UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

CARRERA DE DERECHO

TEMA:

"LA LEGISLACIÓN PENAL ECUATORIANA Y LOS DELITOS INFORMÁTICOS EN LA CIUDAD DE AMBATO."

Proyecto de Graduación previo a la obtención del Título de Abogado de los Juzgados y Tribunales de la República del Ecuador.

AUTOR:

Angel David Poveda Hernández

TUTOR:

Dr. Mg. Klever Pazmiño

Ambato - Ecuador
2015

TEMA:

LA LEGISLACIÓN PENAL ECUATORIANA Y LOS DELITOS INFORMÁTICOS EN LA CIUDAD DE AMBATO.

APROBACIÓN DEL TUTOR

En calidad de Tutor del Trabajo de Investigación sobre el tema **"LA LEGISLACIÓN PENAL ECUATORIANA Y LOS DELITOS INFORMÁTICOS EN LA CIUDAD DE AMBATO."**, del Sr. Ángel David Poveda Hernández Egresado de la Carrera de Derecho de la Facultad de Jurisprudencia y Ciencias Sociales de la Universidad Técnica de Ambato, considero que dicho trabajo de Graduación reúne los requisitos y méritos suficientes para ser sometidos a Evaluación del Tribunal de Grado, que el H. Consejo Directivo de la Facultad designe, para su correspondiente estudio y calificación.

Ambato, 29 de Abril del 2015.

……

Dr. Mg. Klever Pazmiño

TUTOR

APROBACIÓN DEL TRIBUNAL DE GRADO

Los Miembros del Tribunal de grado APRUEBAN el Trabajo de Investigación sobre el tema **"LA LEGISLACIÓN PENAL ECUATORIANA Y LOS DELITOS INFORMÁTICOS EN LA CIUDAD DE AMBATO."** presentado por el Sr. Ángel David Poveda Hernández, de conformidad con el Reglamento de Graduación para obtener el Título Terminal de Tercer Nivel de la U.T.A.

Ambato,……..…..

Para constancia firma:

……..

Presidente

…… ……

Miembro Miembro

AUTORÍA

Los criterios emitidos en el trabajo de investigación **"LA LEGISLACIÓN PENAL ECUATORIANA Y LOS DELITOS INFORMÁTICOS EN LA CIUDAD DE AMBATO."**, como también los contenidos, ideas, análisis, conclusiones y propuestas son de responsabilidad del autor.

Ambato, Abril del 2015.

EL AUTOR

…….

Angel David Poveda Hernández

172245646-2

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga de esta 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 mi 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, Abril del 2015.

EL AUTOR

…….

Angel David Poveda Hernández

C.I. 172245646-2

DEDICATORIA

Con mucho cariño y sencillez quiero dedicar el presente trabajo de graduación a mis padres, hermanas y sobrinos, que constituyeron un apoyo incondicional, en el transcurso de mi vida dentro de todos los ámbitos, sabiendo guiarme y orientarme y al mismo tiempo siendo mi fortaleza para seguir adelante.

AGRADECIMIENTO

Es necesario manifestar mis sinceros agradecimientos en primer lugar a Dios y a la Virgen Santísima por todas las bendiciones recibidas y al mismo tiempo a todas las personas que con su apoyo han contribuido para el desarrollo del presente trabajo de graduación, a la Facultad de Jurisprudencia y Ciencias Sociales de la Universidad Técnica de Ambato, a la Carrera de Derecho y sus docentes, especialmente a mi tutor el Doctor Klever Pazmiño quien con un consejo oportuno supo dirigir el presente trabajo.

ÍNDICE GENERAL

CONTENIDO **Pág**.

CAPÍTULO II
MARCO TEÓRICO

CAPÍTULO III

METODOLOGÍA

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

CAPÍTULO VI

PROPUESTA

ÍNDICE DE TABLAS

Pág.

ÍNDICE DE GRÁFICOS

Pág.

RESUMEN EJECUTIVO

Para desarrollar un proyecto de investigación es importante delimitar una problemática que necesite solución urgente. Y en la actualidad y con el constante avance de los sistemas de información y el continuo aparecimiento de nuevas tecnologías los vacíos legales en las diferentes áreas del Derecho se van haciendo más visibles por lo que la Ley debe reformarse constantemente, obedeciendo así al principio de modernización de la ley y vinculándose estrechamente con el surgimiento de nuevos y desconocidos medios tecnológicos buscado de esta manera regular las actuaciones de las personas en el ámbito legal y a su vez teniendo en cuenta el progreso que ha experimentado la sociedad mismo que supone una evolución en las formas de infringir la ley, dando lugar a la diversificación de delitos tradicionales como la aparición de nuevos actos ilícitos los que requieren un tratamiento apropiado mas no convencional

En el presente trabajo, luego de recolectar datos provenientes de diversas fuentes, tales como: el Código Orgánico Integral Penal, libros Sobre Delítos informáticos, Ciber Delincuencia, Diccionarios Jurídicos y la constante difusión a través los distintos medios de comunicación se ha evidenciado una problemática que surge por un vacío legal en materia de delítos informáticos, es por eso que ésta investigación se enfoca en la aparición de nuevos delitos cometidos a través de sistemas de información y su falta de tipificación dentro del Código Orgánico Integral Penal.

Para suplir está vacío se plantea la reforma a la **SECCIÓN TERCERA del Código Orgánico Integral Penal misma que trata sobre los Delitos contra la seguridad de los activos de los sistemas de información y comunicación la** cual no da una definición exacta de Delito Informático y muchos menos existe una tipificación que incluya, defina, regule y castigue los nuevos delitos informáticos que han surgido con el pasar del tiempo y el avance tecnológico.

Con lo expuesto se pretende que quien haga una revisión de la presente Tesis tenga una idea general del contenido y propósito de la misma.

INTRODUCCIÓN

El presente trabajo de investigación titulado "LA LEGISLACIÓN PENAL ECUATORIANA Y LOS DELITOS INFORMÁTICOS EN LA CIUDAD DE AMBATO" está enmarcado y destinado a identificar un marco general sobre la conceptualización necesaria referente a los delitos informáticos, sus tipos, los bienes jurídicos lesionados por el cometimiento de los mismos, sus principios, la evidencia digital y la informática forense, tratando de presentar una visión global de la situación de los delitos informáticos en el Ecuador en cuanto a su tipificación y sanción de dichas infracciones así como también identificar los retos y brechas que deben ser superados por nuestro país para el tratamiento de los mismos.

El acelerado, desarrollo y perfeccionamiento de los sistemas informáticos no solo ha provocado el beneficio y avance de la sociedad a nivel mundial, sino que de la misma manera y sin menor reparo ha evolucionado el cometimiento de actos ilícitos adaptándose y abusando de las nuevas tecnologías y del avanzado conocimiento que ciertos individuos pueden tener sobre ellas, perpetrando actos delictivos con toda la premeditación del caso o simplemente aprovechando la oportunidad que se les presenta lesionado bienes jurídicos protegidos

La tipificación existente en el Código Orgánico Integral Penal referente a los delitos Informáticos contempla de manera general estos ilícitos sin tomar en cuenta la subdivisión que pueden tener los mismos, además de no constar una definición de estos, sus tipos y los bienes jurídicos lesionados con la aparición de nuevos tipos y menos con una forma adecuada de combatir estos actos ilícitos ya que en al no existir una tipificación clara los operadores de justicia le dan un tratamiento como si se trataran de delitos convencionales

La importancia de este trabajo de investigación radica en que es necesario garantizar la protección de los bienes jurídicos protegidos de la misma manera que se garantizan estos ante el cometimiento de los actos ilícitos convencionales además de identificar la situación actual en cuanto al cometimiento, tipificación y

sanción de los delitos informáticos.

Este proyecto de investigación se encuentra estructurado por capítulos. La modalidad de la investigación es bibliográfica, documental, de campo, de asociación de variables que nos permitirán estructurar predicciones llegando a modelos de comportamiento mayoritario.

Capítulo I, que se encuentra estructurados con El Problema, el Planteamiento de Problema, la Contextualización a niveles macro, meso y micro, Análisis Crítico, Prognosis, Formulación del problema, interrogantes de la Investigación, Delimitación del Objeto de la Investigación, Justificación, Objetivos, General y especifico.

Capítulo II, denominado Marco Teórico que contiene los Antecedentes Investigativos, Fundamentación Filosófica, Fundamentación Legal, categorías fundamentales, Hipótesis, Señalamiento de Variables.

Capítulo III, nombrado como Metodología incluye la Modalidad Básica de la Investigación, Nivel o tipo de la Investigación, Población y Muestra, Operacionalización de las Variables, Plan de Recolección de Información, Plan de Procesamiento de la Información.

Capítulo IV denominado: Análisis e Interpretación de Resultados incluye Análisis de los Resultados, Interpretación de datos, Verificación de Hipótesis.

Capítulo V, en el que se hace constar las Conclusiones y Recomendaciones.

La solución al problema investigado, se propone en el **CAPÍTULO VI**, PROPUESTA, donde se desarrolla los Datos Informativos, Antecedentes de la Propuesta, Justificación, Objetivos, General, Específicos, Análisis de Factibilidad Fundamentación, Modelo Operativo, Previsión de la evaluación, Glosario, Bibliografía, Legisgrafía, Linkografía y Anexos**.**

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

Tema

"LA LEGISLACIÓN PENAL ECUATORIANA Y LOS DELITOS INFORMÁTICOS EN LA CIUDAD DE AMBATO"

Planteamiento del Problema

Contextualización

Macro- Contextualización

Se considera que internacionalmente muy pocos países cuentan con una legislación que sea capaz de penar los delitos informáticos entre los que se tienen, Estados Unidos, Alemania, Austria, Gran Bretaña, Holanda, Francia, España, Argentina y Chile por lo que se puede mencionar que:

- Los Estados Unidos de Norteamérica para el año 1994 implementó dentro de su legislación el Acta Federal de Abuso Computacional la que fue redactada para reemplazar al Acta de Fraude y Abuso Computacional de 1986, y para delitos como estafas electrónicas, defraudaciones y acceso a dispositivos informáticos son sancionados con prisión desde el año 2000 en el que la Cámara de representantes estableció el acta de Firmas Electrónicas, lo que controla de mejor manera la necesidad de dar validez a documentos informáticos -mensajes electrónicos y contratos establecidos mediante Internet- entre empresas (para el B2B) y entre empresas y consumidores (para el B2C).

De la misma manera Alemania sancionó en 1986 la Ley contra la Criminalidad Económica, que contempla los siguientes delitos:

Espionaje de datos, Estafa informática, Alteración de datos, Sabotaje informático.

En el año de 1986, Alemania como un centro vanguardista en los campos de la filosofía y el derecho, declaro algunos nuevos delitos que atentan contra la integridad económica de los sujetos jurídicos, algunos de ellos son:

- Espionaje de datos: Robo de datos importantes obtenidos con el fin de reproducirse en redes.
- Estafa informática: Robo o engaño económico en cuanto a servicios informáticos personalizados.
- Alteración de datos: Cambios en los datos utilizados para algún fin específico a nivel virtual.
- Sabotaje informático: Una o varias acciones que implique daños a sistemas informáticos, con el fin de perjudicar a los programadores responsables de producirlos.

Si tomamos un ejemplo concreto más cercano a nuestro país, nuestras coyunturas sociales y nuestra realidad, podemos poner el caso de Colombia que en 1999 publica su ley 527, la misma que regula el comercio electrónico, firmas digitales y las entidades de certificación, luego en el mes de mayo del año 2000 Perú publica la ley 27269, sobre Ley de Firmas y Certificados Digitales. Luego, le siguen en el 2001 Argentina y Venezuela en el año 2001, luego Chile y Ecuador en el año 2002.

Meso- Contextualización

En el Ecuador así como en los demás países, todos los principios jurídicos, legales y procesales, así como doctrinarios, están presentes en el tratamiento del delito informático, su investigación y juzgamiento, sin embargo las características

propias de este delito que pertenece a una nueva era, a la era de la información y el conocimiento, trasciende al ordenamiento jurídico vigente, constituyendo un elemento de desviación o quiebre del sistema jurídico. (Guerrero, 2013)

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 Orgánico Integral Penal Ecuatoriano, logrando así una protección concreta y específica a este tipo de actos. (Posso, 2014)

Por la falta de tipificación que propicie el tratamiento adecuado a estos delítos se tiene como consecuencia que las personas que cometen estos ilícitos (delincuentes informáticos), queden en total impunidad en delítos no tipificados en nuestra legislación. De tal forma que los perjuicios que se ocasionan a las personas naturales, y a las personas jurídicas de derecho público y privado sea de gran magnitud en el Ecuador, por lo que la investigación determina cuáles delitos son sancionados en nuestra Legislación y que ilícitos deben agregarse a la misma.

Respecto a los delitos que han sido incorporados en el Código Orgánico Integral Penal Se manifiestan los contenidos en la **SECCIÓN TERCERA sobre los Delitos contra la seguridad de los activos de los sistemas de información y comunicación** a partir del articulo 229 hasta el articulo 234 dentro de los cuales no se dan una definición exacta de Delíto Informático y muchos menos existe una tipificación que incluya, defina, regule y castigue los nuevos delitos informáticos que han surgido con el pasar del tiempo y el avance tecnológico.

Micro- Contextualización

Pese a la existencia de una normativa legal que tipifica y sanciona ciertos delítos informáticos la incidencia en el cometimiento de los mismos no es para

nada bajo según investigaciones realizadas sobre el tema, y además de la aparición de nuevas modalidades de cometer estos ilícitos, los que no pueden ser sancionados ya que es necesaria la incorporación de un marco legal que contemple a los delitos informáticos de una manera integral.

De la misma manera en la ciudad de Ambato con el transcurrir de los años y el avance tecnológico se ha evidenciado el cometimiento de delítos informáticos de los mismos cuya consecuencia la principal es la violación de un bien jurídico protegido, razón que conjugada con la falta de Leyes y Normativas Legales que contemplen aspectos significativos y específicos de las nuevas tecnologías y además de la falta de socialización y difusión los hechos delictivos conlleva a que los ofendidos no realicen la respectiva denuncia, y el sujeto activo no reciba la sanción que le correspondería según la gravedad de su acto.

Esta propuesta de tesis sirve para poder identificar un marco general sobre la conceptualización básica necesaria relativa a los delitos informáticos, tipos de delitos, sus objetivos, importancia, sus principios, la evidencia digital y la informática forense.

Árbol de Problemas

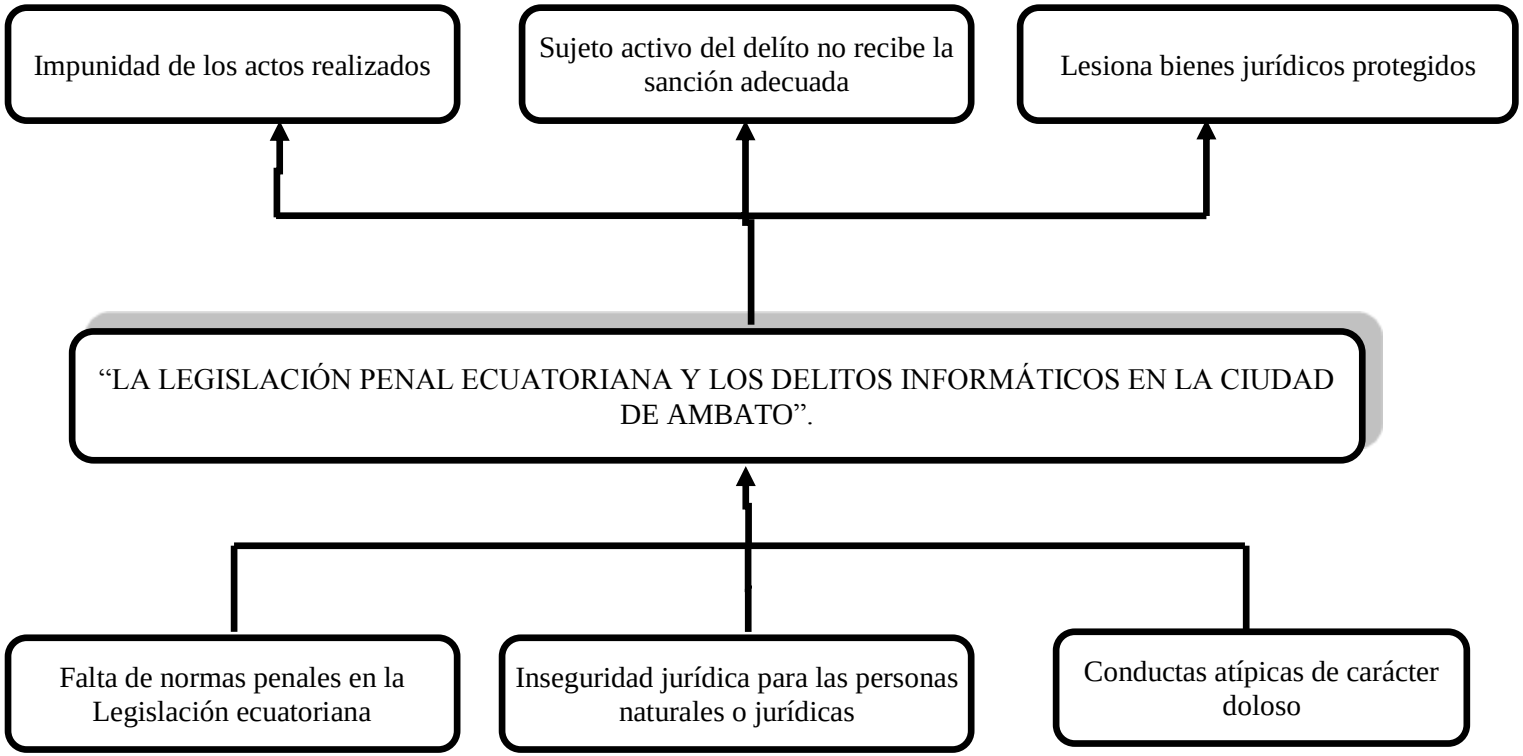


Gráfico No. 1 Relación causa – efecto
Fuente: Investigadora
Elaborado por: David Poveda

Análisis Crítico

La ausencia de tipicidad de una norma jurídica adecuada y específica que tipifique y sancione los delitos informáticos de una manera especializada provoca que estos actos delictivos se queden en la impunidad violentando de esta manera el bien jurídico protegido.

Múltiples son las razones para que los operadores de justicia y a su vez los organismos auxiliares no puedan dar el tratamiento necesario a estos delítos principalmente al no tener una norma jurídica que tipifique de manera directa estos hechos delictivos ya que ante su ausencia suelen asociarlos con los delítos convencionales, este procedimiento en nuestro país es muy cercano a la realidad en la que nos encontramos muy a pesar de la incorporación de los **Delitos contra la seguridad de los activos de los sistemas de información y comunicación contenidos en la sección tercera del Código Orgánico Integral Penal** ya que con la existencia de estos se puede dar sanción a un grupo determinado de ilícitos informáticos, pero existe todavía la necesidad imperativa de que los delitos informáticos sean tratados de una manera más específica, definiendo y tipificando los nuevos ilícitos configurados por la utilización de la tecnología.

Como es evidente en varios de los países tanto latinoamericanos como europeos se hace presente la misma necesidad preponderante de poder frenar el apresurado auge de estos ilícitos, pero en muchos de los casos como en nuestro país el desconocimiento tanto por parte de la parte ofendida como de los mismos operadores de justicia genera una falta de interés y una imposibilidad de denunciar e investigar este tipo de abusos, acarreando consigo un sinnúmero de lesiones a los bienes jurídicos protegidos

Prognosis

La invención de nuevas tecnologías, hace que los medios de cometimiento, en este caso de los delitos informáticos avance junto con estas, es por eso que la Legislación Ecuatoriana para lograr un grado de eficacia y efectividad requiere de

una tipificación plena y clara de aquellos delitos que se cometen en el mundo, y que a la vez requieren de respuestas concretas y precisas, hasta el punto que puedan ser perseguidos desde cualquier país en el que los hechos estén efectivamente tipificados como delitos.

Razón por la cual el Ecuador al no poseer una tipificación adecuada y acorde con las características de los acontecimientos delictivos que día tras día se van multiplicando en su cometimiento y en sus tipos, seguirá siendo blanco de vulneración de derechos al no existir una normativa legal que ampare y proteja de una manera efectiva y precisa.

Formulación del Problema

¿La tipificación y sanción de los delítos informáticos no contenidos en el Código Orgánico Integral Penal puede evitar la impunidad de estos actos ilícitos?

Interrogantes (subproblemas)

- ¿Existe la tipificación y sanción acorde con los delitos informáticos dentro de la legislación ecuatoriana?
- ¿De qué manera la falta de difusión y el desconocimiento de los delitos informáticos genera impunidad en estos actos?
- ¿Es necesario una disposición legal que determine e identifique directa y eficazmente a los delítos informáticos?

Delimitación del Objeto de Investigación

La siguiente Investigación se maneja bajo los siguientes parámetros:

1. **Delimitación del contenido:**

CAMPO: Jurídico
AREA: Derecho Penal Informático

ASPECTO: Delitos Informáticos

2. **Delimitación espacial**

   La presente investigación se desarrollará en los Tribunales Penales de la Corte Provincial de Justicia de Tungurahua, Fiscales especializados de la Provincia de Tungurahua, Abogados en libre ejercicio y Agentes Investigadores de la Policía Judicial.

3. **Delimitación temporal**

   El periodo de estudio del presente tema será durante el año 2014.

4. **Unidades de observación:**

   Funcionarios de la Fiscalía Provincial de Tungurahua
   Jueces de lo Penal
   Abogados en libre ejercicio
   Agentes Investigadores de la Policía Judicial

Justificación

La presente investigación titulada "LA LEGISLACIÓN PENAL ECUATORIANA Y LOS DELITOS INFORMÁTICOS EN LA CIUDAD DE AMBATO", constituye una temática de gran importancia jurídica y social, ya que el derecho con el pasar del tiempo ha ido evolucionado constantemente para acoplarse a los eventos atípicos que de la misma manera van surgiendo y necesitan ser reglamentados de manera adecuada y acorde con la realidad social y tecnológica aplicando principios basados en la esencia misma del ser humano.

El tema motivo del presente estudio es escogido porque la informática en la actualidad es una de las herramientas básicas en el quehacer diario de las personas, razón por la cual personas inescrupulosas ya sea en forma premedita o simplemente aprovechando la oportunidad incurren en conductas ilícitas y lesionan bienes jurídicos protegidos.

Ante el inminente avance de los sistemas informáticos y en virtud de lo anterior, es que se han trazado diversos argumentos y justificaciones respecto de la urgente necesidad de tipificar los delitos informáticos en una norma jurídica y sin contravenir lo dispuesto por el numeral tercero del artículo 13 del Código Orgánico Integral Penal en el que se establece que "queda prohibida la utilización de la analogía para crear infracciones penales, ampliar los límites de los presupuestos legales que permiten la aplicación de una sanción o medida cautelar o para establecer excepciones o restricciones de derechos."

Además de tener muy en cuenta que ante el avance de la tecnología también avanzan junto con ella las nuevas formas de delinquir razón por la cual surgen nuevos actos atípicos mismos que requieren una regulación y una sanción acorde a la falta cometida ya que al no existir una norma legal que regule este inconveniente muchos ilícitos han quedado en la impunidad por el respeto al principio de *Nullum crimen, nulla poena, sine legem*, es decir no hay delito, no hay pena sin ley.

Por tal motivo esta investigación está orientada a determinar establecer en el derecho penal ecuatoriano nuevos delitos informáticos no tipificados y a la par técnicas de investigación, ya que la tipificación del delito tiene que hacerse acorde a los avances de la tecnología.

