UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS ADMINISTRATIVAS Y HUMANÍSTICAS

CARRERA DE ABOGACÍA

TESIS DE GRADO

TEMA:

"LOS DELITOS INFORMÁTICOS Y SU PERJUICIO EN LA SOCIEDAD"

Tesis de investigación presentada previa a la obtención del título de Abogado de los Tribunales y Juzgados de Justicia de la República del Ecuador.

Autor:

Acosta Semblantes Byron Eduardo

Director:

Dr. Segovia Dueñas José Luis

LATACUNGA - ECUADOR

MARZO-2012

AUTORIA

Los criterios emitidos en el presente trabajo de investigación **"LOS DELITOS INFORMÁTICOS Y SU PERJUICIO EN LA SOCIEDAD"**, son de exclusiva responsabilidad del autor.

……

Byron Eduardo Acosta Semblantes

C.I. 050306412-3

AVAL DEL DIRECTOR DE TESIS

En calidad de Director del Trabajo de Investigación sobre el tema: **"LOS DELITOS INFORMÁTICOS Y SU PERJUICIO EN LA SOCIEDAD"**, de Acosta Semblantes Byron Eduardo, postulantes de la Carrera de Abogacía, considero que dicho Informe Investigativo cumple con los requerimientos metodológicos y aportes científico-técnicos suficientes para ser sometidos a la evaluación del Tribunal de Validación de Tesis que el Honorable Consejo Académico de la Unidad Académica de Ciencias Administrativas y Humanísticas de la Universidad Técnica de Cotopaxi designe, para su correspondiente estudio y calificación.

Latacunga, Noviembre; 2011

El Director

Dr. José Luis Segovia Dueñas

UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS ADMINISTRATIVAS Y HUMANISTICAS

Latacunga-Ecuador

APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de Miembros del Tribunal de Grado aprueban el presente Informe de Investigación de acuerdo a las disposiciones reglamentarias emitidas por la Universidad Técnica de Cotopaxi y por la Unidad Académica de Ciencias Administrativas y Humanísticas; por cuanto el postulante: ACOSTA SEMBLANTES BYRON EDUARDO; con el título de tesis: "LOS DELITOS INFORMÁTICOS Y SU PERJUICIO EN LA SOCIEDAD" han considerado las recomendaciones emitidas oportunamente y reúne los méritos suficientes para ser sometido al acto de Defensa de Tesis.

Por lo antes expuesto, se autoriza realizar los empastados correspondientes, según la normativa institucional.

Latacunga, 27 de Febrero; 2012

Para constancia firman:

……..	…….....
Dr. Luis Rodríguez	Dr. Hernán Garzón
PRESIDENTE	MIEMBRO

……

Dra. Cecilia Chancúsig

OPOSITOR

AGRADECIMIENTO

Mis más sinceros y gratos agradecimientos a todas aquellas personas que hicieron posible cumplir con este sueño, a mis familiares y maestros que me supieron apoyar en todo momento, para alcanzar la culminación exitosa de este proyecto; de manera especial a mi pequeño hijo que fue la motivación diaria para seguir sin desmayar hasta alcanzar la meta anhelada.

Byron Acosta Semblantes

DEDICATORIA

Al amor de mi vida mi madre, que se encuentra cuidándome desde lo más recóndito del infinito, quien con su amor, respeto, comprensión y consejos supo guiarme siempre por el sendero del bien.

Gracias mamá.

ÍNDICE

TEMA: **PÁG.**

UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS ADMINISTRATIVAS Y HUMANISTICAS

Latacunga-Ecuador

TEMA: "LOS DELITOS INFORMÁTICOS Y SU PERJUICIO EN LA SOCIEDAD"

Autor: Byron Eduardo Acosta Semblantes

Director: Dr. José Luis Segovia Dueñas

RESUMEN

Los delitos informáticos pueden ser considerados como crímenes electrónicos, tan graves que pueden llegar a ser un problema para el avance de la informática. Sin embargo este puede tener consigo delitos tan graves como el robo, falsificación de documentos, fraudes, chantajes y malversación de caudales públicos. Un ejemplo muy común es cuando una persona llega a robar información y a causar daños de computadoras o servidores que pueden llegar a ser absolutamente virtuales porque la información se encuentra en forma digital y el daño cada vez se vuelve más grande.

Muchas de las personas que cometen este tipo de delitos informáticos tienen diferentes características tales como la habilidad del manejo de los diferentes sistemas informáticos o la realización de tareas laborales que le facilitan el acceso de carácter simple. La investigación sobre "El problema de la falta de conocimiento sobre el proceso que se debe seguir en los casos de delitos informáticos tiene como propósito reflexionar sobre la aplicación del sistema de justicia actual en todos los casos, para esto se realizó la investigación mediante encuestas a los Jueces Provinciales, Miembros del Tribunal y Jueces de garantías penales de Cotopaxi, Fiscales y Abogados en libre ejercicio de la Provincia, de los cuales se obtuvieron resultados para la realización de una propuesta factible que consiste en la inclusión de delitos informáticos en el Código Penal.

La propuesta servirá para mejorar el sistema de administración de justicia en lo concerniente a garantizar los derechos que el Estado asiste a todos los individuos y para garantizar el debido proceso en este caso específico. La propuesta en si consiste en la inclusión de delitos informáticos en el Código Penal, la intención es de coadyuvar a que se respete y garantice los derechos y obligaciones de los ciudadanos, y se desarrollen de acuerdo a las Leyes Nacionales, Convenios y Pactos Internacionales.

UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS ADMINISTRATIVAS Y HUMANISTICAS

Latacunga-Ecuador

TOPIC: "LOS DELITOS INFORMÁTICOS Y SU PERJUICIO EN LA SOCIEDAD"

Autor: Byron Eduardo Acosta Semblantes

Director: Dr. José Luis Segovia Dueñas

ABSTRACT

The computer science misdemeanor could be considered as an electronic crime, as serious that they could become in problem to stop the computer science development. However it could have with them serious crimes like robbery, documents falsification, fraud, blackmail and grafts of public economy. A very common example is when a person goes to steal information and to cause problems in the computers or in the others parts of them that could became absolutely virtual objects because of the information that is found o it in a digital way and the damage that everyday becomes bigger.

Most of the people that do this kind of computer science crime have different characteristics such as the abilities to use the different computer science systems or the workable jobs which make them the access easier, it means in a simple way. The investigation about "the problem for the lack of knowledge about the process that they have to follow when there are computer science crime have as purpose to reflect about the actual justice system application in the hole cases, for this reasons we did the investigation to the Provincial Judges, Tribunal Members and Penal Security Judges from Cotopaxi, Public Attorneys and Lawyers of the province by surveys.

The purpose will help to develop the judge administration system in everything that consists to guarantee the rights that the State gives to the whole people and also the process in this specific case.

The proposal consists in giving the general knowledge about the theme they are trying to the Laws Professionals and Direct Actors of the Judge Administration System by the use of the methodology from the Training Program. The objective goes to makes possible to respect and guarantee the rights and the obligations of the citizen and also to develop international agreements and pacts to the national laws.

INTRODUCCIÓN

A nadie escapa la enorme influencia que ha alcanzado la informática en la vida diaria de las personas y organizaciones, la importancia que tiene su progreso para el desarrollo de un país. Las transacciones comerciales, la comunicación, los procesos industriales, las investigaciones, la seguridad, la sanidad, entre otros, son aspectos que dependen cada día más de un adecuado desarrollo de la tecnología informática. Junto al avance de la informática y su influencia en casi todas las áreas de la vida social, ha surgido una serie de comportamientos ilícitos denominados, de manera genérica, «delitos informáticos».

Para lograr una investigación completa de la temática se establece la conceptualización respectiva del tema, generalidades asociadas al fenómeno, estadísticas mundiales sobre delitos informáticos, el efecto de éstos en diferentes áreas, como poder minimizar la amenaza de los delitos a través de la seguridad, aspectos de legislación informática, y por último se busca unificar la investigación realizada para poder establecer el papel de la Ley Penal frente a los delitos informáticos.

Al final del documento se establecen las conclusiones pertinentes al estudio, en las que se busca destacar situaciones relevantes, comentarios, análisis, entre otros; la revolución tecnológica ha transformado profundamente la realidad del mundo entero, permitiendo a los seres humanos en la actualidad alcanzar lo inimaginable y conseguir nuevos objetivos hasta hace poco inalcanzables, en la aplicación de la telemática todo obstáculo es superado. Estos cambios increíbles ha servido en su mayor para el bienestar de todos los individuos, facilitando la comunicación, los negocios, el acceso a la información entre otros, pero también ha existido quienes han sabido sacar provecho de este avance, hoy en día ya no hace falta armamento sofisticado para delinquir el arma del nuevo delincuente es un teclado

alfanumérico; por ello solo un cabal conocimiento de la aplicación de las nuevas tecnologías y de sus métodos de protección, otorgarían al navegante seguridad al acceder a un ilimitado mundo de nuevas tecnologías.

