entidad financiera.

También notamos que la transferencia electrónica de fondos consiste en el traslado de crédito de una cuenta bancaria a otra y se realiza mediante un procesamiento electrónico, es decir, sin un desplazamiento de dinero en efectivo o líquido que viene a ser lo mismo.

CAJEROS AUTOMÁTICOS: Esto es posible por el uso de una tarjeta que registra los datos personales del cliente, como su número secreto de identificación. Las tarjetas de crédito constituyen documentos mercantiles, ya que son documentos que realizan una operación de comercio y tienen validez y eficacia para hacer constar derechos y obligaciones de ese carácter así como las actuaciones abusivas o ilícitas vinculadas a las tarjetas magnéticas pueden llevarse a cabo por el propio titular o por un tercero que sustrae la tarjeta, la encuentra o la falsifica

Las modalidades de manipulación de cajeros automáticos pueden consistir sobre el acceso a los mismos, ya sea por la utilización de la tarjeta por un tercero y utilización abusiva del cajero por el titular de la tarjeta.

Utilización de la tarjeta por un tercero: La utilización de una tarjeta magnética por un tercero sucede cuando una persona distinta a su titular la utiliza sin el conocimiento y consentimiento de éste.

Aquí la doctrina explica que hay fraude informático por haberse obtenido dinero por esta vía y haber causado un perjuicio a otro en provecho propio, mediante un comportamiento astuto que es la manipulación del cajero automático.

La obtención del dinero del cajero automático que ha conseguido el tercer o ha sido por la sustracción de la tarjeta.

La manipulación del cajero automático se logra utilizando una tarjeta de crédito que ha sido falseada, ya sea porque se le haya introducido a la misma alteraciones que modifiquen los datos de identificación de su titular o de su código.

Esto es así porque realmente no hay ninguna diferencia con que el dinero que se ha obtenido del cajero automático haya sido por el uso de una tarjeta robada que por el contrario.

Que dicha tarjeta haya sido alterada o falseada, ya que el banco realiza la misma disposición patrimonial con un consentimiento viciado, por la creencia errónea de estar entregando el dinero a su titular legítimo. El método que se usa para falsificar o alterar una tarjeta de crédito es cuando se manipula la misma introduciéndola en una máquina denominada pimpinadra, comúnmente conocida como *“el ladrillo”*

La función del ladrillo es copiar la información de la banda magnética de la tarjeta, y posteriormente dicha información es traspasada a un plástico parecido al otorgado por la entidad emisora de la tarjeta original.

Desgraciadamente, la prueba de estos fraudes siempre resulta difícil de obtener, y a falta de prueba no se puede demostrar la responsabilidad de la gente por lo que en la mayoría de los casos dicho fraude queda impune.

Fraudes informáticos: Ahora analizaremos los dos tipos de fraude más comunes que se dan a través de la informática pero aparentemente, los grupos organizados que cometen este tipo de fraude se encuentran en ventaja por estar más equipados que los mismos organismos de seguridad.

Algunas de las cosas que se pueden hacer para mejorar esta situación es actualizar y ser más exigentes en la selección del personal del departamento de seguridad y que el Estado incentive la promulgación de leyes que sean conformes al tiempo en que vivimos.

“Las instituciones financieras como personas jurídicas que manejan valores, lógicamente son los objetivos principales de la delincuencia tanto común como organizada, como aquella cometida por sus propios empleados, en contra de las mismas, y lo cual es un hecho palpable de la evolución y profesionalización del delito”.

Esto tiene razón de ser porque es en estos lugares donde más cantidad de dinero se maneja y donde las transferencias de los mismos se hacen por medio de la tecnología, la cual es el medio para la comisión del fraude bancario. Este fraude es realizado muchas veces por los empleados de la institución, ya que son ellos mismos quienes hacen las transacciones y pueden verse tentados por la cantidad de dinero que manejan.

El sujeto activo comete este fraude utilizando los sistemas computarizados, y lo que generalmente obtiene es el dinero o los documentos de la institución bancaria.

DERECHOS CONSTITUCIONALES VIOLENTADOS POR LA FALTA DE TIPICIDAD DE DELITOS INFORMÁTICOS

CONCEPTO DE DERECHO:

El Derecho como la más importante estructura dentro de la sociedad, sin el cual no es posible el orden, puede ser estudiado desde tres puntos de vista:

1.- Como Ciencia del derecho o Dogmática Jurídica;

2.- Como Teoría General del Derecho; y,

3.- Como Filosofía.

1.- Como Ciencia Del Derecho O Dogmática Jurídica: cuando estudiamos el derecho convertido en figura histórica, positivan las reglas de aplicación a las cosas particulares.

La ciencia del derecho equivale al derecho positivo, ramas jurídicas contenidas en Código de Derecho, que en momento determinado rige la vida de la colectividad, no sólo la técnica sino la interpretación. El derecho es fruto de la necesidad social, de las relaciones sociales y crece adquiriendo desarrollos a medida que crecen dichas necesidades.

2.- Como Teoría General del Derecho: parte en su estudio de derecho positivo vigente y se extiende al análisis del derecho de los demás países.

En síntesis, la Teoría general del derecho, estudia el reencuentro de los principios jurídicos fundamentales que han sido clasificados como derechos,

constituyendo un cimiento, un pilar para obtener los conceptos fundamentales.

3.- Como Filosofía: Estudiando el derecho desde el punto de vista filosófico, cuando a su vez estudiamos la naturaleza, la esencia del derecho.

Estudiando el derecho se origina en la vida cotidiana del hombre y llega al desarrollo de sus normas conforme se desarrolla la sociedad.

DERECHO A LA INTIMIDAD PERSONAL Y FAMILIAR: La intimidad es la parte de la vida de una persona que no ha de ser observada desde el exterior, y afecta sólo a la propia persona. Se incluye dentro del "ámbito privado" de un individuo cualquier información que se refiera a sus datos personales, relaciones, salud, correo, comunicaciones electrónicas privadas, etc.

El derecho que poseen las personas de poder excluir a las demás personas del conocimiento de su vida privada, es decir, de sus sentimientos y comportamientos, una persona tiene el derecho a controlar cuándo y quién accede a diferentes aspectos de su vida particular, el derecho a la intimidad consiste en una especie de barrera o cerca que defiende la autonomía del individuo humano frente a los demás y, sobre todo, frente a las posibles injerencias indebidas de los poderes públicos, sus órganos y sus agentes.

De manera general, la privacidad puede ser definida como aquel ámbito de la vida personal de un individuo, que (según su voluntad) se desarrolla en un espacio reservado y debe mantenerse con carácter confidencial, por otro lado, y según el Diccionario de la Lengua de la Real Academia Española, privacidad se define como "ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión" e intimidad se define como "zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia".

El artículo 12 de la Declaración Universal de los Derechos Humanos, adoptada por la Asamblea General de las Naciones Unidas, establece que el derecho a la

vida privada es un derecho humano, y que: “Nadie será objeto de injerencias arbitrarias en su vida privada, ni su familia, ni cualquier entidad, ni de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”. Asimismo, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, adoptado por la Asamblea General de las Naciones Unidas, consagra, al respecto, lo siguiente: “1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación; 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques”.

En el ámbito regional, el artículo 11 de la Convención Americana sobre Derechos Humanos o Pacto de San José de Costa Rica establece una norma de protección de la honra y dignidad, al disponer: “1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad; 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación; 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques”.

Entonces, el derecho a la intimidad o privacidad consiste en la potestad o facultad que tiene toda persona para mantener en reserva, determinadas facetas de su personalidad, teniendo como uno de sus elementos esenciales la inviolabilidad de la vida privada, referida al escenario o espacio físico en el que se desenvuelve, como es el domicilio, los medios relacionales de comunicación y correspondencia, así como los objetos que contienen manifestaciones de voluntad o de conocimiento, no destinadas originalmente al acceso de personas ajenas o extrañas, lo que involucra escritos, fotografías u otros documentos, debe entenderse que el derecho a la inviolabilidad de correspondencia no se reduce únicamente al ámbito de la correspondencia escrita (es decir, la carta postal), sino que también se extiende a cualquier medio o sistema de comunicación privada de las personas, dado que con el desarrollo y avance de la tecnología, actualmente se

cuenta con múltiples formas y sistemas de comunicación privada como son la telefonía fija, telefonía móvil y el correo electrónico.

DERECHO A LA INVIOLABILIDAD Y AL SECRETO DE LA CORRESPONDENCIA FÍSICA Y VIRTUAL: este derecho asegura a los ciudadanos que no puede ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación. Nadie tiene derecho a investigar la correspondencia ajena y menos a divulgar lo que ahí se mencione salvo que un juez lo ordene.

DERECHO A LA PROTECCIÓN DE DATOS: Los datos de una persona implican información que refleja algunos aspectos íntimos de su vida y en tal sentido su manejo inadecuado puede tener repercusiones graves respecto de su integridad. Por esta razón, a nivel mundial, el tema de datos personales se ha tratado desde hace 30 años aproximadamente, y la legislación ecuatoriana no ha sido la excepción, aunque dicho tratamiento es novedoso y reciente. La protección de datos personales en el Ecuador nace como un nuevo Derecho con la Constitución del 2008, en el numeral 19, del artículo 66; es por eso que parte de este trabajo es, analizar el problema relativo al manejo y manipulación no autorizada de los datos de carácter personal; y por otra, la revisión de la importancia del respeto y reconocimiento de este derecho. Partiendo de la noción de que el marco constitucional ecuatoriano actual necesita mayor control para que el referido Derecho no se vulnere, es necesario precisar aquellas normas jurídicas ecuatorianas, relativas a la protección de datos personales, a fin de delimitar el ámbito de acción dentro del cual las personas pueden desenvolverse en lo que tiene que ver con la protección de la integridad personal, que se podrían vulnerar al momento de un mal uso o uso no autorizado de sus datos personales.

Hipótesis

Hipótesis 1

La falta de tipicidad de los delitos informáticos incide en la violación de los Derechos Constitucionales del ofendido.

Hipótesis Nula

La falta de tipicidad de los delitos informáticos no incide en violación de los Derechos Constitucionales del ofendido.

SEÑALAMIENTO DE LAS VARIABLES

Variable Independiente

Los Delitos Informáticos.

Variable Dependiente

Violación de los Derechos Constitucionales del ofendido.

CAPÍTULO III

METODOLOGÍA

ENFOQUE DE LA INVESTIGACIÓN

La investigación en su trabajo acoge el enfoque: crítico – propositivo de carácter cualitativo y cuantitativo; cuantitativo porque se recabará la información que será sometida a análisis estadístico, cualitativo porque estos resultados estadísticos pasarán a la criticidad con soporte del marco teórico.

MODALIDAD BÁSICA DE LA INVESTIGACIÓN

Bibliográfico - Documental

El trabajo de grado tendrá información secundaría del tema de investigación obtenidos a través de libros, textos, módulos, periódicos, revistas jurídicas, así como de documentos válidos y confiables a manera de información privada.

Linkográfico

El trabajo de grado a más de contar con información bibliográfica y documental, se basará en información digital obtenida a través de las páginas de internet.