Además de establecer la creación de nuevas normas penales sancionadoras, ya que el Derecho Penal tiene por objeto prevenir el delito antes que la represión, por esta razón debe estar claramente establecido en la codificación penal todas las infracciones que pueden constituirse en delitos, y quienes los cometen, tienen que saber las penas a las que podría someterse al infringir la Ley.

Objetivos

Objetivo General

- Determinar la incidencia de la tipificación y sanción de los delitos

informáticos no contenidos en el Código Orgánico Integral Penal y evitar la impunidad de estos actos ilícitos

Objetivos Específicos

- Determinar la situación actual de la tipificación y sanción de delitos informáticos

- Determinar los vacíos jurídicos dentro de la normativa jurídica con relación a los delitos informáticos en la declaración, tipificación penalización de los actos ilícitos en especial en el Código Orgánico Integral Penal

- Implementar una propuesta de solución que mediante la tipificación y sanción de los delitos informáticos evite la impunidad de estos actos ilícitos.

CAPÍTULO II

MARCO TEÓRICO

Antecedentes Investigativos

Revisados que han sido los trabajos de Graduación en la Biblioteca de la Facultad de Jurisprudencia y Ciencias Sociales de la Universidad Técnica de Ambato, de esta ciudad de Ambato, se pudo verificar que no existen trabajos de investigación en los que se considere "LA LEGISLACIÓN PENAL ECUATORIANA Y LOS DELITOS INFORMÁTICOS EN LA CIUDAD DE AMBATO."

Del trabajo titulado "LOS DELITOS INFORMÁTICOS Y SU PERJUICIO EN LA SOCIEDAD" del autor Acosta (2012) cuyas conclusiones fueron: Se ha determinado que los en cargados de la administración de justicia y profesionales en libre ejercicio, tienen la necesidad de conocer la normativa penal vigente en materia referente a delitos informáticos, para acceder a los beneficios y saber cuáles son las limitantes que la ley impone a los ciudadanos sobre el tema de los delitos informáticos. Existe la aceptación respecto de la posibilidad de que se implemente un Capítulo exclusivo sobre los delitos informáticos en el Código Adjetivo Penal.

Los Delitos Informáticos son parte del Derecho Penal, que va íntimamente ligado a la humanidad de la persona en razón del ejercicio y goce de sus derechos, y que se traduce como una norma legal que debe también ser respetada y garantizada.

En su mayoría los Jueces de la Sala Especializada de lo Penal, Miembros del Tribunal y Jueces de Garantías Penales de Tungurahua, así como los Fiscales

y profesionales del derecho en libre ejercicio investigados; conocen sobre lo que es el delito informático y desconocen el procedimiento que hay que seguir en los mismos por no existir la presencia de estas causas en nuestro medio, en su esencia se lo realizó como ayuda para solucionar los problemas de administración de Justicia Penal, que existe para sancionar este tipo de delitos.

Muy pocos profesionales del derecho conocen del procedimiento que hay que seguir en estos casos, según lo refleja las encuestas realizadas; que arrojan los resultados detallados anteriormente.

Como reflexión ante ésto, considero que el derecho debe tener la facultad de adaptarse a los nuevos espacios de socialización, en este caso la web como espacio de intercambio, es un espacio potencial de delito y por esto el derecho debe incursionar en un análisis inmediato y una incorporación inmediata de conocimiento en los consultorios jurídicos y mecanismos primarios de ejecución del derecho.

De la investigación titulada DELITOS COMETIDOS A TRAVÉS DE SISTEMAS INFORMÁTICOS del autor Ron (2010) cuyas conclusiones fueron:

Los Delitos Informáticos son el resultado de la consideración de lesividad, que la sociedad a través del Legislador ha dado a los actos atentatorios realizados a través de la tecnología informática y la comunicación, a bienes jurídicos tradicionales, que merecieron reformas al Código Penal, así como la consideración de bien jurídico tutelado a la información, para evitar la afección de otros bienes jurídicos tradicionales. Pese a que se discute si los delitos informáticos son estrictamente tales, o solo nuevas formas de perpetración del delito, la mayor parte de legislaciones, han incluido reformas al Código Penal que contienen delitos en donde, son los medios de información son el objeto del delito, ya que responden a la necesidad social y procesal en donde los administradores de justicia dejaban en la impunidad ciertas conductas, porque el medio de su comisión era poco tradicional, diluía la responsabilidad del autor, e impedía un ajuste irrestricto al tipo, lo que a su parecer impedía la subsunción del

acto al hecho considerado antijurídico, quedando el mismo en la impunidad. (Ron Torres, 2010)

Los delitos informáticos, son actos que no han logrado llegar a un modo correcto de tipificación, procedimiento ni tratamiento del problema, podrían ser incluso abordados como un nuevo debate necesario en el mundo del derecho.

El surgimiento de nuevos delitos como este nos lleva a preguntarnos: ¿Qué debe hacer el derecho frente a las nuevas formas de delito que se dan con los avances tecnológicos y científicos?

La única y mejor forma de responder esta pregunta subyace en las formas de relación social y en los principios básicos del derecho que aluden a la defensa de la propiedad privada.

Pero de igual forma esta nueva ola reformatoria al delito tradicional, hizo punibles nuevos actos, en donde al fin de la acción dañosa es la información tratada, generada o archivada por medios informáticos y/o transmitida por medios telemáticos, ya que si bien se pueden afectar bienes jurídicos tradicionales, como la propiedad, seguridad, fé pública, la intimidad, o simplemente con un valor personal, que se vería afectado directamente como consecuencia de esta acción y que no era posible su adecuación en los delitos tradicionales. (Ron Torres, 2010)

Como ya he mencionado creo que si nos adentramos en los confines de la lógica jurídica, estos procedimientos son legítimos, posibles y pueden plantearse desde el principio de respeto a la integridad de los sujetos jurídicos a partir del respeto a la propiedad sobre lo que ellos son capaces de producir y generar.

Pese a que esta discusión doctrinaria siga, la realidad ha respondido a esta incógnita, estas acciones afectan tanto a otros bienes jurídicos tradicionales como a la información, la cual es tan importante en esta cuarta era, que como sociedad la estamos viviendo, la de la Sociedad de la Información, en donde es precisamente la información acumulada y tratada, el medio productivo que la

sustenta y que necesariamente genera en el individuo que la posee, la necesidad de protección y luego, por la dinámica en la economía, movilizada al aparato estatal a fin de que se cree mecanismos de prevención para su vulneración y concomitantemente para su sanción. (Ron Torres, 2010)

Ahora, las formas de abordar el espacio del tiempo son diferentes y dentro de estos nuevos espacios virtuales deben existir normas de regulación y separación de la información. Al no contar con un espacio físico definido, nos queda pensar que el espacio de lo virtual debe estar regulado pero no precisamente por los Estados dentro de su jurisdicción. El campo de acción del Estado es un país, este se encuentra delimitado por costumbres, hábitos, etnias, cultura pero si hablamos del plano empírico, la delimitación del espacio de acción estatal son los límites de dicho país.

El espacio virtual no es el mismo que el espacio físico, no son equivalentes el uno del otro. El campo de acción de los delitos informáticos es un campo construido de forma orgánica y en red. Por orgánico quiero decir interconectado funcionalmente y en red se refiere a la estructura total que deriva de dichas interconexiones funcionales.

Cabe hacer un paréntesis en este punto y aclarar que el espacio virtual ha logrado abarcar relaciones sociales que se realizan en el espacio físico: relaciones mercantiles, afectivas, de derecho, de hecho, y de muchos otros tipos utilizados a diario, este traslado se da debido a que el espacio virtual es un espacio construido básicamente a partir de la comunicación.

Finalmente, la mejor forma de regular estos espacios sería a través del uso de mecanismos reguladores internos del espacio informático.

Para esto, encontramos en el mundo concreto, la posibilidad de sanción a través de la cooperación en red en el mundo real, o mejor dicho, el mundo que está atravesado y regulado a partir del espacio/tiempo concretos. Esta coordinación se lograría a través de la cooperación internacional solamente.

Fundamentación Filosófica

El investigador se alinea en el paradigma Crítico Propositivo porque considera que de esta manera se determina la realidad y así dar un análisis Crítico – Propositivo porque los problemas parten de situaciones reales y tiene por objeto transformar esa realidad, al mejoramiento colectivo o individual implicados en ella. Por tanto, los problemas de investigación arrancan de la acción.

Según el paradigma Crítico – Propositivo el diseño de investigación se puede definir como dialéctico, porque se va generando a través del diálogo del grupo investigador. Es crítico porque cuestiona la situación actual, y es propositivo no solo porque se detiene en la observación de los fenómenos, sino que busca y plantea alternativas de solución social del problema investigado. La finalidad de esta investigación es realizar un análisis amplio acerca de la problemática originada en el acometimiento de delitos y su relación directa con la aplicación de sanciones a adolescentes.

Fundamentación Epistemológica

La presente investigación se inclina por el subjetivismo, el realismo y sobretodo el relativismo el mismo que sostiene que las cualidades de un elemento provienen de la relación con otras cosas.

Para acotar, veo en el subjetivismo la posibilidad de respetar a los sujetos como agentes de creación de lo interno, en el caso de mi investigación, los resultados se asientan sobre las acciones de sujetos. Considero que el derecho en sí, debe y puede asegurar el bien de los sujetos en el espacio social, ya que en su planteamiento ve el respeto a las normas para lograr una convivencia sana. Desde ese punto de vista, el problema que yo planteo alineado con los fundamentos del derecho es subjetivista.

El realismo está basado en tomar las variables concretas de la realidad para emitir un juicio, un delito es básicamente la puesta en evidencia de varias acciones

aisladas y el veredicto debe llevar a cabo una deliberación justa. El derecho en su aplicación busca los hechos concretos y reales, por tanto es una práctica realista.

Finalmente, viene el relativismo que a mi forma de verlo es la visión más importante al momento de comprender las formas en que se relacionan los factores que componen un problema entre sí, las acciones pueden tomarse de varias formas. Cuando existen delitos que no se están tomando de manera seria, puede que exista un mal uso del relativismo. Lo bueno de esta corriente es que es muy versátil al momento de entender e incorporar nuevas formas de solucionar conflictos y ver el mundo.

Fundamentación Sociológica

La presente investigación tiene un enfoque social ya que al determinar las causas del comportamiento atípico de los adolescentes, encontramos factores externos e internos como son la familia, la educación y la sociedad, que conllevan a que los adolescentes infrinjan la ley.

Este enfoque favorece la comprensión y explicación de los fenómenos sociales acerca de la falta de tipificación de los delitos informaticos, con el afán de encontrar soluciones a esta problemática social

Fundamentación Legal

En el Ecuador a partir de que el Código Orgánico Integral Penal entro en vigencia el pasado diez de agosto del dos mil catorce son sancionados una diversidad de delitos informáticos, pero el amplio alcance de las Nuevas Tecnologías de Información y Comunicación o también conocidas como NTIC'S se genera no solo el avance a pasos agigantados para los actos lícitos de las personas sino que también genera y propicia de cierto modo la aparición de nuevas y avanzadas formas de delinquir dejando en vulnerabilidad a los ciudadanos razón por la cual es necesario hacer referencia a las normativas legales que regulan estos actos en el Ecuador.

Constitución de la República del Ecuador - 2008

El Art. 66 determina en los numerales 19 y 20 que "reconoce y garantiza a las personas 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" y "reconoce a los ciudadanos su derecho a la protección de sus datos, es decir nadie puede invadir la vida privada de los individuos". Al estar garantizado este derecho en la Carta Magna se convierte en deber primordial del Estado a través de los Organismos competentes evitar cualquier tipo de delito informático y de ocurrir sancionarlo con la severidad del caso.

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 señalaba que "la información es un derecho de las personas que garantiza el Estado".

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 Política del Ecuador vigente, 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.

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; la interpretación de la Ley y el ejercicio de la Propiedad Intelectual se rigen por la legislación ecuatoriana y por los tratados internacionales incorporados al cuerpo legal ecuatoriano. 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.

Código Orgánico Integral Penal

Que fue publicado el lunes 10 de febrero de 2014 Registro Oficial Nº 180 cuerpo legal en el que se introdujeron ciertos delitos informáticos con su respectiva sanción estando estas contenidas en la SECCIÓN TERCERA Delitos contra la seguridad de los activos de los sistemas de información y comunicación esto a partir del artículo 229 hasta el artículo 235.

El Artículo 229 determina acerca de la revelación ilegal de base de datos sanciona el cometimiento de este delito con pena privativa de la libertad de uno a tres años sea que el cometimiento del mismo fuere realizado en provecho propio de quien lo comete o de un tercero realizando de una manera voluntaria e intencionada la violación del secreto contenido en una base de datos o cualquier otro medio semejante ya sea este electrónico o informático, endureciéndose la pena si el delito fuera cometido por un servidor público o por empleados bancarios que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.

El Artículo 230 que hace referencia a la Interceptación ilegal de datos establece la sanción con pena privativa de libertad de tres a cinco años:

Las personas que sin orden judicial previa, intercepten, escuchen, desvíen, graben u observen, un dato informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.

Las personas que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, Software malicioso que busque de tal manera inducir a una persona a ingresar a una dirección o sitio de web diferente a la que quiere acceder ya sea este un servicio financiero, pago electrónico o cualquier otro sitio personal o de confianza.

De la misma manera es el numeral 3 del mismo artículo se establece la protección de la clonación de tarjetas que contengan cintas magnéticas de datos y a la vez el numeral 4 sanciona a la persona que facilite la comisión del delito contenido en el numeral 3.

El Artículo 231 que se refiere a la Transferencia electrónica de activo patrimonial es importante para la presente investigación ya que por medio de la manipulación dentro del funcionamiento del programa, sistema informático o telemático que contenga los activos de una persona se configura otro delito que es la apropiación no consentida de un activo patrimonial mismo que será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial para sí mismo o para otra persona.

Así mismo el **Artículo 232 habla sobre el Ataque a la integridad de sistemas informáticos** sancionando con pena privativa de la libertada de tres a cinco años a la persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de

información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, así mismo a quien desarrolle o comercialice, dispositivos o programas informáticos maliciosos destinados a causar los efectos antes indicados, si este acto se realizara a bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.

En el **Artículo 233 se encuentra contenida la sanción para los Delitos contra la información pública reservada legalmente** misma que será de tres a cinco años para la persona que destruya o inutilice información clasificada de conformidad con la Ley y de la misma forma será sancionado el servidor público que se apodere de esa información.

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

Ley de Propiedad Intelectual

La Ley de Propiedad Intelectual (LPI.) publicada en el Registro Oficial N° 320 del 19 de Mayo de 1998, nace con el objetivo de brindar por parte del Estado una adecuada protección de los derechos intelectuales y asumir la defensa de los mismos, como un elemento imprescindible para el desarrollo tecnológico y económico del país. El organismo nacional responsable por la difusión, y aplicación de las leyes de la Propiedad Intelectual en el Ecuador es el INSTITUTO ECUATORIANO DE PROPIEDAD INTELECTUAL (IEPI), el mismo que cuenta con oficinas en Quito, Guayaquil y Cuenca. Es una persona

jurídica de derecho público, con patrimonio propio, autonomía administrativa, económica, financiera, y operativa, con sede en la ciudad de Quito.

Ley Especial de Telecomunicaciones

La Ley Especial de Telecomunicaciones fue publicada en el Registro Oficial N° 996 del 10 de Agosto de 1992, en el que se declara que es indispensable proveer a los servicios de telecomunicaciones de un marco legal acorde con la importancia, complejidad, magnitud tecnología y especialidad de dichos servicios, así como también asegurar una adecuada regulación y expansión de los sistemas radioeléctricos, y servicios de telecomunicaciones a la comunidad que mejore de forma permanente la prestación de los servicios existentes.

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.

Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, en su Capítulo III Articulo 49, Acción de Habeas Data establece que "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".

En la Constitución Política del Ecuador vigente (2008), en su capítulo tercero de las Garantías Jurisdiccionales de su sección quinta Art. 92 sobre la acción de Habeas Data, también se establece recurso jurídico de Habeas Data. De acuerdo a la especificación contemplada en la Ley de Comercio Electrónico, Firmas Digitales y Mensajes de Datos, en su título quinto de las infracciones

informáticas, los delitos informáticos que se tipifican, mediante reformas al Código Penal hoy contenidas en el Código Orgánico Integral Penal. Hemos visto la definición de los delitos informáticos, su principal insumo que es la evidencia digital y las técnicas o mecanismos con los procedimientos existentes para su investigación, vale destacar, entonces que los profesionales dedicados a la persecución de actos ilícitos en los que se utilizan medios tecnológicos, se mantengan a la vanguardia de conocer los avances que se den de ésta índole, y de esta manera mantenerse preparados y reaccionar de manera adecuada ante los actos cometidos por la delincuencia informática.

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 comentan relacionados con las tecnologías.

Categorías Fundamentales

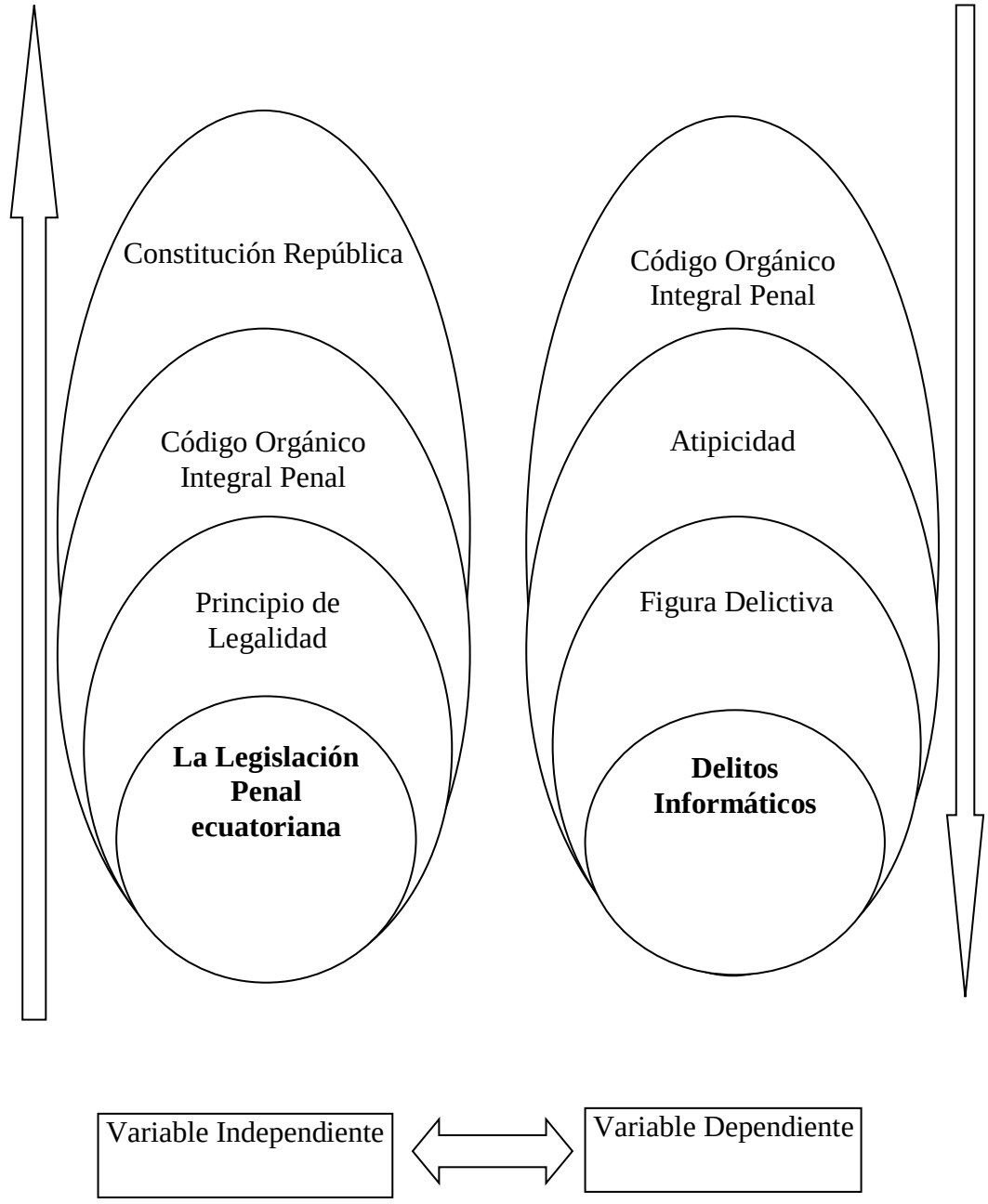


Gráfico No. 2 Categorías Fundamentales

Fuente: Investigador

Elaborado por: David Poveda

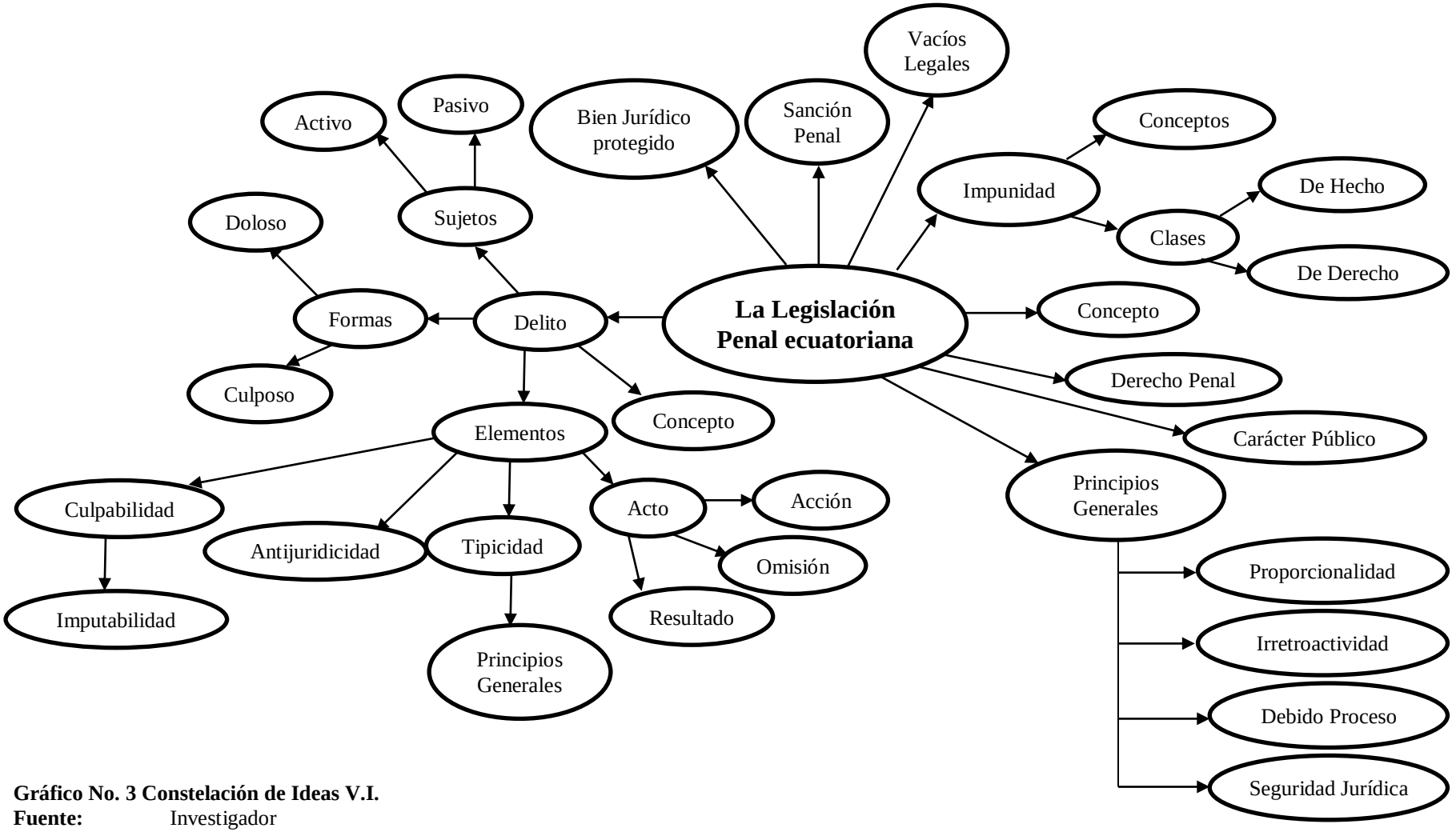


Gráfico No. 3 Constelación de Ideas V.I.
Fuente: Investigador
Elaborado por: David Poveda