El Capítulo I comprende el Marco Teórico, empezando con los antecedentes investigativos, para luego centrarse en la fundamentación científica, el desarrollo investigativo se lo realizó a profundidad, documentando exhaustivamente la temática propuesta, para lo cual se ha tomado aspectos contemplados en la bibliografía propuesta así como en información existente en el Internet.

El Capítulo II, constituye el Marco Metodológico, en el cual se ha descrito la modalidad y el tipo de investigación, la población a investigarse, se describe los métodos y técnicas que se emplearon en la investigación, se dan a conocer los resultados alcanzados en la misma, se realiza la verificación de la idea a defender para terminar con la exposición de las conclusiones y proponer algunas recomendaciones.

El Capítulo III, constituye exclusivamente el Marco Propositivo, donde podemos encontrar la introducción, el objetivo general y los específicos, la justificación, la fundamentación, para finalmente llegar al Programa de Capacitación acerca de los problemas existentes dentro de los procesos de juzgamiento en los casos de los delitos informáticos.

En el presente trabajo investigativo se empleó la investigación de carácter descriptiva, ya que permitió descubrir el grado de conocimiento que tienen los encuestados acerca de sus derechos y obligaciones, con el propósito de proponer la implementación de estos delitos en la Ley Penal; la metodología que se utilizó fue el diseño no experimental de investigación, que permitió observar la inadecuada aplicación de la norma Penal en el caso de los Delitos Informáticos.

CAPÍTULO I

1. FUNDAMENTOS TEÓRICOS

1.1. Antecedentes

Los problemas jurídicos que se plantean a raíz de las actividades en el ciberespacio son de variada naturaleza. Muchos de ellos provienen del uso de nombres de firmas comerciales de los servidores, que chocan con derechos de propiedad industrial previamente adquiridos, como las marcas comerciales registradas. Otros problemas provienen de la información que puede ser publicada en la red, que puede afectar la honra de terceras personas, derechos de propiedad intelectual, como el derecho de autor, o que puede importar la realización de actividades absolutamente prohibidas, como la pornografía infantil, y otros tipos en contra de las personas y los bienes, o fuertemente protegidas, como la propagación de datos privados, la existencia de legislaciones ordinarias independientes de los países, la comisión de delitos que no reconocen la existencia de las fronteras tradicionales entre países. Por último, existe toda la problemática que proviene del comercio electrónico realizado a través de estos medios, tales como la formación del consentimiento, la prueba de los contratos, la legislación y jurisdicción aplicable a dicha actividad, las consecuencias fiscales.

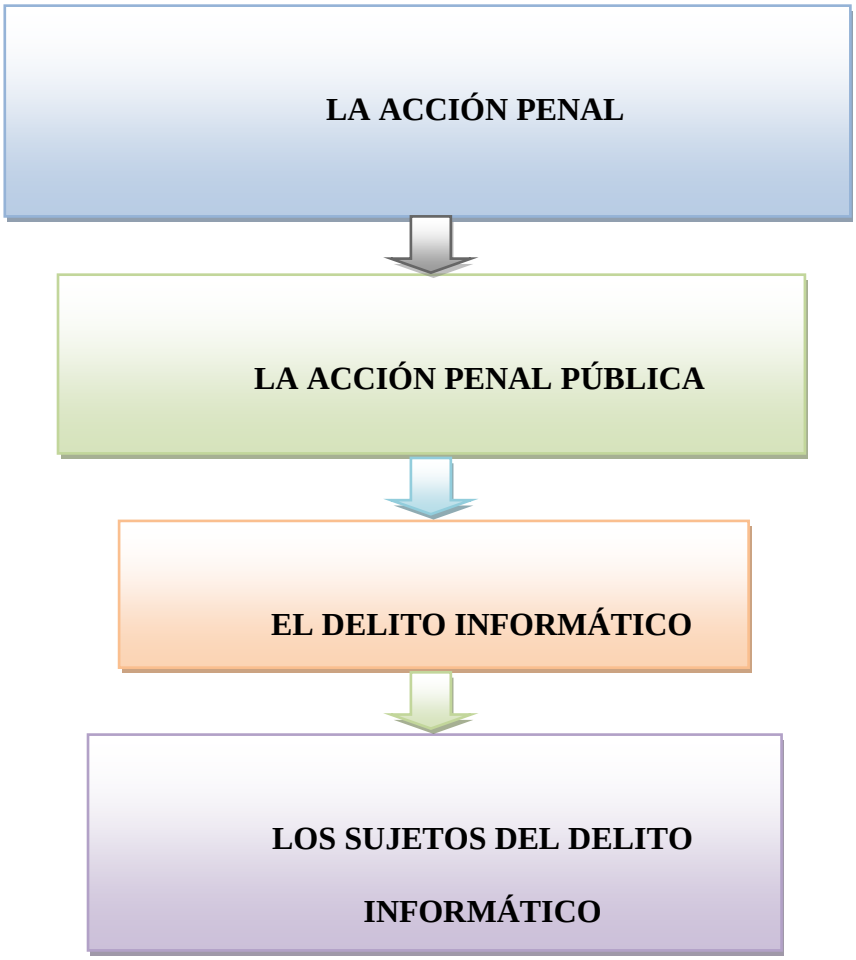
Desde hace aproximadamente diez años la mayoría de los países europeos han hecho todo lo posible para incluir dentro de la ley, la conducta punible penalmente, como el acceso ilegal a sistemas de cómputo o el mantenimiento ilegal de tales accesos, la difusión de virus o la interceptación de mensajes

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.

Por otra parte, existen diversos tipos de delito que pueden ser cometidos y que se encuentran ligados directamente a acciones efectuadas contra los propios sistemas. Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que la diferencia entre sí, es la naturaleza en cuanto al tipo de delitos cometidos. Al respecto, según un estudio publicado en el Manual de las Naciones Unidas en la prevención y control de delitos informáticos (Nº. 43 y 44), el 90% de los delitos realizados mediante la computadora fueron ejecutados por empleados de la propia empresa afectada.

Este creciente nivel de criminalidad mediante este sistema se puede explicar por la dificultad de reprimirla en forma internacional, ya que los usuarios están esparcidos por todo el mundo y, en consecuencia, existe una posibilidad muy grande de que el agresor y la víctima estén sujetos a leyes nacionales diferentes las mismas que hacen imposible o dificultan la aplicación de sanciones para este tipo de infracciones. Además, si bien los acuerdos de cooperación internacional y los tratados de extradición bilaterales intentan remediar algunas de las dificultades ocasionadas por los delitos informáticos, sus posibilidades son limitadas.

1.2. Categorías Fundamentales



1.2. Marco Teórico

1.2.1. Acción Penal

El tratadista en materia penal LLORE M. Víctor, en su obra Derecho Procesal Penal Ecuatoriano, Fondo de la Cultura Ecuatoriana. Cuenca,(1990), indica que "la acción penal puede considerarse bajo dos aspectos: uno subjetivo y otro objetivo; que subjetivamente es el poder jurídico que compete al Ministerio Público de activar las condiciones para obtener del juez la decisión sobre la realizabilidad de la pretensión punitiva del Estado, derivada de un hecho que la ley prevé como delito. Que objetivamente, la acción penal es el medio con que el órgano ejecutivo, constreñido a abstenerse de la coerción directa en las relaciones penales, determina la intervención de la garantía jurisdiccional en orden a su pretensión punitiva" Pág.12.

La acción penal es la energía que anima todo el proceso que por dos razones es estrecha la concepción de que al hablar de la acción penal, se dice que el objeto de la misma es conseguir la imposición de la pena al reo. Que tales razones son las siguientes:

En primer lugar el fin de la acción penal no es hacer que se llegue a una condena, sino el de hacer que se determine la verdad a propósito de un delito que se dice cometido y que se inculpa a una determinada persona, determinación que no es raro que se llegue a la conclusión de que el hecho no ha existido, o que no se trata de delito, o que el acusado no lo ha cometido o que no ha tomado parte en él. Por otra parte el juicio no tiene vida por sí mismo, sino que en su estructura, en su contenido y fines a de marchar paralelamente al derecho penal, respondiendo al estado en que este se halle.

Con relación a la naturaleza jurídica de la acción nos dice: Que en el campo penal, debe considerarse el derecho de acción como un derecho autónomo, o por lo mismo distinto del derecho subjetivo de castigar del Estado, el cual lo hace valer por medio de la acción cuando existen los presupuestos para ello. Y que debe observarse que el ejercicio no puede delegarse en órganos que no sean estatales y que la improcedencia de la acción no prejuzga la existencia de aquél derecho.