De campo

El investigador acudirá a recabar información al lugar donde se genera los hechos para así poder actuar en el contenido y así pretender cambiar una realidad; además se realizará encuestas a las unidades de observación consideradas en el presente trabajo de grado.

NIVEL O TIPO DE INVESTIGACIÓN

Observatorio

Esta investigación se fundamentará en la técnica de la observación, es decir, se mirará atentamente el fenómeno, pues se familiariza con la situación actual para describir modelos de comportamiento que coadyuven al planteamiento de soluciones en la propuesta planteada.

La observación será directa, puesto que el investigador se pondrá en contacto con Funcionarios de la Fiscalía Provincial de Tungurahua, Jueces de Garantías Penales, Jueces de Tribunales de Garantías Penales, profesionales del derecho en libre ejercicio profesional, así como también víctimas de los delitos informáticos; por lo que será una observación participante, el investigador compartirá al recoger la investigación.

Se tratará de aplicar una observación estructurada en lo que se refiere a la metodología, con el fin de registrar en forma ordenada las situaciones que son motivo de estudio, se realizará una observación individual, debido a la intervención de un solo investigador para recopilar la información respectiva. Por el lugar, se utilizará la observación de Campo, puesto que el trabajo investigativo se cumplirá en el ambiente seleccionado.

Modelatorio

Se trabajará con normas inmersas en el área como son: Constitución de la República; Código Penal; Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos; Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional; Ley Orgánica de Transparencia y Acceso a la Información Pública.

Asociación de Variables

La investigación se llevará a nivel de asociación de variables porque permite estructurar predicciones a través de la medición de relaciones entre variables. Además se puede medir el grado de relación entre variables y a partir de ello determinar tendencias o modelos de comportamiento mayoritario.

POBLACIÓN Y MUESTRA

Población

Las unidades de observación determinadas en la delimitación son:

Cuadro Nº 1.- Población y muestra

ITEMS	UNIDADES DE OBSERVACIÓN	POBLACIÓN
1	Funcionarios de la Fiscalía Provincial de Tungurahua	4
2	Jueces de Garantías Penales del cantón Ambato	2
3	Jueces de Tribunales de Garantías Penales de Tungurahua	6
4	Abogados en libre ejercicio profesional en el cantón Ambato	10
5	Víctimas de delitos informáticos en el cantón Ambato	10
TOTAL		32

Fuente: Diego Fernando Posso López

Elaborado: Diego Fernando Posso López

Muestra

En virtud de que la población a investigarse Funcionarios de la Fiscalía Provincial de Tungurahua, Jueces de Garantías Penales del cantón Ambato, Jueces de Tribunales de Garantías Penales de Tungurahua, Abogados en libre ejercicio

profesional y Víctimas de delitos informáticos del cantón Ambato, no sobrepasa el número de cien elementos, no amerita aplicar ninguna fórmula de estadística, por tanto se constituye la muestra.

OPERACIONALIZACION DE LAS VARIABLES

VARIABLE INDEPENDIENTE: Los Delitos Informáticos.

Cuadro Nº 2.- Los delitos informáticos

CONCEPTUALIZACIÓN	DIMENSIÓN	INDICADORES	ÍTEMS BÁSICOS	TÉCNICAS E INSTRUMENTOS
Delito Informático es el acto mediante el cual se utiliza sistemas y medios informáticos para el cometimiento de una infracción.	➢ Sistema Judicial ➢ Personas ➢ Sociedad	➢ Constitución de la República del Ecuador ➢ Código Penal ➢ Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos	¿Cómo incide los delitos informáticos en el sistema judicial? ¿Cómo investigar los daños causados a las personas víctimas de delitos informáticos?	• Encuesta • Cuestionario

Fuente: Diego Fernando Posso López

Elaborado: Diego Fernando Posso López

VARIABLE DEPENDIENTE: Violación de los Derechos Constitucionales del Ofendido.

Cuadro Nº 3.- Violación de los derechos constitucionales

CONCEPTUALIZACIÓN	DIMENSIÓN	INDICADORES	ÍTEMS BÁSICOS	TÉCNICAS E INSTRUMENTOS
Derechos Constitucionales son el conjunto de normas de convivencia, establecidas en la Constitución para regular las relaciones entre las personas, y entre las personas y la administración.	➢ Persona ➢ Sociedad ➢ Estado	➢ Constitución de la República del Ecuador ➢ Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional ➢ Ley Orgánica de Transparencia y Acceso a la Información Pública	¿Por qué se genera la violación de los derechos constitucionales del ofendido en delitos informáticos? ¿Cómo afecta a la sociedad, la violación de los derechos constitucionales del ofendido de delitos informáticos?	• Encuesta • Cuestionario

Fuente: Diego Fernando Posso López

Elaborado: Diego Fernando Posso López

RECOLECCIÓN DE INFORMACIÓN

Encuesta.

Es un estudio observacional en el cual el investigador busca recaudar datos por medio de un cuestionario prediseñado, y no modifica el entorno ni controla el proceso que está en observación. Los datos se obtienen a partir de realizar un conjunto de preguntas normalizadas dirigidas a una muestra representativa o al conjunto total de la población estadística en estudio, formada a menudo por personas, empresas o entes institucionales, con el fin de conocer estados de opinión, características o hechos específicos. El investigador debe seleccionar las preguntas más convenientes, de acuerdo con la naturaleza de la investigación.

La encuesta será aplicada en el cantón Ambato, Provincia de Tungurahua a las siguientes personas:

- Funcionarios de la Fiscalía Provincial de Tungurahua;
- Jueces de Garantías Penales del cantón Ambato;
- Jueces de Tribunales de Garantías Penales de Tungurahua;
- Abogados en libre ejercicio profesional; y,
- Víctimas de delitos informáticos del cantón Ambato.

Validez y confiabilidad.

La validez de los instrumentos vendrá dado por la técnica llamada "Juicio de Expertos"; mientras que su confiabilidad se la hará a través de la aplicación de una prueba piloto a un grupo reducido de iguales características del universo a ser investigado, para detectar posibles errores y corregirlos a tiempo, antes de su aplicación definitiva.

Cuadro Nº 4.- Recolección de la información

PREGUNTAS BÁSICAS	EXPLICACIÓN
1. - ¿Para qué?	Para alcanzar los objetivos de investigación
2.- ¿De qué personas u objetos?	Funcionarios de la Fiscalía Provincial de Tungurahua, Jueces de Garantías Penales del cantón Ambato, Jueces de Tribunales de Garantías Penales de Tungurahua, Abogados en libre ejercicio profesional y Víctimas de delitos informáticos del cantón Ambato
3. - ¿sobre qué aspectos?	Indicadores
4. - ¿Quién? ¿Quiénes?	Investigador
5.- ¿Cuándo?	De enero a diciembre de 2012
6.- ¿Donde?	Ciudad de Ambato, provincia de Tungurahua
7.- ¿Cuántas veces?	La prueba piloto y prueba definitiva
8.- ¿Qué técnica de recolección?	Encuesta
9.- ¿Con qué?	Cuestionario
10.- ¿En qué situación?	En las oficinas, en horas de trabajo.

Fuente: Investigador

Elaborado: Investigado

PLAN DE PROCESAMIENTO DE LA INFORMACIÓN

Los datos recopilados en la presente investigación, serán trasformados por medio de los siguientes procedimientos:

- Revisión crítica de la información recogida, es decir limpieza de información defectuosa, contradictoria, incompleta, no pertinente, etc.

- Repetición de la recolección, en ciertos casos individuales, para corregir fallas de constelación.

- Tabulación o cuadros según las variables.

- Cuadros de una sola variable, cuadro con creces de variables, etc.

- Manejo de información (reajustes de cuadros con casilla vacía o con datos tan reducidos cuantitativamente, que no incluyen significativamente los análisis).

- Estudio estadístico de datos para representación de resultados.

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS

- Análisis de resultados estadísticos, definiendo tendencias o relaciones importantes acorde a los objetivos e hipótesis.

- Interpretación de los resultados, apoyados en el marco teórico de acuerdo al aspecto pertinente.

- Comprobación de hipótesis.

- Establecimiento de conclusiones y recomendaciones.

Organización de Resultados

Para efectos de cumplir con la metodología propuesta, donde se indica que es factible, la investigación de campo se utilizó la Encuesta, diseñadas para investigar a las personas que tienen conocimiento, siendo estos: Funcionarios de la Fiscalía Provincial de Tungurahua; Jueces de Garantías Penales del cantón Ambato, Jueces de Tribunales de Garantías Penales de Tungurahua, Abogados en libre ejercicio profesional, y Víctimas de delitos informáticos del cantón Ambato.

Una vez aplicadas las encuestas, se realiza la tabulación respectiva y las demás actividades que este capítulo requieren, para dar mayor significación a la propuesta que pretende establecer como resultado del trabajo.

A continuación se detalla los resultados obtenidos de las encuestas mismas que están representadas mediante cuadros estadísticos, y el respectivo análisis e interpretación de acuerdo a cada pregunta formulada en el cuestionario.

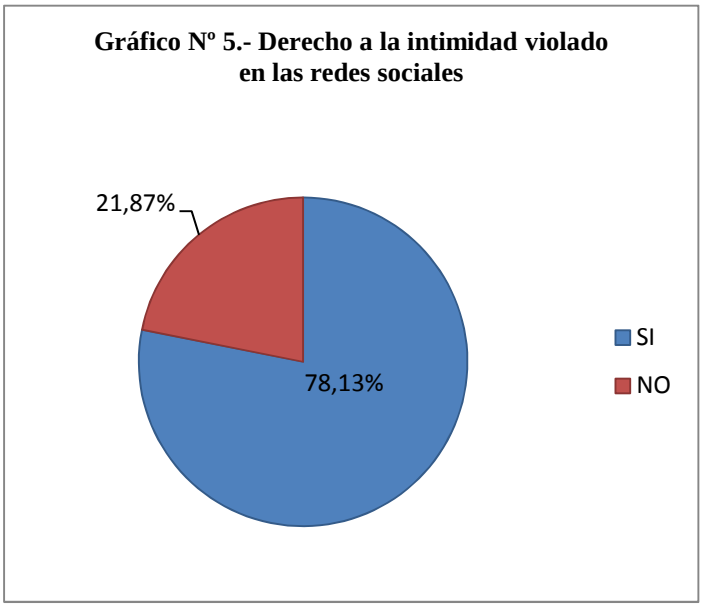
1.- ¿CREE QUE SU DERECHO A LA INTIMIDAD SE ENCUENTRA VIOLADO EN LAS REDES SOCIALES DE COMUNICACIÓN A TRAVÉS DE INTERNET?

Cuadro Nº 5.- Derecho a la intimidad violado en las redes sociales

ALTERNATIVA	FRECUENCIA	%
SI	25	78,13
NO	7	21.87
TOTAL	32	100

Elaborado: Diego Fernando Posso López

Fuente: Encuesta.



Fuente: Cuadro Nº5

Elaborado: Diego Fernando Posso López

Análisis. De la pregunta Nº 1 ¿**Cree que su derecho a la intimidad se encuentra violado en las redes social de comunicación a través de internet?**; veinticinco (25) de los encuestados contestaron que SI, que representan el 78,13%; y siete (7) de los encuestados contestaron que NO, que representan el 21,87%, constituyendo de esta manera el 100%.