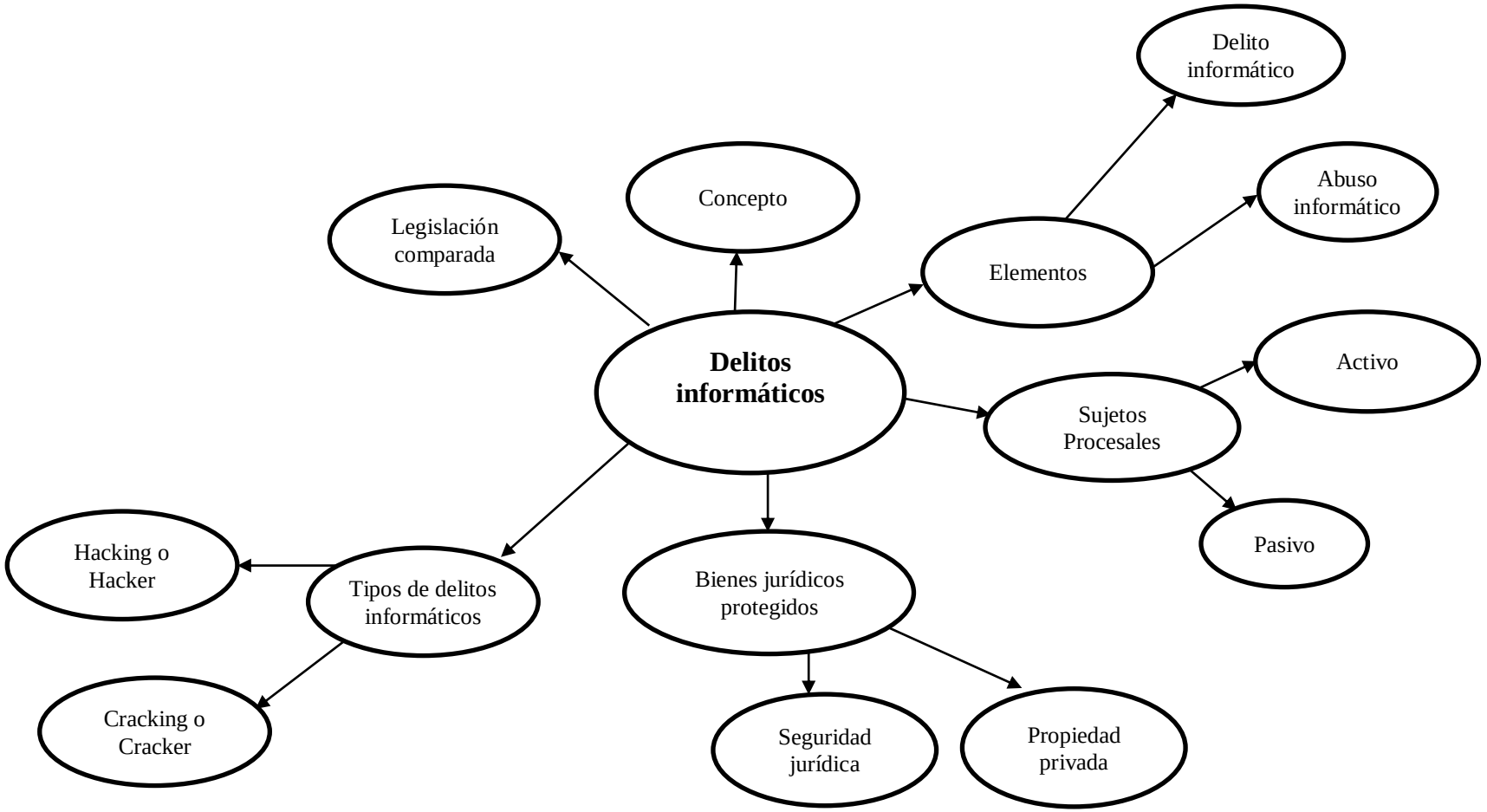


Gráfico No. 4 Constelación de Ideas V.D.
Fuente: Investigador
Elaborado por: David Poveda

Definición de categorías fundamentales

Variable independiente

Constitución Ecuatoriana

La Constitución de la República del Ecuador es la norma jurídica fundamental del Estado, es decir la ley suprema que sirve para reglar su organización y establecer las relaciones del Poder Público con las Funciones y Órganos del mismo y las de las personas y la sociedad con el Estado, además de ser el fundamento y la fuente de la autoridad jurídica que sustenta la existencia del Ecuador y de su gobierno.

La supremacía de esta constitución está por sobre cualquier otra norma jurídica, proporciona el marco para la organización del Estado ecuatoriano, y para la relación entre el gobierno con la ciudadanía ecuatoriana.

Código Orgánico Integral Penal

El Código Orgánico Integral Penal, es un conjunto unitario, ordenado y sistematizado de las normas jurídicas punitivas del Estado, representa un verdadero cambio radical del sistema penal ecuatoriano además se adecua a las realidades tanto políticas, sociales y económicas que sufre el país, busca plasmar el ius puniendi que significa la facultad sancionadora del Estado. (Espín, 2014)

El código penal, es el segmento de leyes que se encargan de delimitar las penas y regimientos que se dan sobre los delitos, este conjunto es altamente punitivo. En el corazón del código penal se encuentra inscrita la necesidad de cambios.

Es más podríamos afirmar que de cierta forma y hasta cierto punto, las realidades políticas y sociales han producido conflictos, es más, si lo vemos desde un punto de vista sociológico los problemas y conflictos son necesarios y

funcionales al sistema social.

De esta manera, el Estado mismo a través del legislador, busca evitar la aplicación de penas arbitrarias, ya que sólo puede ser sancionada penalmente una conducta cuando ésta se consigna expresamente en el mismo Código Orgánico Integral Penal y con la sanción que el mismo establece, su finalidad como está establecido en el Art.1 es " normar el poder punitivo del Estado, tipificar las infracciones penales, establecer el procedimiento para el juzgamiento de las personas con estricta observancia del debido proceso, promover la rehabilitación social de las personas sentenciadas y la reparación integral de las víctimas (Espín, 2014)

Principio de Legalidad

El principio de legalidad es un principio de propio del derecho público, que tiene por objetivo garantizar la seguridad jurídica. Rige entre otras ramas, el derecho penal y el derecho tributario. En el derecho tributario podemos definir que por medio de este se exige que la ley establezca de una manera clara el derecho imponible, los sujetos obligados al pago, el sistema o la base para determinar el hecho imponible, la fecha de pago, las infracciones, las sanciones, y las exenciones, así como el órgano legalizado para recibir el pago por los tributos.

Con el objeto de reforzar este principio se establece la reserva de la ley, que obliga a regular la materia concreta con normas que posea rango de ley. Por lo tanto son materias vedadas al reglamento y a las normativas emanadas del poder ejecutivo.

Este principio sirve también para dar más facultades al poder legislativo en ciertas materias, de sensibilidad especial relativas a al afectación de derechos fundamentales. Es decir es una forma de impulsar la separación de poderes.

"Nadie podrá ser juzgado ni sancionado por un acto u omisión que, al momento de cometerse, no esté tipificado en la ley como infracción penal,

administrativa o de otra naturaleza; ni se le aplicará una sanción no prevista por la Constitución o la ley. Sólo se podrá juzgar a una persona ante un juez o autoridad competente y con observancia del trámite propio de cada procedimiento."

Legislación Penal Ecuatoriana

Es el conjunto de normas que hacen referencia, algunas a los fundamentos en que se ampara el Derecho Penal, y varias a los tipos penales que señalan las infracciones y las sanciones que se les aplica a personas (imputables e inimputables) declaradas responsables mediante fallo ejecutoriado; y, otras que indican los procedimientos que deben seguirse en cada caso concreto para, de la imputación física o material poder llegar a la absolución o a la condena.

HISTORIA

"El constitucionalismo surgió en Europa hace algo más de medio siglo para poder construir un nuevo orden de cosas en la vida social. Su contenido nació, ante todo, de la experiencia europea de las guerras que lo precedieron, desde 1914 hasta 1945, y de las causas de esas guerras." (Botero Marino, 2013)

Se calcula que entre los años de 1939 y 1945 se tuvo más de 50 millones de muertos y desplazados de forma violenta; el constitucionalismo representa la oposición radical a estas acciones o a alguna repetición que pueda haber de la misma es así como toma forma de un fenómeno jurídico-político en contra el totalitarismo y autoritarismo.

Todo esto debe acoplarse a un paradigma que esté relacionado con el constitucionalismo, el paradigma no debe verse ni confundirse con otras formas de representación.

Dicho lo anterior, es cierto, sin embargo, que aún persisten acepciones de "Constitución" y, sobre todo, de "constitucionalismo", que no corresponden fielmente con el significado que acabamos de señalar. Se trata sin duda, de

posiciones explicables por la pura inercia histórica y por su desconexión con el movimiento más vivo y relevante que la afirmación y la expansión del Estado constitucional ha venido produciendo. Obedecen más al pasado que al presente (Reyes, 2007)

Dicho de otro modo, el constitucionalismo tiene posibilidades de convertirse en paradigma, ya que es una construcción histórica en tanto aprobada por este filtro social, y da respuestas de experiencias del pasado que se han construido en la vida humana. Este paradigma puede tener variaciones considerables pero va a precautelar siempre por defender esta lucha histórica antes mencionada.

DEFINICIÓN

El constitucionalismo requiere, en primer lugar, de la existencia de unos instrumentos jurídicos que garanticen la aplicación de la Constitución; y estos no son otros que los propios del control judicial, bien mediante la aplicación de las normas constitucionales por los tribunales ordinarios o bien, también, mediante la creación de los tribunales específicos: los tribunales constitucionales.

Las constituciones precisan de garantías políticas, por supuesto, pero también e inexorablemente de garantías jurídicas, sólo posibles, es decir, efectivas, cuando están aseguradas por controles jurisdiccionales. (Reyes, 2007)

De lo que se puede decir que constitucionalismo es la forma que encontró la sociedad de racionalizar el poder político para de esta forma someterlo a la ley para asi poder defender a los entes más débiles de la sociedad y a cierto tipo de minorías conforme a normas impuestas por la legislación.

El constitucionalismo es entonces un sistema incorporado y sistemático cuyo criterio de acción es la constitución, no se debe tomar netamente como un campo de aplicación de la ley puesto que es el campo de la carta magna de un Estado. Esto implica que es el documento que rige la cultura jurídico-política de

un país, es la abstracción de modos de pensar y proceder, de discernir entre lo correcto y lo incorrecto. Me gustaría afirmar que el constitucionalismo es un punto de encuentro entre las grandes dicotomías morales de un pueblo.

El constitucionalismo procura el máximo logro de la cultura política, al superar el maquiavelismo que justifica al poder por sus fines, y hace que el poder tenga su fin en sí mismo como razón del Estado, que fue la práctica del absolutismo, resulta pues verdadero decir que el constitucionalismo es la técnica de la libertad. (Sachica, 2007)

Aquí, el poder viene a ser una estructura que funciona a través del logro de metas específicas. En el Estado de derecho, a diferencia del Estado planteado por Maquiavelo, existen normas a nivel social que devienen en una aprobación o desaprobación de lo que se hace en base a la evaluación jurídica de las acciones.

Además, podríamos mencionar aquí a los Estados de bienestar como Estados participativos donde la participación ciudadana como mecanismo de veeduría compone varios mecanismos en que se puede crear espacios de libertad para todos.

ANÁLISIS DEL ART 1 CONSTITUCIÓN

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

La soberanía radica en el pueblo, cuya voluntad es el fundamento de la autoridad, y se ejerce a través de los órganos del poder público y de las formas de participación directa previstas en la Constitución.

Los recursos naturales no renovables del territorio del Estado pertenecen a su patrimonio inalienable, irrenunciable e imprescriptible.

Análisis: El Ecuador desde sus principios

EL Ecuador es un Estado constitucional en el sentido de que siempre ha respetado su carta magna, este documento se ha reformado varias veces pero lo ha hecho en la búsqueda de sostener la república, el derecho y la soberanía de un pueblo.

Esta es la voluntad de la cual se habla en el primer artículo de la constitución, la voluntad como fundamento jurídico, es y responde a un grupo de experiencias de una sociedad. Es decir, los grandes principios que fundan el desarrollo del Ecuador en cuanto a derechos, están normados por su aprendizaje histórico y por las conclusiones de sus coyunturas.

Nuestro país, es un país que basa su ingreso en la exportación de materias primas en tanto materias no renovables o renovables a plazos muy largos (que es lo mismo), el patrimonio de estos recursos se basa en la posibilidad de asegurar ese medio de supervivencia. Pero también se basa en que el cuidado de los recursos asegura mantener el espíritu de nuestro país mega diverso.

Es innegable que el afán de soberanía tiene conexión directa con el amor a la Pacha mama.

Supremacía Constitucional

La Constitución está compuesta por un conjunto de normas que no sólo deben servir para ser declamadas o invocadas líricamente, sino, fundamentalmente, para prevalecer sobre cualquier otra norma legal. Por ello, todo país que se precie de vivir en un Estado de Derecho debe asegurar que en su territorio se cumpla con lo que dispone su Constitución, no sólo por parte de los gobernados sino también por parte de los poderes constituidos". Nos dice el Abogado Iván Castro Patiño en su publicación que la titula "La Inconstitucionalidad por Omisión", publicada en la Revista Jurídica de la Universidad Católica de Guayaquil, I Tomo, Revista Nro. 16 del año 2003.

> El artículo 272 de la Constitución Política del Ecuador, consagra el principio de la supremacía constitucional, en los términos siguientes: "La Constitución prevalece sobre cualquier otra norma legal. Las disposiciones de leyes orgánicas y ordinarias, decretos leyes, decretos, estatutos, ordenanzas, reglamentos; resoluciones y otros actos de poderes públicos, deberán mantener conformidad con sus disposiciones y no tendrán valor sin, de algún modo, estuvieren en contradicción con ella o alteren sus prescripciones." La doctrina prevaleciente en la actualidad, parte de la base de que, sin desconocer su carga política, la Constitución es fundamentalmente norma jurídica, que reclama plena vigencia y determina la vida en sociedad. (Patiño, 2010)

Podemos decir al respecto que la constitución clarifica los reglamentos que aterrizan en normas sociales y jurídicas.

El espacio de acción de la constitución viene a ser o a expresarse en todos los aspectos de la vida social, las contradicciones que se presenten en lo cotidiano pueden entonces resolverse a partir de un análisis constitucional del derecho de las instituciones o personas implicadas.

> Al respecto Francisco Fernández Segado opina: "El dogma liberal de la soberanía absoluta del Parlamento, como es sobradamente conocido, ha sido sustituido en nuestro tiempo por el de la soberanía de la Constitución…". En afirmar esta concepción han sido particularmente reiterativos los tribunales constitucionales europeos, a través de la doctrina de la fuerza o eficacia normativa de la Constitución, que complementó la concepción de la supremacía de la Constitución, que inicialmente sólo se aplicaba cuando una norma de inferior jerarquía violaba su contenido, ampliándola a los casos en que, de cualquier otro modo, se impedía o enervaba su eficacia.
>
> El Tribunal de Garantías Constitucionales del Ecuador, ahora Tribunal Constitucional, en acertadas resoluciones de los últimos años ha consagrado la referida doctrina. (Patiño, 2010)

La constitución como punto consensual entre varios mecanismos y sistemas en los que se inscriben por integración las acciones cotidianas de los individuos, presenta una ruptura con el dogma liberal en el cual prima la idea del individualismo.

Los tribunales de Ecuador, se inscriben en esta lógica dinámica ya que deben asegurar el cumplimiento de la constitución en cada acción social que tenga que ver con el derecho, en este caso se podría decir que la mayoría de las acciones y hechos sociales se pueden leer desde allí.

La Carta Política en su artículo 272, establece que la "Constitución prevalece sobre cualquier otra norma legal", y que todas "las disposiciones de leyes orgánicas y ordinarias, decretos - leyes, decretos, estatutos, ordenanzas, reglamentos, resoluciones y otros actos de los poderes públicos, deberán mantener conformidad con sus disposiciones y no tendrán valor si, de algún modo, estuvieren en contradicción con ella o alteraren sus prescripciones. Si hubiere conflicto entre normas de distinta jerarquía, las cortes, tribunales, jueces y autoridades administrativas lo resolverán, mediante la aplicación de la norma jerárquicamente superior." Es importante manifestar que los tratados internacionales se encuentran bajo las disposiciones de la Constitución. (Patiño, 2010)

Es decir que las acciones externas deben pasar por el filtro de la constitución, este reglamento tiene la capacidad máxima de regular las acciones y decisiones relativas a su entorno inmediato. Aquí, el tema de la jurisdicción es básico para comprender los campos de acción puesto que la jurisdicción física como abstracción de dimensiones culturales, particularidades simbólicas, formas de pensar y todas estas expresiones particulares y pertenecientes a un país, toman sentido en la constitución que establece "las reglas del juego".

El principio de supremacía constitucional constituye una eficiente protección de la libertad y dignidad del individuo, cuyos lineamientos se encuentran expresados en la Constitución Política del país, estableciendo que

todos los poderes del Estado cumplan con todo lo dispuesto en la misma, en cuya parte dogmática considera como normas y principios supremos la defensa de los derechos y libertades de los individuos dotándoles de supremacía respectiva de conformidad al orden jerárquico que ha sido creado. (Jimbo, 2008)

La supremacía constitucional es un mecanismo muy eficiente al momento de garantizar la seguridad de los individuos que pertenecen a la previamente mencionada jurisdicción del accionar de la ley, ahora podríamos asegurar que la constitución tiene una especial capacidad proteccionista, por esto se conoce como carta magna. Cumple un papel maternal en relación a su funcionalidad como ley, es un instrumento de protección del orden que la ha creado con el fin de proteger y garantizar derechos.

En conclusión, la Constitución de un país es la Norma Suprema o la Ley madre que contiene los procedimientos para la creación de la normatividad que siempre dependerá de ésta; este principio de superioridad o supremacía de toda norma constitucional es eficaz porque a través de este, no habrá ningún acto o norma con rango de ley que sea contradictoria a la Constitución. (Jimbo, 2008)

La supremacía de la Constitución no es, entonces, un principio arbitrario. Una constitución tiene la función y la capacidad de augurar por el orden dentro de un espacio sumamente grande, por ende debe abarcar una serie de estamentos que aseguren la propensión a desarrollar todos aquellos que rigen la norma de un país.

Hasta hace poco los jueces de cualquier nivel dictaban su pronunciamiento con prevalencia de la norma jurídica secundaria, su posición eminentemente legalista, descuidaban a la norma fundamental, no relacionaban sus fallos con lo dispuesto en la norma constitucional; en la actualidad creemos que se ha superado y corregido este grave error jurídico. (Jimbo, 2008)

El Art. 424 y 425 de la Constitución de la República, que consagra expresamente el "Principio de Supremacía", establece la superioridad jerárquica de la Constitución sobre todo el ordenamiento jurídico interno.

La Constitución de la República reposa su soberanía y supremacía en los artículos 424 y 425, de este modo se marca una jerarquización de la Constitución en relación a otras leyes, acuerdos y ordenanzas diversas.

LA ACCIÓN DE HABEAS DATA tal como se encuentra concebida por nuestra Constitución, tiene estrecha relación con los derechos de las personas protegidos por los números 8 y 21 del artículo 23 de la misma, a saber: El derecho a la honra y a la buena reputación y a la intimidad personal y familiar"; y, "El derecho a guardar reserva sobre sus convicciones políticas y religiosas. Nadie podrá ser obligado a declarar sobre ellas. En ningún caso se podrá utilizar información personal de terceros sobre sus creencias religiosas y filiación política, ni sobre datos referentes a salud y vida sexual, salvo para satisfacer necesidades de atención médica". Este segundo derecho protegido por nuestra Norma Suprema, tiene también relación con el derecho a la intimidad señalado por el primero de los numerales anotados.

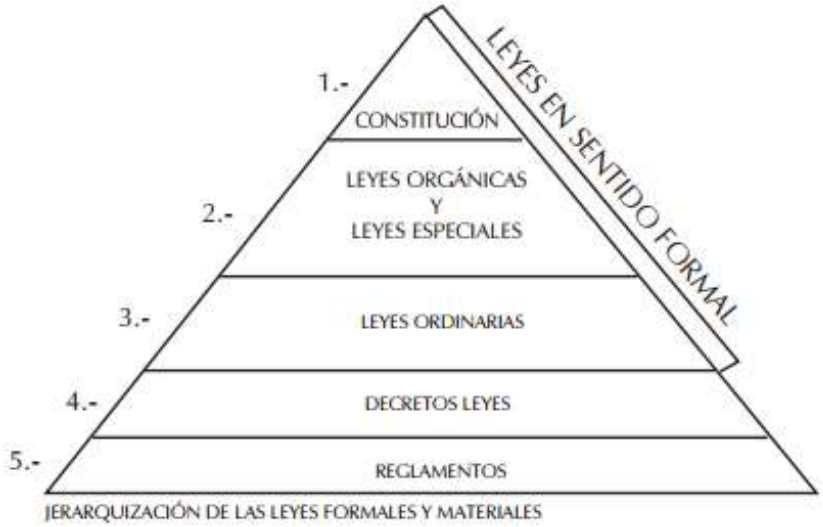
En la actualidad, debido al avance tecnológico en el campo informático a más de contar con registros de datos personales en la web, se ve más claro el deber del Estado de proteger de alguna manera a los ciudadanos con respecto a la utilización que se dé a la información que sobre cualquier persona pueden encontrarse en cualquier tipo de institución. Hoy en día es común que la generalidad de las personas tenga que depositar en algún momento, información sobre sí mismas, en instituciones públicas (por ejemplo en nuestro país el caso del Servicio de Rentas Internas que es depositario de buena parte de información personal a través de las declaraciones de impuesto a la renta, o a la Policía Nacional que exige información personal para el otorgamiento de licencias o matrículas), o en instituciones privadas (por ejemplo las empresas en las cuales se dejan carpetas con el curriculum vitae o los bancos que contienen información personal sobre sus clientes, relacionada con sus ingresos económicos).

Por los motivos señalados, existen en la mayoría de legislaciones del mundo, principios protectores dirigidos a garantizar una información veraz sobre las personas o sus bienes, y nuestro país no es la excepción. Esta garantía está

establecida en el artículo 94 de nuestra Constitución de la siguiente manera: "Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito". Tal y como se encuentra enunciado este principio constitucional, en nuestro país, la acción de hábeas data se dirige a proteger por una parte el derecho de las personas a obtener los documentos que contienen información sobre sí misma y sus bienes, de la institución en la cual reposen; y por otra, el derecho a obtener información del uso que se les esté dando y con qué propósito se utilice tal información. Por lo tanto, a mi criterio, las garantías protegidas por la Constitución son claramente el derecho a la intimidad (lo cual depende del tipo de información) y el derecho a la honra y buena reputación (que tiene que ver con el uso de la información).