LEONE, Giovanni en su obra Tratado de Derecho Procesal Penal Edit. Ediciones Jurídicas Europa-América Argentina (1994); nos explica que "por su particular función y sus particulares aspectos, la acción penal se presenta a una primera visión empírica, como la actividad de un órgano del Estado encaminada a obtener una decisión del juez penal en relación a un hecho que constituye delito y que se supone cometido por alguien. Pero que cuando se parte, sin embargo de una configuración jurídica de dicha actividad, se perfilan las posiciones siguientes:" Pág. 9-10.

a) La acción penal como derecho subjetivo frente al juez.
b) La acción penal como derecho potestativo.
c) La acción penal como manifestación de voluntad a la cual está condicionado el ejercicio de la jurisdicción penal.

Se puede definir a la acción penal también como el requerimiento del Ministerio Público de una decisión del juez sobre una noticia de crimen (notitiacriminis), que tiene como contenido un hecho determinado correspondiente a una hipótesis penal; y agrega, que a fin de intentar un nuevo camino que represente la confluencia de las dos distintas concepciones de la acción como derecho subjetivo y de la acción como derecho potestativo, cree preciso fijar ciertas premisas, como son:

a. La acción penal es obligatoria.
b. La acción penal determina la obligación del juez de emitir la requerida decisión sobre la deducida notitia criminis.
c. La acción penal no determina obligación alguna a cargo del imputado, una situación de sujeción, por cuanto él nada puede hacer para alejar de sí el hecho jurídico producido por la acción.

www.latinoseguridad.com: "La acción penal es en la doctrina más generalizada, el poder jurídico de promover la actuación jurisdiccional a fin de que el juzgador pronuncie acerca de la punibilidad de hechos que el titular de aquélla reputa constitutivos de delito". No supone en definitiva, sino el ejercicio del derecho de acusación por quien lo tenga atribuido como medio de provocar el ejercicio del derecho para penar por parte del Estado, a quien corresponde y que en lugar de proceder directamente al castigo del culpable, hace depender su aplicación del resultado de un proceso jurisdiccional, en el que la defensa del inculpado se halle garantizada.

BORJA OSORNO, Guillermo; en su obra titulada Derecho Procesal Penal (1996), nos comenta que "la acción penal surge de un delito, son sus presupuestos precisamente delito y delincuente. De todo acto con apariencias delictivas, que ataca la existencia y la conservación de la sociedad, nace la acción penal para la sanción del culpable". Pág. 4.

Desde el punto de vista personal y analizando las diversas concepciones de los autores citados diremos que la acción penal es la facultad que tiene el Ministerio Público para provocar la función del órgano jurisdiccional, siempre que se hayan reunido los elementos que integran el tipo penal y la presunta responsabilidad, con la finalidad de que se aplique la pena correspondiente, al responsable de la comisión de un delito que tenga el carácter de punitivo en la ley.

La acción penal es aquella que se origina a partir de un delito y que supone la imposición de un castigo al responsable de acuerdo a lo establecido por la ley; de esta manera, la acción penal es el punto de partida del proceso judicial**.** La acción penal, por lo tanto, supone un ejercicio de poder por parte del Estado y un derecho a la tutela para los ciudadanos que sufren las consecuencias de un delito cometido contra su persona**.**

Una vez iniciada una acción penal, su primera etapa consiste en la investigación (la búsqueda de pruebas), la persecución (el ejercicio de la acción ante el tribunal competente) y la acusación (se exige un castigo). Durante el juicio, cada uno de estos pasos es concretado y, en base a la acción, el juez se encarga de dictar la resolución conforme a lo estipulado por las leyes vigentes.

1.3.1.1. Donde Nace la Acción Penal

Los orígenes de la acción penal se remontan a los tiempos en que el Estado se hizo acreedor del monopolio del uso de la fuerza. En este sentido, la acción penal viene a remplazar a la venganza personal o a la autodefensa, ya que es el Estado el que asume la defensa y el resarcimiento del derecho que tienen sus ciudadanos.

El antecedente más remoto del Ministerio Público quizá lo encontremos en Grecia en la figura del arconte, magistrado que intervenía en los juicios en representación del ofendido y sus familiares por la incapacidad o la negligencia de éstos. Se ha insistido, sin embargo, que entre los atenienses la persecución de los delitos era una facultad otorgada a la víctima y a sus familiares.

En Roma los funcionarios denominados "judices questiones" tenían una actividad semejante a la del Ministerio Público por cuanto estaban facultados para comprobar los hechos delictivos, pero sus atribuciones características eran puramente jurisdiccionales. El Procurador del César, del que habla el Digesto en

el libro primero, título diecinueve, ha sido considerado también como un antecedente de la institución debido a que, en representación del César, tenía facultades para intervenir en las causas fiscales y cuidar el orden en las provincias del Imperio.

Más tarde, a mediados del siglo XIV el Ministerio Público interviene en forma abierta en los juicios del orden penal, pero sus funciones se precisan de modo más claro durante la época napoleónica en la que, inclusive, se estableció su dependencia del poder ejecutivo por considerársele como representante del interés social en la persecución de los delitos.

1.3.1.2. Características de la Acción Penal

a) Carácter Público de la Acción Penal.

www.latinoseguridad.com: Tomando en consideración el fin y el objeto de la acción penal, la doctrina le atribuye un carácter público debido a que "se dirige a hacer valer el derecho público del Estado a la aplicación de la pena a quien ha cometido el delito; aunque el delito cause un daño privado, la sociedad está interesada fundamentalmente en la aplicación de la pena destinada a protegerla.
Se ha afirmado que la acción penal pierde en parte el carácter de pública al instituirse la querella; pero, tal institución no modifica de ninguna forma su carácter público pues únicamente queda condicionada a un requisito de procedibilidad".

La acción penal es pública, porque tiende a satisfacer un interés público o colectivo, porque pertenece a la sociedad a quien defiende y protege, porque son públicos su fin y su objeto, porque es público el derecho que lo rige y porque público es también el órgano que la ejercita.

Tal como nos dice MAURACH, Reinhart, en su obra Tratado de Derecho Penal, Edit. Jurídico Andina, (1994);quien manifiesta que esto quiere decir que "el derecho a castigar al culpable pase de manos del Estado, que es a quien exclusivamente le corresponde, a las del ofendido por el delito ni tampoco que la facultad de ejercitar la acción, que incumbe a la Fiscalía pertenezca en esta clase de delitos al particular. El titular del derecho de castigar sigue siendo el Estado, y el ejercicio de la acción en todo momento va a verificarse por el Ministerio Público; hoy Fiscalía". Pág. 13.

b) Carácter Único de la Acción Penal.

Porque no existe una acción en especial para cada delito, sino que se utiliza por igual para toda conducta, que envuelve en su conjunto a todos los delitos, ya que su fin y su estructura son siempre los mismos y no es aceptable que se le asigne diferentes modalidades como las que se establecen en relación a las conductas típicas.

La acción penal es única, ya que del conocimiento del delito o delitos que se hubieren cometido, la Fiscalía se encargará de reunir todas las pruebas y vestigios que encierren éstos en forma general, la persecución e investigación siempre será para la conducta típica de que se trate de los delitos sin que se establezca en la investigación modalidades diferentes como las que se establecen en relación a los delitos.

c) Carácter Indivisible de la Acción Penal.

Es indivisible debido a que produce efectos para todos los que toman parte en la concepción, preparación y ejecución de los delitos o para quienes les auxilian por concierto previo o posterior. Su ejercicio recae en contra de todos los participantes del hecho delictuoso; no se puede perseguir solo a uno o algunos de los responsables.

d) Carácter Intranscendental de la Acción Penal.

La acción penal, no puede ser trascendental, ya que sus efectos deben limitarse solamente a la persona responsable del delito por lo que no puede extenderse la acusación a familiares o terceros, la acción penal siempre se llevará a cabo hacia la persona física que se imputa el delito con las pruebas debidamente relacionadas a la conducta típica.

e) Carácter Inevitable y Obligatorio de la Acción Penal.

Es obligatorio que la Fiscalía en cuanto tenga reunidos los requisitos legales para ejercitar la acción penal, la inicie y una vez ejercitado, no puede dejar de cumplir con los actos posteriores.

La inevitabilidad de la acción penal consiste en que no se puede aplicar ninguna pena sino a través del ejercicio de la acción penal que provoque una decisión jurisdiccional. La Acción es necesaria para obtener tanto una declaración negativa como afirmativa.

f) Carácter Autónomo de la Acción Penal.

Significa que la acción penal es independiente a la función jurisdiccional, lo que no se debe confundir con un poder potestativo del estado o por lo menos no ejercitándolo a su libre arbitrio, sino más bien este deber como atribución de la Fiscalía, debe ejercitarse sin que para este ejercicio deba intervenir algún otro órgano o institución del Estado.

