UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

CARRERA DE DERECHO

TEMA:

LOS DELITOS INFORMÁTICOS Y EL DERECHO CONSTITUCIONAL A LA SEGURIDAD PÚBLICA

Trabajo de Graduación previa a la obtención del Título de Abogada de los Juzgados y Tribunales de la República del Ecuador

AUTORA:

Grace Alexandra Echeverría Mera

TUTOR:

Dr.: Juan Carlos Harb

Ambato – Ecuador

2015

TEMA:

LOS DELITOS INFORMÁTICOSY EL DERECHO CONSTITUCIONAL A LA SEGURIDAD PÚBLICA

APROBACIÓN DEL TUTOR

En calidad de Tutor del trabajo de Investigación sobre el tema: **"LOS DELITOS INFORMÁTICOS Y EL DERECHO CONSTITUCIONAL A LA SEGURIDAD PÚBLICA"** de la Srta. Grace Alexandra Echeverría Mera, Egresada 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 la Evaluación del Tribunal de Grado, que el H. Consejo Directivo de la Facultad designe para su correspondiente estudio y calificación.

Ambato, 16 de Diciembre del 2014.

EL TUTOR

.....

Dr. Juan Carlos Harb

APROBACIÓN DEL TRIBUNAL DE GRADO

Los Miembros del Tribunal de Grado, APRUEBAN el Trabajo de Investigación sobre el tema: **"LOS DELITOS INFORMÁTICOS Y EL DERECHO CONSTITUCIONAL A LA SEGURIDAD PÚBLICA",** presentado por la Señorita Grace Alexandra Echeverría Mera, de conformidad con el Reglamento de Graduación para obtener el Título Terminal de Tercer Nivel de la UTA.

Ambato,……..

Para constancia firman:

……

Presidente

…….…… ……..……..……..

Miembro Miembro

AUTORÍA

Los criterios emitidos en el trabajo de investigación **"LOS DELITOS INFORMÁTICOSY EL DERECHO CONSTITUCIONAL A LA SEGURIDAD PÚBLICA"**, como también los contenidos, ideas, análisis, conclusiones, y propuestas son de responsabilidad de la autora.

Ambato, 13 de Marzo del 2015

LA AUTORA

…….

Grace Alexandra Echeverría Mera

C.C.1804945994

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, 13 de Marzo del 2015

LA AUTORA

……..…….

Grace Alexandra Echeverría Mera

C.C.1804945994

DEDICATORIA

Cuando estuve a punto de rendirme me dieron fuerzas y sin importar nada me apoyaron siempre me enseñaron a levantarme y luchar ya que todo en la vida se consigue con esfuerzo mis padres han sido mi modelo a seguir Mamita Berthita y Papito Luchito para ustedes padres amados.

A mi hijito Mathias que con su sonrisa me ha dado impulsos para alcanzar mis metas.

A mis hermanas, hermanos por sus consejos como unos verdaderos amigos siempre los llevo en mi corazón.

AGRADECIMIENTO

Quiero en primer lugar agradecer a Diosito por su protección, por darme la salud, la vida para realizar este trabajo de investigación

Un arduo agradecimiento a la Universidad Técnica de Ambato especialmente a mi Facultad de Jurisprudencia y Ciencias Sociales

Quiero agradecer a todos mis maestros por los conocimientos que me han proporcionado

También quiero agradecer a mi tutor del proyecto al Dr. Carlos Mayorga por el incentivo y la ayuda otorgada

Agradecerle infinitamente a mi tutor del trabajo de investigación al Dr. Juan Carlos Harb quien ha sabido guiarme correctamente y ayudarme en todo lo necesario para solventar la investigación.

ÍNDICE GENERAL

PÁGINAS PRELIMINARES **Pág.**

Portada..... i
Tema:..... ii
Aprobación del Tutor..... iii
Aprobación del Tribunal de Grado..... iv
Autoría..... v
Derechos de Autor..... vi
Dedicatoria..... vii
Agradecimiento..... viii
Índice General..... ix
Índice de Cuadros..... xiv
Índice de Gráficos..... xvi
Resumen Ejecutivo..... xviii

Introducción..... 1

CAPITULO I

EL PROBLEMA

Tema:..... 3
Planteamiento del Problema..... 3
Contextualización..... 3
Macro..... 3
Meso..... 3
Micro..... 1
Árbol del Problema..... 5
Análisis Crítico..... 6
Prognosis..... 7
Formulación del Problema..... 7
Interrogantes de la Investigación..... 7
Delimitación del Objeto de la Investigación..... 7
Delimitación de Contenido:..... 8

Unidades de Observación 8
Justificación del Problema 8
Objetivos 9
Objetivo General 9
Objetivos Específicos 9

CAPÍTULO II
MARCO TEÓRICO

Antecedentes Investigativos 10
Fundamentación 12
Filosófica 12
Legal 13
Constitución de la República del Ecuador 2008 13
Doctrinaria 14
Categorías Fundamentales 16
Atributos de la Variable Independiente 17
Atributos de la Variable Dependiente 18
Delitos Informáticos 19
Derecho Penal 19
Delitos de Acción Pública 19
Definición de Varios Autores 20
Orígenes 21
Clasificación 23
Los datos Falsos o Engañosos (Data Diddling) 23
Pishing 23
Skimming 24
Bombas Lógicas (Logic Bombs). 24
Manipulación de los Datos de Salida 24
Falsificaciones Informáticas 25
Manipulación de Programas o los “Caballos de Troya 25
Sabotaje Informático 26
Fuga de Datos 26
Apropiación de Informaciones Residuales 26

Suplantación de Personalidad 26
La Técnica del Salami 27
Ciberterrorismo. 27
Pornografía Infantil por Internet. 27
Acceso no Autorizado a Servicios Informáticos 28
La Llave Maestra 28
El Espionaje Informático 29
Características de los Delitos Informáticos 29
Sujetos del Delito Informático 30
Sujeto Activo 30
Sujeto Pasivo 32
Maneras de Protección de Información 32
Otras Medidas que se deben Tomar en Cuenta son: 34
Pasos para Detectarlos e Investigarlos 35
Identificación de Incidentes 36
Recopilación de Evidencias Digitales 36
Preservación de la Evidencia Digital 37
Análisis de la Evidencia 37
Documentación y Presentación de Resultados 37
Derecho Constitucional a la Seguridad Pública 38
Derechos Humanos 38
Constitución de la República del Ecuador. 38
Orígenes 38
Definición 40
Principios de la Seguridad Pública y del Estado 41
El Sistema 42
Tratados Internacionales 42
Declaración de los Derechos Humanos 45
La Policía y el orden Público dentro de los Elementos de Seguridad 46
Concepto de Policía 47
Factores que Inciden en la Alteración de la Seguridad Pública 48
Niveles de Inseguridad 49
Individual 50

Comunitaria 50
Nacional 51
Hipótesis 51
Señalamiento de Variables 51

CAPÍTULO III

METODOLOGÍA

Enfoque de la Investigación 52
Modalidad Básica de la Investigación 52
Bibliográfica Documental 52
De Campo 53
Nivel o Tipo de la Investigación 53
Exploratorio 53
Descriptiva 53
Asociación de Variables 54
Población y Muestra 54
Fórmula Aplicada para la Muestra 54
Operacionalizacion de Variables 56
Variable Independiente: Delitos Informáticos 56
Variable Dependiente: Derecho Constitucional a la Seguridad Pública 57
Recolección de Informaciòn 58
Plan de Recolección de Información 58
Procesamiento y Análisis 59
Plan de Procesamiento de la Información 59
Análisis e Interpretación de Resultados 59

CAPÍTULO IV

ANÁLISIS DE RESULTADOS

Análisis e Interpretación de Datos 60
Verificación de la Hipótesis 91
Combinación de Frecuencias 91
Planteamiento de la Hipótesis 91
Selección del Nivel de Significación 91

Especificaciones del Estadístico 91
Especializaciones de la Región de Aceptación y Rechazo 92
Recolección de datos de los Cálculos de las Estadísticas 93
Cálculo de Ji }= Cuadrado 95

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

Conclusiones 97
Recomendaciones..... 98

CAPÍTULO VI

PROPUESTA

Tema:..... 100
Datos Informativos..... 100
Antecedentes de la Propuesta..... 101
Justificación..... 102
Objetivos 103
Objetivo General 103
Objetivos Específicos..... 103
Análisis de Factibilidad..... 103
Político 103
Social..... 104
Género 104
Fundamentación Científica-Técnica 104
Metodología 105
Metodología. Modelo Operativo de la Propuesta 109
Administración..... 110
Previsión de la Evaluación..... 110

Bibliografía 112
Linkografía..... 113
Anexos..... 114
Glosario 124

ÍNDICE DE CUADROS

Pág.

Cuadro No. 1 Población y muestra 54
Cuadro No. 2 V. I: Delitos Informáticos 56
Cuadro No. 3 V. D: Derecho Constitucional a la Seguridad Pública 57
Cuadro No. 4 Plan de Recolección de Información 58
Cuadro No. 5 Pregunta No. 1 61
Cuadro No. 6 Pregunta No. 2 62
Cuadro No. 7 Pregunta No. 3 63
Cuadro No. 8 Pregunta No. 4 64
Cuadro No. 9 Pregunta No. 65
Cuadro No. 10 Pregunta No. 6 66
Cuadro No. 11 Pregunta No. 7 67
Cuadro No. 12 Pregunta No. 8 68
Cuadro No. 13 Pregunta No. 9 69
Cuadro No. 14 Pregunta No. 10 70
Cuadro No. 15 Pregunta No. 1 71
Cuadro No. 16 Pregunta No. 2 72
Cuadro No. 17 Pregunta No. 3 73
Cuadro No. 18 Pregunta No. 4 74
Cuadro No. 19 Pregunta No. 5 75
Cuadro No. 20 Pregunta No. 6 76
Cuadro No. 21 Pregunta No. 7 77
Cuadro No. 22 Pregunta No. 8 78
Cuadro No. 23 Pregunta No. 9 79
Cuadro No. 24 Pregunta No. 10 80
Cuadro No. 25 Pregunta No. 1 81
Cuadro No. 26 Pregunta No. 2 82
Cuadro No. 27 Pregunta No. 3 83
Cuadro No. 28 Pregunta No. 4 84
Cuadro No. 29 Pregunta No. 5 85
Cuadro No. 30 Pregunta No. 6 86
Cuadro No. 31 Pregunta No. 7 87

Cuadro No. 32 Pregunta No. 8 88
Cuadro No. 33 Pregunta No. 9 89
Cuadro No. 34 Pregunta No. 10 90
Cuadro No. 35 Recolección de datos de los cálculos de las estadísticas 93
Cuadro No. 36 Frecuencias Observadas 94
Cuadro No. 37 Cálculo de Ji }= Cuadrado 95
Cuadro No. 38 Modelo Operativo de la Propuesta 109
Cuadro No. 39 Previsión de la Evaluación 110

ÍNDICE DE GRÁFICOS

Pág.

Gráfico No. 1 Árbol de Problemas..... 5
Gráfico No. 2 Categorías Fundamentales 16
Gráfico No. 3 Atributos de la variable independiente..... 17
Gráfico No. 4 Atributos de la variable dependiente..... 18
Gráfico No. 5 Pregunta No. 1..... 61
Gráfico No. 6 Pregunta No. 2..... 62
Gráfico No. 7 Pregunta No.3..... 63
Gráfico No. 8 Pregunta No. 4..... 64
Gráfico No. 9 Pregunta No. 5..... 65
Gráfico No. 10 Pregunta No. 6..... 66
Gráfico No. 11 Pregunta No. 7..... 67
Gráfico No. 12 Pregunta No. 8..... 68
Gráfico No. 13 Pregunta No. 9..... 69
Gráfico No. 14 Pregunta No. 10..... 70
Gráfico No. 15 Pregunta No. 1..... 71
Gráfico No. 16 Pregunta No. 2..... 72
Gráfico No. 17 Pregunta No. 3..... 73
Gráfico No. 18 Pregunta No. 4..... 74
Gráfico No. 19 Pregunta No. 5..... 75
Gráfico No. 20 Pregunta No. 6..... 76
Gráfico No. 21 Pregunta No. 7..... 77
Gráfico No. 22 Pregunta No. 8..... 78
Gráfico No. 23 Pregunta No. 8..... 79
Gráfico No. 24 Pregunta No. 10..... 80
Gráfico No. 25 Pregunta No. 1..... 81
Gráfico No. 26 Pregunta No. 2..... 82
Gráfico No. 27 Pregunta No. 3..... 83
Gráfico No. 28 Pregunta No. 4..... 84
Gráfico No. 29 Pregunta No. 5..... 85
Gráfico No. 30 Pregunta No. 6..... 86
Gráfico No. 31 Pregunta No. 7..... 87

Gráfico No. 32 Pregunta No. 8..... 88
Gráfico No. 33 Pregunta No. 9..... 89
Gráfico No. 34 Pregunta No. 10..... 90
Gráfico No. 35 Cálculo de Ji }= Cuadrado..... 96

RESUMEN EJECUTIVO

AUTORA: Grace Alexandra Echeverría Mera
TUTOR: Dr. Juan Carlos Harb.

A través del tiempo la sociedad en todo el mundo ha ido cambiando, pero este cambio no solo ha sido para bien sino que en un gran índice para el camino equivocado esto se ve reflejado en varios acontecimientos de delitos suscitados que provocan un gran temor en las personas, como en los reportajes que mencionan que las calles no son seguras, hoy en día hay que salir y mirar para todas partes pues no se sabe si se podría ser la próxima víctima de un delito.

Las leyes tratan de conseguir seguridad pero las mismas deben evolucionar ya que las mentes de los infractores siempre buscan una entrada para cometer un daño a los demás, este es el caso de los delitos realizadas a través de los sistemas informáticos.

Es de conocimiento en todo el mundo que el internet es la herramienta que ayuda a que las cosas se den con mayor rapidez como una transacción financiera o conversar con alguien en otro País, en fin una gran gama de actividades, pero que pasa si no se mantiene la seguridad necesaria, esto es lo más preocupante, los delitos informáticos desconciertan a los legisladores y a la sociedad.

Las personas que cometen un delito informático la mayor parte son especialistas que no dejan huellas en el acto por ende es realmente fundamental la preparación y una profunda investigación para detenerlos y encontrar las evidencias.

Si existe una debilidad en las personas es la confianza, por consiguiente deben tener todo en constante protección, los ciberinfractores aprovechan el mínimo descuido para conseguir información y apropiarse de lo que no es suyo, el nuevo Código Integral Penal sanciona este tipo de delitos, pero sigue una pregunta en cuestión que tan fuerte debe ser la justicia para que al fin se consiga el respeto y la armonía en la sociedad.

INTRODUCCIÓN

La presente investigación tiene como tema **"LOS DELITOS INFORMÁTICOS Y EL DERECHO CONSTITUCIONAL A LA SEGURIDAD PÚBLICA"** el mismo que fue escogido por parte de la investigadora**,** luego de identificar las diversas controversias que genera esta problemática en el medio principalmente por el gran temor infundido en la sociedad. Si bien se da cumplimiento a lo que tipifica el Código Orgánico Integral Penal respecto del tema, es necesario contar con articulados que posibiliten al juzgador ejercer su actividad judicial de mejor manera, ya que de ellos depende que los postulados constitucionales sean cumplidos a cabalidad.

La importancia está vinculada con varios factores como son el impacto que causa este tipo de delito en contra del afectado, puesto al atentar contra su seguridad, es indiscutible tratar parámetros que ayuden a la regulación de las normas sancionadoras establecidas.

Es de gran interés recalcar que la Constitución de la República del Ecuador se halla encaminada al buen vivir y por consiguiente a que todos se mantengan en armonía y para ello la seguridad pública es primordial para la protección de toda la ciudadanía.

La presente investigación se halla conformada por VI capítulos los mismos que se encuentran estructurados y elaborados de la siguiente forma:

EL CAPÍTULO I, se inicia con el planteamiento del problema, la contextualización basada en macro, meso, y micro; de una forma global, en macro a nivel nacional en meso, y local en micro, permitiendo dar de una forma visual algunos datos de la presente investigación, luego de esto las interrogantes, que nos ayuda a interpretar por qué y para qué desarrollamos la investigación y el tipo de beneficios que se obtendrá con esta tesis, y para finalizar se determinan los objetivos generales y específicos los cuales reflejan lo que se desea alcanzar con la profunda investigación.

EL CAPÍTULO II, se enfoca en el Marco Teórico el cual es complejo, comenzando con los antecedentes investigativos, es decir, los inicios en donde se basa el problema, seguido se toma en cuenta la fundamentación filosófica, legal y doctrinaria ya que sin esto el problema no tendría ningún sentido continuarlo investigando, además cabe mencionar que el marco teórico necesita de una constelación de ideas para saber todo lo que se pretende investigar. Se termina el capítulo con el planteamiento de la hipótesis y señalamiento de variables.

EL CAPÍTULO III, explica claramente el modelo y el proceso metodológico a base del enfoque de la investigación necesitando saber el modelo de metodología adaptada, la obtención de la muestra, la aplicación de la fórmula adecuada y los pasos que se utilizan en la recolección de información, es decir, encuestas y entrevistas.

EL CAPÍTULO IV, muestra el contenido sobre el análisis, interpretación de resultados y verificación de la hipótesis, contiene gráficos, análisis e interpretación de resultados previos a tabulaciones realizadas y los datos obtenidos durante la realización de la investigación.

EL CAPÍTULOV, se plantean las conclusiones y recomendaciones a las que se ha llegado el tema de investigación, anhelando que los delitos informáticos sean analizados de una forma consiente ya que afectan a la ciudadanía y que las personas protejan su información para que terceras personas no hagan uso malicioso de la misma.

EL CAPÍTULOVI, finalmente es la culminación del trabajo de investigación en donde se consta la propuesta es decir una posible solución al problema de investigación, mencionando los antecedentes de la propuesta, la justificación, objetivos, análisis de factibilidad para determinar si es conveniente realizar la investigación, fundamentación, metodología, y previsión de la evaluación.

Se concluye la investigación con la Bibliografía, cuerpos legales, Linkografía, Anexos y Glosario, utilizada y aplicada en la problemática.

CAPITULO I

EL PROBLEMA

Tema:

"LOS DELITOS INFORMÁTICOS Y EL DERECHO CONSTITUCIONAL A LA SEGURIDAD PÚBLICA"

Planteamiento del problema

Contextualización

Macro

El delito sigue a la sociedad como su misma sombra, así lo afirma (Enrico Ferri, Criminalista: Italiano 1986). En el mundo los delitos informáticos han ocasionado un sin número de consecuencias encontrándose personas sin ningún tipo de temor que utilizan los sistemas informáticos para delinquir afectando a la sociedad en general. En otros países se tiende a resumir como un fraude informático del cual el criminal obtendrá un beneficio por obtener el ingreso de datos de manera ilegal. Esto requiere que el criminal posea un alto nivel de técnica y por lo mismo es común que sea una persona especialista en manejo de las redes de información y pueda ingresar a ella para alterar, datos como generar información falsa que lo beneficie, dañando los sistemas informáticos protegidos y protagonizando un alcance extremadamente peligroso de un 78% de casos a nivel global según datos obtenidos por la INTERPOL.

Meso

En nuestro país encontramos que el ordenamiento jurídico ha intentado avanzar

en materia penal, sin embargo en la Constitución del 2008 protege a la seguridad pública ya que han existido numerosos casos en el Ecuador, ocasionando una gran inseguridad en la base de datos de las personas, lo cual simplemente conlleva a que exista mayor delincuencia en la sociedad.

El Dr. Lara Jorge en su obra titulada El derecho al Internet, (2001) menciona "es necesario para enfrentar a la llamada criminalidad informática que los tipos penales tradicionales sean remozados, es decir actualizados para así consolidar la seguridad jurídica por eso es necesario que el Ministerio Público en cumplimiento de su deber constitucional y legal instruya y facilite las herramientas necesarias a los, Agentes Fiscales y personal de apoyo a fin de combatir esta clase de comportamientos ilegales que afectan directamente a la sociedad ecuatoriana en su conjunto".pag.19.

Lo cual conlleva alrededor de 7486 denuncias ingresadas de presuntos delitos informáticos que se han cometido es decir el 40% de casos indagados en el país.Cabe mencionar que estos estudios los realizaron GMA Y Kaspersky, estas estadísticas guardan relación con los reportes de la Fiscalía General del Estado

Micro

Hoy en día muchos usuarios no confían en la seguridad de los sistemas informáticos, pues temen que alguien pueda conseguir el número de su tarjeta de crédito mediante el uso de la red, en la ciudad de Ambato se toma en cuenta este aspecto por lo que la fiscalía tiende a través de sus agentes investigadores y varios peritos a indagar sobre estos casos.

Así también exige que la ley debe garantizar la protección por ende es necesario que se mantenga en un profundo énfasis en los delitos informativos para evitar que se ocasionen grandes dificultades de la armonía social. En Ambato se ha receptado la cantidad de 100 denuncias ingresadas de delitos informáticos es decir el 10% de casos investigados en la Fiscalía Provincial de Tungurahua de acuerdo a los informes de las denuncias ingresadas en la SAI en el año 2013.

ÁRBOL DEL PROBLEMA

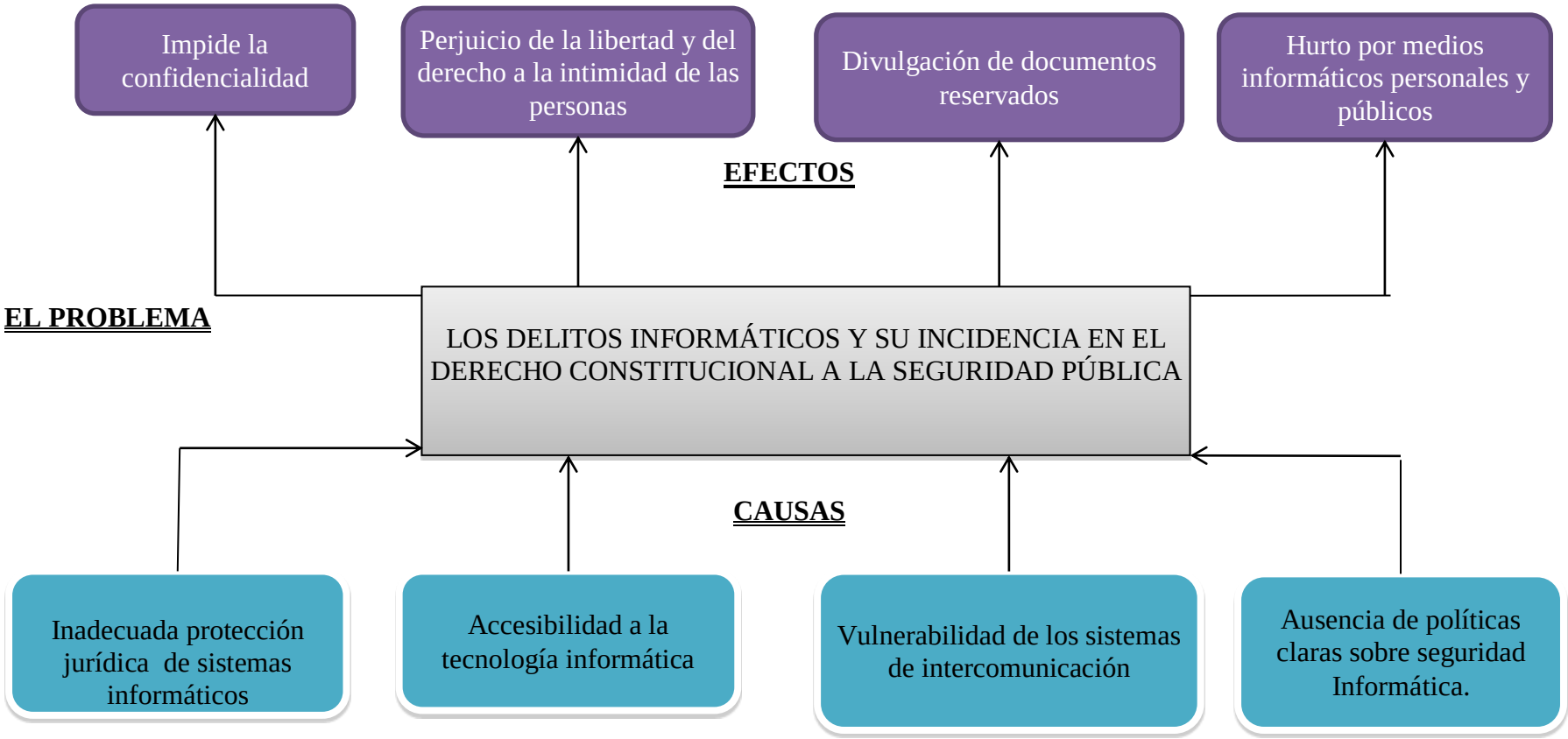

Gráfico No. 1 Árbol de Problemas

Análisis Crítico

El bienestar personal, psicológico, social, laboral, político y económico de los ecuatorianos, se ve reflejado en la seguridad de cada uno de los ciudadanos, es decir un Estado en el cual se pueda ingresar a una red informática de manera tranquila y realizar sus actividades diarias.