Interpretación Lógica. Como se observa del análisis del resultado, el 78,13% de las personas consideran que si se encuentra violentado el derecho a la intimidad en las redes de comunicación a través de internet en la ciudad de Ambato; en tanto que el 21,87% de las personas no creen que se encuentre violentado el derecho a la intimidad en las redes de comunicación a través de internet en la ciudad de Ambato. Por lo tanto, se interpreta que no existe seguridad en las redes sociales de comunicación.

2.- ¿CONSIDERA QUE LAS COMPRAS A TRAVÉS DE INTERNET SON SEGURAS?

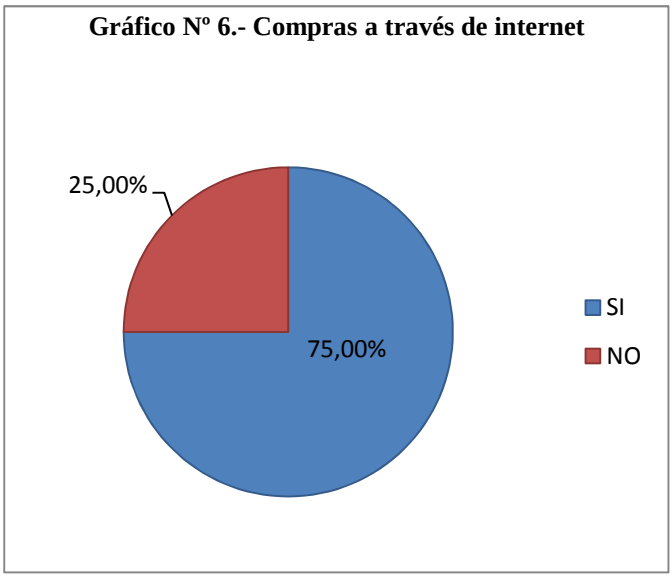
Cuadro Nº 6.- Compras a través de internet

ALTERNATIVA	FRECUENCIA	%
SI	8	25
NO	24	75
TOTAL	32	100

Elaborado: Diego Fernando Posso López

Fuente: Encuesta

Gráfico Nº 6.- Compras a través de internet



Fuente: Cuadro Nº6

Elaborado: Diego Fernando Posso López

Análisis. De la pregunta Nº 2 ¿Considera que las compras a través de internet son seguras?; ocho (8) de los encuestados contestaron que SI, que representan el 25%; y vente y cuatro (24) de los encuestados contestaron que NO, que representan el 75%, constituyendo de esta manera el 100%.

Interpretación Lógica. Como se observa del análisis del resultado, el 25% de las personas consideran **que las compras a través de internet son seguras** en la ciudad de Ambato; en tanto que el 75% de las personas no creen que **las compras a través de internet sean seguras** en la ciudad de Ambato. Por lo tanto, se interpreta que no existe seguridad en las en las compras atreves del internet.

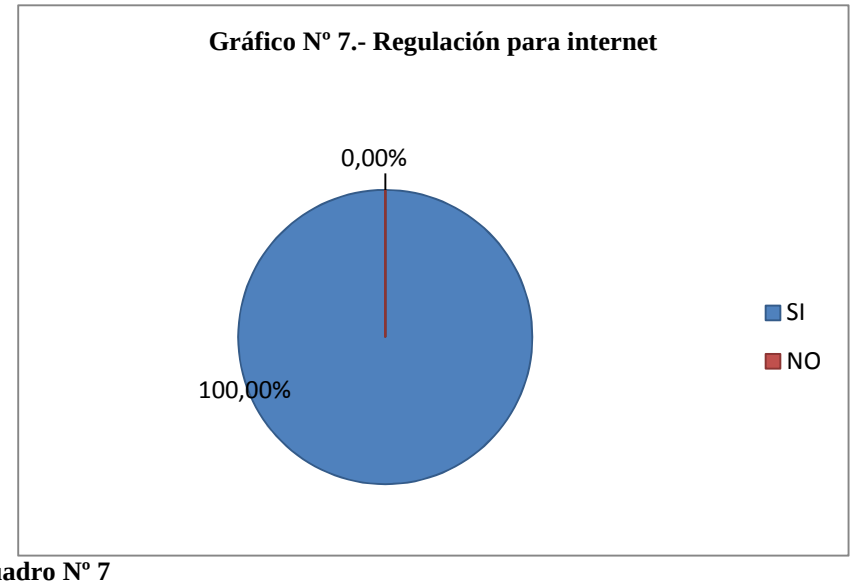
3.- ¿CREE NECESARIA UNA REGULACIÓN PARA INTERNET?

Cuadro Nº 7.- Regulación para internet

ALTERNATIVA	FRECUENCIA	%
SI	32	100
NO	0	0
TOTAL	32	100

Elaborado: Diego Fernando Posso López

Fuente: Encuesta



Fuente: Cuadro Nº 7

Elaborado: Diego Fernando Posso López

Análisis. De la pregunta Nº 3 ¿Cree necesaria una regulación para internet?; treinta y dos (32) de los encuestados contestaron que SI, que representan el 100%; y cero (0) de los encuestados contestaron que NO, que representan el 0%, constituyendo de esta manera el 100%.

Interpretación Lógica. Como se observa del análisis del resultado, el 100% de las personas consideran que es necesaria una regulación para internet en la ciudad de Ambato; en tanto que el 0% de las personas no cree necesaria una regulación para internet en la ciudad de Ambato. Por lo tanto, se interpreta que es necesaria una regulación en las redes sociales y en las compras por internet.

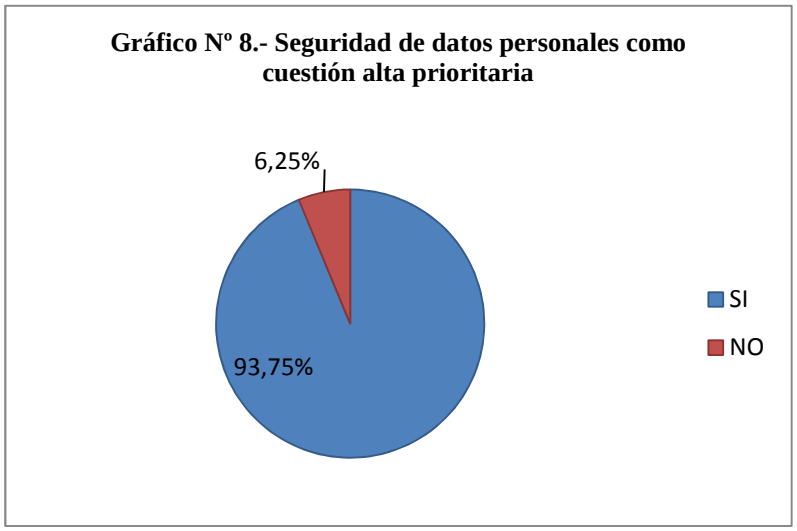
4.- ¿CONSIDERA USTED QUE LA SEGURIDAD A LOS DATOS PESONALES ES UNA CUESTIÓN ALTA PRIORIDAD?

Cuadro Nº 8.- Seguridad de datos personales como cuestión alta prioritaria

ALTERNATIVA	FRECUENCIA	%
SI	30	93,75
NO	2	6,25
TOTAL	32	100

Elaborado: Diego Fernando Posso López

Fuente: Encuesta



Fuente: Cuadro Nº8

Elaborado: Diego Fernando Posso López

Análisis. De la pregunta Nº 4 ¿Considera usted que la seguridad a los datos personales es una cuestión alta prioridad?; treinta (30) de los encuestados contestaron que SI, que representan el 93.75%; y dos (2) de los encuestados contestaron que NO, que representan el 6.25%, constituyendo de esta manera el 100%.

Interpretación Lógica. Como se observa del análisis del resultado, el 93,75 de las personas consideran que la seguridad a los datos personales es una cuestión alta prioridad en la ciudad de Ambato; en tanto que el 6,25% de las personas no considera que la seguridad a los datos personales sea una cuestión alta prioridad en la ciudad de Ambato. Por lo tanto, se interpreta que la seguridad de los personales es de extrema prioridad y que se debe mantener en absoluta reserva cada uno de estos bancos o bases de datos.

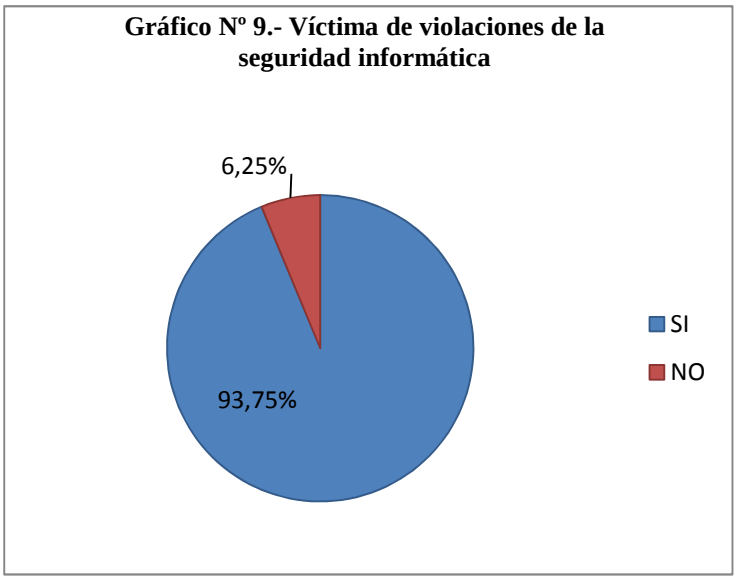
5.- ¿USTED HA SIDO VÍCTIMA DE VIOLACIONES DE LA SEGURIDAD INFORMÁTICA?

Cuadro Nº 9.- Víctima de violaciones de la seguridad informática

ALTERNATIVA	FRECUENCIA	%
SI	30	93,75
NO	2	6,25
TOTAL	32	100

Elaborado: Elaborado: Diego Fernando Posso López

Fuente: Encuesta



Fuente: Cuadro Nº 9

Elaborado: Diego Fernando Posso López

Análisis. De la pregunta Nº 5 ¿Usted ha sido víctima de violaciones de la seguridad informática**?**; treinta (30) de los encuestados contestaron que SI, que representan el 93.75%; y dos (2) de los encuestados contestaron que NO, que representan el 6.25%, constituyendo de esta manera el 100%.

Interpretación Lógica. Como se observa del análisis del resultado, el 93,75 de las personas consideran que han sido víctima de violaciones de la seguridad informática en la ciudad de Ambato; en tanto que el 6,25% de las personas no considera que hayan sido víctima de violaciones de la seguridad informática en la ciudad de Ambato. Por lo tanto, en la ciudad de Ambato tenemos un porcentaje alto de las personas que han sufrido de ataques informáticos.