1.3.1.3. Principios Fundamentales de la Acción Pena

a) Principio de Legalidad.

Esto significa que la Fiscalía tiene la obligación de ejercitar la acción penal cuando se hayan llenado los extremos del derecho material y procesal, ya que el proceso no es un acto discrecional de la Fiscalía. La mayoría de los países del mundo, entre estos el nuestro han adoptado el principio de legalidad.

b) Principio Oficioso de la Acción Penal.

Para algunos autores la oficialidad significa asignar a órganos especiales del estado el oficio de promover y ejercitar la acción penal; para otros la oficiosidad se identifica con la publicidad, oficiosidad es frecuentemente confundido con el principio de la publicidad de la acción del cual no es indeclinable corolario, ya que de la publicidad de la acción no podemos deducir su oficialidad. El principio de la oficialidad consiste en que el ejercicio de la acción penal debe darse siempre a un órgano especial del Estado llamado Fiscalía, distinto del jurisdiccional, y no a cualquier ciudadano ni a la parte lesionad.

d) Principio de la Verdad Real, Material o Histórico de la Acción Penal.

La aplicación de este principio a la acción penal, y al Ministerio Público que es quien la ejercita, es clara. La acción penal deberá dirigirse a la búsqueda de la verdad material o real, y no a establecer formalismos que comprometan al procesado, creando así un concepto erróneo de la realidad de los hechos. El Ministerio Público no es un acusador forzoso que deba siempre perseguir al procesado, a pesar de su inocencia."

1.3.1.4. Historia e Importancia de la Acción Penal en el Derecho Procesal Penal

Con mucha claridad, la doctrina asegura que el principio según el cual el estado persigue el delito de oficio no puede ser hallado en los derechos antiguos. En el antiguo derecho romano se desarrolló lo que se denomina la acción popular y en los derechos germanos la acción privada.

Se dice que en la antigüedad la persona que sufría un daño ejercitaba la acción penal. Era los tiempos de la venganza privada cuando el hombre defendía por sí mismo sus derechos, había la ley del Talión que establecía que al agresor se le aplicara lo mismo que él le había hecho al ofendido.

La ley del Talión era la similitud de la venganza .El Talión representa limitaciones objetivas de la venganza, la primera mediante la proporción del castigo a la materialidad de la ofensa. La segunda limitación objetiva de la venganza era la composición, que era una indemnización que, como pena pecuniaria, está obligada a aceptar el ofendido.

En el siglo XII A.C. ,en Grecia, Dracón optó por imponer la pena de muerte a todos los delitos .Hubo periodos donde se prescindió de la ley del Talión , pero un siglo después Solón la volvió a restablecer pero con un sentido más jurídico .

ROXIN Claus, en su obra traducida al español, La Evolución de la Política Criminal, El Derecho Penal y el Proceso Penal, Tirant Lo Blanch, (1993); hace recuerdo que "en el caso de la acción privada, el procedimiento penal era iniciado por acción del ofendido o de su familia. Esta regulación halló su fundamento en que originariamente no se distinguía entre consecuencias jurídicas, civiles y penales de un hecho y, por consiguiente, tampoco entre procedimiento civil y

penal; si se puede indemnizar un daño corporal a través del pago de una enmienda al lesionado o un homicidio pagando un importe de dinero a la familia del muerto, entonces no hay mucho interés público en la causa y el procedimiento penal transcurre de un modo similar a un proceso civil en el cual, a causa de una acción no permitida ,se reclama una reparación del daño". Pág.31.

Por la acción popular, los ciudadanos tuvieron en sus manos el ejercicio de la acción, no solo el ofendido del delito, sino también los ciudadanos solicitaban a la autoridad la represión del ilícito. La acción popular tiene su origen en Roma, se nombraba a un ciudadano para que llevara ante el tribunal del pueblo la voz de la acusación.

En Grecia, en cambio, existían los temosteti cuyo deber era denunciar los delitos ante el senado. Durante la Edad Media, los señores feudales eran quienes ejercitaban dicha acción; se abandona la idea de que el ofendido del delito fuera el encargado de acusar y se ponía en manos de un ciudadano independiente el ejercicio de la acción, se reformaba así el procedimiento toda vez que un tercero ajeno a la víctima del delito era quien perseguía al responsable y procuraba su castigo.

Debemos puntualizar que dentro del derecho griego, el Rey, el concejo de ancianos y la asamblea del pueblo, en ciertos casos llevaban a cabo juicios orales de carácter público para sancionar a quienes ejecutaban actos que atentaban contra los usos y costumbres. El ofendido, o cualquier ciudadano, presentaban y sostenía acusación ante el Arconte; el acusado se defendía a sí mismo, aunque en ciertas ocasiones le auxiliaban algunas personas.

Los romanos adoptaron, poco a poco, las instituciones del derecho griego y con el tiempo las transformaron, otorgándoles características muy peculiares que, más

tarde, se emplearían a manera del modelo clásico, para establecer el moderno Derecho de Procedimientos Penales.

1.3.1.5. La Acción Procesal

Para estudiar las diferentes teorías de la acción, en sus diversas concepciones, utilizadas por la doctrina de muchos tratadistas, se hace necesario el conocimiento de las" diferentes opiniones que sobre la acción han empleado los doctrinarios a través de los tiempos; lo que se considera son las más importantes concepciones, sin despreciar, obviamente, la valía de otros autores.

COUTURE ETCHEVERRY, Eduardo J., quien en su obra Fundamentos del Derecho Procesal Civil (1991) dice: que "la acción es el poder jurídico que tiene todo sujeto de derecho de acudir a los órganos jurisdiccionales para reclamarles la satisfacción de una pretensión; este derecho ha sido confundido históricamente con otros poderes jurídicos y facultades a los que se confiere el mismo nombre".Pág.6.

Pero la doctrina, asegura luego de una tarea que lleva casi un siglo, ha logrado aislarlo y determinar su esencia, habiendo sido objeto de una formulación especial en el Art. 10 de la Declaración Universal de los Derechos Humanas aprobada por la Asamblea General de las Naciones Unidas el 10 de diciembre de 1948.

La acción en justicia es en cierto modo, a criterio del autor antes indicado es el sustitutivo civilizado de la venganza, por ello estas consideraciones nos llevan hacia el carácter público de la acción, en cuanto a su finalidad inmediata. La acción no procura solamente la satisfacción de un interés particular, sino también la satisfacción de un interés de carácter público.

1.3.1.6. Función de la Acción Penal en el Código de Procedimiento Penal

VACA ANDRADE, Ricardo en su Manual de Derecho Procesal Penal, (1999) señala con claridad, que "así como a los particulares les está prohibido realizar actos violentos de autodefensa de sus derechos, la prohibición rige también para el Estado, por ello, cuando se comete un delito o un hecho que tiene apariencia de delito, las autoridades públicas no aplican de manera directa e inmediata las sanciones previstas en la ley penal sustantiva". Pág. 20.

Es indispensable que, previamente, se instaure un proceso penal de acuerdo a las normas constitucionales y del Derecho Procesal Penal, para garantizar efectivamente el derecho a la defensa que tiene el sospechoso o el imputado. Así mirado, el proceso penal es, a la vez, un instrumento de juzgamiento y hasta de represión, si se quiere, pero también lo es de respeto a las garantías constitucionales, en cuanto, tan solo cuando se han cumplido los actos procesales pertinentes a cada etapa, de investigación y de juzgamiento, se puede declarar oficialmente si una persona es culpable o inocente.

Por ello se puede afirmar que el fundamento del ejercicio de la acción penal, antes que legal, en el caso ecuatoriano, es eminentemente constitucional, en virtud de que una vez perpetrado el delito, la acción penal entra en funcionamiento. Debemos recalcar que la tutela efectiva es un derecho de protección que se encuentra elevado a rango constitucional (Art. 75 de la Constitución) y también se encuentra desarrollado en el artículo 23 del Código Orgánico de la Función Judicial como principio de tutela judicial efectiva de los derechos.

Podemos decir, que el fundamento de la acción Penal está contenido de manera constitucional en la disposición constitucional arriba transcrita y que la acción

penal es un verdadero derecho a la tutela jurídica. El ejercicio de la acción penal pública en facultad de la Fiscalía está expresamente señalado en el artículo 195 de la Constitución de la República.

La acción es un poder jurídico concedido por Estado a las personas. Pero esta acción, se dice como tal poder, no puede ejercerse, no puede tomar vida hasta tanto no se cometa la infracción, por lo cual decimos que la infracción es el presupuesto necesario para el ejercicio dela acción. "Entre la acción y el ejercicio de la acción media la infracción". En consecuencia, ésta no es el objeto de la acción, es el presupuesto del ejercicio de la acción.