Teoría de la pirámide jurídica de Kelsen

La teoría de la pirámide de Kelsen la que fundamenta los principio de constitucionalidad y explica la supremacía constitucional según Kensel la Constitución es la norma que tiene mayor jerarquía ubicándola en la cima de la pirámide por el creada de la que se derivan y a la que se deben todas las demás leyes que se ubican debajo. La pirámide de Kelsen según el tipo y supremacía de leyes se la puede observar en el gráfico a continuación



Fuente:http://www.alfonsozambrano.com/nueva_doctrina/23102011/ndp-teoria_piramide_kelsen.pdf

A partir de este esquema, se puede demostrar que la constitución tiene supremacía por encima de las otras leyes sí, pero además se muestra que la capacidad normativa de la constitución es superior.

a) La relación entre las normas está basada en la vinculación que tiene a partir de los principios de infra y supraordinación. Ahora, la mejor forma de comprender esto es a partir de una comparación sistemática entre las diversas leyes.

b) La lógica de las normas delimita su creación, es decir, la norma que esté por encima de otra delimita las dimensiones de su acción y todo su planteamiento.

Esto se da por la relación de superioridad/ inferioridad que existe entre ellas.

c) La unidad de las leyes se da en el momento en que se encuentran las unas delimitadas por las otras.

d) Este sistema integrado delimita el orden jurídico de las normas y leyes.

Si tomamos a la lógica jurídica como la aplicación de operaciones sistemáticas para comprender la forma en que los sistemas integrados de acción se encuentran relacionados, entonces tenemos que necesariamente van a existir grados de ordenamiento y organización de las leyes.

Ahora, esta ley en particular permite comprender la forma en que las leyes encuentran su producción en el seno de otras, entonces no pueden transgredirse en este orden. Si tenemos a la constitución en la cima de esta pirámide que hemos construido, entonces su regimiento sobre las otras no se da únicamente a nivel de su capacidad de inscribir los derechos más elementales de los ciudadanos de una sociedad.

Se da también desde un punto de vista técnico ya que delimita el orden lógico de accionar las leyes.

Este ordenamiento no es entonces un proceso aislado ni mucho menos desorganizado.

Delito

Conducta típica, antijurídica y culpable constitutiva de infracción penal. Eugenio Cuello Calón define el delito como una acción antijurídica, típica, culpable y sancionada con una pena. RODRÍGUEZ MAN- ZANERA Luis considera que delito es "la acción u omisión que castigan las leyes penales, es la conducta definida por la ley".

En sentido amplio, delito es sinónimo de infracción mientras que en sentido estricto, delito es una infracción cuyo autor puede ser castigado con penas correccionales, esto es, con pena de privativas de la libertad.

Es decir que delito es toda acción u omisión que por malicia o negligencia culpable, da lugar a un resultado dañoso, estando prevista o tipificada en la ley penal dicha acción u omisión con el señalamiento de la correspondiente pena o castigo. Cuando dicha conducta no alcanza la gravedad precisa para ser calificada como delito, puede encuadrarse en las faltas o delitos menores, cuya tipificación en la ley penal se hace separadamente de los delitos.

Cuando la pena venga determinada por la producción de un ulterior resultado más grave, sólo se responderá de éste si se hubiere causado, al menos, por culpa.

Se dice que hay delito doloso cuando el autor del mismo ha querido el resultado dañoso; cuando no se quiere dicho resultado, pero tampoco se evita, se dice que hay delito culposo.

Es delito de comisión el que conlleva una actividad del autor que modifica la realidad circundante; y se habla de delito de omisión cuando la conducta delictiva del autor ha consistido en un no hacer o abstención de actividad.

Elementos del delito

Antijuricidad.

La antijuricidad se define como aquel desvalor que posee un hecho típico que es contrario a las normas del derecho en general, es decir, no sólo al ordenamiento, supone que la conducta que se ha realizado está prohibida por la ley, como lo define el Art 29 del Código Orgánico Integral Penal, "Para que la conducta penalmente relevante sea antijurídica deberá amenazar o lesionar, sin justa causa, un bien jurídico protegido", como lo es la vida.

La clasificación de la antijuricidad es la siguiente:

Antijuridicidad formal: se afirma que una conducta es formalmente antijurídica, cuando es meramente contraria al ordenamiento jurídico. Por tanto, la antijuricidad formal no es más que la oposición entre un hecho y la norma jurídica positiva.

Antijuridicidad material: se dice que una conducta es materialmente antijurídica cuando, habiendo transgredido el ordenamiento jurídico tiene, además, un componente de dañosidad social, es decir, ha lesionado o puesto en peligro un bien jurídico protegido.

Tipicidad

Se denomina tipicidad al encuadramiento de la conducta humana al tipo penal, dicha norma es escrita y además se encuentra regulada en el Código Orgánico Integral Penal en el Art. 25 "Los tipos penales describen los elementos de las conductas penalmente relevantes ", así cuando la ley describe el asesinato diciendo "el que mate a otra persona" la conducta típica está dada por el hecho concreto de matar a otro.

En el tipo se incluyen todas las características de la acción prohibida que

fundamenta positivamente su antijuricidad. Pero no siempre se pueden deducir directamente del tipo estas características y hay que dejar al juez la tarea de buscar las características que faltan. Ello se debe a la dificultad de plasmar legalmente tales características en el tipo legal.

Principios Generales de la Tipicidad.

- Nullum crimen sine lege. No hay delito sin ley, no hay delito sin previa ley penal escrita y estricta.
- Nullum crimen sine tipo. No hay delito sin tipo, una conducta no puede ser considerada delictiva sin estar descrita por un ordenamiento penal.
- Nullapoena sine tipo, No hay pena sin que exista el tipo penal.
- Nullapoena sine lege. No hay pena sin previa ley que establezca la punición de un delito.

Acto.

El acto jurídico es el hecho, humano, voluntario o consciente y lícito, que tiene por fin inmediato establecer entre las personas relaciones jurídicas, crear, modificar o extinguir derechos y obligaciones. Para que se dé el acto jurídico no basta con que haya un sujeto y un objeto con bastante capacidad, se necesita algo que los ponga en relación, estableciendo un lazo o un vínculo que los una, haciendo pasar la relación jurídica del estado de posibilidad al estado de existencia.

En tal razón nadie puede ser condenado por un acto ilícito sin que este se halle expresamente declarado, como infracción por la ley penal, sin que esta se encuentre establecida con anterioridad sancionado a una persona no por lo que es, sino por lo que este hace.

La infracción se entiende cometida dependiendo de los efectos de la:

- Acción.
- Omisión.

- Resultado.

Acción.

La acción es el comportamiento humano impulsado por la voluntad, conciencia e intención, que causa la modificación del mundo exterior. No puede constituir acción el mero pensamiento y la simple disposición de ánimo, ni la mera resolución delictiva que no se traduzca en actos exteriores.

VON LISZT, Franz Ritter, jurista y político alemán distingue tres elementos de la acción:

- Una acción humana movida por la voluntad.
- Una modificación del mundo exterior.
- Un tercer elemento que vincula la acción y el resultado que es la relación de la causalidad.

Omisión.

La omisión es un concepto normativo, que presupone una expectativa de la realización de la acción exigida por el mandato.

El Código Orgánico Integral Penal en su Art. 26 inciso segundo manifiesta: "Responde por delito preterintencional la persona que realiza una acción u omisión", lo que significa que si alguien resulta lastimando por alguna de estas acciones el infractor será sancionado con dos tercios de la pena aplicable al ilícito aunque no hubiera premeditado causar el daño.

Resultado.

Para que la acción tenga relevancia para el Derecho Penal, tiene que producir un cambio en el mundo exterior, es decir tiene que haber un delito cometido para que haya un resultado o una consecuencia y que puede ser formal o

material, y que puede colocarse en el peligro a que se sujeta en un bien jurídico. Además siempre tiene que existir el nexo entre el delito y el responsable del mismo.

Culpabilidad.

La culpabilidad es la conciencia antijurídica de la conducta, tipificada en el Art 34 del Código Orgánico Integral Penal, es decir supone la reprochabilidad del hecho ya calificado como típico y antijurídico, fundada en el desacato del autor frente a la ley, por medio de su conducta mediante la cual menoscaba la confianza general en la vigencia de las normas.

En resumen la culpabilidad es la voluntaria omisión de la diligencia en calcular las consecuencias posibles previstas del propio hecho o como lo tipifica el Art 27 del Código Orgánico Integral Penal "Actúa con culpa la persona que infringe el deber objeto de cuidado, que personalmente le corresponde, produciendo un resultado dañoso".

Atipicidad

Entendemos por atipicidad el fenómeno en virtud del cual un determinado comportamiento humano no se adecua a un tipo legal.

La atipicidad a su vez puede ser de carácter absoluto (cuando la conducta examinada no es subsumible en ningún tipo penal) o relativo (por no aparecer alguno o algunos de los elementos de la descripción comportamental), examinemos brevemente el alcance de estos dos fenómenos, haciendo especial referencia al delito putativo, ya que consideramos que presenta gran importancia en nuestra legislación.

Cuando hablamos de atipicidad relativa, nos encontramos con la falta de adecuación típica que se refiere a uno de los elementos que integran el tipo, así: los sujetos, la conducta o el objeto.

Habrá atipicidad relativa en relación con los sujetos activo o pasivo, cuando el hecho descrito en la ley penal es realizado por persona que no reúne las condiciones señaladas en el tipo, o cuando el titular del bien jurídico tutelado tampoco presenta dichas calidades.

Tal como lo manifiesta Bustamante Hernández José Luis.

Imputabilidad.

La Imputabilidad es la capacidad del ser humano para entender que su conducta lesiona los intereses de sus semejantes y para adecuar su actuación a esa comprensión es atribuir a alguien las consecuencias de su manera de obrar, para lo cual el acto debe ser realizado con discernimiento, intención y libertad.

Es un concepto jurídico de base psicológica del que dependen los conceptos de responsabilidad y culpabilidad.

Quien carece de estas capacidades, bien por no tener la madurez suficiente como los menores de edad o bien por sufrir graves alteraciones psíquicas como los enajenados mentales, no pueden ser declarados culpables ni pueden ser responsables penalmente de sus actos ya que bajo este tipo de condiciones un individuo es inimputable en nuestra legislación.

Formas de culpabilidad

Delitos Dolosos.

El DOLO es la acción positiva de causar daño, también se la define como la voluntad de cometer un delito a sabiendas de su ilicitud en los actos jurídicos.

La infracción dolosa es intencional y preterintencional, cuando el acontecimiento dañoso o peligroso es el resultado de la acción o de la omisión de la ley.

Delitos Culposos.

El delito es culposo cuando se produce un resultado descrito y sancionado en la ley penal, a causa de no haber previsto ese resultado siendo previsible, se verifica por:

- Imprudencia.- no existe intención de causar daño.
- Culpa grave.- esta equivale a dolo.
- Culpa leve.- es la falta de aquella diligencia.
- Culpa levísima.- es la falta de esmerado cuidado.

Sujetos del delito

Los Sujetos del delito son las personas en las que recaen directamente las consecuencias de la acción delictiva además de personas jurídicas como empresas o cualquier tipo de instituciones que también se ven afectadas por individuos o bandas delictivas.

Sujeto Activo.

El Sujeto Activo del Delito es la persona individual con la suficiente voluntad, conciencia y capacidad penal que realiza la conducta tipificada en la ley penal correspondiente.

Solamente una persona individual puede cometer delitos, aún en los casos de asociación criminal, las penas recaen sólo en sus miembros integrantes. Solo en la persona individual se da la unidad de voluntad y el principio de individualidad de la pena.

Sujeto Pasivo.

El Sujeto Pasivo del Delito es el titular del interés jurídico lesionado o puesto en peligro.

Pueden ser:

- La Persona Individual.
- Personas jurídicas.
- La Sociedad.
- El Estado.

Bienes Jurídicos Protegidos

Teniendo en cuenta que el bien jurídico tutelado lo constituyen todos aquellos derechos, valores o atributos de la persona que el Estado encuentra merecedores de protección a través del Derecho Penal, se puede afirmar que en el caso de los delitos informáticos existe una pluralidad de bienes que son afectados o puestos en peligro.

Por un lado las acciones que van dirigidas al sabotaje, el daño, la destrucción o pérdida de equipos de computación afectan, lesionan o ponen en peligro el bien Jurídico patrimonio, Por otro, los delitos que se sirven o utilizan de un equipo informático para su realización pueden de igual manera afectar diversos bienes, como lo serían la indemnidad sexual (caso de la pornografía infantil), la privacidad o el mismo patrimonio en los casos de fraudes informáticos cometidos por Internet. También debe tomarse en cuenta que el uso de ordenadores para la reproducción no autorizada de libros, películas música, etc., afecta valores de propiedad intelectual pero implícitamente éstas acciones tienen una motivación económica por lo que a su vez redundan en la afectación al bien jurídico patrimonio.

Es por eso que al hablar de delitos informáticos es válida la afirmación que los mismos afectan una diversidad de bienes legalmente tutelados por lo que puede considerarse pluriofensivo.

Estas reflexiones sirven de base para proponer por parte del autor la siguiente clasificación de los delitos informáticos, distinguiéndose entonces dos tipos a saber:

a) Delitos Informáticos contra el patrimonio y la propiedad intelectual.

b) Delitos Informáticos que atentan contra la privacidad, la intimidad, la libertad o indemnidad sexual.

Sanción penal

La sanción es la consecuencia jurídica a la manera de obrar de una persona estas sanciones por lo general son específicamente privativas de la libertad que se da solo en delitos graves como lo es el asesinato.

El Código Orgánico Integral Penal en su Art. 51 al define a la pena como "una restricción a la libertad y a los derechos de las personas, como consecuencia jurídica de sus acciones u omisiones punibles", de esta manera se legitimando la potestad que tiene el Estado para aplicar la pena observando los preceptos del debido proceso y otorgando los derechos y garantías prescritas en la Constitución.

Las sanciones penales son privativas de la libertad y no privativas de la libertad, en este caso se presentan medidas sustitutivas a la cárcel como lo es tratamiento médico, psicológico, servicio comunitario, comparecencia periódica ante la autoridad competente, suspensión de la licencia de conducir etc. Con estas medidas el legislador tiene como finalidad la no neutralización de las personas de la sociedad sino por el contario la reinserción de estos.

Delitos Informáticos

El término informática se obtiene de la transposición de las palabras Información Automática, que fue utilizado por primera vez en el idioma francés con las acepciones 'information automatique.

La informática es definida en el Diccionario de la Real Academia de la Lengua Española como el conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores.

Ahora bien con respecto al delito informático Tiedemann señala: “Con la expresión criminalidad mediante computadoras se alude a todos los actos antijurídicos según la ley penal vigente (o socialmente dañosos y por eso penalizables en el futuro) realizados con el empleo de un equipo automático de procesamiento de datos”.

Por su parte la Organización de las Naciones Unidas al referirse a la delincuencia informática lo hace de la siguiente manera: “A menudo, se le considera una conducta proscrita por la legislación y/o la jurisprudencia, que implica la utilización de tecnologías digitales en la comisión del delito; se dirige a las propias tecnologías de la computación y las comunicaciones; o incluye la utilización incidental de computadoras en la comisión de otros delitos”.

De estas definiciones se desprende que no solamente la propagación de virus u otros ataques a sistemas operativos de los ordenadores deben ser considerados como delitos informáticos, ya que se debe incluir dentro de estas todas aquellas acciones que atentan contra el bien jurídico merecedor de protección y que se valen o utilizan para su comisión de una computadora. En ese sentido puede definir el delito informático como toda aquella acción típica y antijurídica, que se sirve o utiliza de una computadora para su realización, o bien va dirigida a obtener el acceso no autorizado a registros o programas de un sistema informático, o a producir un resultado de daño en ésta o de los sistemas que la misma hace operar.

Como se podrá analizar, el ámbito de actuación en este tipo de conductas implica el ataque o intencionalidad de daño a un sistema operativo de la computadora, la intromisión o acceso a bases de datos o archivos que las mismas contengan, o bien la utilización de este aparato tecnológico y de comunicación como medio o instrumento para la realización de delitos.

Elementos

Siguiendo la metodología y el ámbito técnico del análisis de los ilícitos a

través de la teoría del delito, diremos que el elemento descriptivo (apreciado a través de la vista u otros sentidos) de esta clase de delitos lo sería la computadora, las bases de datos o registros informáticos o bien los bienes materiales e intelectuales afectados a través de un sistema informático u ordenador para citar algunos.

Con respecto al elemento normativo Zaffaroni: señala: “aparecen cuando los tipos acuden a valoraciones jurídicas o éticas. Normalmente el tipo se vale de descripciones para individualizar programas, pero en ocasiones lo hace mediante estas remisiones a elementos de carácter valorativo”.

Debe entenderse entonces que dicho elemento se aprecia intelectualmente, en el caso en particular de los delitos informáticos es necesario auxiliarse de la informática u otra ciencia para comprenderlos, en ese sentido dentro de los elementos normativos de este tipo de ilícitos tenemos los daños producidos a los equipos, a los programas o bases de datos, la pérdida patrimonial, la identidad sexual, etc.

Sujetos Procesales

Muchas de las personas que cometen los delitos informáticos poseen ciertas características específicas tales como la habilidad para el manejo de los sistemas informáticos o la realización de tareas laborales que le facilitan el acceso a información de carácter sensible. En algunos casos la motivación del delito informático no es económica sino que se relaciona con el deseo de ejercitar, y a veces hacer conocer a otras personas, los conocimientos o habilidades del delincuente en ese campo.

Muchos de los "delitos informáticos" encuadran dentro del concepto de "delitos de cuello blanco", término introducido por primera vez por el criminólogo estadounidense Edwin Sutherland en 1943. Esta categoría requiere que: el sujeto activo del delito sea una persona de cierto estatus socioeconómico; su comisión no pueda explicarse por falta de medios económicos, carencia de recreación, poca

educación, poca inteligencia, ni por inestabilidad emocional.

El sujeto pasivo en el caso de los delitos informáticos puede ser individuos, instituciones crediticias, órganos estatales, etc. que utilicen sistemas automatizados de información, generalmente conectados a otros equipos o sistemas externos.

Sujeto Activo

Las personas que cometen los "Delitos informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos. Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los cometidos. De esta forma, la persona que "entra" en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

El nivel típico de aptitudes del delincuente es tema de controversia ya que para algunos en el nivel de aptitudes no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

Sujeto Pasivo

En primer término tenemos que distinguir que sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el

sujeto activo, y en el caso de los "delitos informáticos" las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los "delitos informáticos", ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos.

Dado lo anterior, "ha sido imposible conocer la verdadera magnitud de los "delitos informáticos", ya que la mayor parte de los delitos no son descubierto o no son denunciados a las autoridades responsables" y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos; la falta de preparación por parte de las autoridades para comprender, investigar y dar tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada "cifra oculta" o "cifra negra".

Por lo anterior, se reconoce que "para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, una análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento".

En el mismo sentido, podemos decir que mediante la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras, y alertando a las potenciales víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática, y si a esto se suma la creación de una adecuada

legislación que proteja los intereses de las víctimas y una eficiente preparación por parte del personal encargado de la procuración, administración y la impartición de justicia para atender e investigar estas conductas ilícitas, se estaría avanzando mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más.

Bienes Jurídicos Protegidos

Dentro de los delitos informáticos, podemos decir que la tendencia es que la protección a los bienes jurídicos, se le haga desde la perspectiva de los delitos tradicionales, con una re-interpretación teleológica de los tipos penales ya existentes, para subsanar las lagunas originadas por los novedosos comportamientos delictivos.

Esto sin duda da como regla general que los bienes jurídicos protegidos, serán los mismos que los delitos re-interpretados teleológicamente o que se les ha agregado algún elemento nuevo para facilitar su persecución y sanción por parte del órgano jurisdiccional competente.

De otro lado otra vertiente doctrinaria supone que la emergente la Sociedad de la Información hace totalmente necesaria la incorporación de valores inmateriales y de la INFORMACIÓN misma como bienes jurídicos de protección, esto tomando en cuenta las diferencias existentes por ejemplo entre la propiedad tangible y la intangible.

Esto por cuanto la información no puede a criterio de Pablo Palazzi ser tratada de la misma forma en que se aplica la legislación actual a los bienes corporales, si bien dichos bienes tiene un valor intrínseco compartido, que es su valoración económica, es por tanto que ella la información y otros intangibles son objetos de propiedad, la cual esta constitucionalmente protegida.

En fin la protección de la información como bien jurídico protegido debe tener siempre en cuenta el principio de la necesaria protección de los bienes

jurídicos que señala que la penalización de conductas se desenvuelva en el marco del principio de "dañosidad" o "lesividad". Así, una conducta sólo puede conminarse con una pena cuando resulta del todo incompatible con los presupuestos de una vida en común pacífica, libre y materialmente asegurada.

Así inspira tanto a la criminalización como a descriminalización de conductas. Su origen directo es la teoría del contrato social, y su máxima expresión se encuentra en la obra de BECCARIA "Los Delitos y las Penas" (1738-1794). Se define como un bien vital, "bona vitae", estado social valioso, perteneciente a la comunidad o al individuo, que por su significación, es garantizada, a través del poder punitivo del Estado, a todos en igual forma. En conclusión podemos decir que el bien jurídico protegido en general es la información, pero está considerada en diferentes formas, ya sea como un valor económico, como uno valor intrínseco de la persona, por su fluidez y tráfico jurídico, y finalmente por los sistemas que la procesan o automatizan; los mismos que se equiparan a los bienes jurídicos protegidos tradicionales tales como: Œ

EL PATRIMONIO, en el caso de la amplia gama de fraudes informáticos y las manipulaciones de datos que da a lugar. Œ

LA RESERVA, LA INTIMIDAD Y CONFIDENCIALIDAD DE LOS DATOS, en el caso de las agresiones informáticas a la esfera de la intimidad en forma general, especialmente en el caso de los bancos de datos. Œ

LA SEGURIDAD O FIABILIDAD DEL TRÁFICO JURÍDICO Y PROBATORIO, en el caso de falsificaciones de datos o documentos probatorios vía medios informáticos. Œ

EL DERECHO DE PROPIEDAD, en este caso sobre la información o sobre los elementos físicos, materiales de un sistema informático, que es afectado por los de daños y el llamado terrorismo informático. Por tanto el bien jurídico protegido, acoge a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde esta se almacena o transfiere.

Para los autores chilenos Claudio Magliona y Macarena López, sin embargo los delitos informáticos tienen el carácter de pluriofensivos o complejos, es decir "que se caracterizan porque simultáneamente protegen varios intereses jurídicos, sin perjuicio de que uno de tales bienes está independientemente tutelado por otro tipo". En conclusión no se afecta un solo bien jurídico, sino una diversidad de ellos. Por tanto podemos decir que esta clase de delincuencia no solo afecta a un bien jurídico determinado, sino que la multiplicidad de conductas que la componen afectan a una diversidad de ellos que ponen en relieve intereses colectivos, en tal sentido de María Luz Gutiérrez Francés, respecto de la figura del fraude informático nos dice que: "las conductas de fraude informático presentan indudablemente un carácter pluriofensivo.

En cada una de sus modalidades se produce una doble afección: la de un interés económico (ya sea micro o macrosocial), como la hacienda pública, el sistema crediticio, el patrimonio, etc., y la de un interés macrosocial vinculado al funcionamiento de los sistemas informáticos".

Por tanto diremos que el nacimiento de esta nueva tecnología, está proporcionando a nuevos elementos para atentar contra bienes ya existentes (intimidad, seguridad nacional, patrimonio, etc.), sin embargo han ido adquiriendo importancia nuevos bienes, como sería la calidad, pureza e idoneidad de la información en cuanto tal y de los productos de que ella se obtengan; la confianza en los sistemas informáticos; nuevos aspectos de la propiedad en cuanto recaiga sobre la información personal registrada o sobre la información nominativa. En tal razón considero que este tipo de conductas criminales son de carácter netamente pluriofensivo.