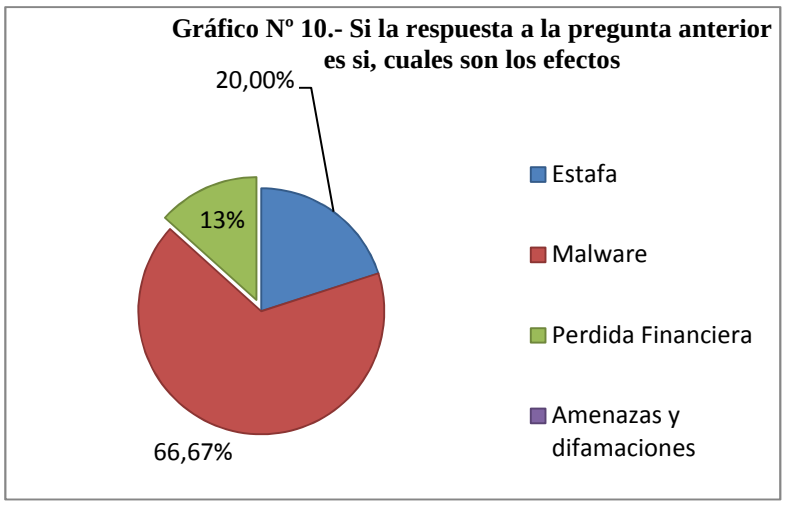
6.- SI LA RESPUESTA A LA PREGUNTA ANTERIOR ES SI, ¿CUÁLES FUERON LOS EFECTOS DE ESAS VIOLACIONES?

Cuadro Nº 10.- Si la respuesta a la pregunta anterior es si, cuales son los efectos

ALTERNATIVA	FRECUENCIA	%
Estafa	6	18,75
Malware	20	62,5
Perdida financiar	4	12.50
Amenazas y difamaciones	0	00,0
TOTAL	30	100

Elaborado: Diego Fernando Posso López

Fuente: Encuesta



Fuente: Cuadro Nº 10

Elaborado: Diego Fernando Posso López

Análisis. De la pregunta Nº 6 ¿**Si la respuesta a la pregunta anterior es Si, ¿Cuáles fueron los efectos de esas violaciones**; seis (6) de los encuestados consideran que fueron víctimas de estafa , que representan el 18,75%; veinte (20) de los encuestados fueron víctima de Malway, que representan el 62,50%; cuatro

(4) de las personas encuestadas manifiestan ser víctimas de hurto de cuentas bancarias, que representan el 12.50% y ninguna manifiesta ser víctimas de amenaza o difamación, constituyendo de esta manera el 100%.

Interpretación Lógica. Como se observa del análisis del resultado, En donde más se encontró violación se la seguridad informática se vio un alto porcentaje en las víctimas de los virus informáticos más novedosos por el hecho de descargar programas que esconden detrás de los programas y búsqueda de información.

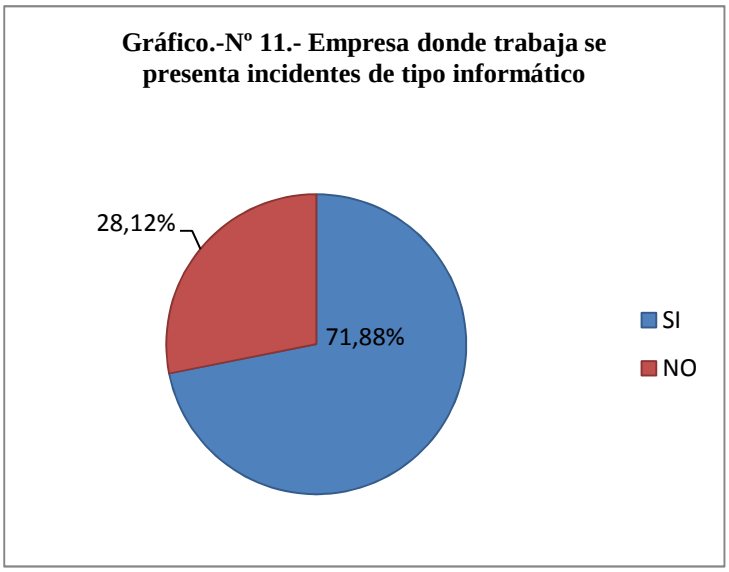
7.- ¿EN LA EMPRESA O ENTIDAD DONDE TRABAJA, SE PRESENTA INCIDENTES DE CARÁCTER INFORMÁTICO?

Cuadro Nº 11.- Empresa donde trabaja se presenta incidentes de tipo informático

ALTERNATIVA	FRECUENCIA	%
SI	23	71,88
NO	9	28,12
TOTAL	32	100

Elaborado: Diego Fernando Posso López

Fuente: Encuesta



Fuente: Cuadro Nº 11

Elaborado: Diego Fernando Posso López

Análisis. De la pregunta Nº 8 ¿En la empresa o entidad donde trabaja, se presenta incidentes de carácter informático?; veinte y tres (23) de los encuestados contestaron que SI, que representan el 71,88%; y nueve (9) de los encuestados contestaron que NO, que representan el 28,12%, constituyendo de esta manera el 100%.

Interpretación Lógica. Como se observa del análisis del resultado, el 71,88 de las personas consideran que en la empresa o entidad donde trabaja, se presenta incidentes de carácter informático en la ciudad de Ambato; en tanto que el 28,12% de las personas no considera que en la empresa o entidad donde trabaja, se presenta incidentes de carácter informático en la ciudad de Ambato. Por lo tanto, esto se debe a la poca información que poseen en unos casos y en otros al abuso del internet por parte de los mismos empleados.

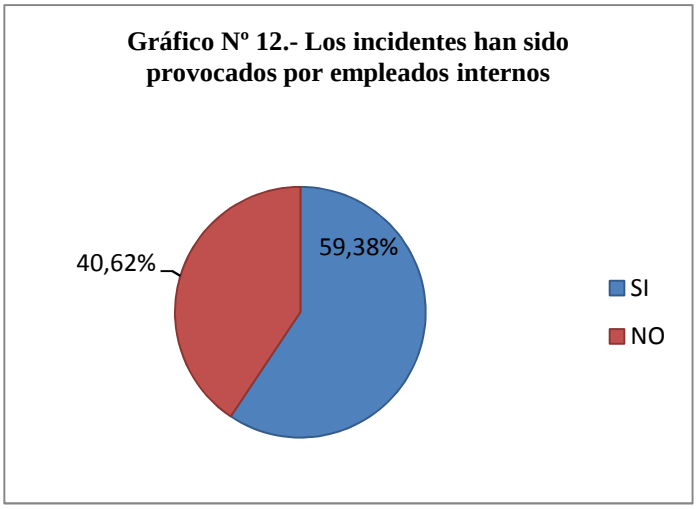
8.- ¿EN CASO DE HABER RESPONDIDO SI EN LA PREGUNTA ANTERIOR, LOS INCIDENTES HAN SIDO PROVOCADOS POR EMPLEADOS INTERNOS DE LA ENTIDAD?

Cuadro Nº 12.- Los incidentes han sido provocados por empleados internos

ALTERNATIVA	FRECUENCIA	%
SI	12	52,17
NO	11	47,83
TOTAL	23	100

Elaborado: Diego Fernando Posso López

Fuente: Encuesta



Fuente: Cuadro Nº 12

Elaborado: Diego Fernando Posso López

Análisis. De la pregunta Nº 8 ¿En caso de haber respondido si en la pregunta anterior, los incidentes han sido provocados por empleados internos de la entidad?; doce (12) de los encuestados contestaron que SI, que representan el 52,17%; y once (11) de los encuestados contestaron que NO, que representan el 47,83%, constituyendo de esta manera el 100%.

Interpretación Lógica. Como se observa del análisis del resultado, el 52,17% de las personas consideran que los incidentes de carácter informáticos han sido provocados por empleados internos de la entidad en la ciudad de Ambato; en tanto que el 47,83% de las personas no consideran que los incidentes informáticos han sido provocados por empleados internos de la entidad en la ciudad de Ambato. Por lo tanto, si han sido provocados por los usuarios de la empresa misma por motivos de desconocimiento y por la facilidad que ahora todo mundo tiene para el uso del internet.

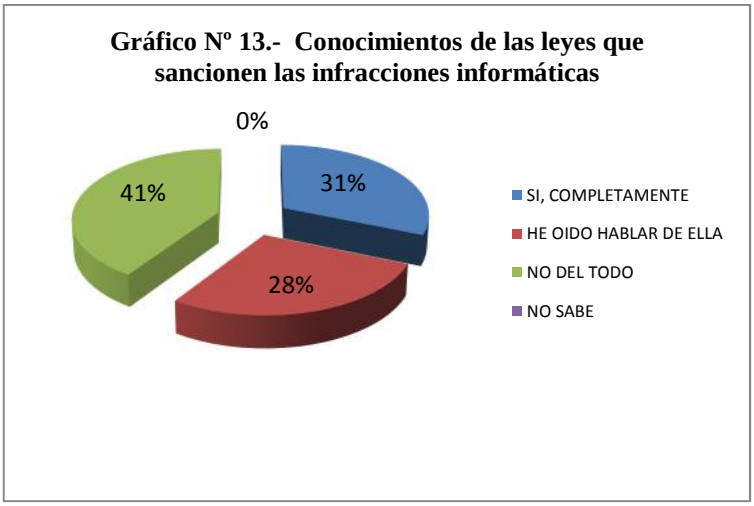
9.- ¿CONOCE LAS LEYES DEL ECUADOR QUE PERMITAN SANCIONAR LAS INFRACCIONES INFORMÁTICAS?

Cuadro Nº 13.- Conocimientos de las leyes que sancionen las infracciones informáticas

ALTERNATIVA	FRECUENCIA	%
SI COMPLETAMENTE	10	31,25
NO DEL TODO	9	28,12
HE OÍDO HABLAR	13	40,63
NO SABE		
TOTAL	32	100

Elaborado: Diego Fernando Posso López

Fuente: Encuesta



Fuente: Cuadro Nº 13

Elaborado: Diego Fernando Posso López

Análisis. De la pregunta Nº 9 ¿Conoce las leyes del ecuador que permitan sancionar las infracciones informáticas?; diez (10) de los encuestados contestaron que SI Completamente, que representan el 31,25%; nueve (9) de los encuestados contestaron que NO del todo, que representan el 28,12%; y trece (13) de los encuestados consideran han oído hablar de ello., que representan el 40,63 constituyendo de esta manera el 100%.

Interpretación Lógica. Por el trabajo realizado se pudo conocer que en la Provincia de Tungurahua hay un desconocimiento de las Leyes que rigen la Normativa de todo lo que tiene que ver con respecto a los delitos informáticos y a todas sus derivaciones.

COMPROBACIÓN DE LA HIPÓTESIS

Mediante el procesamiento de investigación exhaustiva se ha llegado a establecer que la falta de tipicidad de los delitos informáticos si violentan los derechos constitucionales del ofendido en la ciudad de Ambato, provincia de Tungurahua.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

Una vez realizadas las encuestas dirigidas a los Funcionarios de la Fiscalía Provincial de Tungurahua; Jueces de Garantías Penales del cantón Ambato, Jueces de Tribunales de Garantías Penales de Tungurahua, Abogados en libre ejercicio profesional, y víctimas de delitos informáticos del cantón Ambato.