En el antiguo Código de Procedimiento Penal se establecían como modos de ejercer la acción penal la excitación fiscal, la denuncia, la acusación particular, la pesquisa que de oficio efectúa el juez, el parte policial informativo o la indagación policial o la orden superior de origen administrativo.

Es importante anotar que de acuerdo con las últimas reformas al Código Procesal se sustituyó el artículo 37 por el siguiente:

Art. 37.- Las acciones por delitos de acción pública pueden ser transformadas en acciones privadas, a pedido del ofendido o su representante, siempre que el juez de garantías penales lo autorice. El fiscal podrá allanarse a este pedido; de no hacerlo, argumentará al juez de garantías penales las razones de su negativa. No cabe la conversión:

a. Cuando se trate de delitos que comprometan de manera seria el interés social.
b. Cuando se trate de delitos contra la administración pública o que afectan los intereses del Estado.

c. Cuando se trate de delitos de violencia sexual, violencia intrafamiliar o delitos de odio.
d. Cuando se trate de crímenes de lesa humanidad.
e. Cuando la pena máxima prevista para el delito sea superior a cinco años de prisión.

Si hubiere pluralidad de ofendidos, es necesario el consentimiento de todos ellos, aunque solo uno haya presentado la acusación particular. Transformada la acción cesarán todas las medidas cautelares que se hayan dictado. Si el ofendido decide presentarse como querellante para iniciar la acción privada, será competente el mismo juez de garantías penales que conocía del proceso en la acción pública.

1.3.1.7. División de la Acción Penal

Se entiende por acción penal la facultad de perseguir o hacer perseguir las responsabilidades por un delito; en nuestro país la acción penal puede ser de dos tipos o clases estas Acción Penal Pública y Privada.

La acción penal pública es aquélla que puede ser ejercida de oficio es decir, de propia iniciativa, sin necesidad de petición previa por los órganos estatales encargados de la persecución penal, esto es, por los Fiscales; es más estos están obligados a ejercerla, en virtud del principio de legalidad, salvo en los casos expresamente previstos por la ley, los delitos de acción pública constituyen la regla absolutamente general en nuestro sistema. En algunos pocos casos, el ejercicio de la acción penal pública está supeditado en su inicio a que la víctima del delito al menos denuncie el mismo a los tribunales, a los fiscales del Ministerio Público o a la policía; éstos son los llamados delitos de acción pública previa instancia particular, y son, entre otros, los de lesiones menos graves, violación de domicilio, entre otros.

En cambio en la acción penal privada puede ser ejercida única y exclusivamente por la víctima del delito, quien, además, puede ponerle término cuando quiera; son muy pocos los delitos de acción privada, destacándose entre ellos los de calumnia e injurias; en estos casos el Ministerio Público no juega ningún papel. Según el Art. 32 del Código de Procedimiento Penal "la acción penal puede ser pública o privada".

1.3.1.7.1. Acción Penal Privada.

Se denomina delito privado o delito de acción privada, en Derecho procesal penal, a un tipo de delito que, por no considerarse de una gravedad tal que afecte al orden público de la sociedad, no puede ser perseguido de oficio por los poderes públicos (es decir, policía, Jueces o Fiscalía), sino que es necesaria la intervención activa de la víctima como impulsora de la acción de la justicia y como parte en el proceso judicial.

El cauce procesal a través del cual una víctima de un delito de acción privada puede perseguir la acción de la justicia se denomina querella; sobre los siguientes delitos:

- El estupro perpetrado en una mujer mayor de dieciséis años y menor de dieciocho.
- El rapto de una mujer mayor de dieciséis años y menor de dieciocho, que hubiese consentido en su rapto y seguido voluntariamente al raptor.
- La injuria calumniosa y la no calumniosa grave.
- Los daños ocasionados en propiedad privada, excepto el incendio.
- La usurpación.
- La muerte a animales domésticos o domesticados.
- El atentado al pudor de un mayor de edad.

Estos procesos se inician, con la presentación de una querella, por parte del ofendido o de un apoderado especial, directamente ante un Juez de Garantías Penales, la misma que debe constar por escrito y contener los requisitos que se enumeran en el artículo 371 del Código de Procedimiento Penal en vigencia.

1.3.1.7.2. Características de la Acción Penal Privada.

www.poderjudicial-gto.gob.mx. (II Encuentro Estatal de Jueces Lic. MARTINEZ PEREZ, Ernesto) determinan las características de la acción privada de la siguiente manera:

Voluntaria.- En el acto de promover la acción penal privada prima la voluntad del titular.

Renunciable.- La acción penal privada es renunciable. La acción penal privada, al ser ejercida por un interés particular, podrá ser renunciable por el mismo que la promovió.

Relativa.- La acción penal privada es relativa, por cuanto la administración de todo el proceso penal y, sobre todo, la capacidad de ejercitar el iuspuniendi está en manos del Estado, el particular tiene por tanto sólo facultades que se enmarcan dentro del control penal estatal.

Por último, cabe señalar que la acción penal privada en la mayoría de los países se encuentra limitada a unos cuantos delitos referidos mayormente al honor y los que afectan bienes jurídicos íntimos de la persona humana, violación de la intimidad personal o familiar, entre otros.

1.3.2. Acción Penal Pública

1.3.2.1. Definición

La acción penal pública es aquella ejercida de forma exclusiva, excluyente y de oficio por la Fiscalía, según de qué normativa procesal se trate, para la persecución de un delito.

En los procesos criminales lo común es la acción pública. En general, la mayoría de estos delitos comienzan a investigarse a partir de una denuncia, pero pueden ser investigados tan pronto tengan los poderes públicos conocimiento de los hechos por cualquier medio. Llegada la noticia de un posible crimen a los organismos del Estado, este actúa sin necesidad de intervención o pedidos de persona alguna, ni siquiera de la víctima directa del crimen, o sus herederos.

El fundamento de la acción pública es que se considera que la sociedad en su totalidad ha sido perjudicada por el delito cometido y el Estado asume entonces el papel de defensa de la sociedad. La mayoría de los países incluye todos, o casi todos, los delitos contemplados en su legislación como de acción pública.

1.3.2.2. Características de la Acción Penal Pública

Se afirma que varias son las características de la acción penal pública:

a) **Publicidad.-** Se dice que por su importancia en la vida de la sociedad, el Estado ha dispuesto que su actividad sea fundamentalmente dirigida a reintegrar la paz social perturbada por el delito, y por ello, La Fiscalía General del Estado, como ente protector de la sociedad ejerce a plenitud integralmente durante todo el desarrollo del proceso penal la acción penal.

b) **Oficialidad.** Se considera un verdadero monopolio de la Fiscalía General del Estado que la Constitución haya determinado que sea el titular de la acción penal pública. Recordemos que en la Constitución de 1998 esta entidad era adscrita al Estado, en cambio en el nuevo marco constitucional y legal del 2008, la Fiscalía General es un órgano de la Función judicial cuyo ámbito de actuación está señalado en la Constitución, en el Código Orgánico de la Función Judicial y en el Código de Procedimiento Penal.

c) **Indivisibilidad.-** La acción penal es única, si bien en el proceso aparecen actos diversos promovidos por el titular de la acción penal, la acción es única y tiene una sola pretensión; la sanción penal que alcanza a todos los que han participado en la comisión del delito. No existen distintas acciones que correspondan a cada agente, sino una acción indivisible.

d) **Obligatoriedad.-** Existe la obligación por parte de la Fiscalía General del Estado de ejercitar la acción penal ante la noticia de la resunta comisión de un hecho ilícito.

En otro aspecto es importante señalar que la acción penal pública es irrenunciable por cuanto quienes ejercen la acción según se asevera, no pueden retractarse del dictamen fiscal acusatorio, de la denuncia o de la acusación particular, con el propósito de impedir que continúe la sustanciación de la causa, pues si bien es verdad que de acuerdo a lo establecido en el Código de Procedimiento Penal cabe el desistimiento de la acusación particular en los procesos por delitos de acción pública, el trámite continúa con la sola intervención del fiscal, ya que de acuerdo con el Código Penal, el perdón de la parte ofendida o la transacción con ésta no extingue la acción pública por una infracción que debe perseguirse de oficio.

1.3.2.3. Acción Penal, Ejercicio de las Etapas del Proceso

El ejercicio de la acción penal se realiza cuando el Ministerio Público concurre ante el Juez y le solicita que avoque conocimiento de un asunto en particular; la acción penal pasa durante el proceso, por tres etapas bien diferenciadas que son: indagación previa, instrucción fiscal, etapa intermedia, etapa de juicio.