Hacking

Es un delito informático que consiste en acceder de manera indebida, sin autorización o contra derecho a un sistema de tratamiento de la información, con el fin de obtener una satisfacción de carácter intelectual por el desciframiento de los códigos de acceso o password, no causando danos inmediatos ni tangibles en

la victima, o bien por la mera voluntad de curiosear o divertirse de su autor.

La voluntad de divertirse generalmente se traducen por paseos por el sistema haciendo alarde de su intromisión. Es lo que se ha llamado JOY RIDING, O PASEOS DE DIVERSIÓN.

Características De esta clase de hacking: el Hacker es una persona experta en materias informaticas y con edad fluctuante entre los 15 y 25 años de edad es por ello que esta delincuencia se ha denominado "SHORT PANTS CRIMES", es decir, en pantalones cortos, su motivación no es la de causar danos sino de obtener personales atisfacciones y orgullos, basados principalmente en la burla de los sistemas de seguridad dispuestos.

Es una persona muy interesada en el funcionamiento de sistemas operativos; aquel curioso que simplemente le gusta husmear por todas partes, llegar a conocer el funcionamiento de cualquier sistema informático mejor que quiénes lo inventaron. La palabra es un término inglés que caracteriza al delincuente silencioso o tecnológico. Ellos son capaces de crear sus propios softwares para entrar a los sistemas. Toma su actividad como un reto intelectual, no pretende producir daños e incluso se apoya en un código ético:
-El acceso a los ordenadores y a cualquier cosa le pueda enseñar cómo funciona el mundo, debería ser limitado y total.
-Toda la información deberá ser libre y gratuita.
-Desconfía de la autoridad. Promueve la descentralización.
-Los Hackers deberán ser juzgados por sus hacks, no por criterios sin sentido como calificaciones académicas, edad, raza, o posición social.
-Se puede crear arte y belleza en un ordenador.
-Los ordenadores pueden mejorar tu vida.

Cracking

El concepto de Cracker, como su nombre nos está indicando (deriva del inglés Crack, que significaría romper) comprende a aquellos usuarios de

ordenadores que tienen los conocimientos y las técnicas necesarias para Romper Sistemas de Seguridad, teniendo esta actividad distintas finalidades y motivos, que varían desde el simple hecho de solamente medir conocimientos, hasta como forma de protesta.

Una de las formas más difundidas en estos últimos tiempos es la del Cracker que realiza una modificación en un funcionamiento de un Software Original, obteniéndose Seriales, aplicaciones conocidas como Keygens (que generan Claves de Producto) y también programan los archivos que se llaman justamente Cracks, que permiten saltear las restricciones de seguridad en el caso del Software Ilegal.

Por otro lado, están aaquellos que se encargan de eliminar las funciones de un Sistema de Seguridad en un ordenador o una red informática, teniendo acceso al mismo, pudiendo obtener información o inclusive realizar modificaciones del mismo, siendo al igual que la anterior una práctica ilegal y por ende penada por la ley.

Sin embargo, existen también Crackers Legales, teniendo esta clasificacion aquellas personas que simplemente realizan actividades de "Crackeo" para medir sus conocimientos, terminando esta actividad cuando la emplean para su propio beneficio (es decir, no distribuyen Software Ilegal, sino que lo utilizan ellos solamente) al igual que también existen Hackers Legales que realizan infiltraciones a sistemas pero no tienen ni Fines de Lucro ni efectúan modificaciones en los mismos, sino que tienen finalidades completamente lícitas en su actividad.

Legislación Comparada

Se debe hacer una comparación entre los países que poseen una legislación aplicable respecto de esta problemática debiendo señalar que por un lado, puede sancionarse una **ley específica**, complementaria del Código Penal. Es la opción por la que se han inclinado, por ejemplo, **Venezuela** –que sancionó su “Ley

Especial contra los Delitos Informáticos" el 30 de octubre de 2001-, **Chile** –que hizo lo propio mediante ley n° 19.223, del 28 de mayo de 1993) y **Alemania** –que el 15 de mayo de 1986 adoptó la "Segunda Ley contra la Criminalidad Económica", que se ocupa casi excluyentemente de la ciberdelincuencia, pero atrapa igualmente algunas figuras ajenas a ella, como, por caso, la utilización abusiva de cheques, **Bolivia**: en su Libro Segundo, el Título XII –destinado a los delitos contra la propiedad- incorpora el Capítulo XI, que tipifica los delitos informáticos. En cambio, ha preferido regular los ciberdelitos en su código penal, esparciendo las diversas figuras en distintos pasajes de su articulado, Paraguay, España6 y Francia, por ejemplo. En nuestro país, en el desarrollo histórico de la legislación penal más reciente, encontramos ejemplos de cada una de estas dos grandes alternativas, aunque la normativa vigente decide incluir la cibercriminalidad en su Código Penal en forma desconcentrada, esto es, incluyendo los distintos tipos legales en los diversos títulos del Libro Segundo del digesto, conforme los variados objetos jurídicos que se desea tutelar.

Hipótesis

La legislación penal ecuatoriana y la incidencia de los delitos informáticos en la ciudad de Ambato

Señalamiento de Variables

Variable Independiente

La Legislación Penal ecuatoriana

Variable Dependiente

Los delitos informáticos en la ciudad de Ambato

CAPÍTULO III

METODOLOGÍA

Enfoque

La presente investigación se encuentra enmarcada en el enfoque crítico propositivo con el que logra diagnosticar un problema previamente encontrado por el investigador para luego dar una alternativa de solución al mismo.

Para llevar a cabo esta Investigación también será necesario utilizar de forma combinada el método inductivo y el deductivo que permitirán a través de la observación y el razonamiento llegar a las conclusiones que se desprenden del problema en estudio.

Modalidad Básica de la Investigación

Investigación de Campo

La presente investigación se desarrollará de la siguiente manera, para la obtención de la información, se realizará de forma directa, es decir, en el lugar en donde se producen los hechos y de acuerdo a los objetivos propuestos.

Entre los instrumentos y técnicas de investigación, se aplicara: la encuesta, con el propósito de obtener información y conocimiento real de la situación actual y preparar la propuesta acorde a las necesidades sociales.

Investigación Bibliográfica – Documental

La Investigación documental depende en gran medida de la información que

se enmarca dentro del objeto de estudio, y para este caso en particular es estrictamente necesario realizar este tipo de Investigación, para tener una idea clara, precisa, y concisa de lo que sucede en la realidad del sector Investigado.

Como fuente secundaria de información para la obtención de datos y desarrollo de la presente investigación, acudiré a varios libros, textos, módulos, códigos, leyes.

En tal sentido debería también considerarse que esta será ante todo una investigación bibliográfica comparativa de la legislación vigente en Ecuador así como también en algunos países de Sudamérica. Ya que debido a la profundidad y alcance es completamente necesario Investigar todo el marco de antecedentes que registra el tema en cuestión.

Nivel o Tipo de Investigación

Asociación de variables

La presente investigación se realizará 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 ellos determinar tendencias o modelos de comportamiento mayoritario.

Analítico – Sintético

Durante todo el proceso de investigación es necesario el análisis y la síntesis para establecer conclusiones o criterios acerca de la aplicación del Principio de Mínima Intervención en el Procedimiento Penal.

Explicativo

Es importante aplicar el método explicativo para así comprobar experimentalmente la hipótesis y descubrir las causas del fenómeno que acarrea el

asesinato cometido por adolescentes infractores y detectar los factores determinantes en la inimputabilidad de éstos, además analizaremos ciertos comportamientos derivados de la misma.

Descriptivo

El método descriptivo que nos ayudara a comparar uno o más fenómenos, situaciones o estructuras y clasificar elementos y modelos de comportamiento según ciertos criterios que servirán para llegar a una solución para el problema de estudio planteado.

Población y Muestra

Población

Es un conjunto definido, limitado y accesible del universo que forma el referente para la elección de la muestra. Es el grupo al que se intenta generalizar los resultados.

En forma determinante la elección de la población afectará profundamente los resultados de la investigación. La población escogida para la realización de este estudio es:

ESTRATOS	UNIVERSO
Funcionarios de la Fiscalía	12
Jueces de Garantías Penales de la ciudad de Ambato	4
Abogados en libre ejercicio	1728
Agentes Investigadores Policía Judicial	16
TOTAL	1760

Tabla No. 1 Tamaño de la Población
Fuente: Investigador
Elaborado por: David Poveda

Muestra

Habitualmente, el investigador no trabaja con todos los elementos de la población que estudia sino sólo con una parte o fracción de ella; a veces, porque es muy grande y no es fácil abarcarla en su totalidad. Por ello, se elige una muestra representativa y los datos obtenidos en ella se utilizan para realizar pronósticos en poblaciones futuras de las mismas características.

La importancia del muestreo radica en que no es necesario trabajar con los 'N' elementos de una población para comprender con un nivel razonable de exactitud la naturaleza del fenómeno estudiado. Este conocimiento se puede obtener a partir de una muestra que se considere representativa de aquella población.

Es por esta razón que la ésta investigación presenta muestras cuantitativas y cualitativas, lo que significa que el investigador tiene desafíos importantes, empero intenta aplicar criterios distintos para seleccionar a los participantes.

Fórmula del Tamaño de la Muestra

Para objetos didácticos y como una manera de fundamentar lo expuesto, por cuanto la población se divide en estratos es necesario utilizar la siguiente fórmula para la extracción del tamaño de la muestra:

Muestra

Para obtener la muestra se aplicará la siguiente fórmula:

$$n = \frac{Z^2 . P . \mathrm{Q} . N}{Z^2 \mathrm{P} . \mathrm{Q} . \mathrm{N} . e^2}$$

n = Muestra de población

Z= Nivel de confianza

P = Probabilidad de concurrencia

Q = Probabilidad de no concurrencia

N = Población

e = Margen de error

Se realiza el cálculo de la muestra de la población de Abogados en libre ejercicio foro Abogados ciudad de Ambato a través de la siguiente fórmula.

$$n = \frac{Z^2 . P . Q . N}{Z^2 P . Q . N . e^2}$$

$$n = \frac{1.96^2 . (0,5)(0,5)1785}{(1,96)^2 0,5(0,5)(1785) . 0,05^2}$$

$$n = \frac{1714.314}{5,4229}$$

n=1714,314

5,4229

$$n = 316,12$$

n= 316

ESTRATOS	MUESTRA
Funcionarios de la Fiscalía	4
Jueces de Garantías Penales de la ciudad de Ambato	4
Abogados en libre ejercicio	316
Agentes Investigadores Policía Judicial	17
TOTAL	341

Tabla No. 2 Tamaño de Muestra
Fuente: Investigador
Elaborado por: David Poveda

Técnicas

La técnica de recolección de información a aplicarse es la encuesta y su medio de realización el cuestionario estructurado el que se aplicará a los grupos mencionados en el cuadro de la muestra con el fin de establecer de mejor forma un diagnóstico al problema presentado.

Operacionalización de Variables

Operacionalización de la Variable Independiente

CONCEPTUALIZACIÓN	DIMENSIONES	INDICADORES	ÍTEMS BÁSICOS	TÉCNICA	INSTRUMENTO
El Proceso Penal Es un conjunto unitario y sistematizado de las normas jurídicas punitivas de un Estado, que en esencia busca sancionar los hechos y actos delictivos que se cometen en la sociedad. La sanción se aplica a través de los órganos del Estado, como por ejemplo la fiscalía.	Normas Jurídicas Acto delictivo Sanción	Tipificación Disposiciones Reglas de conducta Acción Omisión Resultado Prisión y reclusión	¿Considera usted que en la investigación realizada para recabar indicios es la adecuada? ¿Cree usted que existe una adecuada triplicación de delítos informáticos en el COIP? ¿Considera usted que estos delítos necesitan un tratamiento especial? ¿Considera necesario tipificar y sancionar los nuevos delítos informáticos mediante una reforma al COIP?	Encuesta Cuestionario	Anexo1 Anexo 2 Anexo 3

Tabla No. 3 Operacionalización de la Variable Independiente
Fuente: Investigador
Elaborado por: David Poveda

Operacionalización de la Variable Dependiente:

CONCEPTUALIZACIÓN	DIMENSIONES	INDICADORES	ÍTEMS BÁSICOS	TÉCNICA	INSTRUMENTO
Delítos Informáticos Son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático.	Delito Responsabilidad Juzgamiento Derechos de las personas	Acto Típico Antijurídico Culpable Dolo Culpa Penal Civil Tutela Jurídica Seguridad jurídica	¿Conoce que es un delíto informático? ¿Conoce los diferentes tipos de delitos informáticos cometidos en el Ecuador? ¿Conoce los delítos informáticos que están tipificados y sancionados por el COIP? ¿Considera usted que las autoridades encargadas de la administración de justicia están capacitadas para conocer y resolver plenamente este tipo de delítos?	Encuesta Cuestionario	Anexo1 Anexo 2 Anexo 3

Tabla No. 4 Operacionalización de la Variable Independiente
Fuente: Investigador
Elaborado por: David Poveda

Plan de Recolección de la Información

Recolección de Información

El siguiente plan contempla estrategias metodológicas requeridas por los objetivos e hipótesis de investigación, de acuerdo con el enfoque escogido, considerando los siguientes elementos:

- Definición de los sujetos: personas u objetos que van a ser investigados.- Profesionales del Derecho, Profesionales de la Salud, y Pacientes o sus familiares.

- Selección de las técnicas a emplear en el proceso de recolección de información.- Según la información de las matrices de la operacionalización de las variables se va a obtener datos mediante la técnica de entrevista y la Encuesta que son de vital importancia.

- Instrumentos seleccionados o diseñados de acuerdo con la técnica escogida para la investigación.- De acuerdo a las matrices de operacionalización de variables, los instrumentos que se van a utilizar son: cuestionarios estructurados.

Tabla 5: Plan De Recolección de la Información

PREGUNTAS BÀSICAS	EXPLICACIÒN
1. **¿**Para qué?	Para alcanzar los objetivos de la Investigación.
2. ¿De qué personas u objetos?	Funcionarios de la Fiscalía, Jueces de Garantías Penales, Abogados en libre ejercicio.
3. ¿Sobre qué aspectos?	Delitos informáticos y su tipificación en el Código Orgánico Integral Penal
4. ¿Quién?	Investigador : David Poveda
5. ¿Cuándo?	Año 2014
6. ¿Dónde?	Fiscalía Provincial de Tungurahua y Corte

	Provincial de Justicia de Tungurahua.
7. ¿Cuántas veces?	Una sola vez
8. ¿Qué técnicas de recolección?	Encuesta
9. ¿Con qué?	Cuestionarios Estructurados
10. ¿En qué situación?	En el lugar indicado en horas laborables

Tabla No. 5 Plan de Recolección de la Información
Fuente: Investigador
Elaborado por: David Poveda

Procesamiento y Análisis

Plan de Procesamiento de la Información:

Para el procesamiento de la Información se siguió los puestos propuestos por: (Hernàndez Sampieri, 2005, pág. 100)

1. *"Revisión crítica de la información recogida; es decir limpieza de información defectuosa: contradictoria, incompleta, no pertinente, entre otros".*
2. *"Repetición de la recolección, en ciertos casos individuales, para corregir fallas de contestación".*
3. *"Tabulación o cuadros según variables de cada hipótesis: manejo de información, estudio estadístico de datos para presentación de resultados".*
4. *"Todos los datos serán presentados de forma estadística para una mejor interpretación y manejo de los datos obtenidos".*

Para procesar la información obtenida se realizará las siguientes actividades:

La tabulación se realizará en forma computarizada mediante el programa de Microsoft Office Excel 2010.

Una vez tabulados los datos, se representa gráficamente, para lo que nos valdremos del programa Microsoft Office Excel 2010.

Plan de Análisis de la Información

De acuerdo con (Rodrìguez & Rodrìguez, 2012) El análisis de datos consiste: "*En la realización de las operaciones a las que el investigador someterá los datos con la finalidad de alcanzar los objetivos del estudio."*

Sin embargo es importante planificar los principales aspectos del plan de análisis en función de la verificación de cada una de las hipótesis formuladas ya que estas definiciones condicionarán a su vez la fase de recolección de datos.

En palabras de (Rodrìguez & Rodrìguez, 2012) Existen dos grandes familias de técnicas de análisis de datos:

- *"Técnicas cualitativas: en las que los datos son presentados de manera verbal (o gráfica) - como los textos de entrevistas, las notas, los documentos…-*
- *Técnicas cuantitativas: en las que los datos se presentan en forma numérica"*

La presente Investigación se realizará con técnicas cuantitativas de manera que posterior a la recolección de los datos se procederá a clasificará las principales medidas estadísticas que nos permitan elaborar un análisis profundo sobre las evoluciones de las variables planteadas. La comparación de datos se la realizará con el objeto de comprobar la hipótesis y generar las conclusiones y recomendaciones pertinentes.

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Los resultados que a continuación se muestran han sido obtenidos al ejecutar las encuestas al personal que labora en las entidades judiciales de la ciudad de Ambato, con el fin de obtener una base sobre la cual emitir ciertos criterios que serán de utilidad para la verificación de la hipótesis planteada.

En el presente capítulo se encuentran el análisis e interpretación de resultados, verificación de hipótesis, mecanismo importante para el procesamiento de datos ya tabulados, a través de la aplicación de la prueba estadística se podrá verificar la misma, es decir si existe una relación entre la variable independiente y la variable dependiente logrando así definir la influencia existente entre estas variables.

Una vez aplicadas las encuestas se procedió a la codificación de los resultados, para luego tabularlos y convertir dichos datos en porcentajes y representaciones gráficas.

Análisis de los Resultados

Pregunta 1

¿Conoce que es un delíto informático?

Personas Encuestadas	Respuestas		Porcentaje		Total	
	SI	NO	SI	NO		
Funcionarios de la Fiscalía	4	0	100%	0%	4	100%
Jueces de Garantías Penales de la ciudad de Ambato	4	0	100%	0%	4	100%
Abogados en libre ejercicio	67	249	21%	79%	316	100%
Agentes Investigadores Policía Judicial	2	0 15	12%	88%	17	100%
Total	77	264	23%	77%	341	100%

Tabla No. 6 Análisis de la Pregunta 1
Fuente: Investigador
Elaborado por: David Poveda

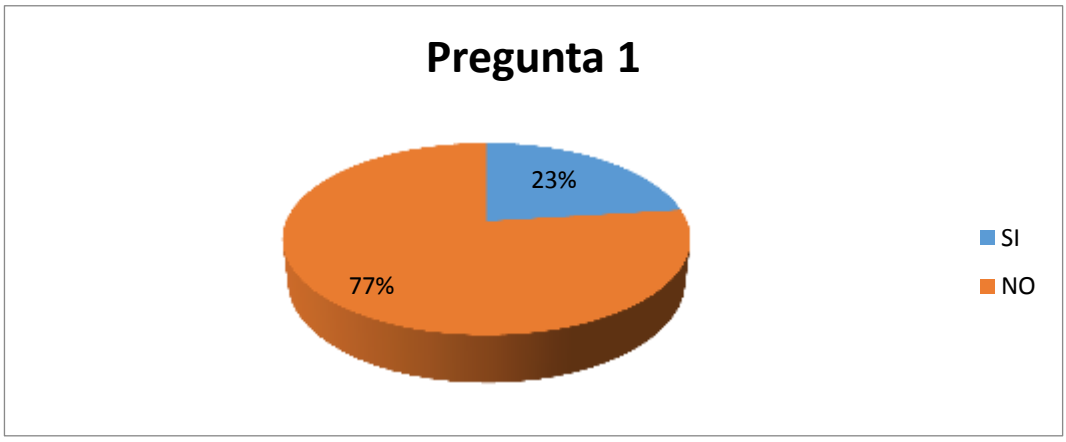


Gráfico No. 5 Interpretación de la Pregunta 1
Fuente: Investigador
Elaborado por: David Poveda

Análisis

De 4 Funcionarios de la Fiscalía Provincial de Tungurahua que fueron encuestados 4 dijeron que si y ninguno dijo que no, equivaliendo esto a un porcentaje de 100% y 0% respectivamente. De los 4 Jueces de Garantías Penales de la Ciudad de Ambato encuestados 4 respondieron que si y ninguno dijo no, esto equivale a un porcentaje de 100% y 0% respectivamente. De 316 Profesionales del Derecho 67 están de acuerdo con la pregunta planteada y 249 no, esto equivale a un total de 21% y 79% respectivamente. De 17 Agentes Investigadores de la Policía Judicial encuestados 2 dijeron que si y 15 que no, esto equivale al 12% y 88% respectivamente. En conclusión podemos deducir que de 341 personas encuestadas 77 dijeron que si y 264 que no, dándonos una totalidad de 23% y 77 % respectivamente.

Interpretación

El 23% de la población encuestada manifiesta que si conoce lo que es un delito informático, mientras que el 77% ha señalado que no. Esto quiere decir claramente que la mayoría de las personas encuestadas no conoce una definición clara y concreta de lo que es un delito informático.

Pregunta 2

¿Conoce los diferentes tipos de delitos informáticos cometidos en el Ecuador?

Personas Encuestadas	Respuestas		Porcentaje		Total	
	SI	NO	SI	NO		
Funcionarios de la Fiscalía	2	2	50%	50%	4	100%
Jueces de Garantías Penales de la ciudad de Ambato	2	2	50%	50%	4	100%
Abogados en libre ejercicio	35	281	11%	89%	316	100%
Agentes Investigadores Policía Judicial	6	11	35%	65%	17	100%
Total	45	296	13%	87%	341	100%

Tabla No. 7 Análisis de la Pregunta 2
Fuente: Investigador
Elaborado por: David Poveda

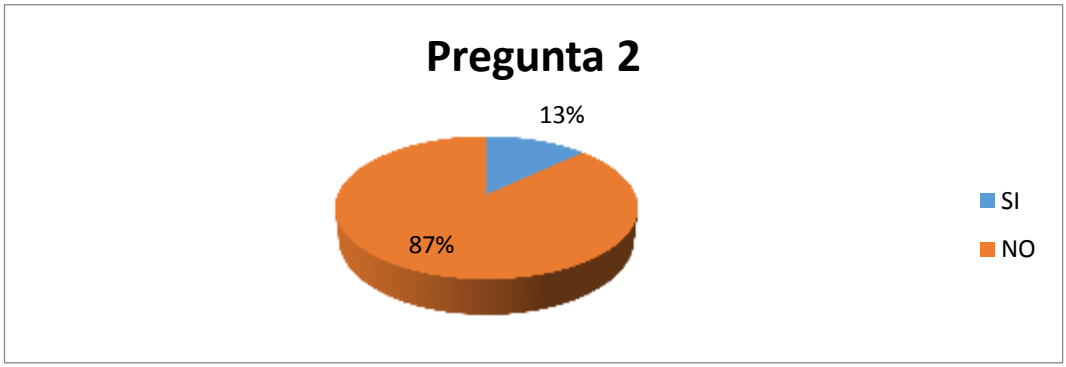


Gráfico No. 6 Interpretación de la Pregunta 2
Fuente: Investigador
Elaborado por: David Poveda

Análisis

De 4 Funcionarios de la Fiscalía Provincial de Tungurahua que fueron encuestados 2 dijeron que si mientras que 2 dijeron que no, equivaliendo esto a un porcentaje de 50% y 50% respectivamente. De los 4 Jueces de Garantías Penales de la Ciudad de Ambato encuestados 2 respondieron que si y de la misma manera 2 dijeron que no, equivaliendo esto a un porcentaje de 50% y 50% respectivamente. De 316 Profesionales del Derecho 35 están de acuerdo con la pregunta planteada y 281 no, esto equivale a un total de 11% y 89% respectivamente. De 17 Agentes Investigadores de la Policía Judicial encuestados 6 dijeron que si y 11 que no, esto equivale al 35% y 65% respectivamente. En conclusión podemos deducir que de 341 personas encuestadas 45 dijeron que si y 296 que no, dándonos una totalidad de 13% y 87 % respectivamente.