CONCLUSIONES

- Es una realidad la presencia de nuevas formas delictivas debidas concretamente a que antes no existía un adelanto informático y electrónico de grandes magnitudes como ahora. Por esa circunstancia, se considera que resulta todavía insuficiente la legislación vigente tanto a nivel nacional como a nivel internacional.

- Debido a la naturaleza de los delitos informáticos, puede volverse confusa la tipificación de éstos, por cuanto a nivel general, se poseen pocos conocimientos y experiencias en el manejo de ésta área. Desde el punto de vista de la Legislatura es difícil la clasificación de estos actos, por lo que la creación de instrumentos legales puede no tener los resultados esperados, sumado a que la constante innovación tecnológica obliga a un dinamismo en el manejo de las Leyes relacionadas con la informática.

- La falta de cultura informática en la provincia de Tungurahua, es un factor crítico en el impacto de los delitos informáticos, cada vez se requieren mayores conocimientos en tecnologías de la información, las cuales permitan tener un marco de referencia aceptable para el manejo de dichas situaciones.

❖ En la mayoría de los casos no se denuncian estos delitos, para evitar la alarma social o el desprestigio por un fallo en la seguridad. Las víctimas prefieren sufrir las consecuencias del delito e intentar prevenirlo para el futuro, antes que iniciar un procedimiento judicial. Esta situación dificulta enormemente el conocimiento preciso del número de delitos cometidos y la planificación de las adecuadas medidas legales sancionadoras o preventivas.

❖ Uno de los problemas de los delitos informáticos, tiene que ver con las diferentes legislaciones en el mundo, y como ya lo hemos visto, un problema global no debe ni puede resolverse con respuestas parciales. Los legisladores deben definir de manera clara e inmediata los tipos penales necesarios para que estos nuevos Ciberdelincuentes nacidos bajo la sombra de la falta de legislación sobre el tema y conscientes de su actuar perjudicial y antijurídico, contengan su accionar cumpliéndose de esta manera la principal finalidad del Derecho Penal que es el prevenir los actos delictivos.

RECOMENDACIONES

Luego de analizar los delitos informáticos y la violación de los derechos constitucionales del ofendido, se recomienda considerar su implementación por sectores: Gubernamental, marco legal, formación, tecnología y sociedad.

En cuanto a la seguridad informática que se le recomienda a la ciudadanía podemos mencionar las siguientes:

1. Contraseña segura o password: Establezca sus contraseñas de tal manera que no puedan ser fácilmente adivinadas por usuarios mal intencionados, evite utilizar su fecha de cumpleaños, su RUC o alguna palabra fácil de adivinar; confórmelas de manera sólida en cuanto a su longitud y contenido (mayúsculas, minúsculas y números), únicas y diferenciadas de otras contraseñas, practicar para ser fácilmente recordadas y cámbielas con frecuencia.

2. Respaldo de información: Haga una copia de todos los archivos que usted considere importantes, en forma periódica, para que en caso de que su computadora se dañe o sea robada, usted cuente con un respaldo y pueda recuperar la información de inmediato.

3. Creación de cuentas de usuario: Le permitirá no sólo tener privacidad en sus sesiones, sino además servirá para restringir el acceso de menores de edad a sitios no adecuados, evitar descargas de programas inseguros y darle seguimiento a las páginas que visitaron.

Se recomienda a la ciudadanía seguir las siguientes prácticas de seguridad para evitar que sea sujeto de un delito informático:

1. En su hogar, instale la computadora en un área de convivencia común y evite colocar el monitor viendo hacia la pared. Establezca con su familia, reglas límites y horarios respecto del uso del internet, manteniendo un diálogo y una comunicación constantes en que se discutan los riesgos a los que se está expuesto al conectarse. Explíqueles que no toda la información existente en el internet es una verdad absoluta. Motívelos a visitar sitios educativos, y disfruten juntos la experiencia.

2. Oriente y supervise a sus hijos para que al entrar a platicar en la sala del chat lo hagan únicamente con personas conocidas y verifiquen que cada interlocutor efectivamente sea quien dice ser, su conocido. Haga que eviten a toda costa las salas públicas.

3. Verifiquen que utilicen un “alias” y que este no sea agresivo o sugestivo, prevéngalos de los acosadores sexuales o personas dedicadas a la pornografía infantil, explíqueles que pueden estar siendo engañados por la persona del otro lado y sensibilícelos para que no acepten jamás una cita con un desconocido que los aborde en línea, ni envíe fotografías ni datos personales por correo

electrónico o en llenado de formularios ante la oferta de recibir regalos o promociones.

4. Advierta a la familia sobre la posibilidad de recibir a través de los programas de mensajería instantánea, un archivo potencialmente dañino; antes de aceptar su transmisión, haga que pregunten a quien lo envían de qué se trata. Revise los archivos recibidos y esté alerta ante la presencia de material con contenido explícitamente sexual.

5. Conozca las contraseñas de las cuentas de correo electrónico de sus hijos menores y monitoreé de vez en cuando el contenido de los mensajes recibidos así como los testigos de sus conversaciones. Evite que su hijo/a pueda estar siendo víctima de pervertidores. Aliéntelos a reportarle cualquier situación extraña o que los haga sentir incómodos.

6. Explique a su familia que el hecho de participar en apuestas, realizar copias ilegales de programas, video juegos, música, fotografías, o cualquier material con derechos de autor, constituye un delito. Enséñeles a tener un comportamiento responsable evitando que usen internet para propagar rumores, molestar o amenazar a otros así como para que eludan la compraventa de productos o la obtención de beneficios económicos sin su autorización.

Utilizando la banca en línea en la actualidad usted puede efectuar transacciones bancarias y pagos de servicios desde su hogar por internet, de esa manera evitará exponerse en la calle a los delincuentes; sin embargo, es preciso observar las siguientes recomendaciones:

1. Al entrar al portal de su banco hágalo de manera directa escribiendo la dirección en el navegador. Evite hacerlo desde otros sitios o desde corres electrónicos, ya que corre riesgo de ser enviado a un sitio que el delincuente “disfrace” para engañarlo y obtener sus contraseñas.

2. No realice operaciones bancarias en sitios públicos como cafés internet o centros de negocios de hoteles, pues corren el riesgo de que algún delincuente haya instalado un programa que copie sus contraseñas.

3. Mantenga a “salvo su identidad electrónica”, es decir su nombre de usuario y contraseña. No los comparta o divulgue y cámbielos con frecuencia. Revise periódicamente sus saldos bancarios y notifique cualquier anomalía directamente a su banco.

4. Efectúe sus compras en línea de manera segura, sepa con quien trata, obtenga la dirección física y los teléfonos del proveedor. Lea detenidamente la descripción del producto y el convenio de compra, así como el costo total del producto, incluyendo el envío. Pague preferentemente con tarjeta de crédito, mantenga un registro impreso de su compra y verifique que tanto los portales bancarios como la tienda en línea cuenten con las señales de seguridad.

Evite el “spam” o llamado correo basura, ha sido uno de los principales vehículos para hacer llegar problemas a los usuarios de correo electrónico. Conozca y utilice los filtros que existen para bloquearlos en su proveedor de internet o correo electrónico.

Usted recibe un correo electrónico donde se indica que su servidor de banca en línea ha sido suspendido por diversas causas y que debe seguir las instrucciones en un “archivo adjunto” para establecerlo. Al momento de ejecutarlos haciéndole “click”, se instala en su computadora, sin que usted lo note, un programa malicioso que registrará todo lo que usted haga en su equipo, así como todo lo que escriba en el teclado y enviará de manera constante y silenciosa a un sitio donde el delincuente determine fácilmente cuáles son las contraseñas de sus cuentas.

En otra modalidad, el correo le indica que su institución financiera requiere la confirmación de sus datos y le solicita que acceda a su sitio en internet

para “solicitarle” el proceso; se incluye en el mismo correo una liga que lo enviará directamente a él. Ya en el sitio, o bien se ejecuta un programa similar al que describe en el inciso anterior o simplemente al ingresar datos o contraseñas, el delincuente los obtiene de manera instantánea.

Se han detectado delincuentes que indican a sus víctimas en el correo enviado, que se comuniquen con un ejecutivo con el fin de verificar algunas irregularidades en su manejo de cuenta, y le proporcionan un número telefónico. Al llamar la persona que contestan lo hace con el nombre de la institución bancaria, pidiéndole que, para acceder a su cuenta, le sea proporcionado el “nombre del usuario y contraseña”, misma que “para su propia seguridad “usted podrá cambiar al final.

En últimas fechas, se ha reportado la llegada de correos electrónicos con noticias sensacionalistas o chismes de la farándula, simulando provenir de medios de información formales e invitando al destinatario a ingresar de inmediato a leer información y observar incluso un video. Evite abrir ese tipo de comunicados si no conoce al remitente.

Detecte y elimine programas espías, los denominados spywares son aplicaciones que llevan a cabo cierto tipo de tareas, tales como: promociones publicitarias, recopilación de información personal o modificación de la configuración del sistema sin su consentimiento. Algunos de los síntomas que puede presentar su PC son la aparición constante de anuncios emergentes, la alteración de la página de inicio al entrar a internet, el cambio de la configuración en el sistema sin la posibilidad de restaurar los ajustes originales, la muestra por parte del explorador de elementos que usted no descargó o simplemente el funcionamiento de su sistema en una velocidad lenta y el bloqueo frecuente del sistema.

Al salir a la calle, procure no utilizar un maletín muy ostentoso para su computadora portátil o laptop, llévela en una mochila que no denote a todos el

contenido. En aviones, guárdele debajo del asiento del frente. Para prevenir olvidos, adquiera una alarma personal para evitar pérdida por parte de niños y ponga en su maletín la contraparte; si usted se aleja comenzará a sonar una alarma. Si requiere llevar a reparar su equipo casero puede camuflarlo metiendo en una funda plástica de una colchoneta forrándolo con una sábana.

Tanto en su computadora personal como en su laptop tenga activado un password; el de arranque al iniciar la sesión de usuario y el password del protector de pantalla que se active cuando la máquina entre en estado de reposo. De igual forma configure su agenda electrónica con una contraseña, para que en caso de robo o extravío, usted cuente con la tranquilidad de que su información no será fácilmente obtenida y utilizada indebidamente.

En los llamados “hotspots” o ambientes inalámbricos, muy populares ya en lugares públicos y donde usted se puede conectar con su laptop o agenda electrónica a internet, incluso de manera gratuita, evite acceder a sus cuentas bancarias así como efectuar compras utilizando sus tarjetas de crédito, ya que existe la posibilidad de que la red a la cual usted se conecte, no sea la de un proveedor seguro y los datos enviados, sean interceptados por delincuentes cibernéticos.

Cuente con un programa antivirus instalado en su computador y bien configurado, manténgalo actualizado constantemente, si es posible diariamente, y realice análisis de virus completos de su máquina por lo menos una vez por semana. De esta forma se mantiene un sistema saludable y se evita le perdida de documentos o archivo por acción de virus.