1.3.2.3.1. Definición de Indagación.

También conocida como etapa procesal o preparatoria, está constituida por actos de investigación que permiten el aseguramiento de elementos de convicción, para poder probar la existencia del hecho en la etapa de juicio y quien o quienes participaron en el mismo. Indagar, tratar de llegar a saber cierta cosa, averiguar. Por mandato Constitucional le corresponde a la Fiscalía prevenir e investigar los hechos en el conocimiento de las causas de oficio o previa denuncia (petición de parte), dirigir y promover esta investigación pre-procesal la cual no debe prolongarse por más de un año en los delitos sancionados con pena de prisión y de dos años en aquellos sancionados con reclusión.

El Código de Procedimiento penal en su Art. 215 nos dice respecto de la indagación previa, que " La Fiscalía o el Fiscal, con la colaboración de la Policía Judicial que actuará bajo su dirección, investigará los hechos presuntamente constitutivos de infracción penal que por cualquier medio hayan llegado a su conocimientos"; esta función además de permitir que la investigación de las infracciones punibles sea realizada bajo parámetros de mayor eficiencia y asegurar la imparcialidad judicial, conlleva la responsabilidad no solo de que la investigación se realice sino de los resultados.

La dirección de la investigación en cuanto a la planificación de la estrategia de persecución penal e investigación significa determinar dos cosas, la primera es

determinar cuál es el delito a perseguir y posteriormente investigar; y dos, establecer cuáles son los elementos del delito que requieren ser probados en juicio; consiguientemente, cuáles diligencias de investigación son relevantes y pertinentes para ello. Es decir el Fiscal es el responsable de ejecutar la estrategia directamente o por delegación a la Policía Judicial en lo que la ley le permite, sin que ello signifique que en la práctica no exista una interacción entre las dos instituciones que permita integrar la experiencia de la policía y de otros organismos de apoyo a la labor de la Fiscalía.

El Fiscal, como representante de la Fiscalía, tiene la facultad de actuar en forma autónoma para realizar por sí mismo las diligencias de investigación, pues el Código de Procedimiento penal regula un conjunto de facultades específicas para recopilar información de toda persona o funcionario público quienes no pueden excusarse de proporcionarla salvo las excepciones contempladas en la misma ley.

Entre otras, la posibilidad de citar a declarar o entrevistar a víctimas, testigos y al mismo imputado, ordenar la realización de pericias, decretar la vigilancia de un lugar para evitar la fuga de un sospechoso o la desaparición de evidencias. No obstante también tiene como facultad, delegar algunas diligencias investigativas a la Policía Judicial.

Características.

Las características de esta etapa del proceso se pueden resumir de la siguiente manera:

- La fiscalía tiene plena vigencia de facultades para poder realizar diligencias de investigación para establecer con precisión que se ha cometido un delito.
- Es el periodo en el que se pueden generar actividades de investigación, sin la presión que genera el dictar la Instrucción Fiscal.

- La pesquisa que se practica por parte del fiscal, tiene que desarrollarse dentro del esquema de respeto a las reglas dentro de las reglas establecidas para el debido proceso.
- Los resultados que se obtengan pueden servir de base de sustentación, para las demás etapas del proceso. Por lo antes indicado, nunca podrá alegarse que lo que se obtenga en esta fase, es fruto de algo sumario, dudoso o escondido. Todo tiene que ser parte de la eficiencia y habilidad del fiscal para manejarse correctamente en esta etapa del proceso.
- Principio de inmediación y celeridad establecidos en la Constitución de la República en su artículo 75.

Procedimiento.

El Código de Procedimiento Penal expresa que cuando el fiscal considere necesario, con el auxilio de la policía judicial, iniciara la investigación de la supuesta comisión de un hecho delictivo que por cualquier medio haya llegado a su conocimiento.

En esta fase el fiscal está facultado a practicar medios de investigación e inclusive a practicar diligencias tales como: recepción de versiones, realizar peritajes, presentarse a la escena del crimen, obtención de información por medio de documentos y solicitar al órgano jurisdiccional algunas medidas cautelares, tales como allanamientos, toma de fluidos corporales, intervención de líneas telefónicas, apertura de correspondencia y grabaciones, por lo tanto a partir de esta fase procesal que es la primera se puede construir el caso.

En cuanto a la reserva de estas actuaciones realizadas por la fiscalía, sin perjuicio de las garantías del debido proceso establecidas y del derecho a la defensa; las actuaciones para el esclarecimiento del delito durante esta fase, se mantendrá en reserva del público en general, sin perjuicio del derecho del ofendido, y de las

personas a quienes se les investiga de tener acceso inmediato, efectivo y suficiente de las investigaciones.

1.3.2.3.2. Instrucción Fiscal.

En la persecución, hay ya un ejercicio de la acción ante los tribunales y se dan los actos persecutorios que constituyen la instrucción y que caracterizan este período. Esta es una etapa del proceso penal en la que el Fiscal en el ejercicio de sus atribuciones, dicta providencias en la cual vincula al imputado directamente al proceso, en virtud de existir a su juicio motivos suficientes sobre su posible participación en el hecho que se investiga. Tiene una duración de noventa días improrrogables y se empiezan a contar a partir de la fecha de notificación al imputado o, de ser el caso, al defensor público o al defensor de oficio designado por el Juez.

En el Art. 221 del Código de Procedimiento Penal contempla la figura de la vinculación, mediante la cual podrá hacerse extensiva la instrucción, por un plazo adicional de treinta días de duración a partir de la notificación con esa resolución al nuevo imputado o al defensor público o de oficio designado por la autoridad respectiva.

Objetivo de la Instrucción Fiscal.

El objetivo principal de esta fase es la de encontrar los elementos necesarios para poder determinar si el imputado tiene responsabilidad en el hecho en el que se le imputa, su vinculación o relación objetiva, asimismo si el acto es constitutivo de delito. Naturalmente para poder llegar al objetivo planteado en esta fase, pueden variar sustancialmente los procedimientos, ya que todos dependerán de la forma en que se inicia el proceso; por una parte podemos encontrar que el caso aparezca como primer acto una denuncia a través de un parte informativo policial, en donde pueden surgir sospechosos o bien que no exista en ese momento alguno

individualizado. En el segundo caso el expediente puede llegar a la oficina del fiscal con una persona detenida en hecho flagrante por la policía.

1.3.2.3.3. Etapa Intermedia.

Que le corresponde privativamente a un juez de derecho, en la que se convoca a las partes procesales a una Audiencia preliminar, y en la que luego de escuchar a las partes procesales, básicamente el juez analiza todo lo actuado por el Fiscal, luego de lo cual dictamina si procede o no el llamamiento a juicio del imputado. En esta etapa el juez puede dictar auto de llamamiento a juicio o auto de sobreseimiento ya sea éste provisional o definitivo.

Es importante señalar que en los juicios de instancia pública oficial o pública de instancia particular, en el que inclusive el ofendido haya presentado su acusación particular, si el Fiscal se abstiene de emitir acusación fiscal, no hay proceso y no se podrá iniciar ningún juicio. Este hecho podría modificarse si el Juez al consultar al Fiscal Superior, cambia de criterio y presenta acusación fiscal, iniciándose así el proceso. En caso contrario, de que el Fiscal Superior ratifique el pronunciamiento del Fiscal inferior, definitivamente no existiría forma de dar inicio al proceso penal. Art. 226 del C. P. P.

El juez evaluará todo lo planteado durante la Instrucción Fiscal, escuchará a las partes y posteriormente decidirá si hay o no presunciones de culpabilidad suficientes para la apertura del juicio. Durante esta audiencia, los sujetos procesales solamente podrán presentar prueba documental para fundamentar sus disposiciones.

Puede ocurrir que en la audiencia preliminar mencionada, el fiscal normalice su acusación, por cuanto éste considere que no existen suficientes indicios para implicar a los acusados, en el cometimiento del delito. En este caso, si luego de

realizada la audiencia, el juez considera necesaria la iniciación del juicio, deberá ordenar que se remitan las actuaciones al fiscal superior para que niegue o ratifique el pronunciamiento del fiscal inferior.

En caso de que el fiscal superior ratifique la opinión del fiscal que realizó la instrucción, el Juez tendrá que aceptar este pronunciamiento como definitivo y dictar el sobreseimiento. En ningún caso, el Juez podrá continuar el proceso y ordenar la apertura del juicio sin la acusación del Fiscal. Esto se debe a que en este proceso, siendo la Fiscalía el titular del ejercicio de la acción penal no puede haber juicio sin una acusación fiscal, de manera que si el fiscal de la causa o su superior no se pronuncian acusatoriamente termina el proceso.

1.3.2.3.4. El Auto de Sobreseimiento.

Sin la acusación fiscal o si a pesar de ella, el juez considera que no se ha demostrado la existencia de la infracción o que no existen los suficientes indicios de la participación del imputado se detendrá la iniciación del proceso penal propiamente dicho, mediante un auto de sobreseimiento que, según la propuesta, suspenderá la substanciación del proceso durante tres años, período dentro del cual únicamente sobre la base de nuevas investigaciones, el fiscal podrá formular una nueva acusación. Transcurrido este tiempo, el sobreseimiento se volverá definitivo (en firme) y se pondrá fin al proceso, sin que el imputado pueda ser nuevamente investigado por este mismo motivo.