La inadecuada protección en los sistemas informáticos involucra grandes perjuicios para las personas, es decir que hoy en día si se ingresa algún tipo de información a los sistemas informáticos puede ocasionar que la persona resulte afectada al darse cuenta que un tercero ingresó a su información y va a hacer uso de la misma.

La accesibilidad tecnológica ha ido avanzando mientras siguen pasando los años pero la curiosidad de la gente se ha sumado a esta situación, por lo que si no ha protegido las redes informáticas va a ser sumamente fácil ingresar y de tal modo incrementar los riesgos de datos no seguros con lo cual se daría énfasis a perjudicados. La vulnerabilidad de los sistemas de intercomunicación a través de la obtención de los chats, líneas telefónicas, redes sociales sin autorización, propicia que la gente no tenga un nivel alto de confidencialidad y se revelen datos reservados interrumpiendo su derecho a la intimidad.

A través del tiempo no se han mencionado normas claras que tipifiquen la conducta de las personas que cometen delitos informáticos esto está siendo erradicado en la actualidad en materia penal.

Es importante también mencionar el tema de contar con un respaldo y protección del sistema informático adecuado y preparado para que las personas ingresen sin que corran algún riesgo, es que no se puede saber que pasará mañana si su cuenta ha sido hackeada y está expuesta a convertirse en una persona víctima de los responsables de estos delitos que lo único que hacen es perjudicar a personas para obtener ingresos o apoderarse de cuentas vulnerando al propietario y asumiendo dinero que no es suyo tal como sucede con las cuentas bancarias.

Prognosis

De no erradicarse los delitos informáticos en la sociedad producirían una crisis económica, social, personal, psicológica ya que las técnicas delictivas utilizadas por los infractores, son cada día más sofisticadas y tienden a prepararse para hackear cuentas no solo de redes sociales sino además de cuentas financieras, esto es un punto demasiado complejo que afectaría a toda la población generando mayor pobreza y poca confidencialidad en el manejo de documentos reservados, esto dificultaría que las relaciones económicas se produzcan de manera rápida y de manera específica a la seguridad pública en el país.

Formulación del problema

¿Cómo los delitos informáticos inciden en el Derecho Constitucional a la Seguridad Pública según los casos presentados en la Fiscalía General del Estado en el periodo 2014?

Interrogantes de la investigación

1. ¿Cuáles son normas sancionadoras aplicadas en los cuerpos legales para los delitos informáticos?

2. ¿Cómo afecta los delitos informáticos a la seguridad pública en el cantón Ambato provincia de Tungurahua?

3. ¿Qué propuesta puede resolver el problema?

Delimitación del objeto de la investigación

Delimitación Espacial: La investigación se realizará en la Fiscalía General del Estado ubicada en la Av. Cevallos y Lalama de esta ciudad de Ambato

Delimitación Temporal: La presente investigación se realizará en el periodo Julio-Octubre 2014.

Delimitación de Contenido:

Campo: Jurídico

Área: Social- Penal

Aspecto: Delitos Informáticos

Unidades de Observación

Fiscal Provincial de Tungurahua

Fiscales de la ciudad de Ambato

Agentes Investigadores

Abogados en libre ejercicio

Personas afectadas

Justificación del problema

El interés de la presente investigación está encaminado a resolver la problemática de los delitos informáticos y el derecho constitucional a la seguridad pública.

La importancia de realizar ésta investigación, radica principalmente en conocer lo que son los delitos informáticos, las sanciones que existen para los responsables que los realicen, y la eficacia para evitar que queden sin su debida pena o sanción. De igual manera con este trabajo investigativo se pretende proponer alternativas para lograr poner un alto sistema informático que proteja a la sociedad para que personas llamadas hackers no puedan acceder a la información.

La factibilidad de realizar la investigación enunciada se respalda porque se propone un estudio amplio tanto doctrinario como legal; así como también se cuenta con todos los medios como son suficiente bibliografía, facilidad de acceso a la información, y con los recursos económicos necesarios para desarrollar la investigación.

La utilidad de la investigación es de gran relevancia puesto que la tranquilidad de la sociedad está en riesgo, al encontrar posibles soluciones de alguna manera

protege a las personas con el fin de que cuiden sus datos informáticos.

El impacto que han tenido los delitos informáticos en la sociedad ha sido radical puesto que el crecimiento y auge que presenta el Internet en los últimos años ha sido insuperable, por ende es necesario conocer de qué se trata para estar alerta en caso de ser víctimas de los mismos.

Los beneficiarios de la investigación será concretamente toda la sociedad con el único fin de que se mantenga su información de una forma segura, sin miedo alguno de que estafadores, denominados hackers, ingresen fácilmente a sus cuentas, contribuirá al conocimiento de la investigadora para fortalecer el estudio en este campo, servirá además a los alumnos que cursen estudios en la Facultad de Jurisprudencia y Ciencias Sociales de la Universidad Técnica de Ambato ya que esta investigación reposará en los archivos de esta institución educativa.

Objetivos

Objetivo General

Analizar cómo los delitos informáticos inciden en el Derecho Constitucional a la Seguridad Pública según los casos presentados en la Fiscalía General del Estado en el periodo 2014.

Objetivos Específicos

Demostrar que los delitos informáticos ocasionan un fuerte daño social y económico vulnerando intereses y estabilidad de los ciudadanos.

Establecer cómo se produce un delito informático, la forma de detectarlo protegiendo la seguridad pública contemplada en la Constitución.

Proponer posibles soluciones al problema establecido.

CAPÍTULO II

MARCO TEÓRICO

Antecedentes investigativos

Al enunciar los antecedentes investigativos se puede recalcar que existe cantidad de casos analizados en cuanto a delitos informáticos se refiere, por lo que varios especialistas en el campo han deducido que existe un fuerte impacto en la sociedad ya que toda seguridad nacional está en riesgo.

Con el avance y desarrollo de la tecnología en los años setenta empiezan los problemas de seguridad en los sistemas. En efecto, con la creación de aplicaciones interactivas de sistemas online, comienzan a verse casos de uso fraudulento del software sobre información protegida de las personas. De aquí la necesidad de las contraseñas identificativas de usuarios para controlar y restringir el acceso a los datos a personas que no deben conocer informaciones ajenas.

En la tesis del Abogado Acosta Byron cuyo tema es "LOS DELITOS INFORMÁTICOS Y SU PERJUICIO EN LA SOCIEDAD" manifiesta que la autora Gutiérrez María considera que el delito informático es "también denominado un fraude que presenta un carácter pluriofensivo de doble afección ya que involucra un interés económico y por otro lado social"pág.134

La conclusión a la que llega es que "con el avance tecnológico se está proporcionando nuevos elementos para atentar contra los bienes de la sociedad y que la información ha ido recayendo en los últimos tiempos" pág.155.

Luego el autor menciona una conclusión importante "Ecuador ha dado los primeros pasos en el desarrollo de iniciativas que permiten la investigación y

sanción de los delitos informáticos, sin embargo, es preciso desarrollar, mejorar e implementar mecanismos que permitan que dichas investigaciones se desarrolle dentro de marcos regulados, controlados y mediante el uso de tecnología apropiada por parte los entes y profesiones dedicados a su investigación" pág.156.

En otro trabajo de tema "DELITOS COMETIDOS A TRAVÉS DE SISTEMAS INFORMÁTICOS" elaborado por el Abogado Ron Torres Diego se habla de la relación Jurídica Informática en la que menciona: "Los avances tecnológicos traen nuevas amenazas a quienes usamos diariamente los sistemas de información, como el caso del Internet donde nos sienten inseguros al momento de navegar en la red, ya que la información que es enviada puede ser modificada de alguna manera o en casos más graves interceptada, para cometer delitos Informáticos, ésta información siempre está expuesta a que personas con ánimos dolosos perjudiquen a los usuarios, los mismos que se encuentran expuesto a la gama de virus informáticos que atentan contra el sistema informático, produciendo grandes pérdidas de información y en muchos ocasiones daños que producen hasta pérdidas económicas"pág.132.

La conclusión que llega es" Los sistemas informáticos han establecido un nivel de desarrollo social en los últimos años, pero cuando podemos saber si estamos frente a un delito informático o no, lo importante es no olvidarnos de este elemento esencial de los delitos informáticos que es de uso doloso del sistema informático, es decir cuando se utiliza el sistema informático con el ánimo de causar daño, de perjudicar, estamos frente a un delito tecnológico."pág.133.

Otra conclusión que incluye en su trabajo es "Para finalizar podemos sumarnos a los criterios de doctrinarios, que consideran necesario legislar sobre aspectos que afecten a ciertos bienes sociales, cuya transgresión provoque serios daños que afecten la convivencia humana, como es el caso de los daños a la información en su generación, tratamiento y transmisión, en donde su vulneración puede provocar incluso el caos mundial; pero así mismo es necesario ser cautos y conservadores en la adaptación de nuevos tipos penales, que puedan resultar reiterativos o provocar problemas de concurso que acaben complicando aún más el vasto

panorama Legislativo de nuestro Estado como en el contexto Internacional" pág.134.

En la tesis "LA PROBLEMÁTICA JURÍDICA EN LA REGULACIÓN DE LOS DELITOS INFORMÁTICO" su autor el Dr. Hugo Imbaquingo menciona que *"*La criminalidad informática organizada ha crecido de manera exponencial, de acuerdo con los informes relacionados con incidentes de seguridad, vulnerabilidades reportadas y los altos costos que estos involucran para la empresa, los mismos, que son aprovechadas por los intrusos que son en conclusión los ciberinfractores" pág.120.

La conclusión a la que llega es "Los efectos que producen los delitos informáticos dentro de la sociedad son muchas veces irreparables, ya que existen problemas al momento de la investigación de este tipo de delitos puesto que no se cuenta con los medios y equipos adecuados en el país para lograr una investigación eficaz que coadyuven al juzgamiento efectivo de los mismos" pág.121.

En otra conclusión manifiesta que" Es una realidad la presencia de nuevas formas delictivas debidas concretamente a que antes no existía un adelanto informático y electrónico de grandes magnitudes como ahora. Por esa circunstancia, se considera que resulta todavía insuficiente la legislación vigente tanto a nivel nacional como a nivel internacional" pág.122

Fundamentación

Filosófica

El presente trabajo es un profundo estudio además de una fuerte recopilación mediante el cual se pone énfasis en aplicar el método social, en el cual se da un gran realce a conocimientos obtenidos en la vida, es decir el medio que nos rodea en preferencia de una gran aplicación de nuestras leyes en base a la seguridad pública. Según la posición constructivista, el conocimiento no es una copia de la

realidad, sino una construcción del ser humano, a través de conocimientos ya adquiridos y relacionarlos con la dificultad de los casos que se han dado en la sociedad. El hombre es un ser social lo que significa que su vocación debe responder a un llamado a la comunidad, en respeto a los derechos de los demás es decir hacer lo que es correcto, se debe tomar en cuenta que el papel de la conciencia moral consiste en autodeterminación y responsabilidad de mis propios actos, debido a que es una relación interna desde ahí viene los delitos informáticos que es más el ocasionar un daño a otras personas a través de involucrarse con sus datos o apropiarse de los mismos.

Legal

Constitución de la República del Ecuador 2008

El art.92 de la Constitución dice: "Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos. Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley. La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de medidas de seguridad necesarias. Si no se atendiera su solicitud, esta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados."

Los artículos 49, 50 y 51 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, se refieren a las garantías que tienen las personas para acceder a los documentos, datos genéticos, bancos o archivos de datos personales

que se hallen en poder de entidades públicas o privadas, casos en que se puede interponer el habeas data y la legitimación activa que puede ser cualquier persona natural o jurídica que puede interponer esta acción constitucional.

La finalidad del Hábeas Data es proteger a la persona de los abusos que pueda sufrir respecto del llamado poder informático. Se entiende por tal, la producción, almacenamiento y transferencia de información personal que pueden realizar instituciones públicas y privadas, empresas y personas en general, en base a los avances tecnológicos que hoy existen. La figura del Hábeas Data es, de conformidad con la normativa constitucional y legal aplicable a la fecha en el Ecuador, una acción de garantía, de rango constitucional, la misma que protege determinados derechos constitucionales.

Doctrinaria

El tratadista Gutiérrez Francés (2011) señala que puede hablarse de criminalidad o delincuencia informática como categoría exclusivamente criminológica y de carácter funcional, para aludir en forma conjunta a los problemas que las nuevas tecnologías presentan al ordenamiento penal. Todas las actividades humanas que a diario se realizan, como transacciones comerciales y bancarias, comunicación, procesos industriales, las investigaciones, la seguridad, chat, correos electrónicos, etc.; son todos aspectos que dependen cada día más de un adecuado desarrollo de la tecnología informática. Sin embargo, este desarrollo tecnológico ofrece un aspecto negativo: ha abierto la puerta a conductas antisociales y delictivas antes impensadas, ofrecen oportunidades nuevas y sumamente complicadas de infringir la ley, y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

Para el jurisconsulto Joel A. Gómez Treviño (2010) La delincuencia informática, la criminalidad informática y de las telecomunicaciones, es una realidad que requiere un análisis de múltiples dimensiones para tratar de comprender sus orígenes y así, poder establecer estrategias de prevención y combate de las mismas. Insinuar que la criminalidad informática es un problema

jurídico, o tecnológico, o social o de negocio exclusivamente es negarnos la posibilidad de construir un modelo más nutrido de relaciones que busquen profundizar en las problemáticas de las vulnerabilidades, de la inseguridad, de los individuos y sus motivaciones.

El tratadista GÓMEZ PERALS (2013) en una conferencia en Chicago menciono: Entonces cuando hablamos de delitos informáticos estamos en presencia de una acción u omisión socialmente peligrosa, prohibida por ley bajo la conminación de una sanción penal. Al igual que en el resto de los delitos existe un sujeto activo que no se habla de delincuentes comunes, sino de personas especializadas en tecnología y otro pasivo. El hecho de que no sea considerado el sujeto activo delincuente común está determinado por el mecanismo y medio de acción que utilice para llegar a producir el daño, quiénes en la mayoría de los supuestos en que se manifiestan y las funciones que desempeñan pueden ser catalogados sujetos especiales.

Por su parte, el tratadista penal italiano Carlos Sarzana, sostiene que los delitos informáticos son: cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo y en su gran mayoría dependen para su investigación y procedimiento judicial de la correcta interpretación de la ley penal, así como la concientización de los jueces de que sólo nos encontramos ante nuevos métodos para estafar o para injuriar, pero en ningún caso ante nuevos delitos. Solo a manera de referencia o explicación objetiva: incoherente sería imaginar que si mañana se pudiese quitar la vida a alguien por medio de internet habría que establecer una nueva figura penal ya que el homicidio no estaría cubriendo esta posibilidad; cuando en derecho, si se lesiona el bien jurídico protegido, no importa cuál sea el medio utilizado, corresponde la aplicación de la ley penal vigente y no se requiere una nueva y específica.

Categorías Fundamentales

Gráfico No. 2 Categorías Fundamentales
Fuente: Investigadora
Elaborado por: Grace Echeverría M

Atributos de la variable independiente

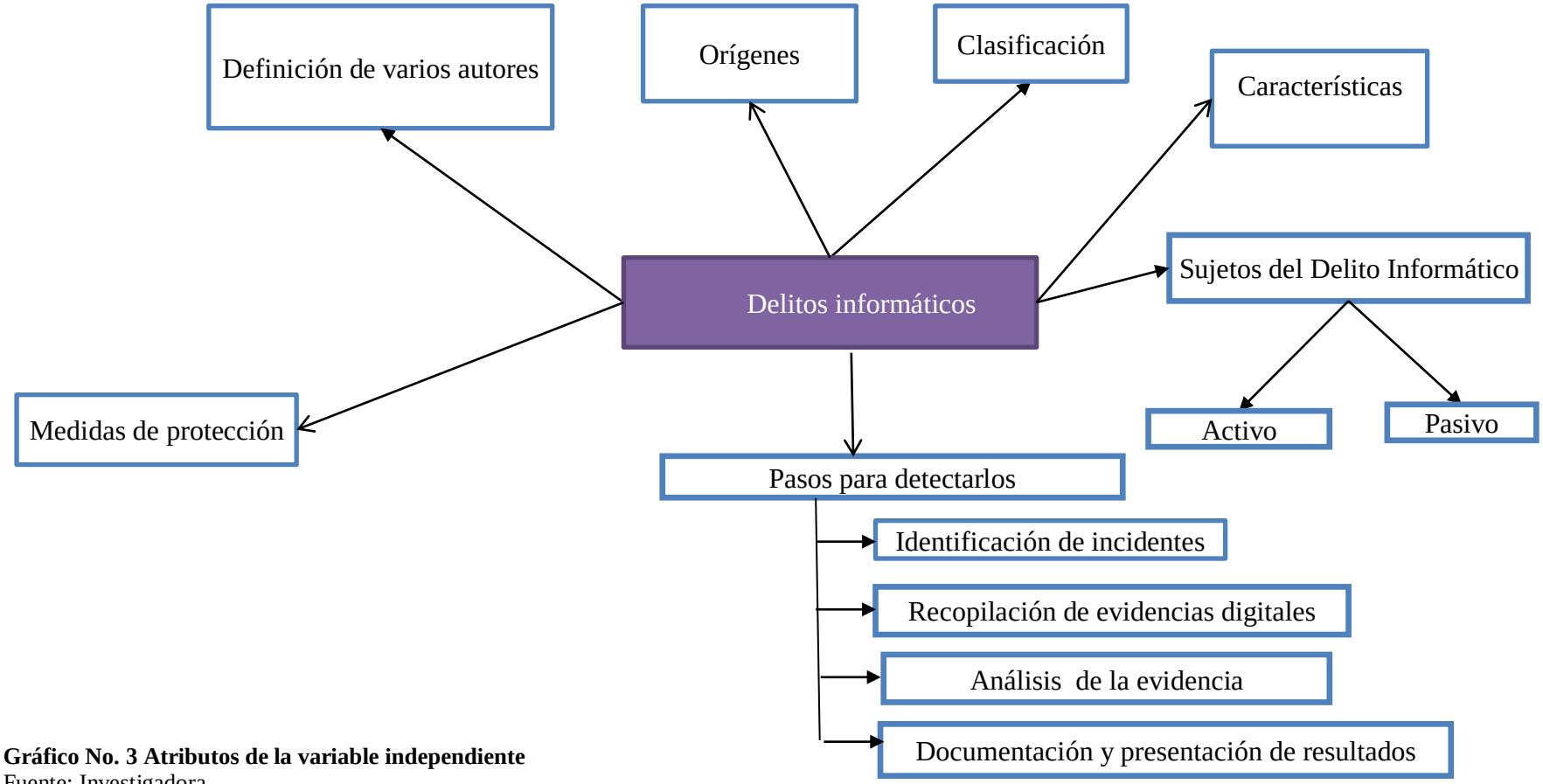

Gráfico No. 3 Atributos de la variable independiente
Fuente: Investigadora
Elaborado por: Grace Echeverría

Atributos de la variable dependiente

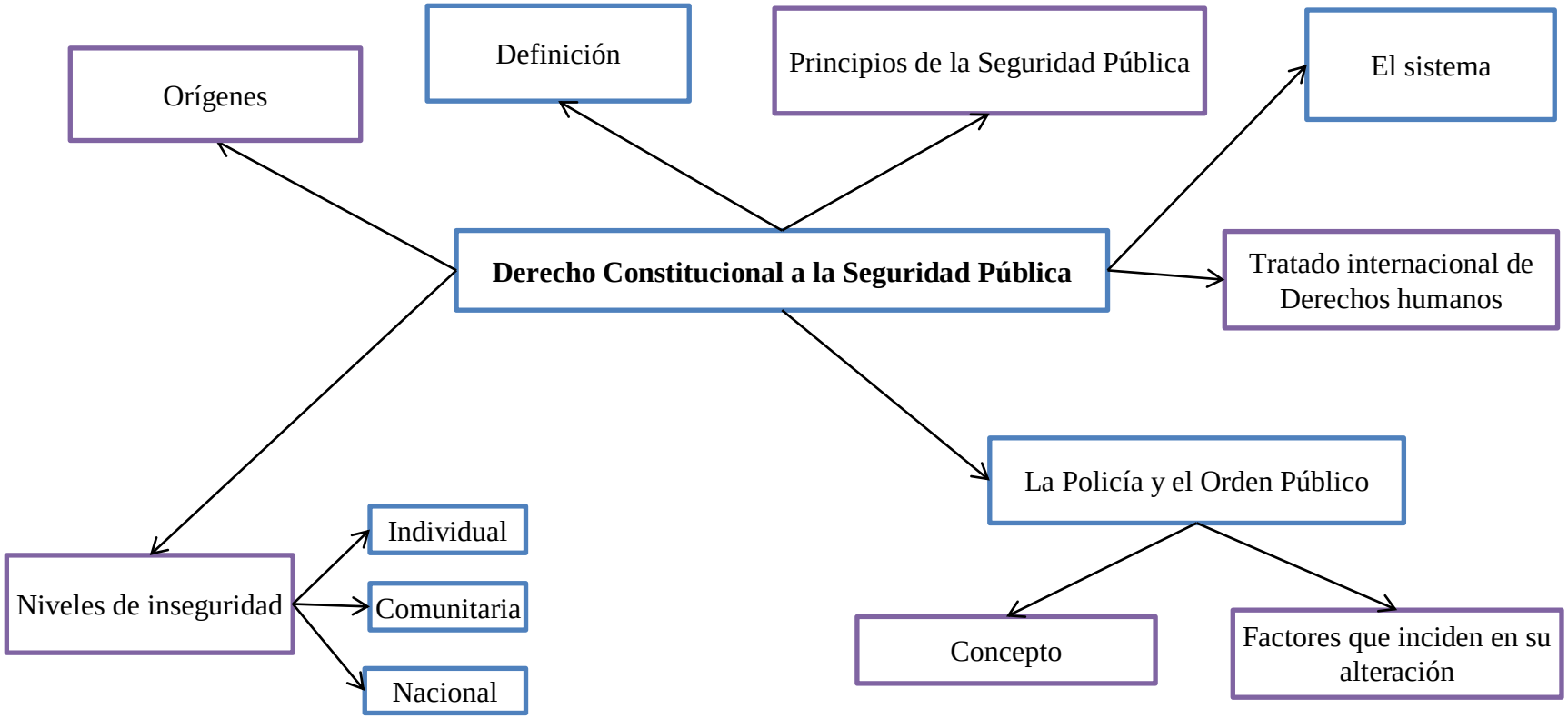

Gráfico No. 4 Atributos de la variable dependiente
Fuente: Investigadora
Elaborado por: Grace Echeverría M.