Interpretación

De la totalidad de encuestados el 87% manifiestan que no conocen los delitos informáticos cometidos en territorio ecuatoriano razón por la que un gran porcentaje de las víctimas de los mismos no pueden denunciar los mismos, esto en contraposición al 13% que manifiesta que si conoce sobre el tema.

De lo que podemos deducir que la gran mayoría de la población desconoce sobre los delitos informáticos cometidos en el Ecuador.

Pregunta 3

Conoce los delítos informáticos que están tipificados y sancionados por el COIP?

Personas Encuestadas	Respuestas		Porcentaje		Total	
	SI	NO	SI	NO		
Funcionarios de la Fiscalía	2	2	50%	50%	4	100%
Jueces de Garantías Penales de la ciudad de Ambato	2	2	50%	50%	4	100%
Abogados en libre ejercicio	29	287	9%	91%	316	100%
Agentes Investigadores Policía Judicial	6	11	35%	65%	17	100%
Total	39	302	11%	89%	341	100%

Tabla No. 8 Análisis de la Pregunta 3
Fuente: Investigador
Elaborado por: David Poveda

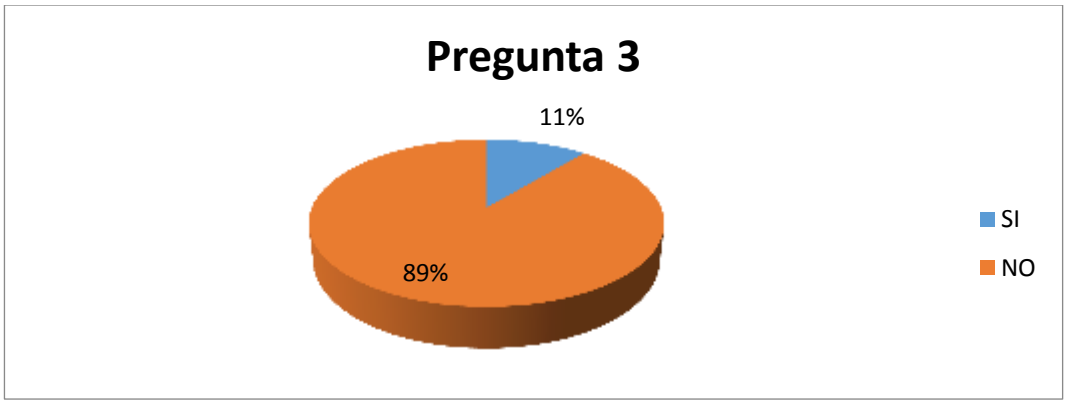


Gráfico No. 7 Interpretación de la Pregunta 3
Fuente: Investigador
Elaborado por: David Poveda

Análisis

De 4 Funcionarios de la Fiscalía Provincial de Tungurahua que fueron encuestados 2 dijeron que si mientras que 2 dijeron que no, equivaliendo esto a un porcentaje de 50% y 50% respectivamente. De los 4 Jueces de Garantías Penales de la Ciudad de Ambato encuestados 2 respondieron que si y de la misma manera 2 dijeron que no, equivaliendo esto a un porcentaje de 50% y 50% respectivamente. De 316 Profesionales del Derecho 29 están de acuerdo con la pregunta planteada y 287 no, esto equivale a un total de 9% y 91% respectivamente. De 17 Agentes Investigadores de la Policía Judicial encuestados 6 dijeron que si y 11 que no, esto equivale al 35% y 65% respectivamente. En conclusión podemos deducir que de 341 personas encuestadas 39 dijeron que si y 302 que no, dándonos una totalidad de 11% y 89 % respectivamente.

Interpretación

El 89% manifiesta que no conoce la tipificación contenida en el Código Orgánico Integral Penal respecto de los delitos informáticos esto frente al 11% dice si conocer al respecto, hecho por el cual se considera necesario la tipificación de los mismos de una manera clara y explícita en relación a los tipos y a la sanción de los mismos.

Pregunta 4

¿Considera usted que las autoridades encargadas de la administración de justicia están capacitadas para conocer y resolver plenamente este tipo de delítos?

Personas Encuestadas	Respuestas		Porcentaje		Total	
	SI	NO	SI	NO		
Funcionarios de la Fiscalía	1	3	25%	75%	4	100%
Jueces de Garantías Penales de la ciudad de Ambato	0	4	0%	100%	4	100%
Abogados en libre ejercicio	35	281	11%	89%	316	100%
Agentes Investigadores Policía Judicial	4	13	24%	76%	17	100%
Total	40	301	12%	88%	341	100%

Tabla No. 9 Análisis de la Pregunta 4
Fuente: Investigador
Elaborado por: David Poveda

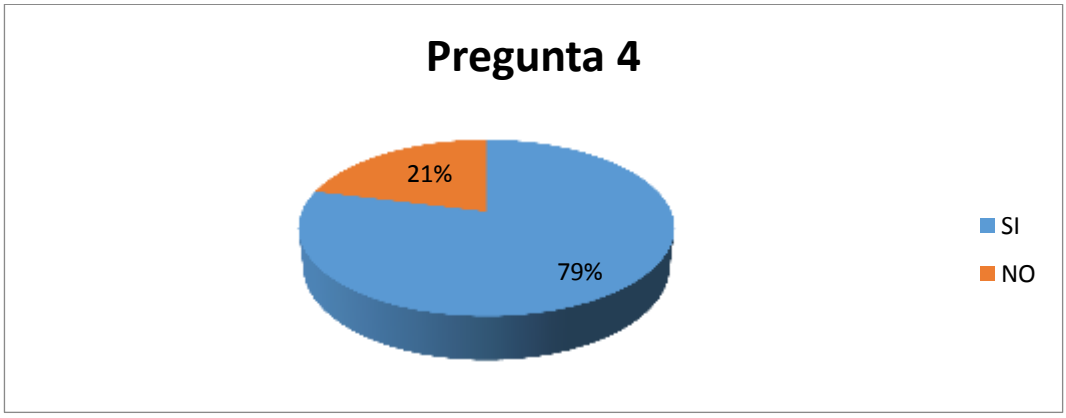


Gráfico No. 8 Interpretación de la Pregunta 4
Fuente: Investigador
Elaborado por: David Poveda

Análisis

De 4 Funcionarios de la Fiscalía Provincial de Tungurahua que fueron encuestados 1 dijeron que si mientras que 3 dijeron que no, equivaliendo esto a un porcentaje de 25% y 75% respectivamente. De los 4 Jueces de Garantías Penales de la Ciudad de Ambato encuestados 0 respondieron que si y mientras 4 dijeron que no, equivaliendo esto a un porcentaje de 0% y 100% respectivamente. De 316 Profesionales del Derecho 35 están de acuerdo con la pregunta planteada y 281 no, esto equivale a un total de 11% y 89% respectivamente. De 17 Agentes Investigadores de la Policía Judicial encuestados 4 dijeron que si y 13 que no, esto equivale al 24% y 76% respectivamente. En conclusión podemos deducir que de 341 personas encuestadas 40 dijeron que si y 301 que no, dándonos una totalidad de 12% y 88 % respectivamente.

Interpretación

El 88% de la población considera que las autoridades encargadas de la administración de Justicia no están capacitadas para conocer y resolver plenamente este tipo de delíto, esto frente al 12% que manifiesta que si lo están.

Pregunta 5

¿Considera usted que en la investigación realizada para recabar indicios es la adecuada?

Personas Encuestadas	Respuestas		Porcentaje		Total	
	SI	NO	SI	NO		
Funcionarios de la Fiscalía	1	3	25%	75%	4	100%
Jueces de Garantías Penales de la ciudad de Ambato	1	3	25%	75%	4	100%
Abogados en libre ejercicio	30	286	9%	91%	316	100%
Agentes Investigadores Policía Judicial	2	15	12%	88%	17	100%
Total	34	307	10%	90%	341	100%

Tabla No. 10 Análisis de la Pregunta 5
Fuente: Investigador
Elaborado por: David Poveda

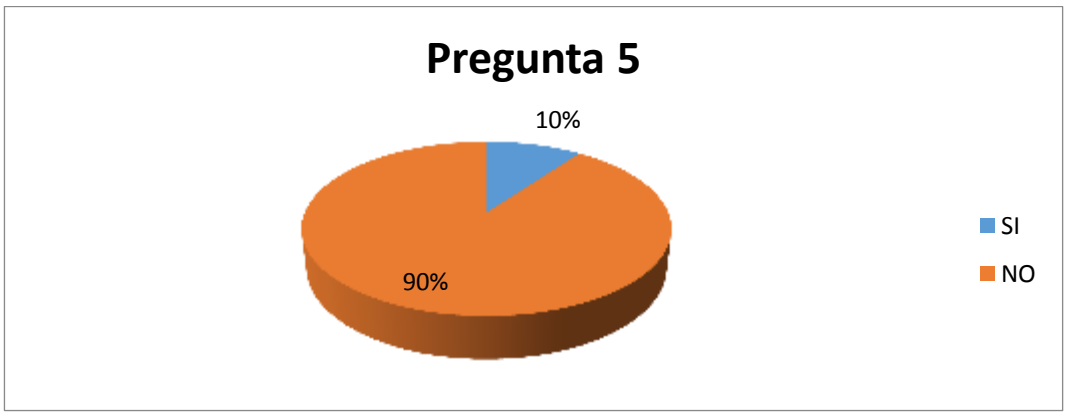


Gráfico No. 9 Interpretación de la Pregunta 5
Fuente: Investigador
Elaborado por: David Poveda

Análisis

De 4 Funcionarios de la Fiscalía Provincial de Tungurahua que fueron encuestados 1 dijeron que si mientras que 3 dijeron que no, equivaliendo esto a un porcentaje de 25% y 75% respectivamente. De los 4 Jueces de Garantías Penales de la Ciudad de Ambato encuestados 1 respondió que si y mientras 3 dijeron que no, equivaliendo esto a un porcentaje de 1% y 75% respectivamente. De 316 Profesionales del Derecho 30 están de acuerdo con la pregunta planteada y 286 no, esto equivale a un total de 9% y 91% respectivamente. De 17 Agentes Investigadores de la Policía Judicial encuestados 2 dijeron que si y 15 que no, esto equivale al 12% y 88% respectivamente. En conclusión podemos deducir que de 341 personas encuestadas 34 dijeron que si y 307 que no, dándonos una totalidad de 10% y 90 % respectivamente.

Interpretación.

El 10% de los encuestados manifiestan que la investigación realizada para recabar indicios es la adecuada, sobreponiéndose a esto el 90% que manifiesta que no lo es.

Pregunta 6

¿Cree usted que existe una adecuada tipificación de delítos informáticos en el COIP?

Personas Encuestadas	Respuestas		Porcentaje		Total	
	SI	NO	SI	NO		
Funcionarios de la Fiscalía	1	3	25%	75%	4	100%
Jueces de Garantías Penales de la ciudad de Ambato	0	4	0%	100%	4	100%
Abogados en libre ejercicio	67	249	21%	79%	316	100%
Agentes Investigadores Policía Judicial	6	11	35%	65%	17	100%
Total	74	267	22%	78%	341	100%

Tabla No. 11 Análisis de la Pregunta 6
Fuente: Investigador
Elaborado por: David Poveda

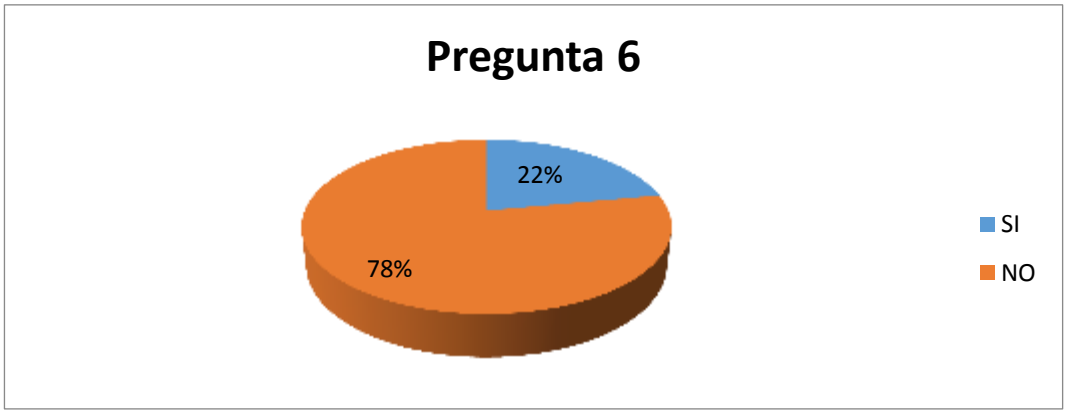


Gráfico No. 10 Interpretación de la Pregunta 6
Fuente: Investigador
Elaborado por: David Poveda

Análisis

De 4 Funcionarios de la Fiscalía Provincial de Tungurahua que fueron encuestados 1 dijo que si mientras que 3 dijeron que no, equivaliendo esto a un porcentaje de 25% y 75% respectivamente. De los 4 Jueces de Garantías Penales de la Ciudad de Ambato encuestados ninguno respondió afirmativamente a esta pregunta mientras 4 dijeron que no, equivaliendo esto a un porcentaje de 0% y 100% respectivamente. De 316 Profesionales del Derecho 67 están de acuerdo con la pregunta planteada y 249 no, esto equivale a un total de 21% y 79% respectivamente. De 17 Agentes Investigadores de la Policía Judicial encuestados 6 dijeron que si y 11 que no, esto equivale al 22% y 78% respectivamente. En conclusión podemos deducir que de 341 personas encuestadas 74 dijeron que si y 267 que no, dándonos una totalidad de 22% y 78% respectivamente.

Interpretación.

El 22% de las personas encuestadas considera que si existe una adecuada tipificación de los delitos Informáticos contenidos en el COIP, esto en contraposición al 78% que señala que no está de acuerdo con la pregunta formulada.

Pregunta 7

¿Considera usted que estos delítos necesitan una mayor sanción?

Personas Encuestadas	Respuestas		Porcentaje		Total	
	SI	NO	SI	NO		
Funcionarios de la Fiscalía	4	0	100%	0%	4	100%
Jueces de Garantías Penales de la ciudad de Ambato	4	0	100%	0%	4	100%
Abogados en libre ejercicio	269	47	85%	15%	316	100%
Agentes Investigadores Policía Judicial	17	0	100%	0%	17	100%
Total	294	47	86%	14%	341	100%

Tabla No. 12 Análisis de la Pregunta 7
Fuente: Investigador
Elaborado por: David Poveda

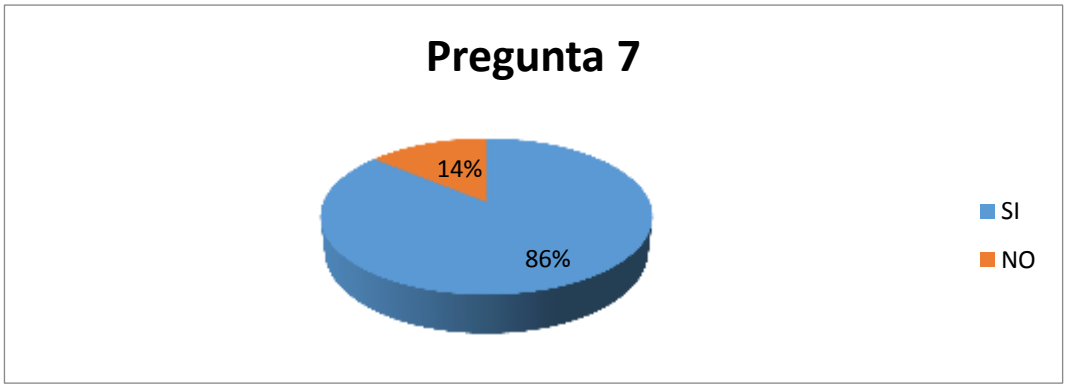


Gráfico No. 11 Interpretación de la Pregunta 7
Fuente: Investigador
Elaborado por: David Poveda

Análisis

De 4 Funcionarios de la Fiscalía Provincial de Tungurahua que fueron encuestados 4 dijo que si mientras que mientras que ninguno dijo que no, equivaliendo esto a un porcentaje de 100% y 0% respectivamente. De los 4 Jueces de Garantías Penales de la Ciudad de Ambato encuestados todos respondieron afirmativamente a esta pregunta y ninguno dijo que no, equivaliendo esto a un porcentaje del 100% y 0% respectivamente. De 316 Profesionales del Derecho 269 están de acuerdo con la pregunta planteada y 47 no, esto equivale a un total de 85% y 15% respectivamente. De 17 Agentes Investigadores de la Policía Judicial encuestados todos dijeron que si, esto equivale al 100% de la aceptación de la pregunta. En conclusión podemos deducir que de 341 personas encuestadas 294 dijeron que si y 47 que no, dándonos una totalidad de 86% y 14% respectivamente.

Interpretación.

El 86% de las personas encuestadas consideran que los delitos informáticos deben tener una sanción mayor a las establecidas en el Código Orgánico Integral Penal, esto en contraposición al 14% de los encuestados que no están de acuerdo.

Pregunta 8

¿Considera necesario tipificar y sancionar nuevos delítos informáticos mediante una reforma al COIP?

Personas Encuestadas	Respuestas		Porcentaje		Total	
	SI	NO	SI	NO		
Funcionarios de la Fiscalía	4	0	100%	0%	4	100%
Jueces de Garantías Penales de la ciudad de Ambato	4	0	100%	0%	4	100%
Abogados en libre ejercicio	257	59	81%	19%	316	100%
Agentes Investigadores Policía Judicial	16	1	94%	6%	17	100%
Total	281	60	82%	18%	341	100%

Tabla No. 13 Análisis de la Pregunta 8
Fuente: Investigador
Elaborado por: David Poveda

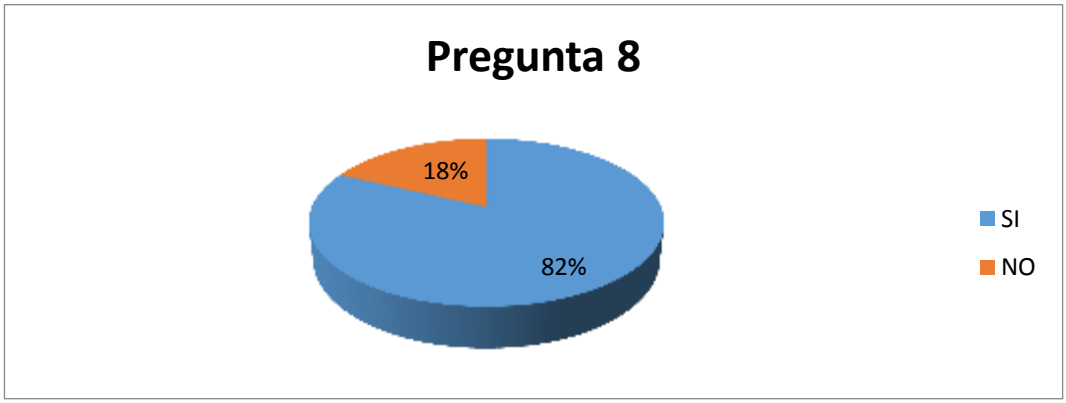


Gráfico No. 12 Interpretación de la Pregunta 8
Fuente: Investigador
Elaborado por: David Poveda

Análisis

De 4 Funcionarios de la Fiscalía Provincial de Tungurahua que fueron encuestados 4 dijeron que si mientras que ninguno dijo que no, equivaliendo esto a un porcentaje de 100% y 0% respectivamente. De los 4 Jueces de Garantías Penales de la Ciudad de Ambato encuestados todos respondieron afirmativamente a esta pregunta y ninguno dijo que no, equivaliendo esto a un porcentaje del 100% y 0% respectivamente. De 316 Profesionales del Derecho 257 están de acuerdo con la pregunta planteada y 57 indican que no, esto equivale a un total de 94% y 6% respectivamente. De 17 Agentes Investigadores de la Policía Judicial encuestados 16 contestaron que si mientras que solo 1 manifestó que no, esto equivale al 94% y al 6% respectivamente. En conclusión podemos deducir que de 341 personas encuestadas 281 dijeron que si y 60 que no, dándonos una totalidad de 82% y 18% respectivamente.

Interpretación.

El 82% considera necesario tipificar y sancionar nuevos delítos informáticos mediante una reforma al COIP, esto en contraposición al 18% que considera que no.

Pregunta 9

¿Conoce que es un hacker y un cracker?

Personas Encuestadas	Respuestas		Porcentaje		Total	
	SI	NO	SI	NO		
Funcionarios de la Fiscalía	2	2	50%	50%	4	100%
Jueces de Garantías Penales de la ciudad de Ambato	2	2	50%	50%	4	100%
Abogados en libre ejercicio	187	129	59%	41%	316	100%
Agentes Investigadores Policía Judicial	6	11	35%	65%	17	100%
Total	197	144	58%	42%	341	100%

Tabla No. 14 Análisis de la Pregunta 9
Fuente: Investigador
Elaborado por: David Poveda

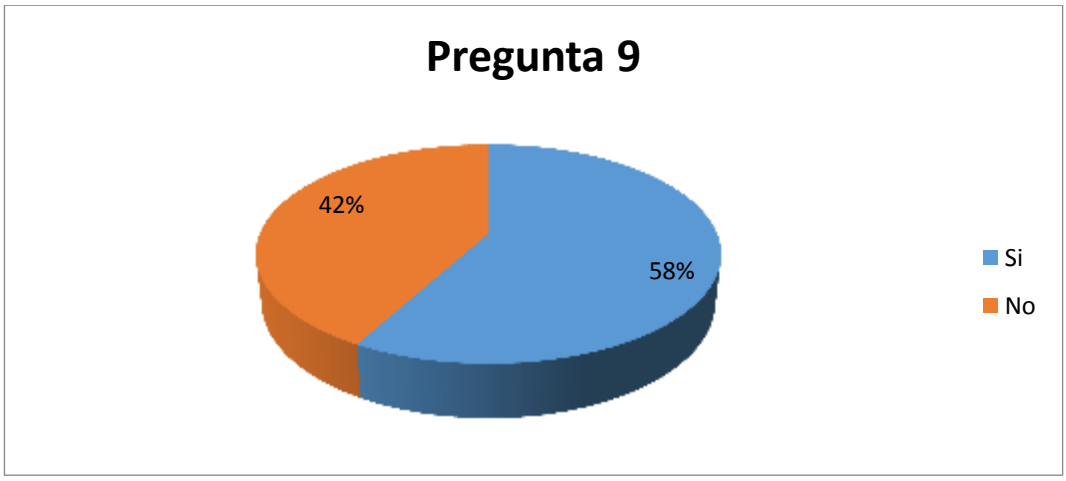


Gráfico No. 13 Interpretación de la Pregunta 9
Fuente: Investigador
Elaborado por: David Poveda

Análisis

De 4 Funcionarios de la Fiscalía Provincial de Tungurahua que fueron encuestados 2 dijeron que si y de la misma manera 2 manifestaron que no, equivaliendo esto a un porcentaje de 50% y 50% respectivamente. De los 4 Jueces de Garantías Penales de la Ciudad de Ambato encuestados 2 dijeron que si y de la misma manera 2 manifestaron que no, equivaliendo esto a un porcentaje de 50% y 50% respectivamente. De 316 Profesionales del Derecho 187 están de acuerdo con la pregunta planteada y 129 indican que no, esto equivale a un total de 59% y 41% respectivamente. De 17 Agentes Investigadores de la Policía Judicial encuestados 11 contestaron que si mientras que 6 manifestaron que no, esto equivale al 35% y al 65% respectivamente. En conclusión podemos deducir que de 341 personas encuestadas 197 dijeron que si y 144 que no, dándonos una totalidad de 58% y 42% respectivamente.

Interpretación.

El 58% de la población encuestada manifiesta que si conoce lo que es un Hacker y un Cracker, esto en contraposición al 42% que manifiesta que no.