De esta manera se modifican las actuales tres clases de sobreseimiento (provisional del proceso y del sindicado, provisional del proceso y definitiva del sindicado; y, definitiva del proceso y del sindicado) por las de sobreseimiento y la de sobreseimiento en firme.

En el caso contrario, si se considera que la acusación del fiscal tiene fundamento, el Juez debe radicar el auto de apertura a juicio, con lo que concluirá esta etapa o se deberá poner el caso inmediatamente en conocimiento del Tribunal penal. Entonces se iniciará la tercera etapa del proceso llamada esta del juicio.

1.3.2.3.5. Etapa del Juicio.

Esta etapa se iniciará con la substanciación del proceso ante el presidente del Tribunal Penal, quien estaría obligado en primera instancia, a designar un defensor para el sindicado en caso de que éste se encuentre imposibilitado para contratarlo. Además deberá convocar a la Audiencia para el juzgamiento y solicitar a las partes que le entreguen la lista de los testigos, ya que estará encargado e dictar las órdenes respectivas para la comparecencia de los mismos. Como se había señalado anteriormente en la instrucción fiscal solo se investiga pero no se prueba, para que todas las indagaciones realizadas por el fiscal alcancen el valor de prueba, estas deberán ser presentadas ante el tribunal penal.

Propósitos de Esta Etapa.

Esta etapa, a criterio de varios autores en materia penal tendrá tres propósitos fundamentales:

a. La prueba de la existencia del delito.
b. La prueba de la culpabilidad del infractor.
c. La imposición de la pena correspondiente al delito cometido, de las medidas de seguridad y del pago del daño causado al ofendido.

Audiencia de Juicio.

Se respetarán los principio de contradicción, oralidad, publicidad, inmediación y concentración; el proyecto determina claramente cómo se realizara la substanciación ante el Tribunal Penal y los pasos que tendrán que seguirse, sobre

todo, en lo que se refiere al orden lógico de intervención de los sujetos procesales, la declaración de los testigos y peritos y la exhibición de pruebas.
Desde el Art. 285, se desarrolla el procedimiento a seguir, el mismo que se ha dividido en dos partes. La primera empezará con la intervención del fiscal, que estuvo a cargo de la instrucción (Art.286). En esta intervención se presentará la acusación y se solicitará que se practiquen las pruebas que se consideren necesarias. A continuación, el ofendido estará obligado a comparecer a juicio para rendir su testimonio, bajo juramento (Art.287), sin duda, este testimonio contribuirá al esclarecimiento de los hechos. Una vez presentado el testimonio, los miembros del Tribunal y los otros sujetos, procesales podrán interrogar al ofendido, siempre y cuando las preguntas sean debidamente formuladas.

A continuación, vendrá la exposición del acusador particular o de su defensor, quien realizará una exposición del motivo de su acusación y solicitará la práctica de las pruebas que considere necesarias, para finalizar esta primera fase de la audiencia, se receptará el testimonio de los peritos y de los testigos pedidos por el fiscal y por el acusado particular.

En la segunda parte de la audiencia, el acusado rendirá su testimonio voluntario, luego de lo cual, podrá ser interrogado por los miembros del Tribunal y las otras partes. Inmediatamente, deberá reconocer los objetos y vestigios de la infracción (Art.296).

Realizado el reconocimiento, el defensor del acusado hará una exposición detallada de los hechos y circunstancias favorables para su defendido y pedirá que se practiquen las pruebas de descargo (Art.297), luego de lo cual, el Tribunal procederá a tomar testimonios de los testigos presentados por el acusado, quienes también podrán ser interrogados por las partes (Art. 298).

Finalmente, se realizaran las demás pruebas ordenadas por el Tribunal y se dará lugar a un debate en el que las partes podrán exponer sus alegatos, luego de lo cual los miembros del Tribunal deberán deliberar sobre lo ocurrido.

Pronunciamiento de la Sentencia.

Si el Tribunal lo considera necesaria, podrá emitir la sentencia al día siguiente de la audiencia y si cree necesario que se reciban nuevas pruebas o que se vuelvan a practicar las ya evacuadas, lo ordenará así y suspenderá su pronunciamiento mientras se practiquen. Concluidos estos actos procesales, el presidente del Tribunal convocará a una nueva audiencia con la sola finalidad de reabrir el debate y pronunciar su sentencia.

1.3.2.3.6. Etapa de Impugnación.

En lo que se refiere a los recursos que se pueden ejercer dentro del proceso también se ha incluido una reforma, ya que se ha suprimido el llamado recurso de nulidad, dejando vigentes los recursos ordinarios de nulidad, apelación, casación y el de revisión.

En cuanto al recurso de apelación, deberá ser debidamente fundamentado y sólo procederá en los siguientes casos:

1. De los autos de nulidad, de prescripción de la acción, de llamamiento a juicio, de sobreseimiento y de inhibición por causa de incompetencia.
2. De la sentencia dictada en el procesos simplificados, procesos abreviados, y las que declaren la culpabilidad o confirmen la inocencia del acusado.
3. Del auto que concede o niega la prisión preventiva.

El recurso de nulidad como tal ha sido eliminado con la finalidad de agilitar la tramitación del proceso, pero se ha previsto que si el momento de resolver un

recurso la Corte respectiva observare una de las causales de nulidad contempladas en el Art.330 del C.P.P., estará obligada a declarar, de oficio o petición de parte, la nulidad del proceso desde el momento en que se produjo la nulidad siempre y cuando esta causa hubiera tenido la influencia en la decisión.

1.3.3. Delitos Informáticos

A continuación, mencionare algunas de las diferentes definiciones que se citan de cómo se puede definir al Delito Informático:

El Dr. TÉLLEZ VALDÉS, Julio menciona en su obra titulada Derecho Informático, (2010) "dos clasificaciones del Delito Informático para efectos de conceptuación, que parten de lo típico y lo atípico. El concepto típico, los Delitos Informáticos son las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin". Pág.19.

www.angelfire.com: DE LA LUZ LIMA, María; en su obra publicada en internet con el tema Modelos de Atención a Víctimas del Delito, dice que el "delito electrónico en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito Informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin."

El departamento de investigación de la Universidad de México, señala como delitos informáticos que son "todos aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio Informático.

El constante progreso tecnológico que experimenta la sociedad, supone una evolución en las formas de delinquir, dando lugar, tanto a la diversificación de los delitos tradicionales como a la aparición de nuevos actos ilícitos. Esta realidad ha originado un debate en torno a la necesidad de distinguir o no los delitos informáticos del resto.

Partiendo de esta compleja situación y tomando como referencia el "Convenio de Ciberdelincuencia del Consejo de Europa", podemos definir los delitos informáticos como: "los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos".

En el Ecuador así como en los demás países, todos los principios jurídicos, legales y procesales, así como doctrinarios, están presentes en el tratamiento del delito informático, su investigación y juzgamiento, sin embargo las características propias de este delito que pertenece a una nueva era, a la era de la información y el conocimiento, trasciende al ordenamiento jurídico vigente, constituyendo un elemento de inflexión o quiebre del tradicional sistema jurídico.

1.3.3.1. Bien Jurídico Protegido

El objeto jurídico es el bien lesionado o puesto en peligro por la conducta del sujeto activo. Jamás debe dejar de existir, ya que constituye la razón de ser del delito, y no suele estar expresamente señalado en los tipos penales.

1.3.3.1.1. Los Bienes Jurídicos Protegidos en el Delito Informático.

Dentro de los delitos informáticos, podemos decir que la tendencia es que la protección a los bienes jurídicos, se le haga desde la perspectiva de los delitos tradicionales, con una reinterpretación teleológica de los tipos penales ya

existentes, para subsanar las lagunas originadas por los novedosos comportamientos delictivos. Esto sin duda da como regla general que los bienes jurídicos protegidos, serán los mismos que los delitos reinterpretados teleológicamente o que se les ha agregado algún elemento nuevo para facilitar su persecución y sanción por parte del órgano jurisdiccional competente.

De otro lado otra vertiente doctrinaria supone que la emergente Sociedad de la Información hace totalmente necesaria la incorporación de valores inmateriales y de la información misma como bienes jurídicos de protección, esto tomando en cuenta las diferencias existentes por ejemplo entre la propiedad tangible y la intangible. Esto por cuanto la información no puede ser tratada de la misma forma en que se aplica la legislación actual a los bienes corporales, si bien dichos bienes tiene un valor intrínseco compartido, que es su valoración económica, es por tanto que ella la información y otros intangibles son objetos de propiedad, la cual está constitucionalmente protegida.