Delitos informáticos

Derecho Penal

Santiago Mir Puig tratadista español (2013) indica que "Derecho Penal no constituye sólo un conjunto de normas dirigidas a los jueces ordenándoles imponer penas o medidas de seguridad, sino también, y antes de ello, un conjunto de normas dirigidas a los ciudadanos que les prohíben bajo la amenaza de una pena la comisión de delitos". pág. 79

En la enciclopedia jurídica Omeba (1988) "derecho penal es la rama del derecho público que establece y regula, mediante un conjunto de normas y principios jurídicos, la represión de la delincuencia por parte del Estado.

Como tal, el derecho penal es también una disciplina jurídica que se encarga de estudiar el fenómeno criminal, el delito, el delincuente y la pena, a partir de lo cual se deducirán sus principios y normas jurídicas". pág. 145

Delitos de acción pública

(ACURIO DEL PINO, 2009) "La acción penal pública es aquella ejercida de forma exclusiva, excluyente y de oficio por el ministerio público, o el juez, según de que normativa procesal se trate, para la persecución de un delito". pág. 27

El delito público se contrapone al delito de acción privada (o delito privado), que se caracteriza porque el particular que ha sido víctima del mismo tiene derecho a perseguir la acción de la justicia activamente a través de una querella.

También existe el delito de acción pública previa instancia particular (o delito semipúblico), en el cual no es necesario que la víctima persiga el delito a través de una querella, pero sí que se exige que medie al menos una denuncia para que los poderes públicos puedan perseguir el delito y enjuiciar al acusado.

Definición de varios autores

Para Landaverde, M. L., Soto, J. G. & Torres, J. M. (2010) hablar de los delitos informáticos primero se tiene que tratar de qué es un delito, y luego de qué es la informática. Un delito es un acto u omisión sancionado por las leyes penales, según el ilustre penalista Cuello Calón (2009) los elementos integrantes del delito son:

El delito es un acto o acción humana, (ejecución u omisión) de carácter antijurídico, debe lesionar o poner en peligro un interés jurídicamente protegido.

El delito debe corresponder a un tipo legal (figura de delito), definido por la Ley, ha de ser un acto típico.

El acto ha de ser culpable, imputable a dolo (intención) o a culpa (negligencia), y una acción es imputable cuando puede ponerse a cargo de una determinada persona.

La ejecución u omisión del acto debe estar sancionada por una pena.

Por tanto, un delito es: una acción antijurídica realizada por un ser humano, tipificado, culpable y sancionado por una pena, mientras que la informática según

Téllez, J. (2012), es "un conjunto de técnicas destinadas al tratamiento lógico y automático de la información para una mejor toma de decisiones".

Ahora si juntamos las definiciones tendremos que los delitos informáticos son: El conjunto de técnicas de carácter antijurídico destinadas al tratamiento lógico y automatizado de la información sancionada por las leyes penales.

Téllez, J. (2012), los define como "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin". (Pàg.26)

Otra definición del mismo autor delitos informáticos: "son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho cuando hacen uso indebido de cualquier medio informático". (Pág. 27)

Téllez, J. (2012) Se entiende Delito como: "acción penada por las leyes por realizarse en perjuicio de algo o alguien, o por ser contraria a lo establecido por aquéllas". (Pág. 27)

Para el Dr. Carlos Sarzana (Criminalista Italiano 2012**) "**Los delitos informáticos se realizan necesariamente con la ayuda de sistemas informáticos o tecnologías similares, atentando contra su integridad, confidencialidad o disponibilidad, como la propiedad común, intimidad, propiedad intelectual, seguridad pública, confianza en el correcto funcionamiento de los sistemas informáticos". (Pág. 78)

RODRIGUEZ, Davara (2011) define "Los delitos informáticos son la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software". (Pág.55)

FERNANDEZ, Rafael (2013), define al delito informático como: ¨ la relación de una acción que reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo, un elemento informático o telemático contra los derechos y libertades de los ciudadanos.¨ (Pág. 49)

Orígenes

Desde hace aproximadamente diez años la mayoría de los países europeos han hecho todo lo posible para incluir dentro de la ley, la conducta punible , como el acceso ilegal a sistemas de cómputo o el mantenimiento ilegal de tales accesos, la difusión de virus o la interceptación de mensajes informáticos; en la mayoría de las naciones occidentales existen normas similares a los países europeos; todos

estos enfoques están inspirados por la misma preocupación de contar con comunicaciones electrónicas, transacciones e intercambios tan confiables y seguros como sea posible.

El uso de los ordenadores o computadores en el mundo jurídico comenzó en 1948, en la cibernética de Robert Wiener. El objeto de la Ley es la de regular los mensajes de datos, firmas electrónicas, servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos a través de redes de información, incluido el comercio electrónico y lógicamente la protección a los usuarios de estos sistemas de cualquier mecanismo de distorsión. Los efectos de la revolución digital se hacen sentir en los distintos sectores de la sociedad como lo es en la economía, la política, la educación, el entretenimiento entre otras. Así pues, la sociedad encontró nuevas formas de interrelacionarse (compras on-line, chats, e-mail, educación a distancia, foros de discusión, etc.), y este fenómeno ha traído y traerá cambios profundos, por lo que es imprescindible estar preparados para enfrentar una evolución tecnológica acelerada, para que no se produzcan efectos negativos

Desde los años ochenta a la presente, se determina que los ataques informáticos se han triplicado en lo que tiene que ver con la seguridad dado el avance de la tecnología, el aumento de número de usuarios conectados a través de redes de comunicación y de ordenadores personales trabajando como terminales del computador central o en procesos locales online.

Todo eso hizo que los factores de riesgo de las empresas se incrementaran por pérdida de un activo tan importante como es la información. Lo cierto es que la realidad del fenómeno fraudulento por medio de, o con ocasión de la informática es preocupante, pese a la dificultad para obtener cifras reales lo que ha llevado a algunos a mitificar la criminalidad informática.

Los delitos informáticos surgen en primera instancia, por la aparición de las computadoras, -recurso inventado para procesar información- en segunda instancia por la propia naturaleza del ser humano que tiende a sacar provecho de

sus recursos, los faltos de ética y ambiciosos promueven conductas ilícitas utilizando ese recursos.

Clasificación

Existen muchos tipos de delitos informáticos, la diversidad de comportamientos constitutivos de esta clase de ilícitos es muy amplia según (CAMACHO LOSA, 2012), el único límite existente viene dado por la conjugación de tres factores: la imaginación del autor, su capacidad técnica y las deficiencias de control existentes en las instalaciones informáticas, por tal razón y siguiendo la clasificación dada por el estadounidense PARKER, Don B (2012) más la lista mínima de ilícitos informáticos señalados por las Naciones Unidas, se ha tratado de lograr una clasificación que desde el punto de vista objetivo sea lo más didáctica posible al momento de tratar esta clase de conductas delictivas. Partiendo desde este punto se puede dar a conocer la siguiente clasificación:

Los Datos Falsos o Engañosos (Data diddling)

Conocido también como introducción de datos falsos, es una manipulación de datos de entrada al computador con el fin de producir o lograr movimientos falsos en transacciones de una empresa. Este tipo de fraude informático conocido también como manipulación de datos de entrada, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos

PISHING

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

SKIMMING

En lo negativo es la técnica delictiva que utiliza tecnología avanzada y facilita al ladrón o hacker robar las claves personales de los cajeros sin necesidad de estar presente, utilizando un dispositivo electrónico diseñado para este fin. Cuando el usuario se aleja, el delincuente ingresa y carga los datos en un sistema con el que puede leerlos y, posteriormente, introducirlos en una tarjeta con banda magnética sin uso, facilitándole hacer una tarjeta clon y procede a estafar.

Bombas Lógicas (Logic Bombs).

Es una especie de bomba de tiempo que debe producir daños posteriormente. Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño.

Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

Manipulación de los Datos de Salida

Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían basándose en tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las

tarjetas de crédito.

Falsificaciones Informáticas

Se produce en dos formas**:**

Como objeto, cuando se alteran datos de los documentos almacenados en forma computarizada

Como instrumentos, las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color basándose en rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer reproducciones de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

Otra manera de falsificar documentos de uso comercial se da a través de la piratería de software¨, es una derivación de la conducta ilícita de ataque a los programas informáticos que están protegidos legalmente; esta conducta comprende diferentes acciones: copiar ilegalmente programas, falsificar y distribuir software, incluso, compartir un programa con un amigo, y la piratería en Internet se refiere al uso automatizado para copiar a distribuir ilegalmente software no autorizado. Los infractores pueden utilizar Internet para todas o algunas de sus operaciones, incluyendo publicidad, ofertas, compras o distribución de software pirata.

Manipulación de Programas o los "Caballos de Troya" (Troya Horses**).**

Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de

computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

Sabotaje informático

Daños mediante la destrucción o modificación de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos (bombas lógicas, virus informáticos, malware, ataques de negación de servicio, etc.).

Fuga de Datos (Data Leakage).

También conocida como la divulgación no autorizada de datos reservados, es una variedad del espionaje industrial que sustrae información confidencial de una empresa. A decir de CAMACHO, Luis (2012), "la facilidad de existente para efectuar una copia de un fichero mecanizado es tal magnitud en rapidez y simplicidad que es una forma de delito prácticamente al alcance de cualquiera". (Pàg.52)

Apropiación de Informaciones Residuales (Scavenging).

Es el aprovechamiento de la información abandonada sin ninguna protección como residuo de un trabajo previamente autorizado. Puede efectuarse físicamente cogiendo papel de desecho de papeleras o electrónicamente, tomando la información residual que ha quedado en memoria o soportes magnéticos.

Suplantación de Personalidad (Impersonation).

Figuras en que concursan a la vez los delitos de suplantación de personas o nombres y el espionaje, entre otros delitos. En estos casos, el delincuente utiliza la

suplantación de personas para cometer otro delito informático. Para ello se prevale de artimañas y engaños tendientes a obtener, vía suplantación, el acceso a los sistemas o códigos privados de utilización de ciertos programas generalmente reservados a personas en las que se ha depositado un nivel de confianza importante en razón de su capacidad y posición al interior de una organización.

La Técnica del Salami (Salami Technique/Rounching Down**)**

Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra. Y consiste en introducir al programa unas instrucciones para que remita a una determinada cuenta los céntimos de dinero de muchas cuentas corrientes

Ciberterrorismo.

Terrorismo informático es el acto de hacer algo para desestabilizar un país o aplicar presión a un gobierno, utilizando métodos clasificados dentro los tipos de delitos informáticos, especialmente los de los de tipo de Sabotaje, sin que esto pueda limitar el uso de otro tipo de delitos informáticos, además lanzar un ataque de terrorismo informático requiere de muchos menos recursos humanos y financiamiento económico que un ataque terrorista común.

Pornografía infantil por Internet.

La INTERPOL define a la pornografía infantil como: "Toda representación, por cualquier medio de comunicación de un niño o niña, inmiscuido en actividades sexuales reales o simuladas, de manera explícita o sugerida, con fines de excitación sexual".

En mi entender, la pornografía infantil alude a actos ilícitos en los cuales existe la explotación del menor en un sentido sexual, manipulándolo para el

enriquecimiento ilegal y perverso del autor que lo emite en la red.

Acceso no autorizado a servicios informáticos

Entre las cuales las más destacadas son:

Las puertas falsas (Trap Doors**)**

Por medio de esta acción se introducen interrupciones en la lógica de los programas, con el propósito de observar, en medio de procesos complejos, si los resultados intermedios son correctos, provocar salidas de control, para guardar resultados intermedios, para comprobarlos posteriormente.

La llave maestra

Es un programa que abre cualquier archivo del computador, con el fin de alterar, borrar, copiar, insertar o utilizar en cualquier forma no permitida, datos que estén ingresados en el computador.

Mediante esta acción, es perfectamente factible alterar los registros, sin que quede evidencia de aquello.

Pinchado de líneas (Wiretapping**)**

Esta infracción se la comete interfiriendo las líneas telefónicas de transmisión de datos, para obtener la información que transita por ellas; esto se realiza por medio de un módem o un radio.

El método más eficiente para proteger la información que se envía por líneas de comunicaciones es la criptografía que consiste en la aplicación de claves que codifican la información, transformándola en un conjunto de caracteres ininteligibles de letras y números sin sentido aparente, de manera tal que al ser recibida en destino, y por aplicación de las mismas claves, la información se

recompone hasta quedar exactamente igual a la que se envió en origen.

El Espionaje Informático

Esto incluye específicamente la divulgación no autorizada de datos reservados.

Características de los delitos informáticos

Para Téllez, José. (2012), los delitos informáticos presentan las siguientes principales características:

Son conductas criminales de cuello blanco (White collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas.

Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.

Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que las realizan.

Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.

Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación que ha existido por parte del Derecho.

Son muy sofisticados y relativamente frecuentes en el ámbito militar.

Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.

Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.

Sujetos del Delito Informático

www.derechoecuador.com: "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 y protegida".

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 infractor en ese campo.

Sujeto activo

De acuerdo al profesor chileno GARRIDO Mario (2013), en su obra Nociones Fundamentales de la Teoría del Delito Edit. Jurídica de Chile "se entiende por tal quien realiza toda o una parte de la acción descrita por el tipo penal. 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". (Pág. 23)

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 delitos cometidos.

El nivel típico de aptitudes del sospechoso que comete un delito informático es tema de controversia ya que para algunos 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.

En algunos casos se puede dar el anonimato del Sujeto Activo, debido a que en esta clase de infracciones puede ser totalmente anónimo y utilizando este anonimato como forma de evadir su responsabilidad, ya que no necesariamente puede usar su propio sistema informático, sino que se puede valer de un tercero, como por ejemplo en el caso del envío de correo no deseado o SPAM, en el cual se puede usar a una máquina zombi, es decir una computadora que está bajo el control del SPAMER y que le permite usarla como una estación de trabajo de su propia red de máquinas zombis, las cuales pertenecen a usuarios desaprensivos que no tienen al día sus medidas de seguridad y que son fácil presa de los hackers y crackers para cometer este tipo de infracciones. También existen programas de enmascaramiento o que no permiten ver la verdadera dirección ya sea de correo electrónico o del numero IP.

Los sujetos activos o personas que realizan o cometen los delitos informáticos, según la actividad que hayan efectuado, son los Hackers, Script Kiddies o criminales informáticos, que "aprovechan sus conocimientos de la informática para utilizar la vulnerabilidad de un sistema con un fin: obtener información privada.

Existen muchos tipos, por ejemplo hacker de sombrero blanco o sombrero negro. El del sombrero blanco seria el que avisa del peligro de un posible atentado en la red informática. El otro, lo usará con fines maliciosos"

Los crackers o vandálico virtual, programadores maliciosos, son individuos de la sociedad moderna que poseen conocimientos avanzados en el área tecnológica e informática, igual que los Hackers, invaden sistemas, descifran claves y

contraseñas de programas, algoritmos de encriptación, roban datos personales, destruyen y cuando crean algo es únicamente para fines personales, son extremadamente precavidos con el manejo de la información, precisamente, para ocasionar el daño inmoral e ilegal a los sistemas informáticos.

Sujeto pasivo

El sujeto pasivo es la persona titular del bien jurídico que el legislador protege y sobre la cual recae la actividad típica del sujeto activo. 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, entre otros que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo perjudicado, es sumamente importante para el estudio de los delitos informáticos, ya que mediante él podemos 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 activo.

Maneras de protección de información

Para guardar datos seguros se debe tomar en cuenta:

La autentificación (promesa de identidad): La prevención de suplantaciones, que se garantice que quién firma un mensaje es realmente quién dice ser. Ésta función se encarga de reunir evidencias para cumplir con un determinado nivel de riesgo, para que la exigencia de identidad sea válida, esto puede ser llevado a cabo mediante comparaciones de algo que el individuo sepa, tenga, sea o pueda hacer y que sea factible de ser comparado. Por ejemplo:

Algo que él sepa: (contraseña) Un código o palabra que solamente él y el sistema conozcan.

Algo que él posea: (foto de identificación) Alguna foto personal que pueda ser comparada con una imagen de la misma persona almacenada en memoria.

Algo que él sea: (apariencia física) Una comparación de cuerpo entero en base a un sistema óptico.

Algo que él pueda hacer: (su firma) Toda firma posee un estilo único que es susceptible de ser analizado por computadora.

La autorización: Se da permiso a una persona o grupo de personas de poder realizar ciertas funciones, al resto se le niega el permiso y se les sanciona si las realizan.

Esto significa que la autorización establece reglas que restringen a los usuarios a llevar acabo solo acciones predefinidas en el recurso de acceso, todos los usuarios sin excepción deberán tener una autorización explícita de la gerencia para tener ingreso a información.

La confidencialidad o privacidad: Es el más obvio de los aspectos y se refiere a que la información solo puede ser conocida por individuos autorizados. Existen infinidad de posibles ataques contra la privacidad, especialmente en la comunicación de los datos.

La transmisión a través de un medio presenta múltiples oportunidades para ser interceptada y copiada.

La integridad de datos: Se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada, copiada, etc., ya sea durante el proceso de transmisión o en su propio equipo de origen.

Es un riesgo común que el atacante al no poder descifrar un paquete de información y sabiendo que es importante, simplemente lo intercepte y lo borre.

La disponibilidad de la información: Se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, ya sea por ataque doloso, mala operación accidental, situaciones fortuitas o de fuerza mayor.

Controles de acceso: Esto es, quién tiene autorización y quién no, para acceder a una información determinada.

Son los requerimientos básicos para la seguridad que deben proveerse de una manera confiable.

Los requerimientos cambian ligeramente, dependiendo de lo que se está asegurando. La importancia de lo que se está asegurando y el riesgo potencial.

Otras medidas que se deben tomar en cuenta son:

Identificación: La función de identificación nos permite establecer como su nombre lo dice, identificadores (nombres, símbolos) para cada usuario y cada recurso del sistema identifica a los usuarios, hardware, software y demás recursos disponibles para el sistema.

Delegación: Para poder mantener y aplicar la función de autorización, es necesario delegar, esta función determina quién y bajo qué circunstancias, podrá ejercitar o cambiar las reglas de autorización.

En los pequeños sistemas, esta tarea puede ser llevada a cabo por el administrador de seguridad, en sistemas muy grandes que poseen una compleja estructura de usuarios, recursos, ubicaciones y actividades puede requerir de un sofisticado mecanismo de delegación que les permita el manejo para actualizar las reglas de autorización en tiempos reales para necesidades reales.

Muchos de los sistemas que se encuentran actualmente en el mercado están diseñados para que solamente el operador designado o controlado pueda cambiar

identificadores de operación.

Seguimiento: Provee registros escritos del uso de los recursos del sistema y de todas las actividades significativas, ofrece beneficios mayores al permitir reconstruir información, hacer respaldos y recuperaciones, puntualizar la contabilidad, seguir pistas e identificaciones, ganar visibilidad y ver que ésta sucediendo. Los sistemas nunca deberían ser diseñados sin tener la capacidad de hacer seguimiento (quién y qué capturó, donde, por qué y cómo), es la manera más efectiva para monitorear la operación, objetivos, reglas y estándares de ejecución.

Reconocimiento: Es necesario que alguien revise el seguimiento, monitoreé las variaciones de actividades con respecto al uso, contenido y comportamiento esperado, en realidad lo que se busca con esta función es llegar más allá del seguimiento, informando a la gerencia o jefatura de todo tipo de irregularidades de cualquier comportamiento inesperado, es entonces cuando la jefatura deberá tomar las acciones correctivas pertinentes.

Podría confundirse el objetivo de esta función con la de seguimiento, sin embargo, la anterior se limita a la capacidad de registrar las operaciones y ésta última se refiere a las acciones de deslindar responsabilidades y revisar oportunamente aquellos registros con el objeto de preparar las acciones correctivas a la brevedad posible

Pasos para detectarlos e investigarlos

Los elementos de prueba dentro de un proceso son de vital importancia, ya que mediante su investigación se llega a determinar la confirmación o negación de lo que corresponde a la verdad.

Es trascendental tener en consideración la formalidad y claridad de los procedimientos o técnicas de análisis utilizados en un proceso de investigación, para brindar mayor claridad y precisión a las observaciones dentro del proceso,

ante un hecho delictivo informático.

Identificación de incidentes

Este es el primer paso que debe asegurar la integridad de la evidencia original, es decir, que no se deben realizar modificaciones ni alteraciones sobre dicha evidencia, en este aspecto se trata de mantener los requerimientos legales.

Adicionalmente, es preciso que el investigador o especialista se cuestione sobre la información obtenida en un sistema que se crea está comprometido.

Se deben establecer los procesos que se están ejecutando en el equipo ante un incidente e identificar algún proceso extraño, u actividades pocos usuales, pero para ello es preciso conocer la actividad normal del sistema

Recopilación de evidencias digitales

Si mediante los hallazgos del proceso de identificación de evidencias se comprueba que el sistema está comprometido, se requiere establecer la prioridad entre las alternativas de: levantar la operación del sistema o realizar una investigación detallada.

1. Generalmente la primera reacción suele ser, restablecer el sistema a su estado normal, pero se debe considerar que este paso podría resultar en que se pierdan casi todas las evidencias que aún se encuentren en la "escena del delito" e incluso puede resultar en el impedimento de llevar a cabo las acciones legales pertinentes.

2. En el caso de que se elija la segunda alternativa y el profesional se encuentra capacitado para realizarlo, se debe iniciar con el proceso de recopilar las evidencias que permitan determinar los métodos de entrada, actividades de los intrusos, identidad y origen, duración del evento o incidente, siempre precautelando evitar alterar las evidencias durante el proceso de recolección.

Preservación de la evidencia digital

En el caso de que se inicie un proceso judicial contra los atacantes del sistema, será necesario documentar en forma precisa y clara como se ha preservado la evidencia tras su recopilación a lo largo de todo el proceso de las fases anteriores, por ello, es indispensable establecer los métodos adecuados para el almacenamiento y etiquetado de evidencias.

Se recomienda la obtención de copias exactas de la evidencia obtenida utilizando mecanismos de comprobación de integridad de cada copia, las cuales deben ser documentadas y agregadas en el etiquetamiento realizado.

El segundo factor que debe sustentarse, en esta etapa, es el proceso de cadena de custodia, donde se establecen las responsabilidades y controles de cada una de las personas que manipulan la evidencia digital.

Análisis de la evidencia

Luego de que ya se han realizado los procesos de identificación, recopilación y preservación de las evidencias digitales, el siguiente paso es el análisis de dichas evidencias cuyo objetivo primordial es la de reconstruir con todos los datos disponibles.

La línea de tiempo en que se realizó el ataque, determinando la cadena de acontecimientos desde el instante anterior al inicio del ataque, hasta su descubrimiento.