Es importante que cada vez que se inserte un dispositivo de almacenamiento externo al computador se realice inmediatamente el análisis de virus, para prevenir el contagio de virus que ataque a la máquina, siempre y cuando el antivirus este actualizado.

Si una persona ha sido víctima de un delito, debe acudir inmediatamente a denunciarlo en las oficinas más cercanas de la Fiscalía General del Estado o de la Policía Judicial. No tema, que el funcionario que recepte su denuncia no debe dar a conocer públicamente la identidad o los datos de las víctimas, cuando dicha información pueda afectar la intimidad o seguridad de la víctima y/o sus familiares. Recuerde que al denunciar el delito, contribuirá a que la Fiscalía conozca cómo opera la delincuencia y pueda tomar medidas preventivas encaminadas a disminuir la impunidad y criminalidad del país.

Si usted se siente intimidado para presentar una denuncia penal, recuerde que la Fiscalía General del Estado dirige el “Sistema Nacional de Protección y Asistencia a Víctimas, Testigos y otros Participantes en el Proceso Penal”, quienes a través de diferentes acciones de protección y asistencia, garantizarán su vida e integridad física, para que con libertad y seguridad pueda ejercer su deber constitucional de denunciar y evitar que los hechos criminales queden impunes.

CAPÍTULO VI

PROPUESTA

Plantear la reforma y agregar artículos innumerados en el Capítulo V de los delitos contra la inviolabilidad del secreto y reformar el artículo 197 del Código Penal, para evitar inmunidad de la infracción por medios electrónicos, así como pérdida de confianza de la sociedad en el sistema judicial penal, falta de protección al derecho a la intimidad y evitar inseguridad Jurídica, derechos que se encuentran protegidos en la Constitución de la República del Ecuador.

DATOS INFORMATIVOS

INSTITUCIÓN:

Universidad Técnica de Ambato

PROVINCIA:

Tungurahua

CANTÓN:

Ambato

NOMBRE DEL INVESTIGADOR:

Diego Fernando Posso López

TELÉFONO:

0322417072

DIRECCIÓN DOMICILIARIA:

Ciudadela Simón Bolívar, pasaje Quijano 510 y Cacique Álvares, cantón Ambato, provincia de Tungurahua.

TIEMPO DE EJECUCIÓN:

Nueve meses

COSTO:

5.319 USD.

ANTECEDENTES DE LA PROPUESTA

Realizada la investigación, se debe mencionar, como problemática principal dentro de nuestro ordenamiento jurídico, los vacíos legales en el Código Penal, ya que, tal como se encuentra estructurada permite la violación de los derechos constitucionales del ofendido.

JUSTIFICACIÓN

Esta propuesta está orientada a cristalizar el anhelo de todos los ciudadanos, de obtener la aplicación de justicia, sin ninguna clase de trasgresión, buscando que el Código Penal sancione los diferentes delitos informáticos, a fin de asegurar los derechos a la intimidad personal y familiar, derecho a la inviolabilidad de secretos virtuales, protección de datos, derecho al patrimonio legalmente adquirido y a la seguridad jurídica.

OBJETIVOS

Objetivo General:

- Reformar del Capítulo V de los delitos contra la inviolabilidad del secreto artículo innumerado, 197 del Código Penal, e incrementar concepto de delitos informáticos en el Código Penal para evitar la violación de los derechos del ofendido en delitos informáticos en la ciudad de Ambato, provincia de Tungurahua.

Objetivos Específicos:

- Buscar los mecanismos necesarios para que se realice la reforma del Código Penal.

- Determinar qué derechos y garantías constitucionales, se protegen al reformar el Código Penal.

- Plantear las propuestas de reformas al Código Penal, en la Asamblea Nacional, a fin de buscar soluciones al problema de transgresión de derechos del ofendido en delitos informáticos, al tipificar y sancionar los delitos informáticos, que acarrean inseguridad jurídica.

ANÁLISIS DE FACTIBILIDAD

La factibilidad que existe ante este trabajo de investigación es muy amplia; ya que, existe la información y datos necesarios para seguir adelante con el tema; es importante recalcar la colaboración de los funcionarios de la Fiscalía Provincial de Tungurahua; Jueces de Garantías Penales del cantón Ambato, Jueces de Tribunales de Garantías Penales de Tungurahua, Abogados en libre ejercicio profesional, y Víctimas de delitos informáticos de la ciudad de Ambato, a través de su contingente se ha logrado cumplir con una investigación minuciosa del tema

propuesto.

Social

Esta propuesta va dirigida a los ofendidos en delitos informáticos, a quienes voluntaria o involuntariamente se les violenta sus derechos: a la intimidad personal y familiar, a la inviolabilidad de secretos virtuales, protección de datos, derecho al patrimonio legalmente adquirido y a la seguridad jurídica.

Económico

Es factible su aplicación puesto que no se requiere de mucha inversión, por lo contrario al realizar las reformas respectivas al Código Penal, el Estado impedirá que se realicen gastos judiciales innecesarios, al conocer denuncias por hurto, robo, estafa; sin considerar la pérdida de tiempo de la fiscalía, que bien podrían emplearlo en tramitar verdaderos delitos.

FUNDAMENTACIÓN

Debemos considerar la problemática Jurídica, ya que si bien es cierto Ecuador ha iniciado los primeros pasos en la generación de Leyes y Normativas Legales que contemplan aspectos significativos de las nuevas tecnologías y también se han establecido penas en el Código Penal y de Procedimiento Penal, aún se siente la ausencia de legislación, por parte de la sociedad, que sea precisa y coherente, para el tratamiento de esta nueva modalidad de delincuencia, por ello es necesaria la incorporación de un marco legal que contemple a los delitos informáticos de una manera integral.

Después de lo citado a lo largo de los capítulos anteriores, los peligros emergentes por el uso de las computadoras conectadas a redes de satélites de alcance global o Internet son enormes. Los delitos cometidos a través de la informática son de la más variada índole y van de lo más simple a lo más

complejo, ya que existe la necesidad de colaborar con el Estado dentro del ordenamiento jurídico existente, mediante la creación de nuevas leyes destinadas a mejorar la administración de justicia en el Ecuador, con la finalidad de asegurar el derecho a la intimidad, inviolabilidad de secretos y a la seguridad jurídica establecida en la Constitución de la República del Ecuador.

La presente propuesta de investigación posee valor legal, porque tiene fundamentación jurídica respecto a los derechos y garantías básicas establecidas en la Constitución de la República, además garantizan su aplicación correspondiente mediante la presentación de un proyecto de ley, que permite su reforma, así lo establece el artículo 134 y siguientes ibídem.

Artículo 134.- Presentación de Proyectos de Ley. *"La iniciativa para presentar proyectos de ley corresponde:*

…5. A las ciudadanas y los ciudadanos que estén en goce de los derechos políticos y a las organizaciones sociales que cuenten con el respaldo de por lo menos el cero punto veinticinco por ciento de las ciudadanas y ciudadanos inscritos en el padrón electoral nacional".

Artículo 136.- Requisitos de los proyectos de ley. *"Los proyectos de ley deberán referirse a una sola materia y serán presentados a la Presidenta o Presidente de la Asamblea Nacional con la suficiente exposición de motivos, el articulado que se proponga y la expresión clara de los artículos que con la nueva ley se derogarían o se reformarían. Si el proyecto no reúne estos requisitos no se tramitará".*

Art. 137.- Procedimiento para la aprobación de los proyectos de ley. *"El proyecto de ley será sometido a dos debates. La Presidenta o Presidente de la Asamblea Nacional, dentro de los plazos que establezca la ley, ordenará que se distribuya el proyecto a los funcionarios de la Asamblea y se difunda públicamente su extracto, y enviará el proyecto a la comisión que corresponda,*

que iniciará su respectivo conocimiento y trámite.

Las ciudadanas y los ciudadanos que tengan interés en la aprobación del proyecto de ley, o que consideren que sus derechos puedan ser afectados por su expedición, podrán acudir ante la comisión y exponer sus argumentos.

Aprobado el proyecto de ley, la Asamblea lo enviará a la Presidenta o Presidente de la República para que lo sancione u objete de forma fundamentada. Sancionado el proyecto de ley o de no haber objeciones dentro del plazo de treinta días posteriores a su recepción por parte de la Presidenta o Presidente de la República, se promulgará la ley, y se publicará en el Registro Oficial".

Artículo 138.- Objeción del Presidente de la República. *"Si la Presidenta o Presidente de la República objeta totalmente el proyecto de ley, la Asamblea podrá volver a considerarlo solamente después de un año contado a partir de la fecha de la objeción. Transcurrido este plazo, la Asamblea podrá ratificarlo en un solo debate, con el voto favorable de las dos terceras partes de sus funcionarios, y lo enviará inmediatamente al Registro Oficial para su publicación.*

Si la objeción fuera parcial, la Presidenta o Presidente de la República presentará un texto alternativo, que no podrá incluir materias no contempladas en el proyecto; igual restricción observará la Asamblea Nacional en la aprobación de las modificaciones sugeridas.

La Asamblea examinará la objeción parcial dentro del plazo de treinta días, contados a partir de la fecha de su entrega y podrá, en un solo debate, allanarse a ella y enmendar el proyecto con el voto favorable de la mayoría de asistentes a la sesión. También podrá ratificar el proyecto inicialmente aprobado, con el voto favorable de las dos terceras partes de sus funcionarios

.

En ambos casos, la Asamblea enviará la ley al Registro Oficial para su

publicación. Si la Asamblea no considera la objeción en el plazo señalado, se entenderá que se ha allanado a ésta y la Presidenta o Presidente de la República dispondrá la promulgación de la ley y su publicación en el Registro Oficial…"

POSIBLE REFORMA AL CÓDIGO PENAL, A TRAVÉS DE PROYECTO CIUDADANO, CUMPLIENDO CON TODOS LOS FUNDAMENTOS LEGALES, JURÍDICOS, FILOSÓFICOS Y POLÍTICOS QUE EMANA NUESTRA CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR.

LA ASAMBLEA NACIONAL

Considerando:

- Que, el artículo 169 de la Constitución de la República establece que el sistema procesal es un medio para la realización de la justicia, y, que las normas procesales consagrarán los principios de simplificación, uniformidad, eficacia, inmediación, celeridad y economía procesal, y harán efectivas las garantías del debido proceso.

-Que, el artículo 172 de la Constitución de la República, en su inciso primero, dispone que las juezas y jueces administraran justicia con sujeción a la Constitución, a los instrumentos internacionales de derechos humanos y a la ley.

-Que, el artículo 66, literal b, numeral 20 de la Constitución de la República establece, como derecho de libertad la intimidad personal y familiar.

- Que, el artículo 66, literal b, numeral 26 de la Constitución de la República establece, garantiza el derecho a la propiedad en todas sus formas, por lo se permite adoptar políticas públicas para el cumplimiento.

-Que, el artículo 82 de la Constitución de la República prescribe, en forma expresa, que el derecho a la seguridad jurídica se fundamenta en el respeto

a la Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicadas por las autoridades competentes.

-**Que**, el artículo 21, numeral 4 del Código de Procedimiento Penal tipifica las reglas de conexidad de las infracciones y que el artículo 51 del Código Penal establece las penas que son aplicables a éstas.