Pregunta 10

¿Considera necesaria la tipificación de las figuras delictivas de hacker y Cracker en el COIP?

Personas Encuestadas	Respuestas		Porcentaje		Total	
	SI	NO	SI	NO		
Funcionarios de la Fiscalía	3	1	75%	25%	4	100%
Jueces de Garantías Penales de la ciudad de Ambato	4	0	100%	0%	4	100%
Abogados en libre ejercicio	287	29	91%	9%	316	100%
Agentes Investigadores Policía Judicial	15	2	88%	12%	17	100%
Total	309	32	91%	9%	341	100%

Tabla No. 15 Análisis de la Pregunta 10
Fuente: Investigador
Elaborado por: David Poveda

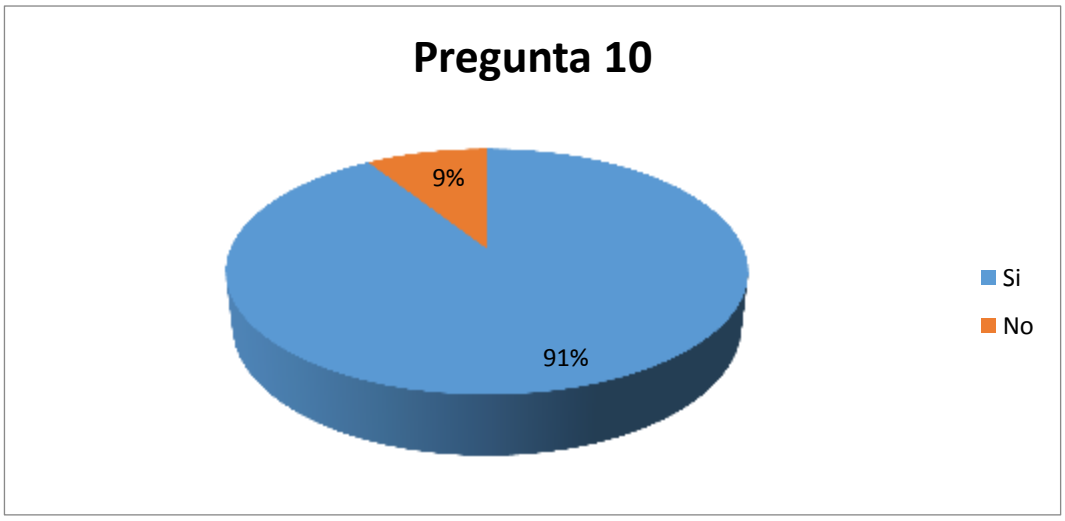


Gráfico No. 14 Interpretación de la Pregunta 10
Fuente: Investigador
Elaborado por: David Poveda

Análisis

De 4 Funcionarios de la Fiscalía Provincial de Tungurahua que fueron encuestados 3 dijeron que si y de la misma manera 1 manifestaron que no, equivaliendo esto a un porcentaje de 75% y 25% respectivamente. De los 4 Jueces de Garantías Penales de la Ciudad de Ambato encuestados 4 dijeron que si y ninguno manifestó que no, equivaliendo esto a un porcentaje de 100% y 0% respectivamente. De 316 Profesionales del Derecho 287 están de acuerdo con la pregunta planteada y 29 indican que no, esto equivale a un total de 91% y 9% respectivamente. De 17 Agentes Investigadores de la Policía Judicial encuestados 15 contestaron que si mientras que 2 manifestaron que no, esto equivale al 88% y al 12% respectivamente. En conclusión podemos deducir que de 341 personas encuestadas 309 dijeron que si y 32 que no, dándonos una totalidad de 91% y 9% respectivamente.

Interpretación.

El 91% de la población encuestada manifiesta que si considera necesaria la tipificación de las figuras delictivas de hacker y cracker en el CIOP, esto en contraposición al 9% que manifiesta que no.

Cuadro Resumen

Preguntas Realizadas	Funcionarios de la Fiscalía Provincial de Tungurahua				Jueces de Garantías Penales				Profecionales del Derecho				Agentes Investigadores de la Policía Judicial				Total			
	Si	%	No	%	Si	%	No	%	Si	%	No	%	Si	%	No	%	Si	%	No	%
Pregunta 1	4	100%	0	0%	4	100%	0	0%	67	21%	249	79%	2	12%	15	88%	77	23%	264	77%
Pregunta 2	2	50%	2	50%	2	50%	2	50%	35	11%	281	89%	6	35%	11	65%	45	13%	296	87%
Pregunta 3	2	50%	2	50%	2	50%	2	50%	29	9%	287	91%	6	35%	11	65%	39	11%	302	89%
Pregunta 4	1	25%	3	75%	0	0%	4	100%	35	11%	281	89%	4	24%	13	76%	40	12%	301	88%
Pregunta 5	1	25%	3	75%	1	25%	3	75%	30	9%	286	91%	2	12%	15	88%	34	10%	307	90%
Pregunta 6	1	25%	3	75%	0	0%	4	100%	67	21%	249	79%	6	35%	11	65%	74	22%	267	78%
Pregunta 7	4	100%	0	0%	4	100%	0	0%	269	85%	47	15%	17	100%	0	0%	294	86%	47	14%
Pregunta 8	4	100%	0	0%	4	100%	0	0%	257	81%	59	19%	16	94%	1	6%	281	82%	60	18%
Pregunta 9	2	50%	2	50%	2	50%	2	50%	187	59%	129	41%	6	35%	11	65%	197	58%	144	42%
Pregunta 10	3	75%	1	25%	4	100%	0	0%	287	91	29	9%	15	88%	2	12%	309	91%	32	9%
Total	4				4				316				17				**341=100%**			

Tabla No. 16 Cuadro Resumen
Fuente: Investigador
Elaborado por: David Poveda

Verificación de Hipótesis

Luego de determinado el problema y una vez realizada la investigación de campo se puede plantear la hipótesis con su correspondiente operacionalización de variables.

Comprobación de la hipótesis con el Chi cuadrado

La hipótesis será verificada mediante el modelo estadístico del Chi cuadrado, que permite establecer la correspondencia de valores observados y esperados, permitiendo la comparación total del grupo de frecuencias a partir de la hipótesis que se quiere verificar y con el propósito de comprobar si los valores de la frecuencia obtenidos en las encuestas y registrados en la tabla son representativos.

Planteamiento de la Hipótesis

Para el cálculo de la verificación se toma en cuenta dos variables de la hipótesis ya planteada, hipótesis alternativa en base a esta se trabaja el planteamiento.

H a (alternativa)

La falta de tipicidad y sanción de los nuevos delitos informáticos inciden en la impunidad de los mismos.

Selección del nivel de significación

Para la verificación hipotética se utilizará el nivel de aceptación que es igual a 0,01 (99%), o igual a $\propto$ 0,05.

Especificación estadística

Se trata de un cuadrado de contingencia de 4 filas por 2 columnas con la aplicación de la siguiente fórmula estadística:

$$X^2 = \frac{\sum (O - E)^2}{E}$$

X^2 = Chi cuadrado

$\sum$ = sumatoria

O = frecuencia observada

E = frecuencia esperada

Especificación de régimen de aceptación y rechazo

Para decidir primero determinaremos los grados de libertad (gl) con el cuadrado formado por 4 filas y dos columnas.

$\propto = 0,05$

$gl = (f-1)(c-1)$

$gl = (4-1)(2-1)$

$gl = (3)(1)$

$gl = 3$

Frecuencia Observada			
Alternativas	**Categorías**		**Total**
	Si	**No**	
¿Considera usted que estos delítos necesitan una mayor sanción?	294	47	341
¿Conoce los delítos informáticos que están tipificados y sancionados por el COIP?	39	302	341
¿Conoce que es un hacker y un cracker?	197	144	341
¿Considera necesaria la tipificación de las figuras delictivas de hacker y Cracker en el COIP?	309	32	341
Total	839	525	1.364

Tabla No. 17 Frecuencia Observada
Fuente: Investigador
Elaborado por: David Poveda

Modelo matemático

$$H\,a = O = E \rightarrow O - E = O$$

$$H\,o = O \neq E \rightarrow O - E \neq O$$

Simbología

Fe: frecuencia esperada

TC: total columnas

TF: total filas

TM: total muestra

$$Fe = \frac{(TC)\,(TF)}{(TM)}$$

Contingencia

	O	**E**	**O - E**	**(O - E) ^{2}**	**(O - E) ^{2} / E**
	294	209,75	84,25	7.098	33,84
	39	209,75	-170,75	29.156	139,00
	197	209,75	-12,75	163	0,78
Si	309	209,75	99,25	9.851	46,96
	47	131,25	-84,25	7.098	54,08
	302	131,25	170,75	29.156	222,14
	144	131,25	12,75	163	1,24
NO	32	131,25	-99,25	9.851	75,05
CHI					573,09

Tabla No. 18 Cálculo del Chi cuadrado
Fuente: Investigadora
Elaborado por: David Poveda

Chi calculado x^2 c

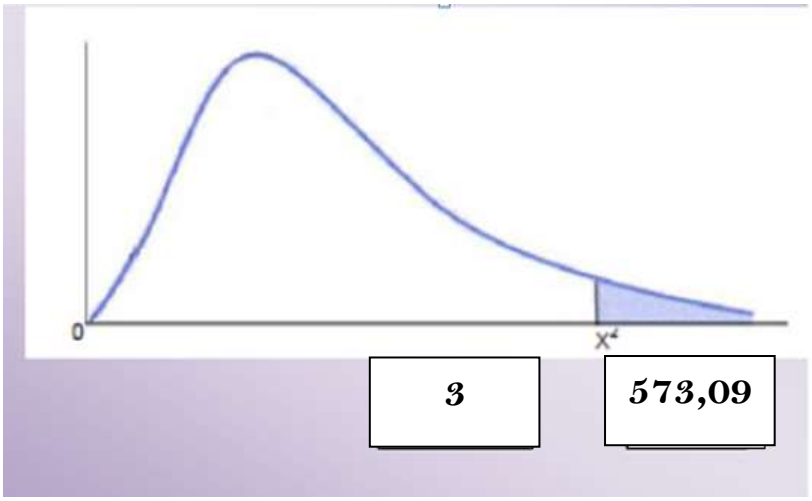
Si **x^2 c ≥ x^2 a** se rechaza la hipótesis nula y se acepta la hipótesis alterna.

$$x^2c \geq x^2 a$$

chi calculado ≥chi tabulado

Con los datos y resultados obtenidos llegamos a verificar que la hipótesis planteada en el Capítulo II dónde: "LA LEGISLACIÓN PENAL ECUATORIANA Y LOS DELITOS INFORMÁTICOS EN LA CIUDAD DE AMBATO." se comprueba. Por lo tanto se aprueba la misma.

Obteniendo como resultado del cálculo del Chi cuadrado 143.21, con un nivel de significación del 0,05 y los grados de libertad de 3; la Chi cuadrada tabulada es 143.21 representada en la Campana de Gauss.



K = 573,09

Gráfico No. 15 Campana de Gauss
Fuente: Investigador
Elaborado por: David Poveda

En definitiva, después de haber investigado y elaborado un cuidadoso estudio de las encuestas realizadas, dentro de lo que es la parte metodológica del presente trabajo, se puede observar que de éstas se desprenden resultados directamente relacionados con la hipótesis planteada "La falta de tipicidad y sanción de los nuevos delitos informáticos incide en la inimputabilidad de los mismos" ya que fue aprobada previa comprobación de los resultados de la misma.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- Se concluye que no existe incidencia entre la tipificación y sanción de los delitos informáticos no contenidos en el Código Orgánico Integral Penal y la impunidad de estos actos ilícitos, ya que de no tener sanciones para delitos específicos no es posible dictar sentencias y los actos lamentablemente no pueden ser juzgados amparándose en la normativa legal.

- La tipificación actual no es la idónea ya que no contempla cierto tipo de delitos ni estipula sus sanciones, por lo que se considera que existen muchos vacíos en el área de Delitos Informáticos dentro del Código Orgánico Integral Penal.

- Existen muchos vacíos jurídicos dentro de la normativa jurídica con relación a los delitos informáticos en la declaración, tipificación penalización de los actos ilícitos en especial en el Código Orgánico Integral Penal por lo que muchos delitos no pueden ser juzgados y los jueces se ven en la obligación de dar a estos el tratamiento como si se trataran de delitos cometidos convencionalmente.

- Es necesario implementar una propuesta de solución mediante la tipificación y sanción de los delitos informáticos para evitar la impunidad de estos actos ilícitos tales como la inclusión de la figura delictiva del Hacking y el Cracking.

RECOMENDACIONES

- Se recomienda buscar alternativas de solución en las que se puedan solucionar los problemas de la tipificación y sanción de los delitos informáticos no contenidos en el Código Orgánico Integral Penal y la evitación de la impunidad de estos actos ilícitos, para que puedan ser sancionados y la ciudadanía no se quede expuesta a este tipo de abusos de tipo legal.

- Se recomienda una mejoría en la tipificación actual para que contemple todo tipo de delitos y estipule sanciones de forma que no existan varios en el área de Delitos Informáticos dentro del Código Orgánico Integral Penal.

- Se recomienda dar a conocer los vacíos jurídicos en la normativa jurídica con relación a los delitos informáticos actos ilícitos en especial en el Código Orgánico Integral Penal para que muchos delitos puedan ser juzgados y los jueces se vean en la obligación de dictar las sanciones según la normativa a los hallados culpables

- Se recomienda implementar una propuesta de solución mediante la tipificación y sanción de los delitos informáticos para evitar la impunidad de estos actos ilícitos

- Se recomienda la creación de una Agencia de Control de la Información misma que se encargará de vigilar de y dar seguimiento a los presuntos Hackers y Crackers en el territorio ecuatoriano.

CAPÍTULO VI

PROPUESTA

Datos Informativos

Título:
"PROYECTO DE LEY REFORMATORIA A LA SECCIÓN TERCERA REFERENTE A DELITOS CONTRA LA SEGURIDAD DE LOS ACTIVOS DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN DEL CÓDIGO ORGÁNICO INTEGRAL PENAL"

Institución Ejecutora: Asamblea Nacional y la Universidad Técnica de Ambato
Investigador: David Poveda
Beneficiarios: La sociedad
Ubicación: Ambato
Tiempo de Ejecución: seis meses.
Equipo técnico responsable: David Poveda
Presupuesto: 16.600 dólares de los Estados Unidos de Norteamérica.

Antecedentes de la Propuesta

El constante avance de la tecnología en los actuales momentos constituyen hasta cierto punto una gran desventaja para el Derecho Penal no solo a nivel del Ecuador sino también a nivel mundial debido a que la aparición de estas nuevas tecnologías van ligadas a este hecho la aparición de nuevos actos ilícitos con nuevas características y elementos constitutivos, es decir estos son los delitos informáticos mismos que a criterio personal deben ser tipificados de forma clara y concreta dentro del Código Orgánico Integral Penal, ya que en la actualidad estos ilícitos no se encuentran tipificados y sancionados como tales.

Los Delitos Informáticos son meramente públicos razón por la cual corresponde al Estado adoptar mecanismos legales, para prevenir y sancionar estos ilícitos comprendiendo que el sujeto activo que lo realiza posee la suficiente voluntad y conciencia base primordial de la razón para proceder a realizarlo en otras palabras es un acto doloso, sin tomar en cuenta la capacidad y el vasto conocimiento en cuanto a sistemas informáticos se refiere

Justificación

La presente investigación constituye una temática de interés para la sociedad y para las Ciencias Jurídicas. Encuentra su justificación en razón de que el Sistema Penal no contempla sanciones para las personas que cometan los delítos informáticos conocidos también como delitos contra sistemas de información conocidos como Hacking y Cracking no es castigado con una pena equivalente al daño ocasionado por el cometimiento de los mismos, y mucho establece una sanción en caso de reincidencia

La importancia del tema radica en la inseguridad pública y la transgresión del bien jurídico protegido ya al permitir que estos actos dolosos sean sancionados con una pena nada proporcional al daño inferido, ya que quien incurra en este ipo de delitos deben ser condenado a una pena privativa de la libertad mucho más severa de las constantes en la sección tercera del Código Orgánico Integral Penal, razones por las que estos ilícitos conocidos técnicamente como Hacking y Cracking deben constar dentro de la tipificación del COIP de una manera clara y expresa y de la misma manera incorporar la definición de delitos informáticos o conocidos también como delitos contra los sistemas de información.

El presente proyecto es de gran impacto social, ya que en un mundo legalizado y globalizado en el que vivimos, es menester del legislador aportar con las leyes necesarias acorde a la actualidad, para que Los Delitos informáticos del Hacking y el Cracking no queden en la impunidad y tampoco se siga cometiendo además de buscar establecer una definición clara de los que es un delito informático y establecer penas privativas de la libertad proporcionales y acorde a

estos actos delictivos ya que los sujetos activos de estos poseen un nivel de formación académico elevado y lo utilizan para la perpetración de actos delictivos.

Es factible porque el investigador cuenta con los recursos necesarios para la presente investigación, otorgados por la Universidad Técnica de Ambato, Facultad de Jurisprudencia y Ciencias Sociales, carrera de Derecho, además con la ayuda en las encuestas practicadas a los Jueces de Garantías Penales con sede en el catón Ambato, Funcionarios de la Fiscalía Provincial de Tungurahua con cede en el cantón Ambato y de la misma manera con los Agentes investigadores de la Policía Judicial de Tungurahua.

Objetivos

Objetivo General

Elaborar un proyecto de ley reformatoria a la sección tercera referente a delitos contra la seguridad de los activos de los sistemas de información y comunicación del código orgánico integral penal.

Objetivos Específicos

- Redacción del proyecto de Ley Reformatoria a la sección tercera referente a delitos contra la seguridad de los activos de los sistemas de información y comunicación del Código Orgánico Integral Penal.
- Socializar el proyecto de Ley Reformatoria a la sección tercera referente a delitos contra la seguridad de los activos de los sistemas de información y comunicación del Código Orgánico Integral Penal..
- Presentar el proyecto de Ley Reformatoria a la sección tercera referente a delitos contra la seguridad de los activos de los sistemas de información y comunicación del Código Orgánico Integral Penal, ante la Asamblea Nacional.

Modelo Operativo de la Propuesta

Tiempo	Actividad	Objetivo	Recurso	Responsable
2 meses	Redacción del Proyecto de Ley Reformatoria a la sección tercera del COIP	Adecuar textualmente la voluntad del pueblo y su soberanía, respecto al Hacking, Cracking y establecer una definición y sanción para delítos informáticos.	Computadora Internet Impresora Libros Revistas Enciclopedias	Investigador
2 meses	Socializar el Proyecto	Dar a conocer a la sociedad en general el beneficio de la tipificación y sanción de estos delitos.	Volantes Gigantografías Publicidad.	
2 meses	Presentación del Proyecto a la Asamblea	Aprobación del Proyecto por la Asamblea que permita exista un cambio	Investigador Comisión Legislativa	

Tabla No. 19 Modelo Operativo
Fuente: Investigador
Elaborado por: David Poveda

DESARROLLO DE LA PROPUESTA

Objetivo 1

Redacción del proyecto de Ley Reformatoria a la sección tercera referente a delitos contra la seguridad de los activos de los sistemas de información y comunicación del Código Orgánico Integral Penal.

La Redacción del proyecto de Ley Reformatoria a la sección tercera referente a delitos contra la seguridad de los activos de los sistemas de información y comunicación del Código Orgánico Integral Penal., es constitucionalmente procedente ya que no violenta Tratados Internacionales,

Además ya que la constitución es garantista de derechos y como uno de los derechos consagrados en la constitución de la República en el Art. 61 numeral 3, que menciona, los ecuatorianos tenemos el derecho de presentar proyectos de iniciativa normativa de ley o de reforma en concordancia con lo que determina el Art. 103 de la misma Carta Magna en la cual se puede crear o reformar como en este caso la ley.

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.

Además se debe considerar la problemática Jurídica, ya que si bien es cierto Ecuador posee Normativas Legales que contemplan aspectos significativos respecto de las nuevas tecnologías y también se han establecido penas en el Código Orgánico Integral 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 más clara y precisa.

REPÚBLICA DEL ECUADOR

LA ASAMBLEA NACIONAL

CONSIDERANDO

QUE, el Art. 1 de la Constitución de la República del Ecuador, en el inciso segundo enmarca que la soberanía radica en pueblo, cuya voluntad es el fundamento de la autoridad, lo cual implica realizar cambios normativos que respondan coherentemente al espíritu de la Constitución

QUE, el Art. 61 numeral 3 Constitución de la República del Ecuador, es derecho de las ecuatorianas y ecuatorianos presentar proyectos de iniciativa popular normativa.

QUE, de acuerdo el Art. 76 de la Constitución de la República del Ecuador, en el numeral 6 dispone la debida proporcionalidad de la infracción respecto a la sanción penal, lo cual implica un castigo justo al ilícito cometido sin ningún tipo preferencia al infractor.

QUE, La Constitución de la República del Ecuador prescribe en el Art. 84, la obligación que tiene la Asamblea Nacional, de adecuar formal y materialmente, las leyes y demás normas jurídicas a los derechos previstos en la Constitución y tratados internacionales.

QUE, Art. 103 de Constitución de la República del Ecuador, propone que la iniciativa popular normativa se ejercerá para proponer la creación, reforma o derogatoria de la norma jurídica.

En ejercicio de sus facultades y atribuciones, constitucionales y legales, expide la siguiente:

PROYECTO DE LEY REFORMATORIA A LA SECCIÓN TERCERA REFERENTE A DELITOS CONTRA LA SEGURIDAD DE LOS ACTIVOS DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN DEL CÓDIGO ORGÁNICO INTEGRAL PENAL

Agréguese previo al Art. 229 del Código Orgánico Integral Penal lo siguiente:

Art. Innumerado.- Delito Informático.- Es toda aquella acción típica y antijurídica, que se sirve o utiliza de una computadora para su realización, o bien va dirigida a obtener el acceso no autorizado a registros o programas de un sistema informático, o a producir daño en ésta o de los sistemas que la misma hace operar.

Es decir implica el ataque o intencionalidad de daño a un sistema operativo de la computadora, la intromisión o acceso a bases de datos o archivos que las mismas contengan, o bien la utilización de este aparato tecnológico y de comunicación como medio o instrumento para la realización de delitos.

Art. Innumerado.- Hacking Delictivo.- Se le considera Hacking delictivo a la conducta propia de las personas con un conocimiento amplio en Informática mismas que dedicadas, por afición u otro interés, a violar programas y sistemas de información o informáticos supuestamente impenetrables, por medio de la escritura en un lenguaje ensamblador o en lenguajes a nivel de sistemas, para acceder a información privada. La persona que incurra en este ilícito será reprimida con una pena privativa de la libertad de 3 a 6 años

Art. Innumerado.- Cracking.- Se considera Cracking a las acciones nocivas realizadas por un conocedor de la informática que pueden ir desde simples destrucciones, como el borrado de información, hasta el robo de información sensible que se puede vender. Altera, suprime o daña la información, por cuanto la

intención del agente es obstaculizar, dejar inoperante o menoscabar el funcionamiento de un sistema o dato informático. La persona que incurra en este ilícito será reprimida con una pena privativa de la libertad de 6 a 8 años

Art. Innumerado.- El Hacker o Cracker que incurra en reincidencia en el cometimiento de los delitos tipificados a partir del artículo 229 hasta el 234 del Código Orgánico Integral Penal serán reprimidos con una pena privativa de la libertad de 10 a 15 años.

Disposición Transitoria Vigésima Cuarta.- El Estado creará la agencia de control de delitos informáticos, quien vigilará, investigará y dará seguimiento a los presuntos Hackers, Crackers y sus operaciones atendiendo así el principio universal de modernización de la ley mismo que contempla la utilización de nuevas tecnologías. Su Financiamiento será responsabilidad del Estado a través del Ministerio del Interior.