Documentación y presentación de resultados

En esta etapa, se procede con el desarrollo de los informes técnicos o periciales que deben contener una declaración detallada del análisis realizado, en el cual se debe describir la metodología, las técnicas, y los hallazgos encontrados.

Derecho Constitucional a la seguridad pública

Derechos Humanos

Ángelo Papacchini (2012) Los derechos humanos son aquellas libertades, facultades, instituciones o reivindicaciones relativas a bienes primarios o básicos que incluyen a toda persona, por el simple hecho de su condición humana, para la garantía de una vida digna. Son independientes de factores particulares como el estatus, sexo, etnia o nacionalidad; y son independientes o no dependen exclusivamente del ordenamiento jurídico vigente.

La fundamentación de los Derechos Humanos, nos lleva necesariamente a pensar tanto en la concepción positivista del Derecho como en la iusnaturalista, de las cuales, como se ha mencionado, se generan una serie de modelos que buscan conceptualizar lo que conocemos como Derechos Humanos.

Constitución de la República del Ecuador.

GARRIDO, Mario (2014) "Es el fundamento y la fuente de la autoridad jurídica que sustenta la existencia del Ecuador, la supremacía de la norma la convierte en el texto principal dentro de la política ecuatoriana, y está por sobre cualquier otra norma jurídica. La constitución proporciona el marco para la organización del Estado ecuatoriano, y para la relación entre el gobierno con la ciudadanía ecuatoriana"

Orígenes

El estudio y análisis del tema de la seguridad se basa en una profunda revisión histórica aunque muy somera, para comprender su desarrollo. Hasta el siglo XVIII la seguridad estuvo ligada básicamente a la personalidad del ser humano; a partir del siglo XIX se desarrollan las teorías de la persona jurídica y el concepto de seguridad pasa a ser de responsabilidad de las instituciones del Estado, consolidándose esta situación durante el siglo XX.

El hombre por su misma condición de ente social es el más complejo el sistema de organización constitucional creado hace tres siglos como consecuencia de avance de ideas democráticas liberales, con el fin de proveer a la sociedad los mecanismos esenciales e indispensables para dar soluciona sus naturales conflictos dentro de un clima de paz y tranquilidad, es así que en el siglo XVIII y XIX siguen dando el referente lógico para el desarrollo del derecho constitucional que busca hacer realidad la más elevada aspiración humana de vivir en un mundo en el que este lejos del miedo y la miseria, se pueda disfrutar de la libertad y la justicia dentro de un ambiente de tolerancia y respeto mutuo

La seguridad en esencia, es propia de la naturaleza social del hombre, en la medida que sólo puede ocurrir en el contexto de las relaciones humanas dentro de la sociedad. En la teoría del Contrato Social y específicamente en la versión de Hobbes, considera a la seguridad como un prerrequisito de la vida social, concomitantemente con la libertad de las personas y la propiedad.

En este sentido todo parece apuntar a la construcción de la convivencia humana dentro de un ambiente de paz, orden y seguridad, sobre la base del respeto a los derechos inmanentes del ser humano, el derecho a una vida digna y justa donde la gran mayoría satisfaga las necesidades y se proyecte hacia un nuevo orden social. Pero al mismo tiempo el tránsito hacia formas sociales más evolucionadas del hombre conlleva a la generación de ciertos niveles de inseguridad cuando los satisfactores de las necesidades pasan a ser cada vez más insuficientes.

Después de la Segunda Guerra Mundial, el mundo se polariza y prevalece una constante guerra fría entre las dos principales potencias. Estados Unidos con el fin de mantener su poder de equilibrio, afianzó en América un sistema de seguridad hemisférica a la luz del Tratado Interamericano de Asistencia Recíproca (TIAR).

Con el fin de precautelar un avance de la ideología comunista, alienta en América Latina la presencia de gobiernos autoritarios y dictatoriales al mismo tiempo que en el país se pone en vigencia la Doctrina de Seguridad Nacional.

La caída del muro de Berlín y del sistema socialista de los países del Este puso fin a la guerra fría, al mismo tiempo que en América resurgen y se consolidan los regímenes democráticos; las controversias fronterizas de los países en su mayoría han sido solucionadas; los conceptos de seguridad van adquiriendo nuevas formas y en el contexto internacional está entendida no sólo como la seguridad de los estados sino como la seguridad de las personas, adquiriendo un espectro mucho más amplio, el mismo que está íntimamente ligado con el desarrollo social de los pueblos y en el cual se inscribe el bienestar de los ciudadanos, la reducción de la pobreza y el aumento del bienestar social, el análisis de las tendencias demográficas y el impacto ambiental.

El Premio Novel de la Paz Adolfo Pérez Esquivel, reiteró algunos de estos postulados en un encuentro sobre seguridad urbana en la ciudad del Mar del Plata, organizado por el Servicio de Paz y Justicia y la Comisión Sudamericana de Paz en Octubre de 1988. Pérez Esquivel señaló que la seguridad no se refería solamente al aspecto delictivo sino también al campo social, puesto que se generaba inseguridad cuando había salarios insuficientes, desocupación o niñez desamparada. Por lo tanto, el tema de la seguridad habría que tratarlo desde los aspectos socio – económicos con el fin de proveer una mejor calidad de vida y una política enfocada a los sectores más pobres.

Definición

A la seguridad Pública en el Derecho Constitucional hay que entenderla como un medio que permite alcanzar las finalidades sociales y humanas trascendentales, lo que es esencial para la existencia humana en sociedad; de allí que es necesario que todos los sectores sociales estén conscientes que es una tarea compartida entre la sociedad civil y la responsabilidad del Estado de garantizar dicha seguridad, definiendo las competencias que cada una de ellas debe asumir; obviamente dentro de un marco normativo al que todos deben someterse para ejercer los derechos y obligaciones en aras del bien común.

La seguridad Pública es un servicio que debe ser universal para proteger a las

personas ya que está vinculada al orden público que no es otra cosa que una forma de vida, un status social establecido y condicionado por la voluntad formal de una comunidad jurídica, en virtud de sus convicciones éticas, sus costumbres, sus necesidades y exigencias más sentidas. En consecuencia, la seguridad pública es la garantía que el Estado proporciona a la nación a través de la Policía Nacional, a fin de asegurar el orden público.

Principios de la Seguridad Pública y del Estado

El artículo 4 de la ley de Seguridad Pública menciona "La seguridad pública y del Estado se sujetará a los derechos y garantías establecidos en la Constitución de la República, los tratados internacionales de derechos humanos, y se guiará por los siguientes principios:

Integralidad.- La seguridad pública será integral para todos los habitantes del Ecuador, comunidades, pueblos, nacionalidades, colectivos, para la sociedad en su conjunto, las instituciones públicas y privadas, y comprende acciones conjugadas de prevención, protección, defensa y sanción. Así, se prevendrán los riesgos y amenazas que atenten contra la convivencia, la seguridad de los habitantes y del Estado y el desarrollo del país; se protegerá la convivencia y seguridad ciudadanas, se defenderá la soberanía y la integridad territorial; se sancionarán las acciones y omisiones que atenten a la seguridad pública y del Estado.

1) Complementariedad.- La seguridad pública es responsabilidad del Estado, que promoverá un orden social democrático que asegure la convivencia pacífica, con la participación y veeduría ciudadana para el mantenimiento de la paz;
2) Prioridad y oportunidad.- El Estado en sus planes y acciones de seguridad, dará prioridad a la prevención basada en la prospección y en medidas oportunas en casos de riesgos de cualquier tipo;
3) Proporcionalidad.- Las acciones de seguridad y la asignación de recursos serán proporcionales a las necesidades de prevención y protección, y a la magnitud y trascendencia de los factores que atenten contra la seguridad de los habitantes y del Estado;

4) Prevalencia.-Ninguna norma jurídica podrá restringir el contenido de los derechos y las garantías constitucionales de los habitantes, comunidades, pueblos, nacionalidades, colectivos. Sólo en casos de estados de excepción podrá temporalmente limitarse el ejercicio del derecho a la inviolabilidad de domicilio, inviolabilidad de correspondencia, libertad de tránsito, libertad de asociación y reunión, y libertad de información de conformidad con la Constitución, y;
5) Responsabilidad.- Las entidades públicas tienen la obligación de facilitar coordinadamente los medios humanos, materiales y tecnológicos para el cumplimiento de los fines de la presente ley. La responsabilidad operativa corresponde a la entidad en cuyo ámbito y competencia radique su misión, funciones y naturaleza legalmente asignadas."

El sistema

El Estado tiene una gran responsabilidad, y deben crearse Instituciones que sean eficientes y que brinden seguridad al usuario que bien podría facilitarse con convenios con las diferentes firmas calificadas dentro de la electrónica, que den seguridad otorgando un resguardo a la información que circula por las redes interconectadas, sean estas redes abiertas como el internet o cerradas como una intranet o redes internas que se instalen en las Instituciones.

Tratados Internacionales

En un primer término, debe considerarse que en 1983, la Organización de Cooperación y Desarrollo Económico (OCDE) con su sede en Francia, inició un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas computacionales.

La Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, que entró en vigor en septiembre de 2003, es el principal instrumento internacional en la lucha contra la delincuencia organizada. La

Convención tiene 147 Estados signatarios y 100 Estados Parte y de la cual forma parte el Ecuador, en dicha convención se pone de manifiesto las reglas básicas sobre la prosecución de Delincuencia Organizada Transnacional, dichas reglas hacen especial mención a los delitos relacionados con la legitimación de activos y los de corrupción. También se mencionan a los llamados "delitos graves" que son de acuerdo con el Art. 2 "toda conducta que constituya un delito punible con una privación de libertad de tres años o con una pena más grave". En el caso de las llamadas infracciones informáticas todas ellas son delitos graves de acuerdo a la definición de la Convención, en tal razón se encuadran en su ámbito de aplicación de la convención de conformidad al Art. 3, siempre que dichos delitos sean de carácter transnacional y entrañen la participación de un grupo delictivo organizado.

De igual forma se debe tomar en cuenta que la Convención da la posibilidad de conseguir capacitación y asistencia de parte de los Estados signatarios en la prevención e investigación de esta clase de delitos e insta a contar con programas de capacitación y entrenamiento a las personas responsables del cumplimiento de la ley como Jueces, Fiscales y Policías. También insiste en el uso de Técnicas Especiales de Investigación como la vigilancia electrónica.

Los adelantos en la tecnología de las comunicaciones han determinado que surgieran nuevas oportunidades para la comisión de delitos sumamente complejos, en particular un aumento significativo del fraude en la Internet, y esas oportunidades han sido explotadas por los grupos delictivos organizados.

La tecnología de las comunicaciones también confiere más flexibilidad y dinamismo a las organizaciones delictivas; el correo electrónico se ha convertido en un instrumento de comunicación esencial independiente del tiempo y la distancia.

Las autoridades encargadas de hacer cumplir la ley suelen adaptarse con lentitud a las nuevas tendencias, mientras que los grupos delictivos organizados tienden a hacerlo rápidamente y a aprovechar los adelantos tecnológicos debido a

los inmensos beneficios que producen sus actividades ilícitas.

Los países con economías en transición o en situaciones de conflicto son particularmente vulnerables al crecimiento de ese tipo de delincuencia. En tales casos, la delincuencia organizada plantea una amenaza real para el desarrollo de instituciones reformadas, como la policía, los servicios de aduana y el poder judicial, que pueden adoptar prácticas delictivas y corruptas, planteando un grave obstáculo al logro de sociedades estables y más prósperas.

El Gobierno del Ecuador, inscrito en el proceso de consolidación de la Unión de Naciones Suramericanas (UNASUR) y ratificando su postura radical al cambio estructural de la política regional de seguridad, asume la responsabilidad de construir una seguridad con enfoque integral, que responda a un diagnóstico propio de la problemática del país en que vivimos.

A diferencia de los conceptos tradicionales de seguridad cuya razón de ser era el Estado, este nuevo enfoque sitúa al ser humano como eje principal y transversal, incorporando a la ciudadanía como actor protagónico de los procesos de seguridad individual y colectiva.

Este nuevo enfoque que el Ecuador inicia, también está en concordancia con los conceptos de seguridad humana, los mismos que desde hace más de una década han venido debatiéndose y desarrollándose en este nuevo paradigma de la seguridad centrada en el ser humano. La seguridad humana, es la condición necesaria para la subsistencia y calidad de vida de las personas y sociedades y sus componentes abarcan la seguridad económica, la seguridad alimentaria, la seguridad sanitaria, la seguridad ambiental, la seguridad política, la seguridad comunitaria y la seguridad personal, dándole justamente al ser humano atención a todas sus necesidades para su bienestar.

De igual manera, es indispensable desarrollar condiciones tendientes a la producción nacional de ciencia y tecnología e implementar sistemas de seguridad electrónica y tecnológica, así como propiciar mecanismos de cooperación regional

para la transferencia de tecnología.

Es primordial desarrollar sistemas integrados de investigación y producción científica y tecnológica, con el propósito de potenciar las capacidades, habilidades y experticias de las y los profesionales, de esta manera se logrará mayores grados de autonomía del país y la disminución de la dependencia y vulnerabilidad a fin de propiciar un entorno más seguro, puesto que la dependencia externa y los imperios tecnológicos generan inseguridad y vulneran los intereses nacionales.

Para el autor Fernando Carrión dice "la seguridad Pública busca dar seguridad a la ciudadanía en el ejercicio público y privado del ejercicio de sus derechos y deberes, por eso se la obtiene en un estado social de derecho donde la libertad del respeto del derecho ajeno es legal, legítima y democrática actuando conforme a las leyes en beneficio de la sociedad para su respectiva protección"

Declaración de los Derechos Humanos

En su Artículo 3 menciona "Todo individuo tiene derecho a la vida, a la libertad y a la seguridad de su persona".

El objeto de los derechos humanos es el estudio de los derechos de las personas, reconocidos a nivel nacional e internacional y, los cuales en cierto estado de la civilización, aseguran la conciliación entre la afirmación y protección de la dignidad de la persona y el mantenimiento del orden público.

Por el contrario, desde la perspectiva de los derechos humanos y el Estado constitucional de derechos y justicia, cuando se parte del tema de seguridad no podemos limitarnos a la lucha contra la delincuencia, sino que se debe hablar de cómo crear un ambiente propicio y adecuado para la convivencia pacífica de las personas en contextos de igualdad y justicia social.

En materia de Derechos Humanos se fortalece el ejercicio de la soberanía estatal debe impartirse siempre respetando las demandas de libertad de sus

ciudadanos. Incluso son los individuos y la comunidad internacional los que puede demandar jurídicamente a un Estado por los excesos que se comentan en el control del orden público interno. Para este efecto existen múltiples convenios internacionales de los cuales el Ecuador es signatario y cuyo cumplimiento es obligatorio o podrá ser llevado a las cortes internacionales en caso de incumplimiento.

La policía y el orden Público dentro de los elementos de seguridad

La Comandancia General de la Policía Nacional dentro del marco del Plan de Fortalecimiento Institucional ha manifestado en términos prácticos una profunda preocupación por crear una cultura de prevención del delito.

El aumento progresivo de las diferentes formas de delincuencia desde los más tradicionales hurtos, violación de la propiedad privada, trata de blancas, hasta los más actuales como el lavado de dinero, tráfico de órganos, secuestros y utilización ilícita de los avances tecnológicos obliga que se ponga atención en la seguridad, como el proceso social que finalmente dinamiza, fortifica y acrecienta el desarrollo humano.

El mantenimiento de la seguridad interna y del orden público en una sociedad determinada debe cumplirse estrictamente dentro del respeto a la libertad de las personas y a los derechos fundamentales que los amparan. Se sabe que la imagen cristiana y humanitaria del hombre se constituye a partir de la certeza de que el ser humano, por sus características específicas, tiene una dignidad inconfundible e irrevocable que exige respeto y libertad.

La preservación de estos principios elementales de convivencia es un deber y una obligación de todo Estado de derecho. Pero esta no es una obligación de carácter moral sino que es una obligación jurídica tanto dentro del campo nacional como internacional. El derecho y las normas legales son los encargados de regular las actividades, fijar atribuciones, competencias, premios y castigos, a toda la estructura estatal destinada a mantener la seguridad el orden público.

Es tan universal el reconocimiento de estos componentes primordiales de la función de la policía que, con términos similares o análogos, se halla expresada en cualquier sistema de los diferentes países. Así lo considera la Constitución Política del Ecuador en el Art. 183 inciso 4to. que dice: "La Policía Nacional tendrá como misión fundamental garantizar la seguridad y el orden público".

Concepto de Policía

El origen de la Policía tiene sus bases en la esencia misma de la convivencia social, ya que es allí donde surge la posibilidad de la perturbación del orden que no es sino la ruptura del equilibrio existente entre el interés particular y el interés público o común. Desde la antigüedad ha sido conocida la policía como función del Estado; por ende existe varias definiciones entre estas:

Aristóteles con su concepción propia de la policía manifiesta: "Policía es buen orden, gobierno de la ciudad, apoyo del pueblo, el primero y más grande de todos los bienes"

Platón, define a la policía como "la vida arreglo y ley que mantiene la ciudad"

Sócrates en su concepción filosófica manifiesta "La policía es el alma de la ciudad que obra los mismos efectos que el sentimiento en el hombre, la que lo piensa todo; quien arregla todas las cosas, quien hace o procura toda la felicidad a los ciudadanos y quienes se paran y alejan de la sociedad los males y calamidades".

Al establecer una definición de Policía es evidente que existen afirmantes definiciones de orden pública las mismas que a continuación revelan lo siguiente.

De acuerdo con la definición presentada en la Enciclopedia OMEBA (1894), orden público "es el conjunto de condiciones fundamentales de vida social instituidas en una comunidad jurídica, las cuales, por afectar centralmente a la organización de esta, no pueden ser alteradas por la voluntad de los individuos ni,

por la aplicación de normas extrajeras. Como realidad estimable, el orden público es una forma de vida, un estatus social establecido y condicionado por la voluntad formal de una comunidad jurídica."(Pág. 896)

El diccionario de la Real Academia de la Lengua define como Orden público "El estado de legalidad moral en que las autoridades ejercen sus atribuciones propias y los ciudadanos las respetan y cumplen"

El tratadista Bartolomé Fiorini en su obra Seguridad Pública emergente (2012) se refiere al orden público "desde un concepto jurídico funcional que tiene que ver con los bienes comunes, es decir aquellos que interesa a la sociedad en su conjunto, más no a ninguna persona en particular; citándose entre ellos a la moral pública, la costumbre moral, los precios máximos de las mercancías vitales y que se hacen accesible al colectivo social."(Pág. 78)

Factores que inciden en la alteración de la seguridad pública

Un sin número de factores intervienen en la alteración del orden público y van desde aquellos que son de carácter estructural del estado y que son de largo alcance; y, aquellos que son de carácter coyuntural. Entre los primeros se cuentan:

La falta de continuidad de los planes y programas de desarrollo del Estado, los mismos que responden a la política del gobierno de turno, y por lo general han dejado inconclusas las obras que son de servicio a la comunidad, truncando de esta manera las aspiraciones más sentidas de la población ecuatoriana.

La irracional e inequitativa distribución de la escasa riqueza del estado marginando a sectores muy importantes del derecho a los servicios sociales básicos para su subsistencia: salud, educación, vivienda, entre otros.

La irracionalidad del gasto público generador principal del déficit fiscal.

La falta de concertación política frente a los objetivos nacionales permanentes

y actuales en medio del conflicto de intereses de los partidos políticos por beneficiar su propios intereses particulares de determinados sectores de la sociedad en perjuicio de los más pobres; dando lugar a un trato discriminatorio y fomentando de esta manera el regionalismo y afectando así al desarrollo integral del país.

Este ha sido el escenario que ha contribuido a deteriorar la calidad de vida de la población, siendo más lejana la satisfacción de las necesidades básicas de nutrición, educación, vivienda, empleo, servicios públicos, justicia y seguridad.

Con relación a los dos últimos, serios cuestionamientos se han hecho por la falta de garantías del Estado y de la Administración de Justicia, amplios sectores de la población ecuatoriana no han sido merecedores de la protección que garantice una convivencia civilizada de allí que se han manifestado expresiones de violencia, de atentado a la integridad de las personas, desconociendo las leyes que nos rigen para dar paso al impulso instintivo de autodefensa, pero atentando a los más elementales derechos del ser humano como es la vida, ya que los grupos de autodefensa actúan irracionalmente castigando muchas veces a gente inocente.

Niveles de inseguridad

El resultado de esta realidad hace que los ecuatorianos no puedan sentirse seguros, ni siquiera aquellos que ostentan el mayor poder económico, político y social; pues, las medidas de seguridad han resultado insuficientes, la proliferación de empresas de seguridad privada tampoco han contribuido a reducir la inseguridad y por el contrario en un gran porcentaje son causantes de la propia inseguridad.

Frecuentemente la opinión pública se siente alarmada por atentados contra altos personajes de la política y de los negocios, y ya no sorprende a nadie que en edificios lujosos o en cárceles comunes empiecen a caer afectados.

Las causas de la inseguridad se manifiestan en varias modalidades que resultan

muchas veces de la insuficiencia de recursos para satisfacer las necesidades básicas de la población; de la falta de atención a los sectores más necesitados en obras y servicios de uso comunitario, de las discrepancias políticas y sociales que impiden una participación ciudadana en las actividades del Estado; de las diferencias ideológicas y culturales del pueblo; de la profunda crisis ética y moral, generalizada en toda la sociedad.

A la seguridad hay que analizarla en sus diferentes niveles; individual, comunitaria, nacional o colectiva con sus características propias y el grado de participación que tiene el Estado en cada uno de ellos.

Individual

Con relación a la seguridad individual, el hombre debe saber y estar confiado en que sus derechos y garantías individuales deben ser respetados tales como: los de libertad, de expresión, de propiedad privada, de libre movilización, de protección contra el crimen; así como los problemas de salud, educación, alimentación, vivienda y subsistencia.

Si bien es cierto que al hombre le asisten derechos individuales, pero es necesario pensar que no se encuentra solo y por el contrario convive en sociedad, situación que impone un marco de seguridad social que vienen a ser los elementos que dan estabilidad a las relaciones políticas, económicas y sociales.

Tanto la seguridad individual como la colectiva, son modalidades que le compete asumir al Estado y se circunscriben en una de las funciones del Estado que es la de garantizar el orden público, requisito fundamental para el desarrollo del país.

Comunitaria

La seguridad comunitaria o de grupo es otro de los deberes ineludibles del Estado, que consiste en proteger al grupo social contra diversas interferencias, a

fin de permitir las satisfacciones de los intereses y aspiraciones de la comunidad.

La seguridad colectiva se fortalece sobre la base de la integración de grupos de países en cuya estructura el Poder Nacional de los miembros responden frente a situaciones adversas, con el fin de alcanzar los objetivos del bienestar común.

Nacional

La seguridad nacional tendrá que apoyarse en el Poder Nacional para la conquista y mantenimiento de los objetivos nacionales permanentes: soberanía, integridad, territorial, integración nacional, justicia social, democracia, desarrollo integral y protección del medio ambiente.

Algunos autores como (GARCES POZO 2012) en su obra Seguridad Nacional Interna coincide en definir a la seguridad nacional como "toda acción encaminada a procurar la preservación del orden público institucional del país, de modo que asegure el libre ejercicio de la soberanía de la nación en el interior como en el exterior, con acomodo a las disposiciones establecidas en la Constitución Política del Estado, a las leyes de la república y a las normas del derecho internacional, según corresponde."

Hipótesis

Los delitos informáticos inciden en el Derecho Constitucional a la Seguridad Pública.