-**Que,** el artículo 136 de la Constitución de la República y el numeral 1 del artículo 56 de la Ley Orgánica de la Función Legislativa disponen que los proyectos de ley deberán referirse a una sola materia, en este caso, la penal .

-**Que**, es necesario introducir reformas al Código Penal, con la finalidad de asegurar los derechos a la intimidad, personal y familiar, inviolabilidad de los secretos correspondencia física y virtual, protección de datos, derecho al patrimonio legalmente adquirido y a la seguridad jurídica, de conformidad con lo previsto en los artículos 66 y 82 de la Constitución de la República.

En uso de sus atribuciones expide las siguientes reformas al Código Penal:

Art. 197.- Incorpórese al artículo: “medios electrónicos” y elimínese “medios afines”

- Serán reprimidos con pena de dos meses a un año de prisión, quienes interceptaren, sin orden judicial conversaciones telefónicas o realizaren por medios electrónicos y quienes se sustrajeran o abrieran sobres de correspondencia que pertenecieren a otro sin autorización expresa.

Se exime la responsabilidad de quien lo hizo cundo la intercepción telefónica o medios electrónicos se produce por un error, en forma accidental o fortuita.

Art. Innumerado del Capítulo V, los delitos contra la inviolabilidad del secreto. Sustitúyase, por el siguiente: sustitúyase “prisión de 1 a 6 años, multa de 1.000 a

10.000 dólares de los Estados Unidos de Norte América

“El que empleando cualquier medio electrónico, informático o a fin, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto confidencialidad y reserva o simplemente vulnerar la seguridad será reprimido con prisión de 1 a 6 años, dependiendo de la gravedad de la información y multa de o 1000 a 10000 dólares de los Estados Unidos de Norte América (…)”.

Incorpórese dos artículos, innumerados, al Título II, Capítulo V, de los delitos contra la inviolabilidad del secreto. Los siguientes artículos:

Art. (…).- USO DE VIRUS (SOFTWARE MALICIOSO)

La persona o personas que produzcan, trafiquen, adquieran, distribuyan, vendan, envíen, introduzcan o extraigan del territorio nacional virus (software malicioso) u otro programa de computación de efectos dañinos será sancionado con una pena de dos a tres años de prisión y con una multa de mil a diez mil dólares americanos.

Art (…).- APROPIACIÓN DE PROPIEDAD INTELECTUAL

Quien sin autorización de su propietario y con el fin de obtener algún provecho económico reproduzca, modifique, copie, distribuya o divulgue un software u otra obra del intelecto humano, que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información, será sancionado con prisión de uno a cuatro años y multa de mil a cuatro mil dólares americanos.

Art (…).- FRAUDE INFORMÁTICO

Son responsables de fraude informático la persona o personas que con ánimo de lucro y valiéndose de cualquier método o medio, alteren, manipulen, o modifiquen el funcionamiento de un programa informático, sistema informático, telemático, o

un mensaje de datos para lucrar para sí o para otros un activo patrimonial de otra persona, en perjuicio de ésta o de un tercero, serán sancionados con pena de prisión de uno a cuatro años y con multa de 1.000 a 10.000 dólares.

Art (…).- DAÑOS INFORMÁTICOS
Son responsables del delito de daños informáticos, la persona o personas que utilizando cualquier método o medio destruyan, alteren, deteriore, inutilicen, supriman o dañen: datos, bases de datos, programas informáticos, documentos electrónicos o cualquier mensaje de datos contenido en cualquier soporte lógico, sistema informático, o telemático; y serán reprimidas con reclusión menor de dos a cuatro años y con multa de 1.000 a 12.000 dólares o con una de estas dos penas.

Art (…).- DE LA FALSIFICACIÓN INFORMÁTICA
Son responsables de falsificación informática las personas que con ánimo de lucro, o bien para causar un perjuicio a un tercero, utilizando cualquier medio alteren o modifiquen documentos electrónicos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema informático o telemático, ya sea:

1.- Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter esencial.

2.- Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad.

Cualquier alteración, falsificación, simulación, falsa suposición o imputación de un mensaje de datos. Será reprimido con reclusión menor ordinaria de ocho meses a cinco años y multa de 5.000 a 15.000 dólares o con una de estas dos penas.

Si la infracción de falsificación informática es cometida por un funcionario público, la pena será de reclusión menor extraordinaria de 5 a 10 años y multa de 10.000 a 40.000.

La presente reforma entrará en vigencia a partir de su publicación en el Registro Oficial.

METODOLOGÍA OPERATIVA DE LA PROPUESTA

Cuadro Nº 14.- Metodología operativa

INDICADOR	SITUACIÓN ACTUAL	RESULTADOS ESPERADOS	ACTIVIDADES	RESPONSABLES
Concientización	Existe falta de tipicidad de los delitos informáticos.	Que se actualice de acuerdo a la realidad social, el Código Penal para obtener una adecuada aplicación de justicia.	Análisis profundo de los delitos informáticos, investigación social de interés por parte de los asambleístas.	Presidente Constitucional, Fiscalía, jueces de garantías penales y asambleístas.
Capacitación	Monitoreo, facilismo y un desinterés casi general.	Mejor aplicación de justicia, igualdad social y respecto íntegro de derechos constitucionales.	Estudios, encuestas, seguimientos a las causas; y, funcionarios con óptima capacitación.	Organismos nacionales, funcionarios, estudiantes y la sociedad en general.
Reforma	Del Código Penal, permite vulneración de derechos constitucionales del ofendido en delitos informáticos.	Cristalización de justicia, y conformidad del ordenamiento jurídico con lo determinado en la Constitución de la República del Ecuador.	Reformar el Capítulo V de los delitos contra la inviolabilidad del secreto artículo innumerado, 197 Código Penal, e incrementar cinco art. innumerados; a través de proyecto de Ley.	Asamblea Nacional.

Elaborado: Diego Fernando Posso López

ADMINISTRACIÓN

La reforma al Código Penal del Capítulo V de los delitos contra la inviolabilidad del secreto artículo innumerado, 197 del Código Penal, e incrementar concepto de delitos informáticos en el Código Penal, estará bajo la dirección del investigador, la creación del proyecto de Ley será planteada por el Consejo de la Judicatura, una vez atendidas la propuesta, dado el trámite legal a la reforma.

El objetivo es sacar adelante esta propuesta; ya que, no puede quedar únicamente en lo teórico, por ello se tendrá que sugerir a la sociedad en general, para que se cumpla con la propuesta realizada por el investigador.

PREVISIÓN DE LA EVALUACIÓN

Se plantea la evaluación a la reforma y su implementación.

Se considera un tiempo mínimo de seis meses posteriores a la implementación de la reforma para verificar los resultados obtenidos.

La evaluación será formativa continua, debido a que toda acción del hombre debe ser evaluada para cumplir con lo propuesto, siempre existirá enmiendas y correcciones acorde a las necesidades que son propias del desarrollo de la propuesta y contribuir a satisfacción de todos quienes estamos inmersos en sistema jurídico-social.

BIBLIOGRAFÍA

Libros:

1. PÁEZ RIVADENERIA, J. J., & ACURIO DEL PINO, S. (2010). Derecho y Nuevas Tecnologías. Quito, Ecuador: Corporación de Estudios y Ediciones.
2. CLOUGH, J. (2010). PRINCIPLES OF CYBERCRIME. Cambridge, UK: Cambridge University Press.
3. KSHETRI, N. (2010). The Global Cybercrime Industry. North Carolina, USA: Springer.
4. MARTÍNEZ, J. J. (2009). Computación Forense. Descubriendo los rastros informáticos. Bogotá, Colombia: Alfaomega.
5. MARTÍNEZ, J. J. (2010). El Peritaje Informático y la Evidencia Digital. Bogotá, Colombia: Universidad de Los Andes.
6. PASCALE, M. (2007). Manual de Peritaje Informático. Montevideo, Uruguay: Fundación de Cultura Universitaria.

Revistas:

1. Manual de Autoprotección y Seguridad Ciudadana (2010), Dirección Nacional de Política Criminal y la Dirección Nacional de Policía Judicial del Ecuador

2. Revista de Estadísticas Criminales (2009),Fiscalía General del Estado del Ecuador

3. Manual de Manejo de Evidencias Digitales y Entornos Informáticos (2009),Fiscalía General del Estado del Ecuador

Cuerpos Legales:

1. Constitución de la República del Ecuador

2. Ley Orgánica de Transparencia y Acceso a la Información Pública

3. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

4. Código de Procedimiento Penal

5. Código Penal

6. Ley de Propiedad Intelectual

7. Ley Especial de Telecomunicaciones

8. Ley Orgánica de Control Constitucional

9. Código de Procedimiento Civil

LINKOGRAFÍA

1. Delitos Informáticos en el Código Penal Español
   http://www.delitosinformaticos.com

2. Delitos Informáticos
   http://www1.lunarpages.com/derechohoy/informatico.htm

3. Problemáticas de la ley sobre Delitos Informáticos
   www.abogadosdetalca.cl

4. Reflexiones sobre los Delitos Informáticos motivadas por los desaciertos de la Ley Chilena”
http://www.ctv.es/

5. Figuras delictivo - informáticos tipificadas en Chile
http://www.alfa-redi.org/

6. El Fraude y Los Daños Informáticos
http://www.delitosinfomaticos.com/

7. Delito de Estafa Informática
http://www.delitosinfomaticos.com/

8. Los Delitos de Hacking en sus Diversas Manifestaciones
http://www.alfa-redi.org/

9. http://es.wikipedia.org/wiki/Wikipedia:Portada

ANEXOS

ANEXO Nº 1

ENCUESTA Nº 1

DIRIGIDA A: Funcionarios de la Corte Provincial de Justicia de Tungurahua, Funcionarios de la Comisaría de la Mujer y la Familia de la ciudad de Ambato; y, Abogados en libre ejercicio profesional.

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

TEMA: "LOS DELITOS INFORMÁTICOS Y LA VIOLACIÓN DE LOS DERECHOS CONSTITUCIONALES DEL OFENDIDO"

INSTRUCTIVO:

Lea detenidamente las preguntas formuladas y marque con una X dentro del paréntesis de la respuesta que usted considere correcta.

CUESTIONARIO:

1. ¿CREE QUE SU DERECHO A LA INTIMIDAD SE ENCUENTRA VIOLADO EN LAS REDES SOCIALES DE COMUNICACIÓN A TRAVÉS DE INTERNET?

SI ( ) NO ( )

2. ¿CONSIDERA QUE LAS COMPRAS A TRAVÉS DE INTERNET SON SEGURAS??

SI ( ) NO ( )

3. ¿CREE NECESARIO UNA REGULACIÓN PARA INTERNET?

SI ( ) NO ( )

4. ¿CONSIDERA USTED QUE LA SEGURIDAD A LOS DATOS PESONALES ES UNA CUESTIÓN ALTA PRIORIDAD?

SI ( ) NO ( )

5. ¿USTED HA SIDO VÍCTIMA DE VIOLACIONES DE LA SEGURIDAD INFORMÁTICA?