Objetivo 2

Socializar el proyecto de Ley Reformatoria a la sección tercera referente a delitos contra la seguridad de los activos de los sistemas de información y comunicación del Código Orgánico Integral Penal

Tiempo	Actividad	Objetivo	Técnica	Recurso
1 meses	Presentación	Dar a conocer sobre el beneficio de la Propuesta	Disertación	Recibir a los asistentes y entrega de material
1 meses	Antecedentes y Justificación	Justificar porque es necesario tipificar las figuras del Hacking y el Cracking en COIP	Magistral	Recortes de periódico, internet, medios de comunicación
2 meses	Exposición	Obtener apoyo a la propuesta	Magistral	Exposición del tema, preguntas y respuestas
2 meses	Conclusiones	Satisfacer las inquietudes respecto a la tipificación las figuras del Hacking y el Cracking en COIP	Foro abierto	Aspectos relevantes del tema

Tabla No. 20 Objetivo 2
Fuente: Investigador
Elaborado por: David Poveda

Objetivo 3

Presentar el proyecto de Ley Reformatoria a la sección tercera referente a delitos contra la seguridad de los activos de los sistemas de información y comunicación del Código Orgánico Integral Penal

PROCESO DE APROBACIÓN	
Actividad	**Objetivo**
Iniciativa	Contar con el apoyo del 0.25 % de los ciudadanos inscritos en el padrón electoral nacional para el proyecto de Reforma. Presentar ante quien preside la Asamblea. Remita a los legisladores Remitan a la Comisión Legislativa correspondiente para análisis.
Debates	Que en el primer debate se realicen las observaciones necesarias para la aprobación. Que en el segundo debate aprueben el proyecto.
Veto presidencial	Remitido al Presiente de la Republica, este apruebe el proyecto.
Publicación	Sea promulgada en el Registro Oficial y entre en vigencia para que tenga plena eficacia jurídica.

Tabla No. 21 Objetivo 3
Fuente: Investigador
Elaborado por: David Poveda

Bibliografía

ACURIO DEL PINO SANTIAGO, Delitos Informáticos Generalidades. Publicado en http://www.oas.org/juridico/spanish/cyb_ecu.htm

ACURIO DEL PINO, Santiago; "Delitos Informáticos, Manual de docencia sin lugar ni fecha".

ALTMARK DANIEL. Informática y Derecho "Aportes de doctrina Internacional" Vol. I y II Ed. DEPALMA. Bs. Aires. Argentina. 1988.

ANDRADE SANTANDER, Diana. El Derecho a la Intimidad, Centro Editorial Andino, Quito – Ecuador, 1998.

ASENSIO, Pedro Alberto de Miguel; "Derecho Privado de Internet"; Tercera Edición Actualizada Civitas; Año 2002; Madrid – España.

BECCARIA, C; De Los Delítos Y De Las Penas; Madrid: Edit. Imprenta nacional, 1986.

BERDUGO GOMEZ DE LA TORRE, Ignacio: Honor y libertad de expresión. Tecnos. Madrid, 1.987.

CISNEROS, Germán; "Metodología Jurídica"; Librería Jurídica Cevallos; Primera Edición; Quito-Ecuador; 2003.

Enciclopedia Jurídica Omeba.

CARRASCOSA, Valentín; POZO, María; RODRIGUEZ, E. P., (1999) Tema: "La contratación Informática: El Nuevo Horizonte Contractual"

CLOUGH, J. (2010). PRINCIPLES OF CYBERCRIME. Cambridge, UK: Cambridge University Press.

DAVARA R, Miguel A; (1997) "Manual de Derecho Informático".

GUTIÉRREZ FRANCÉS, Mª Luz. "Fraude informático y estafa", Centro Publicaciones del Ministerio de Justicia, Madrid, 1991.

MARTÍNEZ, J. J. (2009). Computación Forense. Descubriendo los rastros informáticos. Bogotá, Colombia: Alfaomega.

MARTÍNEZ, J. J. (2010). El Peritaje Informático y la Evidencia Digital. Bogotá, Colombia: Universidad de Los Andes.

NIEVES GALARZA, Ricardo E; (2009) "Derecho Informático, Los Documentos Electrónicos".

PÁEZ RIVADENERIA, J. J., & ACURIO DEL PINO, S. (2010). Derecho y

Nuevas Tecnologias. Quito, Ecuador: Corporación de Estudios y Ediciones.
PASCALE, M. (2007). Manual de Peritaje Informático. Montevideo, Uruguay: Fundación de Cultura Universitaria.
PEÑA VALENZUELA, Daniel; "Aspectos Legales de Internet y del Comercio Electrónico"; Ediciones Dupre Ltda.; Año 2001; Colombia.
REYNA ALFARO, Luis Miguel; "El Bien Jurídico en el Delito Informático"; Abogado, Director de la Revista Electrónica de Derecho Penal.
ROMEO CASABONA, Carlos María. "Delitos informáticos de carácter patrimonial", Informática y Derecho Nº 9,10 y 11, UNED, Centro Regional de Extremadura, Mérida, 1996.
SOLANO, Orlando; "Manual de Informática".
ZABALA B, Jorge E; (2005) "Tratado de Derecho Procesal Penal".
ZAMBRANO PASQUEL, Alfonso, Proceso Penal y Garantías Constitucionales, Corporación de Estudios y Publicaciones, Quito, 2005.
ZAVALA BAQUERIZO, Jorge; Tratado de Derecho Procesal Penal, Tomo VII Editorial Edino, Guayaquil, 2004.

Legislación utilizada:

Constitución de la República del Ecuador - 2008
Código Orgánico Integral Penal
Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos
Ley de Propiedad Intelectual
Ley Orgánica de Transparencia y Acceso a la Información Pública.
Ley Especial de Telecomunicaciones
Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional

LINKOGRAFÍA

www.google.com
http://www.delitosinformaticos.com
http://www.informaticaforense.com
http://www.informatica-juridica.com/trabajos/trabajosDelitoInformatico.asp
http://www.Monografias.com /trabajos6/delin/delin.shtml
http://www.inei.gob.pe www.alexa.com

http://www.iuscibernetica.com /Héctor Ramón Peñaranda Quintero Presidente de http://www.cetid.edu.et la Organización Mundial de Derecho e Informática http://www.experticias.com www.elcomerciodigital.com http://www.forensic-es.org www.wikipedia.com www.ic3.gov.com www.abn.info.ve
http://www.globovision.com
http://www.coe.int/t/dghl/standardsetting/tcy/ ETS_185_spanish.PDF
http://www.oas.org/juridico/
http://www.pensamientopenal.com.ar/node/27142
http://www.derechoecuador.com
http://www.esthermorales.CI/show_art,
http://www.derechotecnologico.com/delitos.html
http://www.tribunalmmm.gob.mx/biblioteca/almadelia/indice
http://www.cad.com.mx/que_es_internet.htm
http://www.delitosinformaticos.com/trabajos/criminalista.pdf
http://www.jalisco.gob.mx/organismos/ijcf/orga.html#Capacitación%20y%20Adiestramiento%20Interno
http://criminologia.usal.es/guia/dp3.htm
http://www.delitosinformaticos.com/trabajos/criminalista.pdf
www.abogadosdetalca.cl
http://eva.utpl.edu.ec/oprnutpl/delito%20informatico.php
http://es.wikipedia.org/wiki/Delito_inform%C3%Altico

ANEXOS

Anexo 1

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

CARRERA DE DERECHO

ENTREVISTA DIRIGIDA A FUNCIONARIOS DE LA FISCALIA

Objeto de estudio: Plantear una solución, a fin de reconocer los nuevos tipos delítos informáticos estén tipificados y sancionados por la normativa legal.

Instructivo: Por favor conteste con sinceridad y veracidad. Buscamos su opinión y conocimiento respecto al tema planteado.

Pregunta No1.- ¿Conoce que es un delíto informático?

Pregunta No2.- ¿Conoce los diferentes tipos de delitos informáticos cometidos en el Ecuador?

Pregunta No3.- ¿Conoce los delítos informáticos que están tipificados y sancionados por el COIP?

Pregunta No4.- ¿Considera usted que las autoridades encargadas de la administración de justicia están capacitadas para conocer y resolver plenamente este tipo de delítos?

Pregunta No5.- ¿Considera usted que en la investigación realizada para recabar indicios es la adecuada?

Pregunta No6.- ¿Cree usted que existe una adecuada tipificación de delítos informáticos en el COIP?

Pregunta No7.- ¿Considera usted que estos delítos necesitan una mayor sanción?

Pregunta No8.- ¿Considera necesario tipificar y sancionar nuevos delítos informáticos mediante una reforma al COIP?

Pregunta No 9. ¿Conoce que es un hacker y un cracker?

Pregunta No 10.- ¿Considera necesaria la tipificación de las figuras delictivas de hacker y Cracker en el COIP?

Gracias por su colaboración.

Anexo 2

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

CARRERA DE DERECHO

ENTREVISTA DIRIGIDA A ABOGADOS EN LIBRE EJERCICIO

Objeto de estudio: Plantear una solución, a fin de reconocer los nuevos tipos delítos informáticos estén tipificados y sancionados por la normativa legal.

Instructivo: Por favor conteste con sinceridad y veracidad. Buscamos su opinión y conocimiento respecto al tema planteado.

Pregunta No1.- ¿Conoce que es un delíto informático?

Pregunta No2.- ¿Conoce los diferentes tipos de delitos informáticos cometidos en el Ecuador?

Pregunta No3.- ¿Conoce los delítos informáticos que están tipificados y sancionados por el COIP?

Pregunta No4.- ¿Considera usted que las autoridades encargadas de la administración de justicia están capacitadas para conocer y resolver plenamente este tipo de delítos?

Pregunta No5.- ¿Considera usted que en la investigación realizada para recabar indicios es la adecuada?

Pregunta No6.- ¿Cree usted que existe una adecuada tipificación de delítos informáticos en el COIP?

Pregunta No7.- ¿Considera usted que estos delítos necesitan una mayor sanción?

Pregunta No8.- ¿Considera necesario tipificar y sancionar nuevos delítos informáticos mediante una reforma al COIP?

Pregunta No 9. ¿Conoce que es un hacker y un cracker?

Pregunta No 10.- ¿Considera necesaria la tipificación de las figuras delictivas de hacker y Cracker en el COIP?

Gracias por su colaboración.

Anexo 3

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

CARRERA DE DERECHO

ENTREVISTA DIRIGIDA A AGENTES INVESTIGADORES DE LA POLICÍA JUDICIAL

Objeto de estudio: Plantear una solución, a fin de reconocer los nuevos tipos delítos informáticos estén tipificados y sancionados por la normativa legal.

Instructivo: Por favor conteste con sinceridad y veracidad. Buscamos su opinión y conocimiento respecto al tema planteado.

Pregunta No1.- ¿Conoce que es un delíto informático?

Pregunta No2.- ¿Conoce los diferentes tipos de delitos informáticos cometidos en el Ecuador?

Pregunta No3.- ¿Conoce los delítos informáticos que están tipificados y sancionados por el COIP?

Pregunta No4.- ¿Considera usted que las autoridades encargadas de la administración de justicia están capacitadas para conocer y resolver plenamente este tipo de delítos?

Pregunta No5.- ¿Considera usted que en la investigación realizada para recabar indicios es la adecuada?

Pregunta No6.- ¿Cree usted que existe una adecuada tipificación de delítos informáticos en el COIP?

Pregunta No7.- ¿Considera usted que estos delítos necesitan una mayor sanción?

Pregunta No8.- ¿Considera necesario tipificar y sancionar nuevos delítos informáticos mediante una reforma al COIP?

Pregunta No 9. ¿Conoce que es un hacker y un cracker?

Pregunta No 10.- ¿Considera necesaria la tipificación de las figuras delictivas de hacker y Cracker en el COIP?

Gracias por su colaboración.

GLOSARIO

1. **ACCESO ALEATORIO.-** Operación de almacenamiento y recuperación de la información en la que el sistema accede directamente a la memoria en base a un parámetro preestablecido.
2. **Acceso no autorizado:** Uso ilegitimo de passwords y la entrada de un sistema informático sin la autorización del propietario.
3. **Archivo.-** Datos estructurados que pueden recuperarse fácilmente y usarse en una aplicación determinada. Se utiliza como sinónimo de fichero. El archivo no contiene elementos de la aplicación que lo crea, sólo los datos o información con los que trabaja el usuario.
4. **Base de datos:** (DataBase). Conjunto de datos relacionados que se almacenan de forma que se pueda acceder a ellos de manera sencilla, con la posibilidad de relacionarlos, ordenarlos en base a diferentes criterios, etc. Las bases de datos son uno de los grupos de aplicaciones de productividad personal más extendidos. Entre las más conocidas pueden citarse dBase, Paradox, Access y Aproach, para entornos PC, y Oracle, ADABAS, DB/2, Informix o Ingres, para sistemas medios y grandes
5. **Bomba lógica o cronológica:** Es aquella que exige conocimientos especializados, ya que requiere la programación de la destrucción o modificación de datos. Es importante destacar, que a diferencia de los virus o gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; es por esta razón, que de todos los dispositivos informáticos criminales, la bomba lógica es la que más daño hace dentro del sistema informático.Es difícilsabercuál es el sujeto, por cuanto se puede programar la detonación para que tenga lugar mucho tiempo después de que se haya marchado elcriminal informático.
6. **Clasificación:** Distribución de un conjunto de acuerdo con un principio de jerarquía lógica. Cuando se trata de libros o documentos se llama clasificación bibliográfica o documental. // Técnica que se utiliza para la identificación, agrupación y distribución sistemática de documentos o cosas semejantes, con características comunes o sistema determinado y que pueden ser con posterioridad diferenciadas según su tipología fundamental. Dicho proceso se

aplica de acuerdo a un esquema lógico predeterminado para señalar su ubicación. Tratándose de documentos, permite además, definir los temas contenidos en ellos.

7. **Cracker:** "Cracker" o "rompedor", también denominado Cracking. Para las acciones nocivas existe la más contundente expresión, sus acciones pueden ir desde simples destrucciones, como el borrado de información, hasta el robo de información sensible que se puede vender. Altera, suprime o daña la información, por cuanto la intención del agente es obstaculizar, dejar inoperante o menoscabar el funcionamiento de un sistema o dato informático.
8. **Comercio Electrónico:** Gracias al avance de las actividades telemáticas (TICs), se beneficia entre otras actividades el comercio pues es muy fácil comprar y vender bienes, brindar servicios desde un escritorio en la oficina o desde el hogar, actividad que se encuentra regulada en nuestro país por le "E Commerce" (Comercio Electrónico).
9. **COMPUTADORA:** Ordenador. En Hispanoamérica se utiliza la palabra computadora, derivada del inglés computer, para designar a los ordenadores.
10. **Cookie:** Cuando se visita una página Web, es posible recibir una Cookie. Este es el nombre que se da a un pequeño archivo de texto, que queda almacenado en el disco duro del ordenador. Este archivo sirve para identificar al usuario cuando se conecta de nuevo a dicha página Web.
11. **Delítos Informáticos** Son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático.
12. **Derecho Informático:** Ya no se dedica al estudio del uso de los aparatos informáticos como ayuda al derecho sino que constituye el conjunto de normas, procesos, relaciones jurídicas que surgen como consecuencia de la aplicación y desarrollo de la informática. Es decir que la informática en general, desde este punto de vista es el objeto regulado por el derecho. Ejm. Ley de Firmas Electrónicas.
13. **Destrucción de datos:** Los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.
14. **Documento electrónico:** Es la representación en forma electrónica de hechos jurídicamente relevantes susceptibles de ser presentados en una forma

humanamente comprensible

15. **Estafas electrónicas:** A través de compras realizadas haciendo uso de la red.
16. **Espionaje:** Acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.
17. **Gurus:** Son los maestros y enseñan a los futuros Hackers. Normalmente se trata se personas adultas, me refiero a adultas, porque la mayoría de Hackers son personas jóvenes, que tienen amplia experiencia sobre los sistemas informáticos o electrónicos y están de alguna forma hay, para enseñar a o sacar de cualquier duda al joven iniciativo al tema. Es como una especie de profesor que tiene a sus espaldas unas cuantas medallitas que lo identifican como el mejor de su serie. El guru no esta activo, pero absorbe conocimientos ya que sigue practicando, pero para conocimientos propios y solo enseña las técnicas más básicas.
18. **Gusanos:** Son aquellos que se fabrican de forma lógica al virus y su intención es infiltrarse en programa de procesamientos de datos o para modificar o destruir los datos,pero es diferente del virus porque no puede regenerarse, por lo tantono es tan grave como el virus.
19. **Hacker:** El término de hacker en castellano significa "cortador". Los "Hackers", son fanáticos de la informática que tan sólo con un computador personal un módem, gran paciencia e imaginación son capaces de acceder, a través de una red pública de transmisión de datos al sistema informatizado de una empresa o entidad pública saltándose todas las medidas deseguridad y leer información, copiarla, modificarla, preparando las condiciones idóneas para llamar la atención sobre la vulnerabilidad de los sistemas informáticos o satisfacer su propia vanidad.
20. **HARDWARE.-** Conjunto de los componentes que integran la parte material de una computadora.
21. **Informática Forense:** es la rama de la informática que se encarga de la recuperación preservación y análisis de evidencias electrónicas tales como: fotografías digitales e-mail, SMS, transacciones bancarias o rastros de cualquier tipo de actividades a través de Internet y que se ejecutan mediante aparatos electrónicos. Estamos hablando de la utilización de la informática forense con una finalidad preventiva, en primer término y cuando la seguridad

ya ha sido vulnerada, recoger los rastros probatorios.

22. **Informática Jurídica:** Es una ciencia que estudia el empleo de aparatos electrónicos como la computadora en el derecho; es decir, la ayuda que el uso de los artefactos informáticos brindan al desarrollo y aplicación del derecho. Ejm. Oficina de Sorteos de la Corte Provincial.
23. **Infracción al copyright de bases de datos:** Uso no autorizado de información almacenada en una base de datos.
24. **Interceptación de e-mail:** : Lectura de un mensaje electrónico ajeno.
25. **Internet:** Red informática mundial, descentralizada, formada por la conexión directa entre computadoras u ordenadores mediante un protocolo especial de comunicación.
26. **INTERNET ADDRESS.-** (Dirección internet) Dirección IP que identifica de forma inequívoca un nodo en una red internet. Una dirección Internet (con "I" mayúscula) identifica de forma inequívoca un nodo en Internet. Ver también: "internet", "Internet", "IP address".
27. **Lammers:** Aquellos que aprovechan el conocimiento adquirido y publicado por los expertos. Si el sitio web que intentan vulnerar los detiene, su capacidad no les permite continuar más allá. Generalmente, son despreciados por los verdaderos hackers que los miran en menos por su falta de conocimientos y herramientas propias. Muchos de los jóvenes que hoy en día se entretienen en este asunto forman parte de esta categoría.
28. **Mensaje de datos:** Es toda aquella información visualizada, generada enviada, recibida, almacenada o comunicada por medios informáticos, electrónicos, ópticos, digitales o similares.
29. **Modem**: Un aparato que cambia datos del computador a formatos que se puedan transmitir mas fácilmente por línea telefónica o por otro tipo de medio.
30. **Narcotráfico:** Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.
31. **Newbie:** Traducción literal de novato. Es alguien que empieza a partir de una WEB basada en Hacking. Inicial-mente es un novato, no hace nada y aprende lentamente. A veces se introduce en un sistema fácil y a veces fracasa en el intento, porque ya no se acuerda de ciertos parámetros y entonces tiene que volver a visitar la pagina WEB para seguir las instrucciones de nuevo.Es el

típico tipo, simple y nada peligroso. Está apartado en un rincón y no es considerado .

32. **Phreoker:** Son tipos con unos conocimientos de telefonía insuperables. Persona que ingresa al sistema telefónico, teniendo o no equipo de computación, con el propósito de apoderarse, interferir, dañar, destruir, conocer, difundir, hacer actos de sabotaje, o hacer uso de la información accediendo al sistema telefónico, busca sabotear, pinchar, pueden clonar líneas de celular captando información del aire.
33. **Pirata Informático:** Es aquella persona que copia, reproduce, vende, entrega un programa de software que no le pertenece o que no tiene licencia de uso, a pesar de que el programa está correctamente registrado como propiedad intelectual en su país de origen o en otro. Esta persona adultera suestructura, su procedimiento de instalación, copiándolo directamente y reproduciendo por cualquier medio la documentación que acompaña al mismo programa. Reproduce; copia algo de lo que no posee derechos de autor.
34. **Sabotaje informático:** Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.
35. **Sistema De Información:** Se entenderá como sistema de información, a todo sistema utilizado para generar, enviar, recibir, procesar o archivar de cualquier forma de mensajes de datos.
36. **Sistema Informático:** Conjunto organizado de programas y bases de datos que se utilizan para, generar, almacenar, tratar de forma automatizada datos o información cualquiera que esta sea.
37. **Sociedad De La Información:** La revolución digital en las tecnologías de la información y las comunicaciones (TIC) ha creado una plataforma para el libre flujo de información, ideas y conocimientos en todo el planeta. Ha causado una impresión profunda en la forma en que funciona el mundo. La Internet se ha convertido en un recurso mundial importante, que resulta vital tanto para el mundo desarrollado por su función de herramienta social y comercial, como para el mundo en desarrollo por su función de pasaporte para la participación equitativa y para el desarrollo económico, social y educativo.
38. **Software:** Conjunto de programas, instrucciones y reglas informáticas para

ejecutar ciertas tareas en una computadora.

39. **Telemática:** neologismo que hace referencia a la comunicación informática, es decir la transmisión por medio de las redes de telecomunicaciones de información utomatizada.
40. **Terrorismo:** Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.
41. **Transferencias de fondos:** Engaños en la realización de este tipo de transacciones. Por otro lado, la red Internet permite dar soporte para la comisión de otro tipo de delitos:
42. **Trashing:** Esta conducta tiene la particularidad de haber sido considerada recientemente en relación con los delitos informáticos. Apunta a la obtención de información secreta o privada que se logra por la revisión no autorizada de la basura (material o inmaterial) descartada por una persona, una empresa u otra entidad, con el fin de utilizarla por medios informáticos en actividades delictivas. Estas acciones corresponden a una desviación del procedimientoconocido como reingeniería social.
43. **Virucker:** Esta palabra proviene de la unión de los términos Virus y Hacker, y se refiere al creador de un programa el cual insertado en forma dolosa en un sistema de cómputo destruya, altere, dañe o inutilice a un sistema de información perteneciente a organizaciones con o sin fines de lucro y de diversa índole.
44. **Virus:** Es una serie de instrucciones de programación que pueden adherirsea los programas legítimos y propagarse aotros programas informáticos.Un virus puede ingresar al sistema por conducto de un soporte lógico (fllopy, CDROM,etc) que ha quedado infectada, así como utilizando el método del Caballo de Troya.
45. **WEB.-** Por éste término se suele conocer a WWW (World Wide Web), creado por el Centro Europeo de Investigación Nuclear como un sistema de intercambio de información y que Internet ha estandarizado. Supone un medio cómodo y elegante, basado en multimedia e hipertexto, para publicar información en la red. Inicial y básicamente se compone del protocolo http y del lenguaje html. Un ejemplo de páginas de éste tipo, es la que tienes delante en estos momentos.

Cronograma de Actividades

Cronograma

ACTIVIDADES	JUNIO				JULIO				AGOSTO				SEPTIEMBRE		
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3
Elaboración del perfil	**X**														
Aprobación del Perfil							**X**								
Ejecución de la Tesis								**X**							
Aplicación de Instrumento									**X**						
Realizar los Objetivos, análisis										**X**					
Análisis de datos											**X**				
Elaboración de la propuesta												**X**			
Aprobación y defensa													**X**		

Tabla No. 22 Cronograma.
Fuente: Investigador
Elaborado por: David Poveda