Señalamiento de Variables

Variable Independiente: Delitos Informáticos

Variable Dependiente: Derecho Constitucional a la Seguridad Pública.

CAPÍTULO III

METODOLOGÍA

Enfoque de la investigación

El presente trabajo de investigación está basado en el paradigma: crítico propositivo ya que se apoya en el hecho de que la vida social es dialéctica, por tanto, su estudio debe abordarse desde la dinámica del cambio social, como manifestación de un proceso anterior que le dio origen y el cual es necesario conocer. NARANJO, Galo y HERRERA al paradigma critico – propositivo lo analizan con una perspectiva razonable partiendo de que : "Introduce la ideología de forma explícita y la auto reflexión crítica en los procesos de conocimiento, la finalidad es la trasformación de la estructura de las relaciones sociales y da respuesta a determinados problemas generados por estas, une el conocimiento teoría y la acción que se constituye en la práctica; está orientada al conocimiento del hombre e implica la participación de los docentes en la auto reflexión"

Además esta investigación se vincula con el paradigma cualitativo y cuantitativo, es cualitativo ya que se utiliza esencialmente técnicas basadas en el análisis del lenguaje, como es la entrevista, y las técnicas de creatividad social. Por otro lado es cuantitativo debido a que se apoya en las técnicas estadísticas, sobre todo la encuesta y el análisis estadístico de datos secundarios.

Modalidad básica de la investigación

Bibliográfica documental

La presente investigación es el producto de la recolección y recopilación de información de delitos informáticos de varios textos entre estos: Derecho y

nuevas tecnologías del Dr. Páez Rivadeneira; el peritaje informático y la evidencia digital del Dr. Acuario del Pino; descubriendo los rastros informáticos del Dr. Pascale; la Ley Orgánica de Transparencia y Acceso a la Información Pública, Ley de Garantías Jurisdiccionales; y la Constitución de la República.

De periódicos como El telégrafo, El Universo y de varias páginas del internet como: www.derechoecuador.com;www.revistajudicial.com; www.seguridadpublica.gob.

De campo

La recolección de la información se la realizó de forma directa en el cantón Ambato por parte de la investigadora, la misma que se la obtuvo por medio de entrevistas y diálogos mantenidos con los funcionarios de la Fiscalía Provincial de Tungurahua y los agentes investigadores, compartiendo sus conocimientos en relación con lo que tiene que ver con los delitos informáticos en materia penal su forma de detectarlo y cuál es el procedimiento que conlleva.

Nivel o tipo de la investigación

Exploratorio

La presente investigación sobre los delitos informáticos y el derecho constitucional a la seguridad pública, nos deja un profundo énfasis en la investigación al tratar de conocer cómo se producen este tipo delitos, el procedimiento y la concentración en si para detectarlos en el cantón Ambato, provincia de Tungurahua.

Descriptiva

Se trata de analizar todos los casos que se han producido delitos informáticos de forma que se pueda entender y visualizar la mejor manera de evitar que se produzcan en el cantón Ambato.

Asociación de variables

El tipo de investigación que se condujo es el de asociación de variables, porque permitió analizar, comparar y valorar el grado de correlación y comportamiento de las variables de estudio.

Población y muestra

Para el desarrollo del trabajo investigativo se contará con la ayuda de varios profesionales del Derecho entre ellos: el Fiscal Provincial Tungurahua, fiscales de Ambato, agentes Investigadores, peritos especializados en informática, profesionales en libre ejercicio y personas afectadas.

ESTRATOS	**UNIVERSO**
Fiscal Provincial de Tungurahua	1
Fiscales de la ciudad de Ambato	16
Agentes investigadores	16
Abogados en libre ejercicio especializados en derecho informático	89
Personas afectadas	30
Total	**152**

Cuadro No. 1 Población y muestra
Fuente: Investigadora
Elaboración: Grace Echeverría M

Fórmula aplicada para la muestra

$$n=\frac{Z^2*P(Q)(N)}{N(E)^2+Z^2*(PQ)}$$

$$n=\frac{1.96^2*0.5(0.5)(152)}{152(0.05^2)+1.96^2(0.5)(0.5)}$$

$$n=\frac{3.8416(38)}{152(0.0025)+3.8416(0.25)}$$

$$n=\frac{145.9808}{0.38+0.9604}$$

$$n=\frac{145.9808}{1.3404}$$

n=108.90

Explicación

n=Muestra

N= Universo o Población

Z = Nivel de Confianza (1.96)

P=Probabilidad de éxito 0.5

Q= Probabilidad de fracaso 0.5

E= Margen de error 0.05

El resultado obtenido en la muestra es de 108.908 utilizando la población de 152 lo cual ayudará para el análisis respectivo y aplicando la fórmula adecuada para realizar el respectivo cálculo fundamental para la presente investigación.

OPERACIONALIZACION DE VARIABLES

VARIABLE INDEPENDIENTE: DELITOS INFORMÁTICOS

CONCEPTUALIZACION	DIMENSIONES	INDICADORES	ITEMS	TECNICA INSTRUMENTAL
La relación de una acción que reuniendo las características que delimitan el concepto de delito, se ha llevado acabo, un elemento informático o telemático contra los derechos y libertades de los ciudadanos. Todas aquellas conductas ilícitas susceptible de ser sancionadas por el derecho penal que hacen uso indebido de cualquier medio o sistema informático	Delito Derecho Penal Conducta ilícita	Acto antijurídico Sanciones Penas COIP Normas sancionadoras. Actos ilícitos del sujeto activo. Condena	¿Conoce cómo se produce un delito informático? ¿Confía en las redes informáticas? ¿Han existido víctimas de delitos informáticos? ¿Se puede comprobar si alguien vulnera un sistema informático?	Teórico: Encuesta Instrumento: Cuestionario de encuesta dirigido a Fiscales, Agentes Investigadores y personas afectadas

Cuadro No. 2 V. I: Delitos Informáticos
Fuente: Investigadora
Elaboración: Grace Echeverría

OPERACIONALIZACION DE VARIABLES

VARIABLE DEPENDIENTE: DERECHO CONSTITUCIONAL A LA SEGURIDAD PÚBLICA

CONCEPTUALIZACION	DIMENSIONES	INDICADORES	ITEMS	TECNICA INSTRUMENTAL
Es la garantía que debe brindar el Estado para garantizar los derechos de los ciudadanos. Es un servicio que protege la integridad física de los ciudadanos y sus bienes. Implica que los ciudadanos pueden convivir en armonía, cada uno respetando los derechos individuales del otro. Es la responsabilidad primaria y esencial del Estado con el fin de proteger, garantizar la libertad, la integridad física y el patrimonio de la población ya que son las bases para un desarrollo sólido en lo económico, político y social para tener certidumbre, confianza, orden.	Garantía Derecho Responsabilidad	Protección Tutela judicial efectiva Justo Legítimo Declaración de los Derechos Humanos Tratados Internacionales Estado Policía Nacional Orden Público	¿Publicar información no permitida provoca sanciones? ¿Los sistemas informáticos cuentan con la protección suficiente? ¿La Fiscalía ha resuelto casos en contra de la Seguridad Pública? ¿Es necesario dar a conocer que atentar contra la Seguridad Pública es un acto delictivo?	Teórico: Encuesta Instrumento: Cuestionario de encuesta dirigido a Fiscales, Agentes Investigadores y personas afectadas

Cuadro No. 3 V. D: Derecho Constitucional a la Seguridad Pública
Fuente: Investigadora
Elaboración: Grace Echeverría M

RECOLECCIÓN DE INFORMACIÒN

En este proceso de investigación se encontraron datos que ayudarán a que exista mayor enlace con el trabajo de campo para generar resultados mediante la agrupación, la ordenación y su respectivo análisis. La recolección de información se dará mediante el apoyo de un plan el mismo que contiene preguntas esenciales para el progreso de la investigación

Plan de Recolección de Información

PREGUNTAS BÁSICAS	EXPLICACIÓN
1.- ¿Para Qué?	Para alcanzar los objetivos de investigación
2.- ¿De qué personas u objetos?	Fiscales, Agentes Investigadores, Peritos en Informática ,Abogados en Libre ejercicio, y Personas Afectadas
3.- ¿Sobre qué aspectos?	Variables
4.- ¿Quién? ¿Quiénes?	Investigadora
5.- ¿Cuándo?	Julio 2014
6.- ¿Dónde?	Fiscalía Provincial de Tungurahua
7.- ¿Cuántas veces?	Dos
8.- ¿Qué técnicas de recolección?	Encuesta – Entrevista
9.- ¿Con qué?	Instrumentos: cuestionario entrevista
10.- ¿En qué situación?	En días laborables de las entidades.

Cuadro No. 4 Plan de Recolección de Información
Fuente: Investigadora
Elaboración: Grace Echeverría M.

Procesamiento y Análisis

Plan de procesamiento de la información

Una vez recogida la información a través de las preguntas de las encuestas realizadas se comenzará una previa tabulación utilizando el programa de Excel para la elaboración de los gráficos y así determinar las respectivas estadísticas que servirán de base fundamental para el profundo análisis e interpretación de los datos obtenidos.

Pasos:

1) Recopilar datos.
2) Definir las variables para obtener los datos.
3) Definir las herramientas estadísticas.
4) Activar el programa de computadora, elaboración de tablas de ingreso de datos, realizar cálculos.
5) Verificar los datos y resultados.
6) Representación gráfica y su interpretación correspondiente.
7) Imprimir resultados.

Análisis e interpretación de resultados

El análisis e interpretación de resultados se dará de acuerdo a los porcentajes obtenidos con los valores señalados tanto en los cuadros como en los gráficos, es decir dando a conocer lo que se ha obtenido luego de las respuestas recibidas de cada pregunta formulada en las encuestas y comparándolas , partiendo sobretodo del plan de procesamiento de información recogida.

CAPÍTULO IV

ANÁLISIS DE RESULTADOS

Análisis e interpretación de Datos

Para alcanzar la metodología propuesta y el plan para el procesamiento de la información, se utilizaron las técnicas de la Encuesta y la Entrevista, diseñadas para investigar a la población determinada.

Con la respectiva aplicación de las encuestas y las entrevistas, se procede a la tabulación respectiva, a través de la cual se dará vida a la propuesta que pretende establecer el resultado de la investigación.

Se procede con un gran énfasis a detallar los resultados obtenidos de las encuestas, las cuales están representadas mediante cuadros estadísticos y el respectivo análisis e interpretación de cada pregunta formulada en el cuestionario

ENCUESTA REALIZADA A 89 ABOGADOS EN LIBRE EJERCICIO DE LA CIUDAD DE AMBATO.

1. **¿Cree usted que la mayor parte de delitos informáticos persiguen fines económicos?**

Cuadro No. 5 Pregunta No. 1

Respuesta	Frecuencia	Porcentaje
SI	**50**	56%
No	**39**	44%
Total	**89**	100%

Elaborado por: Grace Echeverría
Fuente: Encuesta realizada a Abogados en libre ejercicio

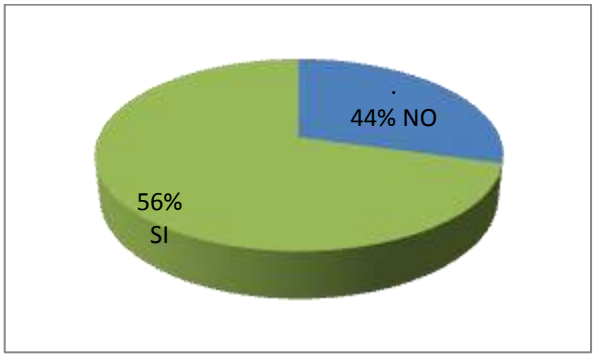

Gráfico No. 5 Pregunta No. 1
Fuente: Encuesta realizada a Abogados en libre ejercicio
Elaborado por: Grace Echeverría M

Análisis: El 56% de los abogados en libre ejercicio respondió que los delitos informáticos persiguen fines económicos, mientras que el 44% respondió que no.

Interpretación: Se puede deducir que los delitos informáticos persiguen fines económicos, esto es lo que más atrae a los ciberinfractores y por eso tratan de infiltrarse a las redes informáticas para la obtención de dinero de una manera ilícita perjudicando a la sociedad.

2. Ha sido víctima de algún tipo de delito informático?

Cuadro No. 6 Pregunta No. 2

Respuesta	Frecuencia	Porcentaje
Si	**36**	41%
No	**53**	59%
Total	**89**	100%

Elaborado por: Grace Echeverría
Fuente: Encuesta realizada a Abogados en libre ejercicio

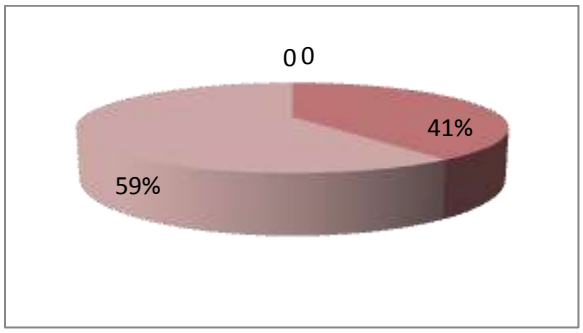

Gráfico No. 6 Pregunta No. 2
Fuente: Encuesta realizada a Abogados en libre ejercicio
Elaborado por: Grace Echeverría M

Análisis: EL 59% de encuestados no ha sido víctima de delitos informáticos, y el 41% en algún momento de su vida fueron si fueron víctimas de delitos informáticos.

Interpretación: Se puede deducir que los delitos informáticos pueden ocasionar un gran daño a todas las personas en cualquier momento de la vida ya que no se está excepto de que pueda ser víctima de esto por tal motivo hay que estar preparados y proteger las cuentas, los ingresos, las claves y no confiar en las redes informáticas que aunque la mayor parte de abogados en libre ejercicio no han sido víctimas de un delito informático quien nos asegura que nosotros no podamos serlo.

3. **¿Considera usted, que su derecho a la intimidad es violentado utilizando el internet u otro mecanismos de sistema informático?**

Cuadro No. 7 Pregunta No. 3

Respuesta	Frecuencia	Porcentaje
Si	**83**	94%
No	**6**	6%
Total	**89**	100%

Elaborado por: Grace Echeverría
Fuente: Encuesta realizada a Abogados en libre ejercicio

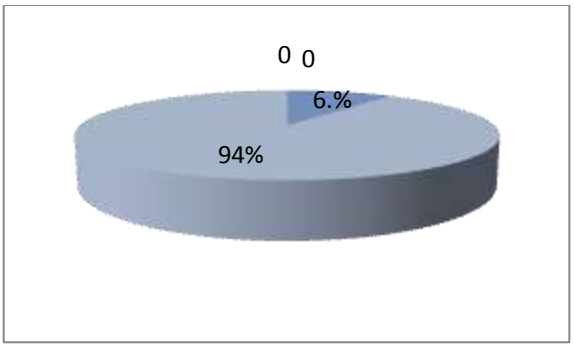

Gráfico No. 7 Pregunta No.3
Fuente: Encuesta realizada a Abogados en libre ejercicio
Elaborado por: Grace Echeverría M

Análisis: El 94% los profesionales en libre ejercicio encuestados considera que si afecta el derecho a la intimidad las comunicaciones en internet, mientras el 6% no considera que esto afecte su derecho a la intimidad.

Interpretación: El internet hoy en día es muy importante sin embargo al obtener los datos de la encuesta se puede deducir que el derecho a la intimidad si se ve afectado utilizando cualquier sistema informático, por consiguiente es necesario mantener protegidos nuestros datos para que terceras personas con ánimo de causar daño no se aprovechen de las circunstancias y se dé inicio a ser un perjudicado por los diversos tipos de delitos informáticos.

4. ¿Considera usted, que las compras a través de internet son seguras?

Cuadro No. 8 Pregunta No. 4

Respuesta	Frecuencia	Porcentaje
SI	**14**	16%
No	**75**	84%
Total	**89**	100%

Elaborado por: Grace Echeverría
Fuente: Encuesta realizada a Abogados en libre ejercicio

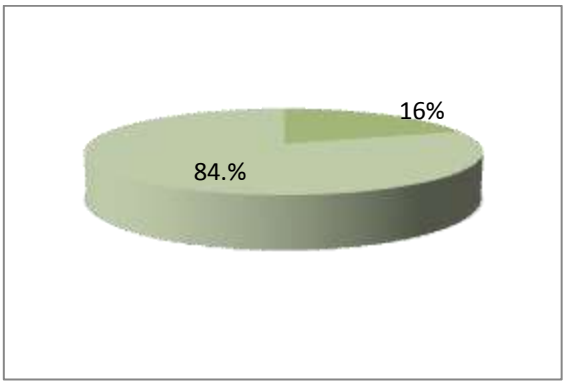

Gráfico No. 8 Pregunta No. 4
Fuente: Encuesta realizada a Abogados en libre ejercicio
Elaborado por: Grace Echeverría M

Análisis: El 16% de los encuestados piensa que sí son seguras las compras por internet mientras que el 84% dice que no es nada seguro las compras a través del internet.

Interpretación: La tecnología sigue avanzando así como también la inseguridad social, no hay que confiar en las compras por internet ya que pueden ser datos falsos, por ende la mayor parte de encuestados contestaron que no son para nada seguras las compras a través de internet.

5. **¿Según su propia experiencia considera usted, que en la investigación de los delitos informáticos existe alguna dificultad?**

Cuadro No. 9 Pregunta No.

Respuesta	Frecuencia	Porcentaje
Si	**78**	88%
No	**11**	12%
Total	**89**	100%

Elaborado por: Grace Echeverría
Fuente: Encuesta realizada a Abogados en libre ejercicio

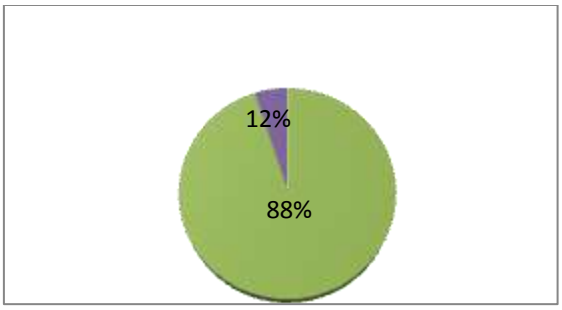

Gráfico No. 9 Pregunta No. 5
Fuente: Encuesta realizada a Abogados en libre ejercicio
Elaborado por: Grace Echeverría M

Análisis: El 12% de los encuestados piensa que en la investigación de los delitos informáticos no tiene conflictos mientras que el 88% afirman que si existen una gran contradicción para la investigación de los delitos informáticos.

Interpretación: Es indispensable mencionar que existe una gran dificultad para las investigaciones de los delitos informáticos ya que son muy difíciles de detectar y por consiguiente una exhaustiva búsqueda de comprobar si las sospechas son correctas pero para esto existen los peritos en informática capaces de realizar una profunda investigación.

6. **¿Piensa usted que deberían existir fuertes sanciones en el Código Orgánico Integral Penal para los que realicen algún tipo de delito informático?**

Cuadro No. 10 Pregunta No. 6

Respuesta	Frecuencia	Porcentaje
Si	**84**	94%
No	**5**	6%
Total	**89**	100%

Elaborado por: Grace Echeverría
Fuente: Encuesta realizada a Abogados en libre ejercicio

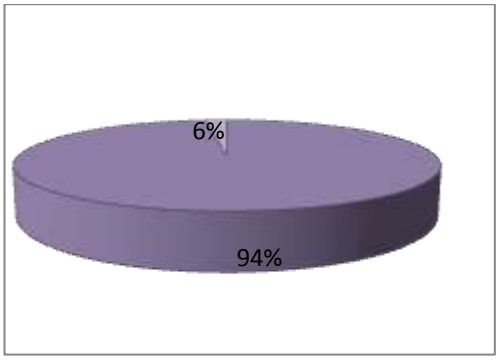

Gráfico No. 10 Pregunta No. 6
Fuente: Encuesta realizada a Abogados en libre ejercicio
Elaborado por: Grace Echeverría M

Análisis: El 94% de los encuestados piensa que es necesaria la implementación de fuertes sanciones en el COIP para los que cometan un delito informático, mientras que el 6% determina que no es necesario.

Interpretación: Nos encontramos en un mundo con avance y cambios por ende para combatir los delitos informáticos es muy necesaria la implementación de fuertes sanciones para que los sujetos que cometen este tipo de delitos no ocasionen ningún daño a las personas.

7. **¿Considera usted que la seguridad pública contemplada en la Constitución corre riesgos al manipular los sistemas informáticos?**

Cuadro No. 11 Pregunta No. 7

Respuesta	Frecuencia	Porcentaje
Si	**87**	98%
No	**2**	2%
Total	**89**	100%

Elaborado por: Grace Echeverría
Fuente: Encuesta realizada a Abogados en libre ejercicio

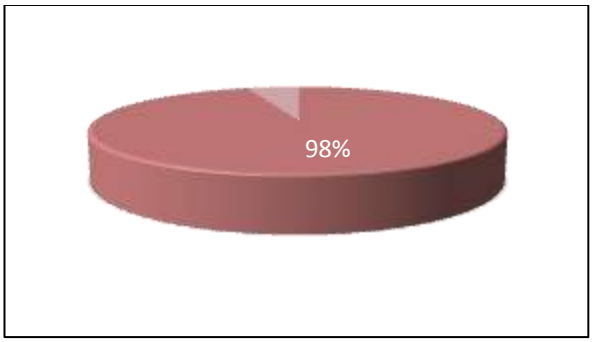

Gráfico No. 11 Pregunta No. 7
Fuente: Encuesta realizada a Abogados en libre ejercicio
Elaborado por: Grace Echeverría M

Análisis: El 98% de los encuestados respondieron que la seguridad pública si corre riesgos al manipular los sistemas informáticos, y el 2% manifiesta que no corre ningún tipo de riesgo la seguridad pública.

Interpretación: La seguridad pública es lo que más se debe proteger ante los ataques a un Estado ya que corre riesgos la seguridad de la ciudadanía por tal razón está consagrado en la Constitución, la mayor parte de encuestado contestó que la seguridad pública si corre riesgos al manipular los sistemas informáticos protegidos.

8. ¿Conoce el procedimiento que se da a los delitos informáticos?

Cuadro No. 12 Pregunta No. 8

Respuesta	Frecuencia	Porcentaje
Si	**77**	87%
No	**12**	13.%
Total	**89**	100%

Elaborado por: Grace Echeverría
Fuente: Encuesta realizada a Abogados en libre ejercicio

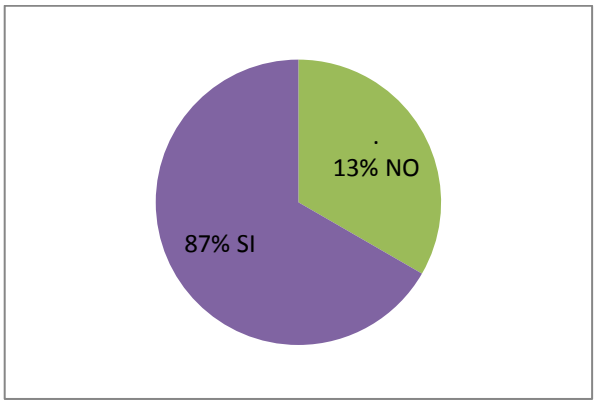

Gráfico No. 12 Pregunta No. 8
Fuente: Encuesta realizada a Abogados en libre ejercicio
Elaborado por: Grace Echeverría M

Análisis: El 13% de los encuestados no conoce el procedimiento que se da en los delitos informáticos mientras que el 87% si conoce el procedimiento de este tipo de delitos.