SI ( ) NO ( )

6.- SI LA RESPUESTA A LA PREGUNTA ANTERIOR ES SI, ¿CUÁLES FUERON LOS EFECTOS DE ESAS VIOLACIONES?

ESTAFA ( )

MALWARE ( )

PERDIDA FINANCIERA ( )

AMENAZAS E IFAMACIONES ( )

7.- ¿EN LA EMPRESA O ENTIDAD DONDE TRABAJA, SE PRESENTA INCIDENTES DE CARÁCTER INFORMÁTICO?

SI ( ) NO ( )

8.- ¿EN CASO DE HABER RESPONDIDO SI EN LA PREGUNTA ANTERIOR, LOS INCIDENTES HAN SIDO PROVOCADOS POR EMPLEADOS INTERNOS DE LA ENTIDAD?

SI ( ) NO ( )

9.- ¿CONOCE LAS LEYES DEL ECUADOR QUE PERMITAN SANCIONAR LAS INFRACCIONES INFORMÁTICAS?

SI COMPLETAMENTE ( )

NO DEL TODO ( )

HE OÍDO HABLAR ( )
NO SABE ( )

GRACIAS POR SU COLABORACIÓN

ANEXO II

GLOSARIO DE TÉRMINOS.-

Delitos.- El delito es definido como una acción típica, anti jurídica, imputable, culpable, sometida a una sanción penal, y a veces a condiciones objetivas de punibilidad. Supone una conducta infraccional del Derecho penal, es decir, una acción u omisión tipificada y penada por la ley.

Violación.- La violación es una agresión de tipo sexual que se produce cuando una persona tiene acceso sexual hacia otra, mediante el empleo de violencias físicas o psicológicas o mediante el uso de mecanismos que anulen el consentimiento de los ofendidos.

Derechos constitucionales.- Los derechos constitucionales son aquellos incluidos en la norma constitutiva y organizativa de un estado generalmente denominada constitución que se consideran como esenciales en el sistema político están especialmente vinculados a la dignidad humana. Es decir, son aquellos derechos que dentro del ordenamiento jurídico disfrutan de un estatus especial en cuanto a garantías (de tutela y reforma).

Telemática.- La Telemática es una disciplina científica y tecnológica, originada por la convergencia entre las tecnologías de las Telecomunicaciones y de la Informática.

Hurto.- Consiste el delito de hurto en el apoderamiento ilegítimo de una cosa mueble, ajena en todo o en parte, que, a diferencia del robo, es realizado sin fuerza en las cosas, ni violencia o intimidación en las personas.

Fraudes.- Acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quien se comete.

Falsificaciones.- Una falsificación es un acto consistente en la creación o

modificación de ciertos documentos, efectos, productos (bienes o servicios), con el fin de hacerlos parecer como verdaderos, o para alterar o simular la verdad.

Estafa.- La estafa es un delito contra la propiedad o el patrimonio. El núcleo del tipo penal de estafa consiste en el engaño. El sujeto activo del delito se hace entregar un bien patrimonial, por medio del engaño; es decir, haciendo creer la existencia de algo que en realidad no existe.

Sabotaje.- Daño que se hace intencionadamente en servicios como forma de lucha contra los organismos que los dirigen: alguien preparó actos de sabotaje para hacer fracasar los Juegos Olímpicos. Acción contraria a una idea o proyecto:

Cyber crime.- Los criminales que cometen crímenes cibernéticos utilizan métodos muy variados, en función de sus habilidades y sus objetivos. Esto no debería sorprender a nadie: después de todo, el crimen cibernético no es más que una actividad "criminal" a la que se suma un ingrediente "informático" o "cibernético".

Tipicidad.- es la adecuación del acto humano voluntario ejecutado por el sujeto a la figura descrita por la ley como delito. Es la adecuación, el encaje, la subsunción del acto humano voluntario al tipo penal. Si se adecua es indicio de que es delito. Si la adecuación no es completa no hay delito.

Software.- Se conoce como *software*[1] *al equipamiento lógico o soporte lógico* de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware.

Hardware.- El término *hardware* (pronunciación.- se refiere a todas las partes tangibles de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos.[1] Son cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado;

contrariamente, el soporte lógico es intangible y es llamado *software*.

Ofendido.- el sujeto pasivo de una infracción u delito.

Manipulación.- manipulación mental, una práctica destinada a influir en la voluntad o libre albedrío, por ejemplo, el lavado de cerebro y el control mental.

Evidencias.- Una evidencia (del latín, video, ver) es un conocimiento que se nos aparece intuitivamente de tal manera que podemos afirmar la validez de su contenido, como verdadero, con certeza, sin sombra de duda.

Datos falsos o engañosos.- conocido también como introducción de datos falsos, es una manipulación de datos de entrada al computador con el fin de producir o lograr movimientos falsos en transacciones de una empresa.

Pishing.- es una modalidad de fraude informático diseñada con la finalidad de robarle la identidad al sujeto pasivo. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños.

Intimidad personal.- Intimidad es la parte interior que solamente cada uno conoce en sí mismo. Es el máximo grado de inmanencia, es decir, aquello que se almacena en el interior.

Tecno dependencia.- Seres inseguros al fin, los humanos solemos tener una relación contradictoria con los objetos tecnológicos. Medios extraordinarios para nuestra expansión, éstos pueden devenir en factores alienantes.

BUSINESSSO FTWAREA LLIANCE.- que es una asociación que actúa legalmente contra la piratería informática en Europa, Asia y Latinoamérica

Fraude procesal.- La historia del fraude, nace de la mitología romana, "*Fraus"*

era la diosa de la traición, una ayudante de Mercurio. La palabra "fraude" tiene su origen en su nombre.

Fraude bancario.- El elemento común en todas las definiciones es la actuación intencional que genera un perjuicio a un tercero. Para redondear el concepto podríamos agregar el elemento de ocultación de las actuaciones indebidas, que acompaña usualmente a la conducta fraudulenta.

DATA DIDDLING.- conocido también como introducción de datos falsos, es una manipulación de datos de entrada al computador con el fin de producir o lograr movimientos falsos en transacciones de una empresa.

TROYAN HORSE.- En informática,se denomina troyano o caballo de Troya (traducción literal del inglés *Trojan horse*) a un software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo pero al ejecutarlo le brinda a un atacante acceso remoto al equipo infectado.[1] [2] El término troyano proviene de la historia del caballo de Troya mencionado en la Odisea de Homero.

SUPERZAPPING.- es un programa informático que abre cualquier archivo del computador por muy protegido que esté, con el fin de alterar, borrar, copiar, insertar o utilizar, en cualquier forma no permitida, datos almacenados en el computador.

TRAP DOORS.- consiste en la práctica de introducir interrupciones en la lógica de los programas con el objeto de chequear en medio de procesos complejos, si los resultados intermedios son correctos, producir salidas de control con el mismo fin o guardar resultados intermedios en ciertas áreas para comprobarlos más adelante.

Anexo III.

Caso Práctico.

SEÑOR AGENTE FISCAL

DISTRITAL DE TUNGURAHUA.

Viviana Cecilia Panimboza Ortiz, ecuatoriana, de 27 años de edad, de estado civil casada, de ocupación empleada privada, domiciliado el parroquia la Merced calle en esta ciudad de Ambato, Provincia de Tungurahua, ante usted comparezco y denuncio:

El único nombre y apellido del demandado que conozco son: Julio Cesar Romoleroux Vanegas propietario de la cuenta Nº1070905619 del Banco de Machala numero de cedula 0927118422.

Es el caso señor fiscal que a inicio del mes Diciembre del 2013, yo le contacte al señor antes nombrado por medio de OLX, porque estaba ofreciendo un carro VOLKSWAGEN BORA en tres mil dólares 3.000 USD, me contacte vía email, sobre el negocio del vehículo él, me indica que el señor vivía en el Ecuador y que había hecho un poder con mercado libre indicando que mercado libre realizaría toda la gestión y entregar, me indican igual forma que para iniciar la transacción debía realizar la trasferencia por el cincuenta por ciento del valor del vehículo para que se inicie la entrega, me pidió los datos para la elaboración de la supuesta factura, me indico que se tenía que escanear el comprobante de la trasferencia al correo electrónico Pago@transacción-mercadolibre.com.ec la trasferencia se realizo al señor Julio Cesar Romoleroux Vanegas a la cuenta del Banco de Machala Nº Nº1070905619 una vez escaneado me indicaron que tenía que cancelar la otra diferencia o el otro cincuenta porciento a la mima cuenta para que me pueda llegar el vehículo y si yo encontraba alguna novedad con el vehículo me devolverían el dinero el señor Julio Cesar Romoleroux Vanegas es el que se tenía que contactar con migo para entregarme el vehículo en calidad de

representante del mercado libre, en la misma factura indicaba que tenían el plazo máximo de dos días para entregar el vehículo.

La primera trasferencia se realiza por mil quinientos dólares americanos 1500 USD, el 10 de diciembre del 2013, desde ese momento me empezaron a llamar constantemente del número que registraba en mi celular como desconocido en el cual me manifestaban que si no daba el otro anticipo no me va a llegar el vehículo y que no hay problema si no me ha llegado el vehículo y que se demora la entrega además es un medio súper seguro y que no existe problema, por lo que accedí a depositar el otro cincuenta por ciento el 12 de diciembre del 2013. Además me manifestaron que me dijeron que me entregarían a mas tardaren dos días, hecho que no ha pasado.

Por cuanto he sido perjudicado económicamente por el señor Julio Cesar Romoleroux Vanegas mediante engaño, y el hecho relatado constituye Delito Público de Instancia Oficial, denuncio la ejecución de este ilícito por el señor los retenciones y cobros ilegales de parte de la Cooperativa Oscus el único nombre y apellido que conozco, en contra de quien se resolverá el inicio de la Instrucción Fiscal correspondiente, a fin de imputar al denunciado respecto de la responsabilidad del delito detallado.

De conformidad con lo dispuesto en el Art. 216 numeral 9 del Código Penal vigente, solicito a Usted Señor Agente Fiscal, se digne pedir al Juez de Derecho, que se dicte las medidas cautelares personales en contra del denunciado, ya que dentro de las normas penales este ilícito esta claramente tipificado como Estafa y Peculado Bancario, concretamente tipificado por los Arts. 257 y 563 del Código Penal.

Por cuanto el denunciado trata de deslindar responsabilidades, pido se solicite al Juez de Derecho, la correspondiente prohibición de salida del país, oficiándose para dicho efecto a Migración y Extranjería.

Solicito que se envié atento oficio al Banco de Machala a fin de ver si el señor Julio Cesar Romoleroux Vanegas es propietario de la cuenta o Nº 1070905619.

No me hallo prohibido para denunciar.

Reconoceré mi firma y rúbrica cuando así lo disponga.

Notificaciones que me correspondan las recibiré en el casillero judicial 580 de mi Abogada patrocinadora Adriana Jiménez, Profesional en derecho a quien autorizo para que con su sola firma suscriba cuanto escrito sea necesario en defensa de mis intereses.

Firmo con mi Patrocinador.

ES LEGAL.

Adriana Jiménez
Abogada
Mat: 18-2010-17

Viviana Panimboza
C.C.1804240925