Interpretación: Se puede emitir un juicio de valor afirmando que los abogados en libre ejercicio encuestados si conocen el procedimiento que se da cuando ocurre un delito informático y cuentan con una gran preparación para resolverlos.

9. **¿Piensa usted que la revelación de datos de una persona afecta directamente a su integridad?**

Cuadro No. 13 Pregunta No. 9

Respuesta	Frecuencia	Porcentaje
Si	**87**	98%
No	**2**	2%
Total	**89**	100%

Elaborado por: Grace Echeverría
Fuente: Encuesta realizada a Abogados en libre ejercicio

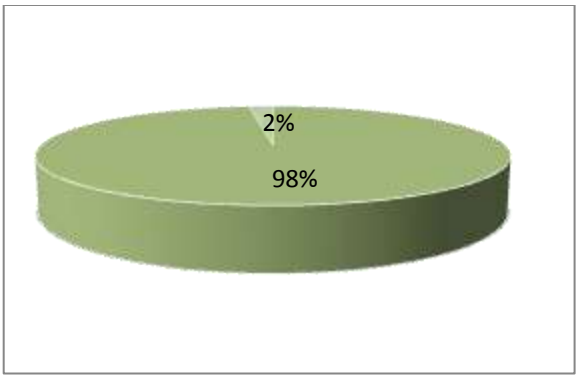

Gráfico No. 13 Pregunta No. 9
Fuente: Encuesta realizada a Abogados en libre ejercicio
Elaborado por: Grace Echeverría M

Análisis: El 98% de los encuestados piensan que si afecta la revelación de datos a la integridad de las personas, y el 2% afirma que no existe ningún daño a la integridad de las personas.

Interpretación: Se puede recalcar que la revelación de datos si afecta directamente a la integridad de la víctima ya que su vida privada está siendo conocida por todos y su prestigio está en boca de todas las personas al darse una promulgación de su intimidad ante la sociedad.

10. ¿Conoce los cuerpos legales que sancionan a los delitos informáticos?

Cuadro No. 14 Pregunta No. 10

Respuesta	Frecuencia	Porcentaje
Si	**88**	99%
No	**1**	1%
Total	**89**	100%

Elaborado por: Grace Echeverría
Fuente: Encuesta realizada a Abogados en libre ejercicio

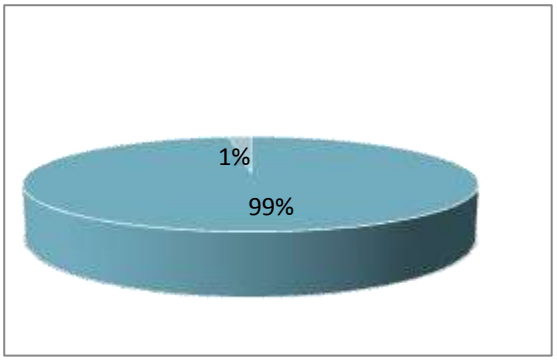

Gráfico No. 14 Pregunta No. 10
Fuente: Encuesta realizada a Abogados en libre ejercicio
Elaborado por: Grace Echeverría M

Análisis: EL 99% de los abogados en libre ejercicio si conocen los cuerpos legales que sancionan a los delitos informáticos, y el 1% de los encuestados no conocen las normas sancionadoras para este tipo de delitos.

Interpretación: Es necesario para la protección el conocimiento de los cuerpos legales que sancionan el cometimiento de un delito informático y al obtener los datos se puede deducir que es realmente prioritario el conocimiento de los cuerpos legales que existen para la respectiva defensa y sanción de un presunto delito informático.

ENCUESTA DIRIGIDA A 17 FISCALES, 16 AGENTES INVESTIGADORES DE LA CIUDAD DE AMBATO

1. **¿Para detectar un delito informático es necesario que la víctima aporte todos los elementos probatorios pertinentes?**

Cuadro No. 15 Pregunta No. 1

Respuesta	Frecuencia	Porcentaje
Si	**28**	84%
No	**5**	16%
Total	**33**	100%

Elaborado por: Grace Echeverría
Fuente: Encuesta realizada a Fiscales, Agentes Investigadores

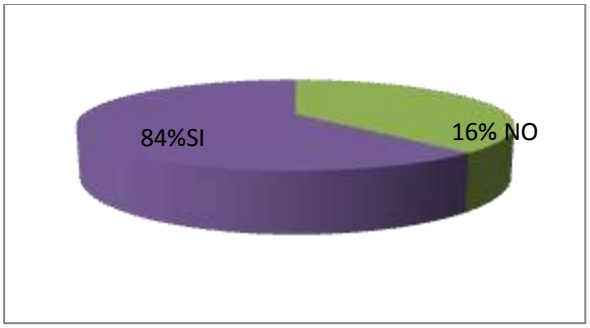

Gráfico No. 15 Pregunta No. 1
Fuente: Fiscales, Agentes Investigadores
Elaborado por: Grace Echeverría M

Análisis: El 16% de los encuestados no consideran necesario que la víctima sea quien entregue los elementos probatorios para la investigación de un delito informático, mientras que el 84% admite que si es necesario que exista colaboración por parte de la víctima al entregar todos los elementos que tenga en su persona en cuanto corresponda a un delito informático.

Interpretación: La colaboración de la víctima en estos casos es indiscutible ya los elementos probatorios que tenga en sus manos propiciaran o ayudaran a que la investigación sea más rápida y se pueda encontrar a los responsables del delito informático.

2. **¿Considera usted que la seguridad pública está siendo vulnerada con el cometimiento de un delito informático?**

Cuadro No. 16 Pregunta No. 2

Respuesta	Frecuencia	Porcentaje
Si	**32**	97%
No	**1**	3%
Total	**33**	100%

Elaborado por: Grace Echeverría
Fuente: Encuesta realizada a Fiscales, Agentes Investigadores

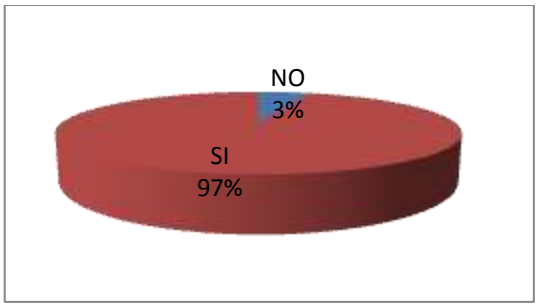

Gráfico No. 16 Pregunta No. 2
Fuente: Fiscales, Agentes Investigadores
Elaborado por: Grace Echeverría M

Análisis: El 97% de los encuestados respondieron que la seguridad pública si es vulnerada con el cometimiento de un delito informático, mientras que el 3% piensa que no.

Interpretación: Se puede emitir un juicio de valor al revisar los datos obtenidos y los delitos informáticos si vulneran a la seguridad Pública de nuestro País perjudicándola notablemente impidiendo la tranquilidad de la ciudadanía.

3. **¿El ciberinfractor de un delito informático puede realizar chantajes o extorsión a las víctimas?**

Cuadro No. 17 Pregunta No. 3

Respuesta	Frecuencia	Porcentaje
Si	**31**	94%
No	**2**	6%
Total	**33**	100%

Elaborado por: Grace Echeverría
Fuente: Encuesta realizada a Fiscales, Agentes Investigadores

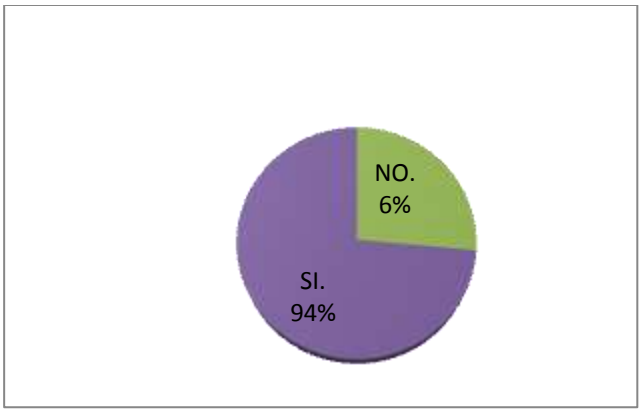

Gráfico No. 17 Pregunta No. 3
Fuente: Fiscales, Agentes Investigadores
Elaborado por: Grace Echeverría M

Análisis: El 6% respondió que un ciberinfractor no recurre a los chantajes o extorción en el caso de un delito informático, mientras que el 94% afirma que un ciberinfractor luego de realizar un delito informático va al camino del chantaje y extorción de sus víctimas.

Interpretación: Es preocupante que un ciberinfractor luego de cometer un delito informático da el paso de los chantajes y extorción de sus víctimas con el fin de perjudicar y obtener beneficios de la misma.

4. **¿Conoce los cuerpos legales que han sido utilizados para la sanciones de los delitos informáticos?**

Cuadro No. 18 Pregunta No. 4

Respuesta	Frecuencia	Porcentaje
Si	**33**	100%
No	**0**	0%
Total	**33**	100%

Elaborado por: Grace Echeverría
Fuente: Encuesta realizada a Fiscales, Agentes Investigadores

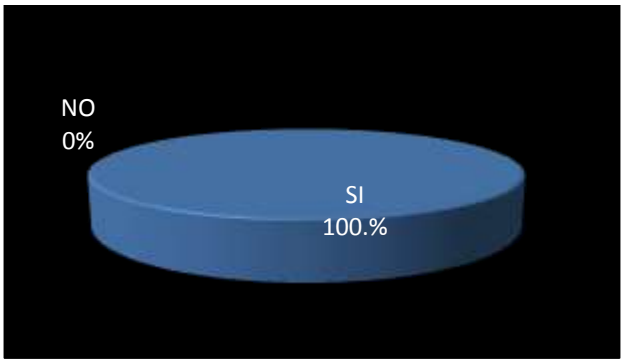

Gráfico No. 18 Pregunta No. 4
Fuente: Fiscales, Agentes Investigadores
Elaborado por: Grace Echeverría M

Análisis: El 100% de los encuestados conoce los cuerpos legales utilizados en los casos de los delitos informáticos.

Interpretación: Con la obtención de los resultados se puede deducir que la preparación es necesaria a través de los cuerpos legales que han sido utilizados para sancionar el cometimiento de un delito informático.

5. **¿En la actualidad los casos de delitos informáticos han aumentado el riesgo de la ciudadanía?**

Cuadro No. 19 Pregunta No. 5

Respuesta	Frecuencia	Porcentaje
Si	**27**	81%
No	**6**	19%
Total	**33**	100%

Elaborado por: Grace Echeverría
Fuente: Encuesta realizada a Fiscales, Agentes Investigadores

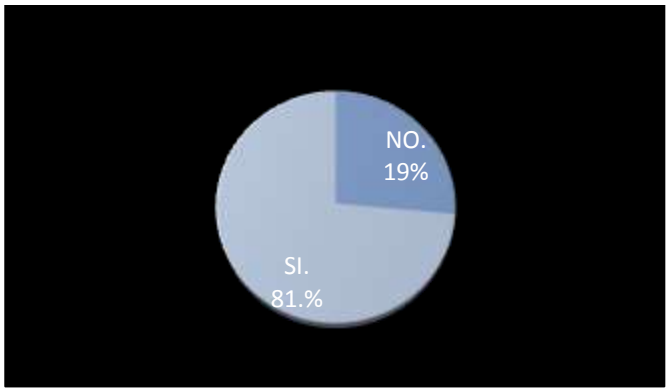

Gráfico No. 19 Pregunta No. 5
Fuente: Fiscales, Agentes Investigadores
Elaborado por: Grace Echeverría M

Análisis: El 81% de encuestados afirman que los delitos informáticos aumentan considerablemente los riesgos de la ciudadanía, mientras que el 19% piensa que los delitos informáticos no aumentan los riegos en la ciudad.

Interpretación: Al emitir un juicio de valor se puede dar a conocer que los delitos informáticos aumentan los riesgos en la ciudad de confiabilidad en todos los ámbitos por eso hay que estar preparados para evitar ser víctimas de estos delitos informáticos.

6. **¿Piensa usted que deberían existir fuertes sanciones en el Código Orgánico Integral Penal para los que realicen algún tipo de delito informático?**

Cuadro No. 20 Pregunta No. 6

Respuesta	Frecuencia	Porcentaje
Si	**32**	97%
No	**1**	3%
Total	**33**	100%

Elaborado por: Grace Echeverría
Fuente: Encuesta realizada a Fiscales, Agentes Investigadores

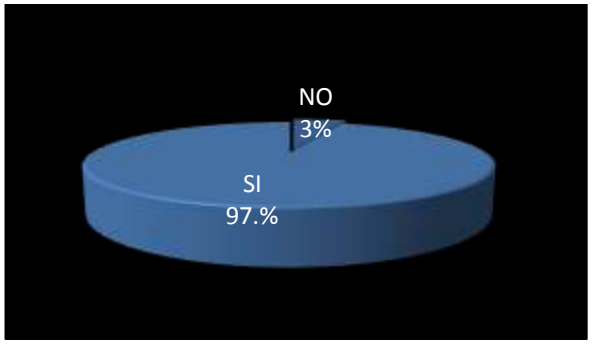

Gráfico No. 20 Pregunta No. 6
Fuente: Fiscales, Agentes Investigadores
Elaborado por: Grace Echeverría M

Análisis: El 97% de los encuestados respondió que deberían existir fuertes sanciones para las personas que cometan un delito informático, mientras que 3% afirma que no debe existir tanta rigidez en las sanciones

Interpretación: La sociedad debe contar con respaldo y seguridad ya que es un requisito primordial que existan fuertes sanciones en el nuevo Código Integral Penal para los sujetos que cometan algún tipo de delito informático.

7. **¿Cree usted que la mayor parte de delitos informáticos persiguen fines económicos?**

Cuadro No. 21 Pregunta No. 7

Respuesta	Frecuencia	Porcentaje
Si	**29**	87%
No	**4**	13%
Total	**33**	100%

Elaborado por: Grace Echeverría
Fuente: Encuesta realizada a Fiscales, Agentes Investigadores

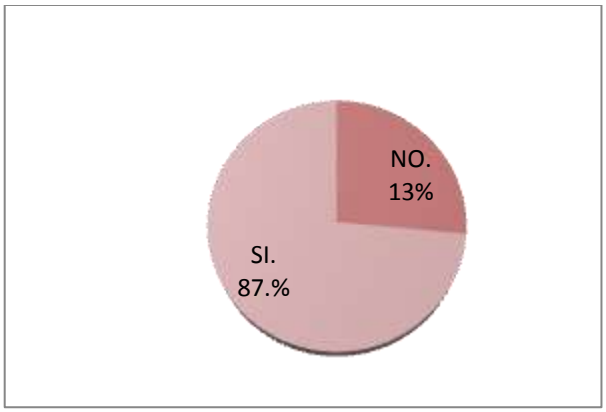

Gráfico No. 21 Pregunta No. 7
Fuente: Fiscales, Agentes Investigadores
Elaborado por: Grace Echeverría M

Análisis: El 87% de los encuestados contestó que los delitos informáticos en su mayoría persiguen fines económicos y el 13% respondió que los delitos informáticos no son tomados en cuenta en su mayoría para la persecución de fines económicos.

Interpretación: Todo delito tiene un fin en común pero en los casos de delitos informáticos en su gran cantidad persiguen fines económicos como una forma de enriquecimiento ilegal.

8. **¿Considera usted que la seguridad a los datos personales es altamente prioritaria en la ciudad de Ambato?**

Cuadro No. 22 Pregunta No. 8

Respuesta	Frecuencia	Porcentaje
Si	**31**	94%
No	**2**	6%
Total	**33**	100%

Elaborado por: Grace Echeverría
Fuente: Encuesta realizada a Fiscales, Agentes Investigadores

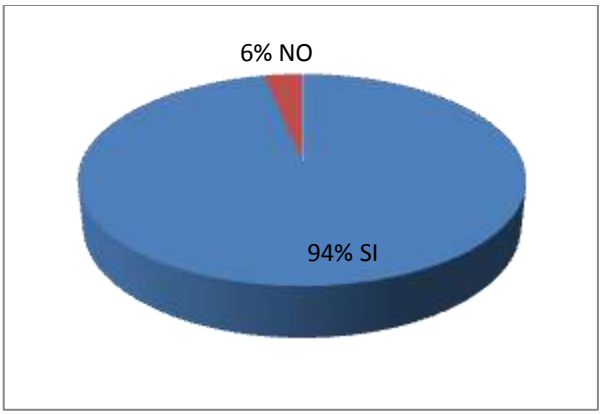

Gráfico No. 22 Pregunta No. 8
Fuente: Fiscales, Agentes Investigadores
Elaborado por: Grace Echeverría M

Análisis: El 94% de los encuestados respondió que sí existe gran prioridad a la seguridad de datos personales mientras que el 6% contesto que no.

Interpretación: Al obtener los resultados se puede determinar que existe una gran preocupación en cuanto a la seguridad de los datos personales de tal manera que se protejan estos derechos de una manera prioritaria.

9. **¿Cree usted que el avance tecnológico en las redes informáticas ha producido un conflicto social que afecta derechos de las personas actualmente?**

Cuadro No. 23 Pregunta No. 9

Respuesta	Frecuencia	Porcentaje
Si	**26**	77%
No	**7**	23%
Total	**33**	100%

Elaborado por: Grace Echeverría
Fuente: Encuesta realizada a Fiscales, Agentes Investigadores

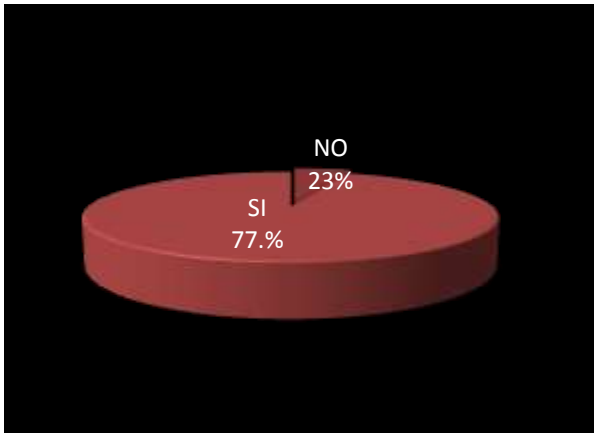

Gráfico No. 23 Pregunta No. 8
Fuente: Fiscales, Agentes Investigadores
Elaborado por: Grace Echeverría M

Análisis: El 77% respondió que el avance tecnológico en las redes informáticas si produce un conflicto social atentando a los derechos de las personas mientras que el 23% contesto que no.

Interpretación: Al tabular los datos obtenidos se demuestra claramente que existe un conflicto social en cuanto se refiere a los derechos de las personas con el constante avance tecnológico existente.

10. ¿Considera usted que los delitos informáticos impiden que exista una Seguridad Pública conforme al derecho Constitucional?

Cuadro No. 24 Pregunta No. 10

Respuesta	Frecuencia	Porcentaje
Si	**33**	100%
No	**0**	0%
Total	**33**	100%

Elaborado por: Grace Echeverría
Fuente: Encuesta realizada a Fiscales, Agentes Investigadores

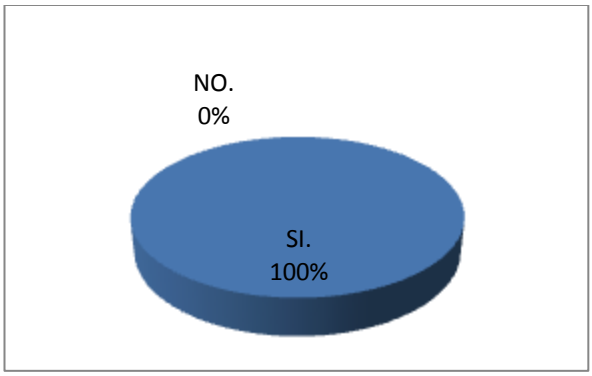

Gráfico No. 24 Pregunta No. 10
Fuente: Fiscales, Agentes Investigadores
Elaborado por: Grace Echeverría M

Análisis: El 100% de los encuestados respondió que los delitos informáticos si impiden que exista una Seguridad Publica conforme al derecho Constitucional.

Interpretación: Se puede deducir que los delitos informáticos de una u otra manera dificultan u obstaculizan una Seguridad Pública según lo contempla nuestra Constitución de la República.

ENCUESTA REALIZADA A 30 PERSONAS AFECTADAS

1. **¿Conoce usted de que se trata un delito informático?**

Cuadro No. 25 Pregunta No. 1

Respuesta	Frecuencia	Porcentaje
Si	**30**	100%
No	**0**	0%
Total	**30**	100%

Elaborado por: Grace Echeverría
Fuente: Personas afectadas

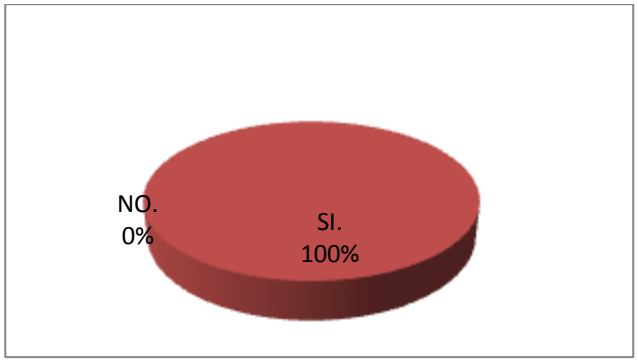

Gráfico No. 25 Pregunta No. 1
Fuente: Personas afectadas
Elaborado por: Grace Echeverría M

Análisis: El 100% de las personas afectadas conocen de qué se trata un delito informático.

Interpretación: Las personas que han sido víctimas de un delito informático conocen por su experiencia social lo que son este tipo de delitos y el daño que ocasionan.

2. **¿Considera usted que los sistemas informáticos necesitan protección en la actualidad.**

Cuadro No. 26 Pregunta No. 2

Respuesta	Frecuencia	Porcentaje
Si	**28**	93%
No	**2**	7%
Total	**30**	100%

Elaborado por: Grace Echeverría
Fuente: Personas afectadas

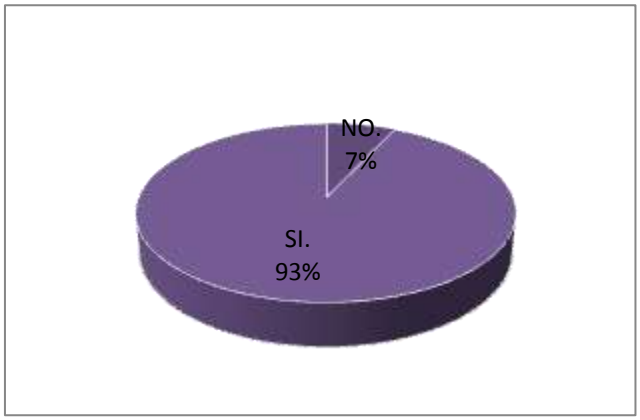

Gráfico No. 26 Pregunta No. 2
Fuente: Personas afectadas
Elaborado por: Grace Echeverría M

Análisis: El 93% de encuestados respondió que si es necesario que exista una mayor protección de los sistemas informáticos y el 7% respondió que no.

Interpretación: Debe existir mayor relevancia en la protección de los sistemas informáticos ya que actualmente están siendo manipulados y a través de los mismos se están vulnerando los derechos de las personas.

3. **¿Cree usted que la mayor parte de delitos informáticos persiguen fines económicos?**

Cuadro No. 27 Pregunta No. 3

Respuesta	Frecuencia	Porcentaje
Si	**27**	90%
No	**3**	10%
Total	**30**	100%

Elaborado por: Grace Echeverría
Fuente: Personas afectadas

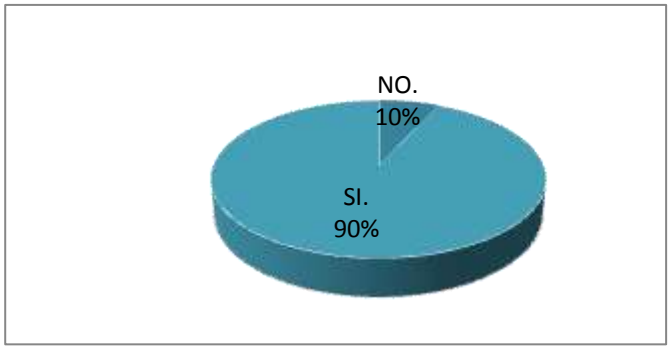

Gráfico No. 27 Pregunta No. 3
Fuente: Personas afectadas
Elaborado por: Grace Echeverría M

Análisis: el 90% de los encuestados opinan que los delitos informáticos persiguen fines económicos, mientras que el 10%respondió que no.

Interpretación: Los delitos informáticos son actos silenciosos que ocultan responsables por ende lo que buscan es obtener beneficios económicos perjudicando a las víctimas.

4. ¿Considera usted que los delitos informáticos son fáciles de detectar?

Cuadro No. 28 Pregunta No. 4

Respuesta	Frecuencia	Porcentaje
Si	**12**	40%
No	**18**	60%
Total	**30**	100%

Fuente: Personas afectadas
Elaborado por: Grace Echeverría M

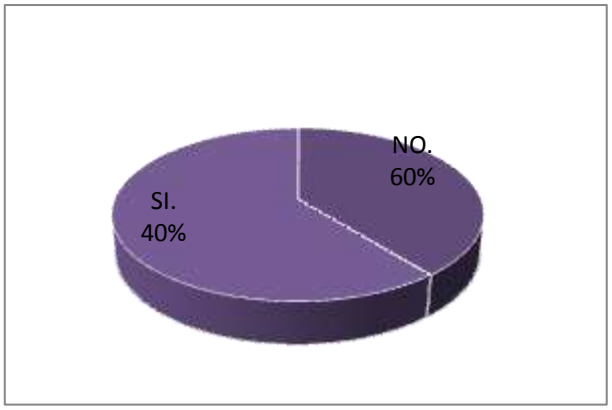

Gráfico No. 28 Pregunta No. 4
Fuente: Personas afectadas
Elaborado por: Grace Echeverría M

Análisis: El 60% de los encuestados piensa que los delitos informáticos no son fáciles de detectar, mientras que el 40% respondió que si son fáciles de detectarlos.

Interpretación: Existe un ardua investigación ya que los delitos informáticos no son fáciles de detectar ya que los realizan personas con una habilidad impresionante en la informática.

5. **¿Considera usted que la seguridad pública contemplada en la Constitución corre riesgos al manipular los sistemas informáticos?**

Cuadro No. 29 Pregunta No. 5

Respuesta	Frecuencia	Porcentaje
Si	**30**	100%
No	**0**	0%
Total	**30**	100%

Fuente: Personas afectadas
Elaborado por: Grace Echeverría M

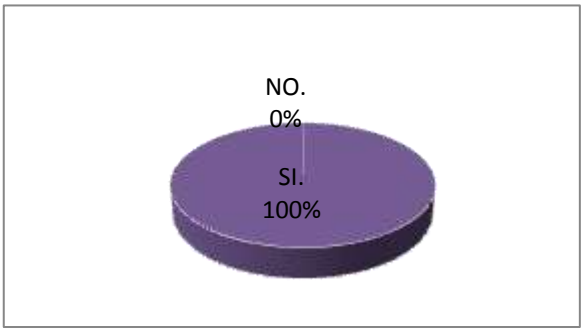

Gráfico No. 29 Pregunta No. 5
Fuente: Personas afectadas
Elaborado por: Grace Echeverría M

Análisis: El 100% de los encuestados respondió que la seguridad pública corre grandes riesgos con la manipulación de los sistemas informáticos.

Interpretación: Se puede emitir un juicio de valor de la información obtenida por el simple hecho de que la seguridad pública si corre un gran riesgo por la aparición de sujetos sin ningún temor a la ley que manipulan la información en los sistemas informáticos.

6. **¿Piensa usted que deberían existir fuertes sanciones en el Código Orgánico Integral Penal para los que realicen algún tipo de delito informático?**

Cuadro No. 30 Pregunta No. 6

Respuesta	Frecuencia	Porcentaje
Si	**30**	100%
No	**0**	0%
Total	**30**	100%

Fuente: Personas afectadas
Elaborado por: Grace Echeverría M

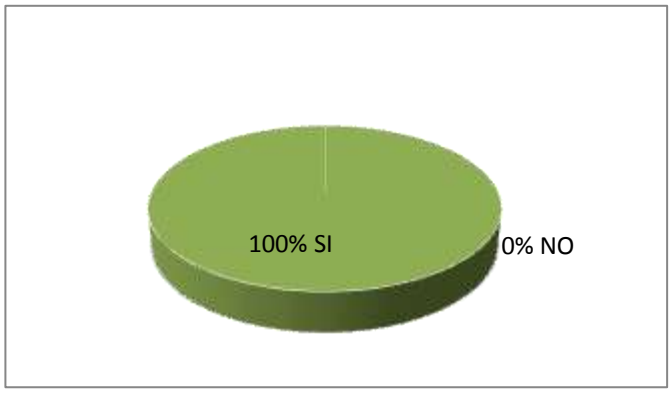

Gráfico No. 30 Pregunta No. 6
Fuente: Personas afectadas
Elaborado por: Grace Echeverría M

Análisis: El 100% de los encuestados respondió que si debe existir fuertes sanciones a las personas que cometan delitos informáticos.

Interpretación: Al ser víctima de un delito informático se debe sentir una gran impotencia a que permanezca en la impunidad estos actos delictivos por ende el Código Orgánico Integral Penal debe mantener sanciones para los que cometan este tipo de delitos sin saltarse ningún tema impidiendo que existan vacíos legales.

7. **¿Considera usted que los delitos informáticos ocasionan daños a la integridad de una persona?**

Cuadro No. 31 Pregunta No. 7

Respuesta	Frecuencia	Porcentaje
Si	**19**	63%
No	**11**	37%
Total	**30**	100%

Fuente: Personas afectadas
Elaborado por: Grace Echeverría M

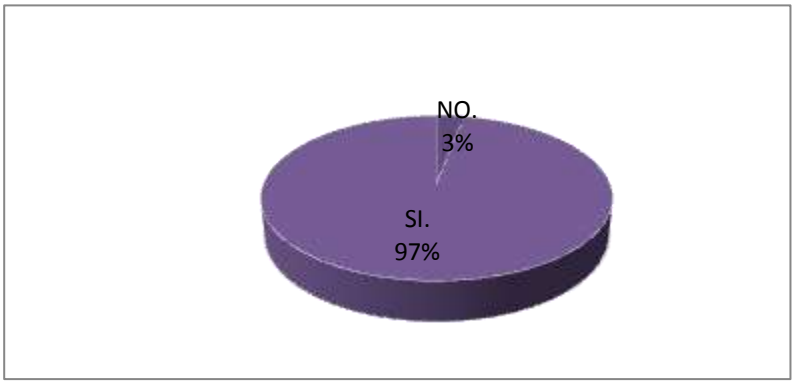

Gráfico No. 31 Pregunta No. 7
Fuente: Personas afectadas
Elaborado por: Grace Echeverría M

Análisis: El 63% de los encuestados respondió que los delitos informáticos si ocasionan daños a la integridad de una persona, y el 37% contesto que no.

Interpretación: Los delitos informáticos si ocasionan daños a la integridad de una persona perjudicándola ya que la información privada al estar en manos equivocadas ocasionarán la divulgación sin consentimiento de la persona afectada.

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

Cuadro No. 32 Pregunta No. 8

Respuesta	Frecuencia	Porcentaje
Si	**22**	73%
No	**8**	27%
Total	**30**	100%

Fuente: Personas Afectadas
Elaborado por: Grace Echeverría M

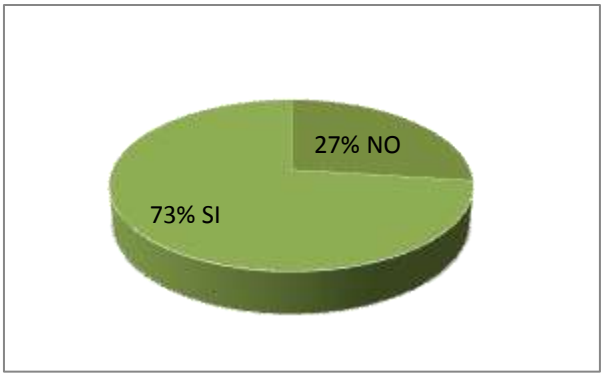

Gráfico No. 32 Pregunta No. 8
Fuente: Personas afectadas
Elaborado por: Grace Echeverría M

Análisis: El 73% de los encuestados contestó que las autoridades de administración de justicia si están preparados para resolver delitos informáticos, mientras que el 27% respondió que no.

Interpretación: Las autoridades encargadas de la administración de justicia de nuestro País se hallan con la preparación suficiente para atender, conocer y resolver los casos de delitos informáticos

9. **¿Conoce usted los cuerpos legales que sancionan el cometimiento de un delito informático?**

Cuadro No. 33 Pregunta No. 9

Respuesta	Frecuencia	Porcentaje
Si	**17**	57%
No	**13**	43%
Total	**30**	100%

Fuente: Personas afectadas
Elaborado por: Grace Echeverría M

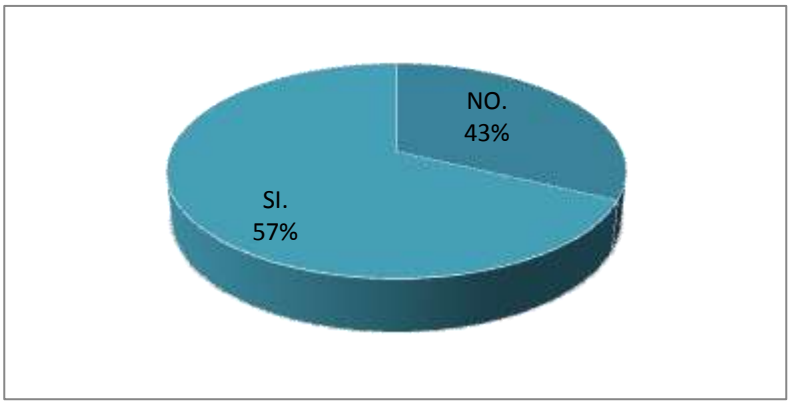

Gráfico No. 33 Pregunta No. 9
Fuente: Personas afectadas
Elaborado por: Grace Echeverría M

Análisis: El 57% de los encuestados respondió que si conoce los cuerpos legales que sancionan el cometimiento de delitos informáticos, y el 43% respondió que no.

Interpretación: Con los datos obtenidos se puede deducir que por la experiencia que han tenido si conocen los cuerpos legales que sancionan el cometimiento de un delito informático.

10. ¿Considera usted que es necesario que exista mayor información para la seguridad de las personas de tal manera que se hallen prevenidas ante este tipo de delitos?

Cuadro No. 34 Pregunta No. 10

Respuesta	Frecuencia	Porcentaje
Si	**30**	100%
No	**0**	0%
Total	**30**	100%

Fuente: Personas afectadas
Elaborado por: Grace Echeverría M

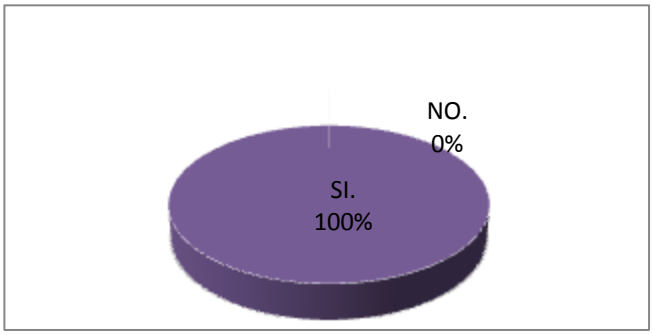

Gráfico No. 34 Pregunta No. 10
Fuente: Personas afectadas
Elaborado por: Grace Echeverría M

Análisis: El 100% de los encuestados contesto que si debería existir mayor información de tal modo que se pueda estar prevenido ante un delito informático.

Interpretación: Se puede deducir que es necesario que exista mayor información para que la ciudadanía se encuentre en alerta, de forma precavida e impidiendo que terceras personas se conviertan en dueños de lo que no es suyo y afecten a través de los sistemas informáticos, perjudicando a la sociedad.

Verificación de la Hipótesis

Para el trabajo de investigación con el único fin de obtener datos claros precisos por excelencia es Chi Cuadrado que nos permite obtener información con la que aceptamos o rechazamos la hipótesis.

Combinación de Frecuencias

Para establecer la correspondencia de las tablas se eligió cuatro preguntas de las encuestas, dos por cada variable de estudio, esto permitirá efectuar el proceso para obtener la combinación o relación necesaria.

Planteamiento de la Hipótesis

H.0. Los delitos informáticos No inciden en el Derecho Constitucional a la Seguridad Publica.

H.1. Los delitos informáticos Si inciden en el Derecho Constitucional a la Seguridad Pública.

Selección del Nivel de significación

Se utiliza el $\infty = 0.01$

Los pasos para verificar la hipótesis son reunir información, compararla con posibles explicaciones, escoger la explicación más probable y formular una o más hipótesis. Después de hacer todos estos pasos se realiza una experimentación en la cual se confirma o no la hipótesis.

Especificaciones del Estadístico

De acuerdo a la tabla de contingencia 4 x 2 utilizaremos la fórmula. 102

$$X2 = \frac{\Sigma\,(0-E)^2}{E}$$

Donde

X2 = Chi o Ji Cuadrado

Σ = Sumatoria

0 = Frecuencias Observadas

E = Frecuencia Esperada

Especializaciones de la región de aceptación y rechazo

Para indicar sobre estas regiones primeramente determinaremos todos los grados de libertad conociendo que el cuadrado está formado por 4 filas y 2 columnas.

gl = (f – 1) . (c – 1)
gl = (4 – 1) . (2 – 1)
gl = (3) - (1)
gl = 3

Entonces con el 3 gl y el nivel de 0.01 tenemos la tabla de X2 siendo el valor de 11.35 por consiguiente se acepta la hipótesis nula para todos los valores de Ji Cuadrado que se encuentran hasta el valor 11.35 y se rechaza la hipótesis nula cuando los valores calculados son mayores a 11.35.

Recolección de datos de los cálculos de las estadísticas

PREGUNTAS	**CATEGORÍAS**		**Subtotal**
	SI	**NO**	
¿Conoce usted los cuerpos legales que sancionan el cometimiento de un delito informático?	**138**	**14**	**152**
¿Piensa usted que deberían existir fuertes sanciones en el Código Orgánico Integral Penal para los que realicen algún tipo de delito informático?	**146**	**6**	**152**
¿Cree usted que la mayor parte de delitos informáticos persiguen fines económicos?	**106**	**46**	**152**
¿Considera usted que la seguridad pública contemplada en la Constitución corre riesgos al manipular los sistemas informáticos?	**150**	**2**	**152**
SUMA	**540**	**68**	**608**

Cuadro No. 35 Recolección de datos de los cálculos de las estadísticas
Fuente: Encuestas
Elaborado por: Grace Echeverría M

Preguntas	SI		NO	
	Observada	**Esperada**	**Observada**	**Esperada**
¿Conoce usted los cuerpos legales que sancionan el cometimiento de un delito informático?	**138**	**135**	**14**	**17**
¿Piensa usted que deberían existir fuertes sanciones en el Código Orgánico Integral Penal para los que realicen algún tipo de delito informático?	**146**	**135**	**6**	**17**
¿Cree usted que la mayor parte de delitos informáticos persiguen fines económicos?	**106**	**135**	**46**	**17**
¿Considera usted que la seguridad pública contemplada en la Constitución corre riesgos al manipular los sistemas informáticos?	**150**	**135**	**2**	**17**
TOTAL	**540**	**540**	**68**	**68**

Cuadro No. 36 Frecuencias Observadas
Fuente: Encuestas
Elaborado por: Grace Echeverría M

Cálculo de Ji }= Cuadrado

O	E	O-E	$(O-E)^2$	$(O-E)^2/E$
138	**135**	**3**	**9**	**0,0667**
14	**17**	**-3**	**9**	**0,5294**
146	**135**	**11**	**121**	**0,8963**
6	**17**	**-11**	**121**	**7,1176**
106	**135**	**-29**	**841**	**6,2296**
46	**17**	**29**	**841**	**49,4706**
150	**135**	**15**	**225**	**1,6667**
2	**17**	**-15**	**225**	**13,2353**
X^2				**79,2122**

Cuadro No. 37 Cálculo de Ji }= Cuadrado
Fuente: Encuestas
Elaborado por: Grace Echeverría M

gl = (f – 1) . (c – 1)

gl = (5 – 1) . (3 – 1)

gl = (4) . (2)

gl = 8

Con un gl de 8 y un 95% de confianza el X^2 Tabular es = 15, 51

Entonces de esta manera se puede comparar se puede comparar los valores de Chi Cuadrado Tabular, con un valor de 15,51, y el Chi Cuadrado Calculado, igual a 79,2122, bajo un 95% de confianza:

X^2 Calculado X^2 Tabular

79,2122 > 15,51

Por consiguiente se rechaza la Hipótesis Nula (H_0) y se acepta la Hipótesis Alterna (H_1), es decir:

Los delitos informáticos Si inciden en el Derecho Constitucional a la Seguridad Pública.

A continuación su representación en un gráfico:

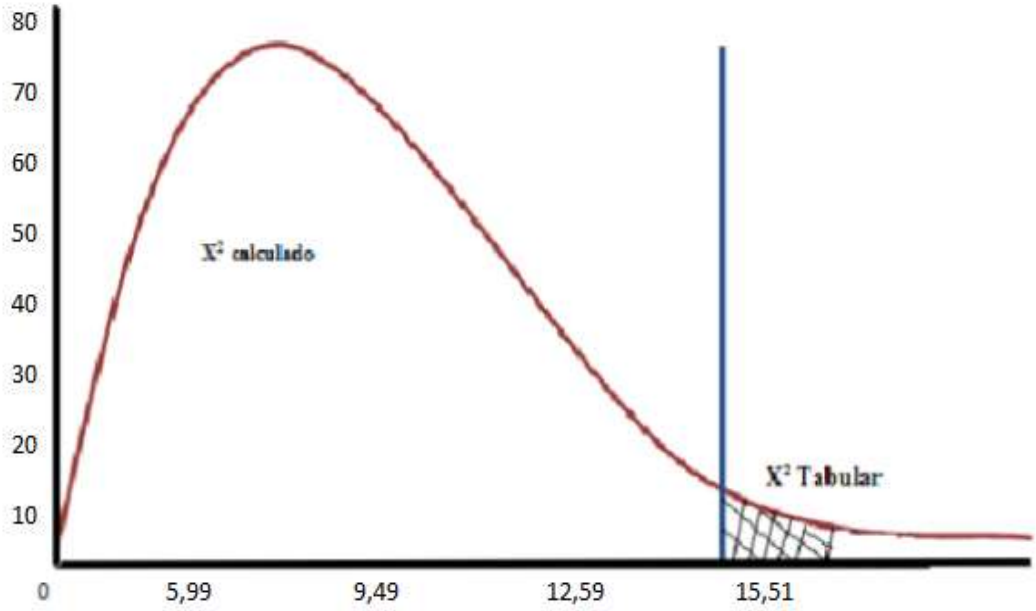

Gráfico No. 35 Cálculo de Ji }= Cuadrado

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Ecuador es un país de constantes cambios que permite la investigación y sanción de los delitos informáticos actualmente, sin embargo es preciso desarrollar, mejorar e implementar mecanismos que permitan que dichas investigaciones mantengan una dirección adecuada, con la capacitación de las personas especializadas dentro de un marco legal apropiado.

La tecnología avanza rápidamente a nivel mundial pero a su vez ocasiona que aparezcan nuevas formas de delinquir, con la utilización por supuesto de los medios tecnológicos que por ser de libre acceso las personas terminan confiándose y agregando información en donde no deberían hacerlo.

De acuerdo a los datos obtenidos en las encuestas el 98% de los involucrados respondieron que la revelación de datos de una persona afecta directamente a su integridad, y además que la conducta delictiva de la persona que comete un delito informático es diferente a la que comete cualquier otro delito, la mayor parte de veces los ciberinfractores son personas con una instrucción académica relevante que utilizan los sistemas informáticos con gran facilidad y de la misma forma tratan de borrar todas las evidencias, de esta forma es difícil detectarlos.

Aquellas personas que no poseen los conocimientos informáticos básicos, son más vulnerables a ser víctimas de un delito informático, estas personas pueden ser las más afectadas si en un momento dado manejan un sistema informático y no han sido asesoradas de una manera adecuada para la utilización de tecnologías con responsabilidad.

Conforme a las encuestas realizadas el 89% de las personas aducen que la información debe contar con las respectivas seguridades para que terceras personas no se aprovechen y ocasionen fuertes daños ya sean económicos o psicológicos, ya que hay que recordar que cualquiera puede ser la próxima víctima del caso.

Los Delitos Informáticos son parte del Derecho Penal, que van encaminados a la protección de las personas en razón del ejercicio y goce de sus derechos respaldados por la Constitución, y que se traduce como una norma legal sancionadora que debe ser respetada y garantizada, por lo que el 99% de los encuestados mencionan que deben existir sanciones rigurosas para las personas que cometen estos tipos de delito.

De acuerdo con los informes relacionados con incidentes de seguridad, vulnerabilidades reportadas, la criminalidad informática organizada ha crecido de manera rápida, y los altos costos que estos involucran para las empresas y la sociedad en general se hallan en una valiosa desventaja.

Recomendaciones

Incentivar a los profesionales del derecho para su formación sobre el tema de los Delitos Informáticos, dando a conocer las respectivas investigaciones dentro del plano legal, para lo cual el respectivo Foro de Abogados en conjunto con el Colegio de Abogados, deberá proponer un seminario para la capacitación a todas los profesionales del derecho.

En los casos de que sea víctima de un delito informático tiene que dar a conocer a la Fiscalía o a la Policía Nacional de tal forma que puedan proceder a las investigaciones pertinentes dando protección a los derechos de la persona afectada.

Para mantener una información protegida es necesario el asesoramiento de una persona con conocimientos informáticos que le puedan ayudar a que la

información ingresada cuente con todo el respaldo y se mantenga de una forma reservada.

Deben existir maestrías en delitos informáticos ya que este delito necesita de una ardua investigación para detectarlo y si los profesionales del derecho no cuentan con una preparación adecuada será más difícil dar soluciones a las personas afectadas.

Procurar la concientización en la sociedad, advertencias en programas televisivos sobre el uso de la tecnología, de este modo se tomarán en cuenta las medidas necesarias para impedir que los hackers o crackers se infiltren en los sistemas informáticos protegidos.

Que se realicen debates públicos acerca de los delitos informáticos y sus consecuencias en la sociedad, enmarcados en doctrina legal y cuerpos normativos, ya que es indiscutible que este tema es de gran trascendencia y que perjudica a toda la ciudadanía, por lo que es una alterativa eficiente mencionar los pasos enmarcados en la ley y en las investigaciones ocurridas.

Los ecuatorianos debemos utilizar las diversas herramientas tecnológicas para procurar adelantos en la vida, no para perjudicar a los demás, ya que al estar atentando en contra de terceros se está actuando de una manera irresponsable y se está cometiendo un delito que aunque es silencioso si afecta a la persona contra la cual se está efectuando.

Reforma al Art 232 del Código Orgánico Integral Penal.

CAPÍTULO VI

PROPUESTA

Tema:

Reforma al Art 232 del Código Orgánico Integral Penal en lo que se refiere al ataque a la integridad de sistemas informáticos.-.

DATOS INFORMATIVOS

NOMBRE DEL INVESTIGADOR

Grace Alexandra Echeverría Mera

TELEFONO

032852103-0999962881

DIRECCIÓN DOMICILIARIA

Febres Cordero y Batalla de Pichincha

TIEMPO DE EJECUCIÓN

El tiempo de ejecución será de seis meses (02 de Abril - 30 de Octubre 2014)

CANTÓN

Ambato

PROVINCIA

Tungurahua

BENEFICIARIOS

Trabajadores, Empleadores, Profesionales del Derecho, Sociedad en General

FINANCIAMIENTO

El financiamiento de esta investigación corresponderá en su totalidad a la investigadora

Antecedentes de la Propuesta

Con el comienzo del presente capitulo para realizar la propuesta se dio paso en primer lugar a revisar tesis anteriores en la Universidad Técnica de Ambato Facultad de Jurisprudencia y Ciencias Sociales de tal forma que pueda ayudar , guiar, solventar y dar una posible solución al trabajo de investigación, luego de ir a la biblioteca y revisar detenidamente se puede emitir un juicio de valor que no existe una propuesta parecida, semejante o igual a la de este trabajo como una forma de protección para que todas las personas mantengan una gran seguridad en sus datos ya que los mismos pueden luego encontrase en manos equivocadas y lo único que ocasionará es un daño relevante los derechos de una persona que se encuentran contemplados en la Constitución de la República, los cuales tienen que ser respetados ya que hay que mencionar la frase que los derechos de una persona comienzan cuando terminan los de los demás.

La tecnología ha ido evolucionando constantemente y los riegos de seguridad han ido decayendo, no solo está en el país sino a nivel mundial, por tal motivo es necesario el profundo análisis de las leyes actuales para la constancia de una armonía social.

En Agosto del 2014 entró en vigencia el Código Orgánico Integral Penal el cual se halla en debates acerca de nuevos delitos incluidos con sus respectivas sanciones para las personas que infrinjan la ley, esto sin estar en contra de la norma superior es decir la Constitución de la República del Ecuador.

El modelo delictivo está progresando día tras día y es primordial tener leyes claras que sancionan a los que ocasionen daños a terceros con la utilización de los sistemas informáticos, ya que la tecnología debe ser utilizada para la superación, no para la destrucción de la ciudadanía.

Se debe tomar en cuenta que los delitos informáticos persiguen fines lucrativos y que las personas que los cometen tienen gran capacidad para efectuarlos incluso en casos sin dejar evidencia, a su vez como es posible que al cometer un delito no tengan sanciones por tal circunstancia indiscutible la necesidad de que la ley restrinja claramente las prohibiciones y las penas a darse dependiendo al delito realizado.

Justificación

Los delitos informáticos se cometen en el ciberespacio, y no se detienen a mirar ni siquiera las fronteras nacionales, es decir puede ocasionarse en cualquier lugar y contra cualquier usuario de ordenador del mundo

Con la aplicación de esta propuesta se logrará que las personas que cometan un delito informático e incurran en chantaje y extorsión de sus víctimas sean sancionados de una forma más rigurosa de tal manera que se estará garantizando lo que la Constitución establece acerca de los derechos protegidos, consiguiendo de esta forma que la sociedad pueda mantenerse en tranquilidad y en confianza de que si sus datos son revelados existirá una pena sancionadora y que se realice investigaciones correspondientes que no quedarán en la impunidad.

Por lo mencionado y desarrollado en la presente investigación se efectuó la siguiente propuesta que está dirigida hacia quienes están llamados a legislar y lograr de alguna manera que se evite el quebrantamiento de los principios que en la ley se establece.

La presente propuesta en si tiene importancia académica, social, económica puesto que con el desarrollo de este trabajo se pone en manifiesto la necesidad del cumplimiento de las leyes sancionadoras a las personas que quieren perturbar a la sociedad.

Respecto a la factibilidad de realización de la presente propuesta, se tomará en cuenta los recursos económicos, humanos, y de tiempo para la ejecución de la

misma.

Objetivos

Objetivo General

Implantar una reforma al COIP en la que se tipifique una sanción rigurosa a las personas que luego de dañar un sistema informático y obtener información de la víctima incurra en chantaje y extorsión de la misma

Objetivos específicos

Aportar elementos de información relevante para la prevención de los delitos informáticos

Proveer las herramientas teóricas, conceptuales y legales de los delitos informáticos y el derecho Constitucional a la Seguridad Pública.

Redactar las reformas al Art 232 del COIP.

Análisis de factibilidad

Político

El tema de los delitos informáticos, en el mundo, es de constantes debates con criterios propios y de gran importancia.

Al plantear una reforma al Art. 232 del Código Orgánico Integral Penal se pretende que el Articulo sea más complejo y se mencione que no sólo dañar o alterar un sistema informático está cometiendo un delito y recibirá una sanción, sino que además la pena debe aumentar en los casos que utilice la información privada de la persona afectada y la esté extorsionando y chantajeando para no publicarla ocasionando un daño profundo a su integridad personal.

Social

Esta propuesta va dirigida de manera directa a toda la sociedad y a los legisladores ya que nuestro País no debe estar en el limbo sino estar consciente de sus derechos y sentirse respaldado por leyes que aseguren protección.

Género

La presente propuesta va enfocada a la sociedad sin discriminación ni distinción de clase dando cumplimiento a lo que establece la Constitución de la República del Ecuador en el Art. 11, numeral 2 que dice: todas las personas son iguales y gozaran de los mismos derechos, deberes y oportunidades.

La aplicación de la propuesta presentada, permitirá que sea más claro las sanciones a las personas que utilicen información de los afectados para su beneficio de tal forma que permita a las investigaciones realizadas por fiscalía que sean directas y precisas con la obtención de los elementos probatorios necesarios.

Fundamentación Científica-Técnica

El ataque a la integridad de los sistemas informáticos se encuentra establecido y tipificado en el Art 232 del Código Orgánico Integral Penal. Los delitos informáticos se encuentran en la Sección tercera, Delitos contra la seguridad de los activos de los sistemas de información y comunicación del Código Orgánico Integral Penal en los artículos 229al 234. Además se halla sustentado en la Constitución en la Sección Quinta Acción de Habeas Data art 92.

Lo que se pretende con el presente trabajo de investigación es que se agregue la parte en que manifiesta que el que dañe los sistemas informáticos y con ánimo de causar daño obtenga la información utilizándole para el chantaje y extorsión de la víctima será sancionado con una pena de siete a nueve años.

Lo que se desea conseguir con la propuesta es el respeto a la información, no puede acceder un tercero, dañar la información y encima obtener beneficios de lucro con el sufrimiento de una persona que no desea que su integridad personal se halle vulnerada y sea conocida por toda la sociedad.

De esta manera se logrará una justicia confiable sin dudas donde el Fiscal investigue y al observar la información se la ponga en manos de un especialista en la informática para detectar cual es el hacker o cracker que lo está cometiendo.

Metodología

El paso inicial para la realización de la presente propuesta fue la investigación y determinación del problema de los ataques a los sistemas informáticos, y como incide en la vulneración de los derechos contemplados en la Constitución atentando de cierto modo a la integridad `personal una vez encontrado el problema se procedió a efectuar la encuesta a profesionales del derecho, agentes investigadores, Fiscales así como también a personas perjudicadas, en base a esta técnica de recolección de información se procedió a realizar un análisis sobre los datos obtenidos y así buscar una alternativa de solución que beneficie a toda la sociedad.

La propuesta que se va a llevar efecto inicialmente tendría lugar con la presentación de la misma ante la Asamblea Nacional.

Considerando

Que, de conformidad con el Artículo 120 de la Constitución de la República, que dice: "La Asamblea Nacional Tendrá las siguientes atribuciones y deberes, además de las que determine la ley", establece en el numeral 6:"Expedir, codificar, reformar y derogar las leyes, interpretarlas con carácter generalmente obligatorio"

Que, conforme la norma suprema en su Artículo 82 manifiesta el derecho a la seguridad jurídica, se fundamente en el respeto a la Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicadas por las autoridades competentes;

Que de conformidad al Artículo 393 de la Constitución de la República, dice "El Estado garantizará la seguridad humana a través de las políticas y acciones integradas para asegurar la convivencia pacífica de las personas, promover una cultura de paz y prevenir las formas de violencia y discriminación y la comisión de infracciones y delitos".

Que conforme a la norma suprema en los derechos de libertad Artículo 66 en el inciso 19 "El derecho a la protección de datos de carácter personal, que incluye el acceso y a la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley".

Que conforme a la norma suprema en los derechos de libertad Artículo 66, en el inciso 21: "El derecho a la inviolabilidad y al secreto de la correspondencia

física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación".

En ejercicio de sus atribuciones constitucionales y legales

RESUELVE

Aprobar la Ley de Agregación al Art, 232 del Código Orgánico Integral Penal.

LEY REFORMATORIA Al ARTÍCULO 232 DEL CÒDIGO ORGÀNICO INTEGRAL PENAL.

Art. Único.- Agréguese al Art. 232 el siguiente texto

La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause malfuncionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.
2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

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

Si la infracción es cometida y la información es utilizada con el ánimo de causar daño recurriendo a chantajes y extorsión de las víctimas la pena será de siete a nueve años.

Esta reforma de Ley entrará en vigencia a partir de su promulgación en el Registro Oficial

Metodología. Modelo Operativo de la Propuesta

Fases	Actividades	Objetivo	Responsable	Recursos	Tiempo	Evaluación
Preliminar	Sustentar teóricamente la reforma al Artículo 232 del Código Orgánico Integral Penal	Impulsar el respaldo de los derechos a la información reservada y a la libertad de las personas	Investigadora	Económicos Tecnológicos Materiales Humanos	**18 días**	Documental con el marco teórico
Operativa	Diseño del proyecto Presentación a la Asamblea Nacional	Instrumentos elaborados en un 70%. Concientización de la importancia que tienen los ataques a los sistemas informáticos	Investigadora	Económicos Tecnológicos Materiales Humanos	**11 días**	Documento de investigación con el proyecto Proyecto
Final	Publicación en el Registro Oficial	Sancione u objete Asamblea Nacional	Investigadora	Económicos Tecnológicos Materiales Humanos	**30 días**	Promulgación

Cuadro No. 38 Modelo Operativo de la Propuesta
Fuente: Investigadora
Elaborado por: Grace Echeverría M

Administración

La propuesta será administrada por parte de la Fiscalía General del Estado de Tungurahua, en coordinación con la Carrera de Derecho de la Facultad de Jurisprudencia y Ciencias Sociales de la Universidad Técnica de Ambato, quienes estudiarán y analizarán la propuesta, y en caso de ser procedente enviarán la presente propuesta a la Honorable Asamblea Nacional, para el trámite de Ley correspondiente.

El objetivo es sacar adelante esta propuesta, puesto que no puede quedar en lo teórico, por ello se tendrá que sugerir a la Asamblea Nacional, para que se cumpla la propuesta realizada por la investigadora.

Previsión de la Evaluación

Preguntas Básicas	**Explicaciones**
¿Quiénes solicitan evaluar?	Los que realizan la propuesta.
Por qué evaluar?	Porque se necesita revisar si la propuesta da resultado
¿Para qué evaluar?	Para verificar el cumplimiento de los objetivos
¿Qué evaluar?	Conocimientos
¿Quién va a evaluar?	Investigadora
¿Cuándo evaluar?	Una vez ejecutada la propuesta
¿Cómo evaluar?	Aplicando técnicas de investigación científica
Con quién evaluar?	Con las personas involucradas

Cuadro No. 39 Previsión de la Evaluación
Fuente: Investigadora
Elaborado por: Grace Echeverría M

Se considera un tiempo mínimo de tres meses posterior a la aprobación de la reforma, para verificar los resultados obtenidos. La evaluación será continua, debido a que toda acción del hombre debe ser evaluada para cumplir con lo propuesto y para admitir que ha existido un avance o desarrollo de conocimientos, debe existir la revisión ya que siempre existirán correcciones, acorde a las necesidades que son propias del desarrollo de la propuesta para contribuir en la reforma planteada.

BIBLIOGRAFÍA

Enciclopedia Juridica Omeba. (1898).

Constituciòn de la Repùblica del Ecuador. (2008).

Ley de Seguridad Pùblica del Ecuador. (2011). Quito.

Plan Nacional de Seguridad Integral . (2012). Quito.

Còdigo Orgànico Integral Penal. (2014).

ACURIO DEL PINO, Santiago. (2011). Delitos Informáticos

AVILA, Luis. A. (2012). Delitos Informáticos.

CABANELLAS, Guillermo. (1990). Diccionario de Derecho Usual. Heliasta.

CAMACHO LOSA, Luis. (2012). El DelitoInformático. Madrid.

FERNANDEZ, Rafael. (2013). Derecho Informático.

GARRIDO MONTT, Mario. (2013). Teoria del Delito .

HERRERA, Rodolfo. (2012). Delitos Informáticos.

LARA RIVERA, Jorge. (2011). Derecho de Internet .

LORENZO, Patricia. (2012). Conceptualizaciòn y Generalidades de los DelitosInformáticos.

MATA, Ricardo. (2013). Delicuencia y Derecho Penal.

NARANJO, Galo. y Herrera. (2008). Tutoria de la Investigación Científica. Ambato: Maxtudio.

PÀEZ, Rivadeneira. Luis. (2013). PeritajeInformático.

PASCALE, Eduardo. (2012). Descubriendo rastros Informáticos.

REBOLLO, Lucrecia. (2010). Derechos Fundamentale y Protecciòn de Datos .

TÈLLEZ, Josè. (2012). DelitosInformáticos y Proteccion Penal a la Intimidad.

TORRES, Andreìna. (2013). La Seguridad Pùblica en Ecuador un concepto en Construcciòn. Quito.

VALLEJO DELGADO, Vicente. (2012). El Delito Informático en la Legislaciòn Ecuatoriana.

ZAMBRANO, Regina. Reyna. (2012). Delitos Informáticos comtemplados en la Ley Ecuatoriana. Primera Edicion.

LINKOGRAFÍA

1. www.delitosInformáticos.com
2. www.derechoecuador.com
3. www.derechotecnològico.com/delitos.html
4. www.tribunalmmm.gob.mx/biblioteca/almadelia/indice
5. http://definicion.de/seguridad-publica/ixzz3G8t98s10
6. http://biblio.juridicas.unam.mx/

ANEXOS


DELITOS INFORMATICOS
pasos para denunciar
nunca le des informacion personal a extraños
no respondas mensajes de extraños
no le des tu password a nadie desconocido
nunca aceptes regalos en linea
nunca recibas fotos de extraños
nunca le mandes fotos a extraños
no hagas citas personales con gente que conociste en internet

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

CARRERA DE DERECHO

ENCUESTA REALIZADA A 83 ABOGADOS EN LIBRE EJERCICIO DE LA CIUDAD DE AMBATO

Objetivo: Determinar si los delitos informáticos inciden en el Derecho Constitucional a la Seguridad Pública

1.- ¿Cree usted que la mayor parte de delitos informáticos persiguen fines económicos?

SI ( ) NO ( )

2. ¿Ha sido víctima de algún tipo de delito informático?

SI ( ) NO ( )

3. ¿Considera usted, que su derecho a la intimidad es violentado utilizando el internet u otro mecanismos de sistema informático?

SI ( ) NO ( )

4. ¿Considera usted, que las compras a través de internet son seguras?

SI ( ) NO ( )

5. ¿Según su propia experiencia considera usted, que en la investigación de los delitos informáticos existe alguna dificultad?

SI ( ) NO ( )

6. ¿Piensa usted que deberían existir fuertes sanciones en el Código Orgánico Integral Penal para los que realicen algún tipo de delito informático?

SI ( ) NO ( )

7. ¿Considera usted que la seguridad pública contemplada en la Constitución corre riesgos al manipular los sistemas informáticos?

SI ( ) NO ( )

8. ¿Conoce el procedimiento que se da en casos de delitos informáticos?

SI ( ) NO ( )

9. ¿Piensa usted que la revelación de datos de una persona afecta directamente a su integridad?

SI ( ) NO ( )

10. ¿Conoce los cuerpos legales que sancionan a los delitos informáticos?

SI ( ) NO ( )

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

CARRERA DE DERECHO

ENCUESTA DIRIGIDA A 17 FISCALES, 16 AGENTES INVESTIGADORES DE LA CIUDAD DE AMBATO

Objetivo: Determinar si los delitos informáticos inciden en el Derecho Constitucional a la Seguridad Pública

1. ¿Para detectar un delito informático es necesario que la víctima aporte todos los elementos probatorios pertinentes?

SI ( ) NO ( )

2. ¿Considera usted que la seguridad pública está siendo vulnerada con el cometimiento de un delito informático?

SI ( ) NO ( )

3. ¿El ciberinfractor de un delito informático puede realizar chantajes o extorción a las víctimas?

SI ( ) NO ( )

4. ¿Conoce los cuerpos legales que han sido utilizados para la sanciones de los delitos informáticos?

SI ( ) NO ( )

5. ¿En la actualidad los casos de delitos informáticos han aumentado el riesgo de la ciudadanía?

SI ( ) NO ( )

6. ¿Piensa usted que deberían existir fuertes sanciones en el Código Orgánico Integral Penal para los que realicen algún tipo de delito informático?

SI ( ) NO ( )

7. ¿Cree usted que la mayor parte de delitos informáticos persiguen fines económicos?

SI ( ) NO ( )

8. ¿Considera usted que la seguridad a los datos personales es altamente prioritaria en la ciudad de Ambato?

SI ( ) NO ( )

9. ¿Cree usted que el avance tecnológico en las redes informáticas ha producido un conflicto social que afecta derechos de las personas actualmente?

SI ( ) NO ( )

10. ¿Considera usted que los delitos informáticos impiden que exista una Seguridad Pública conforme al derecho Constitucional?

SI ( ) NO ( )

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

CARRERA DE DERECHO

ENCUESTA REALIZADA A 30 USUARIOS AFECTADOS

Objetivo: Determinar si los delitos informáticos inciden en el Derecho Constitucional a la Seguridad Pública

1. ¿Conoce usted de que se trata un delito informático?

SI ( ) NO ( )

2. ¿Considera usted que los sistemas informáticos necesitan protección en la actualidad.

SI ( ) NO ( )

3. ¿Cree usted que la mayor parte de delitos informáticos persiguen fines económicos?

SI ( ) NO ( )

4. ¿Considera usted que los delitos informáticos son fáciles de detectar?

SI ( ) NO ( )

5. ¿Considera usted que la seguridad pública contemplada en la Constitución corre riesgos al manipular los sistemas informáticos?

SI ( ) NO ( )

6. ¿Piensa usted que deberían existir fuertes sanciones en el Código Orgánico Integral Penal para los que realicen algún tipo de delito informático?

SI ( ) NO ( )

7. ¿Considera usted que los delitos informáticos ocasionan daños a la integridad de una persona?

SI ( ) NO ( )

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

SI ( ) NO ( )

9. ¿Conoce usted los cuerpos legales que sancionan el cometimiento de un delito informático?

SI ( ) NO ( )

10. ¿Considera usted que es necesario que exista mayor información para la seguridad de las personas de tal manera que se hallen prevenidas ante este tipo de delitos?

SI ( ) NO ( )

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

ENTREVISTA DIRIGIDA AL FISCAL PROVINCIAL DE TUNGURAHUA

FECHA…….

ENTREVISTADORA……

ENTREVISTADO……...

ASPECTO: DELITOS INFORMATICOS Y EL DERECHO CONSTITUCIONAL A LA SEGURIDAD Pública.

HORAS……

OBJETIVO: Conocer la argumentación profesional del Fiscal Provincial de Tungurahua sobre el tema.

1) Cree usted que deberían existir fuertes sanciones para las personas que cometen un delito informático?

……
……
……
……
……

2) Cual es el procedimiento que se ha tomado en los casos de los delitos informáticos?

……
……
……

……
……

3) Actualmente Fiscalía cuenta con Peritos Informáticos

……
……
……
……
……

4) ¿Qué es lo principal que se toma en cuenta para determinar la preexistencia de un delito informático?

……
……
……
……
……
……

5) ¿Con el cometimiento de un delito informático se puede vulnerar a la Seguridad Publica contemplada en nuestra Constitución?

……
……
……
……
……
……

GLOSARIO

Cracker: El término cracker "black hat" se utiliza para denominar a las personas que emplean sus elevados conocimientos informáticos para robar información, distribuir virus, introducirse ilegalmente en redes, eliminar la protección anti copia del software comercial, burlar la seguridad de determinados sistemas informáticos.

Daño: En sentido amplio, toda suerte de mal material o moral. Más particularmente, el detrimento, perjuicio o menoscabo que por acción de otro se recibe en la persona o en los bienes. El daño puede provenir de dolo, de culpa o de caso fortuito, según el grado de malicia, negligencia o casualidad entre el autor y el efecto. En principio, el daño doloso obliga al resarcimiento y acarrea una sanción penal; el culposo suele llevar consigo tan sólo indemnización; y el fortuito exime en la generalidad de los casos, dentro de la complejidad de esta materia.

Derecho informático: Se denomina derecho Informático al conjunto de normas, reglas y principios jurídicos que tiene por objeto evitar que la tecnología pueda conculcar (infringir, vulnerar) derechos fundamentales del hombre que se ocupan de la regulación derivadas de la producción, uso comercialización de los bienes informáticos, así como la transmisión de datos.

Hacker: Se denominan hackers a los especialistas en tecnologías de la información y telecomunicaciones en general, aunque actualmente, se utiliza este término para referirse a aquellos que utilizan sus conocimientos con fines maliciosos como el acceso ilegal a redes privadas, el robo de información, etc. Según algunos expertos, es incorrecto asociar éste término únicamente con aquellas prácticas fraudulentas, **"**White Hat**":** especialistas en informática que utilizan sus conocimientos con el fin de detectar cualquier tipo de vulnerabilidad, errores o fallos de seguridad, etc. para poder solucionarlos y evitar posibles ataques.

Honor.- El honor es la percepción que el propio individuo tiene de sí mismo

en cuanto a su prestigio dentro de un grupo, es su reputación social.

Intranet: Una red concebida para organizar y compartir la información, así como para efectuar transacciones digitales dentro de una empresa.

IP: Internet Protocolo: Es el conjunto de normas técnicas que especifican la emisión de datos a través de internet.

Password: Termino utilizado para identificar la clave secreta o privada de acceso a un programa o cuenta.

Seguridad Jurídica.- Cualidad del ordenamiento que produce certeza y confianza en el ciudadano sobre lo que es Derecho en cada momento y sobre lo que, previsiblemente lo será en el futuro. La seguridad jurídica establece ese clima cívico de confianza en el orden jurídico, fundada en pautas razonables de previsibilidad, que es presupuesto y función de los Estados de Derecho.