En conclusión podemos decir que el bien jurídico protegido en general es la información, pero está considerada en diferentes formas, ya sea como un valor económico, como uno valor intrínseco de la persona, por su fluidez y tráfico jurídico, y finalmente por los sistemas que la procesan o automatizan; los mismos que se equiparan a los bienes jurídicos protegidos tradicionales tales como:

- **El Patrimonio**.- En el caso de la amplia gama de fraudes informáticos y las manipulaciones de datos que da a lugar.

- **La Reserva, la Intimidad y Confidencialidad de los Datos**.- En el caso de las agresiones informáticas a la esfera de la intimidad en forma general, especialmente en el caso de los bancos de datos.

- **La Seguridad o Fiabilidad del Tráfico Jurídico y Probatorio**.- En el caso de falsificaciones de datos o documentos probatorios vía medios informáticos.

- **El Derecho de Propiedad**.- En este caso sobre la información o sobre los elementos físicos, materiales de un sistema informático, que es afectado por los de daños y el llamado terrorismo informático.

Por tanto el bien jurídico protegido, acoge a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde esta se almacena o transfiere.

Podemos decir que esta clase de delincuencia no solo afecta a un bien jurídico determinado, sino que la multiplicidad de conductas que la componen afectan a una diversidad de ellos que ponen en relieve intereses colectivos, en tal sentido de GUTIÉRREZ FRANCÉS, María Luz; (1990) respecto de la figura del fraude informático nos dice que: "las conductas de fraude informático presentan indudablemente un carácter pluri-ofensivo. En cada una de sus modalidades se produce una doble afección: la de un interés económico (ya sea micro o macro social), como la hacienda pública, el sistema crediticio, el patrimonio, etc., y la de un interés macro social vinculado al funcionamiento de los sistemas informáticos"**.** Pág.35.

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

En tal razón considero que este tipo de conductas criminales son de carácter netamente pluri-ofensivo. Un ejemplo que puede aclarar esta situación, es el de un hacker que ingresa a un sistema informático con el fin de vulnerar la seguridad éste y averiguar la información que más pueda sobre una determinada persona, esto en primer lugar podríamos decir que el bien jurídico lesionado o atacado es el derecho a la intimidad que posee esa persona al ver que su información personal es vista por un tercero extraño que sin autorización ha vulnerado el sistema informático donde dicha información está contenida. Pero detrás de ese bien jurídico encontramos otro un bien colectivo que conlleva a un ataque a la confianza en el funcionamiento de los sistemas informáticos. Es decir, de intereses socialmente valiosos que se ven afectados por estas nuevas figuras, y que no solo importan la afección de bienes jurídicos clásicos.

1.3.3.2. Tipos de Delitos Informáticos

Existen muchos tipos de delitos informáticos, la diversidad de comportamientos constitutivos de esta clase de ilícitos es inimaginable, a decir de CAMACHO LOSA, en un artículo publicado en el internet señala que el único límite existente viene dado por la conjugación de tres factores: la imaginación del autor, su capacidad técnica y las deficiencias de control existentes en las instalaciones informáticas, por tal razón y siguiendo la clasificación dada por el estadounidense DON B. Parker más la lista mínima de ilícitos informáticos señalados por las Naciones Unidas, he querido lograr una clasificación que desde el punto de vista objetivo sea lo más didáctica posible al momento de tratar esta clase de conductas delictivas, se ponemos a consideración del lector en forma breve en qué consiste cada una de estas conductas delictivas:

1.3.3.2.1. Los Fraudes.

Los Datos Falsos o Engañosos.

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

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.

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.

Falsificaciones Informáticas.

- **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.

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.

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.

Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes. El robo de identidad es uno de los delitos que más ha aumentado. La mayoría de las víctimas son golpeadas con secuestros de cuentas de tarjetas de crédito, pero para muchas otras la situación es aún peor. En los últimos c años, millones de personas han sido víctimas de delincuentes que han abierto cuentas de tarjetas de crédito o con empresas de servicio público, o que han solicitado hipotecas con el nombre de las víctimas, todo lo cual ha ocasionado una red fraudulenta que tardará años en poderse desenmarañar.

1.3.3.2.2. El sabotaje informático.

Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

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.

Gusanos.

Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

Virus Informáticos y Malware.

Son elementos informáticos, que como los microrganismos biológicos, tienden a reproducirse y a extenderse dentro del sistema al que acceden, se contagian de un sistema a otro, exhiben diversos grados de malignidad y son eventualmente, susceptibles de destrucción con el uso de ciertos antivirus, pero algunos son capaces de desarrollar bastante resistencia a estos.

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.

Ataques de Denegación de Servicio.

Estos ataques se basan en utilizar la mayor cantidad posible de recursos del sistema objetivo, de manera que nadie más pueda usarlos, perjudicando así seriamente la actuación del sistema, especialmente si debe dar servicio a mucho usuarios Ejemplos típicos de este ataque son: El consumo de memoria de la máquina víctima, hasta que se produce un error general en el sistema por falta de memoria, lo que la deja fuera de servicio, la apertura de cientos o miles de ventana, con el fin de que se pierda el foco del ratón y del teclado, de manera que la máquina ya no responde a pulsaciones de teclas o de los botones del ratón, siendo así totalmente inutilizada, en máquinas que deban funcionar ininterrumpidamente, cualquier interrupción en su servicio por ataques de este tipo puede acarrear consecuencias desastrosas.

1.3.3.2.3. El Espionaje Informático y el Robo o Hurto de Software.

Este tipo de delitos informáticos se pueden sub dividir en los siguientes:

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 Luis Camacho Loza, "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".

Reproducción no Autorizada de Programas Informáticos de Protección Legal.

Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado

dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, considero, que la reproducción no autorizada de programas informáticos no es un delito informático, debido a que, en primer lugar el bien jurídico protegido es en este caso el derecho de autor, la propiedad intelectual y en segundo lugar que la protección al software es uno de los contenidos específicos del Derecho informático al igual que los delitos informáticos, por tal razón considero que la piratería informática debe ser incluida dentro de la protección penal al software y no estar incluida dentro de las conductas que componen la delincuencia informática.

1.3.3.2.4. El Robo de Servicios.

Hurto del Tiempo del Computador.

Consiste en el hurto del tiempo de uso de las computadoras, un ejemplo de esto es el uso de Internet, en el cual una empresa proveedora de este servicio proporciona una clave de acceso al usuario de Internet, para que con esa clave pueda acceder al uso de la supercarretera de la información, pero sucede que el usuario de ese servicio da esa clave a otra persona que no está autorizada para usarlo, causándole un perjuicio patrimonial a la empresa proveedora de servicios.

Apropiación de Informaciones Residuales (Scavenging).

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

Parasitismo Informático (Piggybacking) y 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.

1.3.3.2.5. El Acceso no Autorizado a Servicios Informáticos.

Las Puertas Falsas (Trap Doors).

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

La Llave Maestra (Superzapping).

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

Su nombre deriva de un programa utilitario llamado *superzap,* que es un programa de acceso universal, que permite ingresar a un computador por muy protegido que se encuentre, es como una especie de llave que abre cualquier rincón del

computador. Mediante esta modalidad es posible alterar los registros de un fichero sin que quede constancia de tal modificación.

Pinchado de Líneas (Wiretapping).

Consiste en interferir las líneas telefónicas de transmisión de datos para recuperar la información que circula por ellas, por medio de un radio, un módem y una impresora.

Como se señaló anteriormente 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.

Piratas Informáticos o Hackers.

El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

1.3.3.3. Situación Internacional

Durante los últimos años se ha ido perfilando en el ámbito internacional un cierto consenso en las valoraciones político jurídicas de los problemas derivados del mal uso que se hace las computadoras, lo cual ha dado lugar a que, en algunos casos, se modifiquen los derechos penales nacionales.

En un primer término, debe considerarse que en 1983, la Organización de Cooperación y Desarrollo Económico (OCDE) 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.

Las posibles implicaciones económicas de la delincuencia informática, su carácter internacional y, a veces, incluso transnacional y el peligro de que la diferente protección jurídica penal nacional pudiera perjudicar el flujo internacional de información, condujeron en consecuencia a un intercambio de opiniones y de propuestas de solución. Sobre la base de las posturas y de las deliberaciones surgió un análisis y valoración iuscomparativista de los derechos nacionales aplicables así como de las propuestas de reforma. Las conclusiones político-jurídicas desembocaron en una lista de acciones que pudieran ser consideradas por los Estados, por regla general, como merecedoras de pena.

De esta forma, la OCDE en 1986 publicó un informe titulado Delitos de Informática: análisis de la normativa jurídica, en donde se reseñaban las normas legislativas vigentes y las propuestas de reforma en diversos estados miembros y se recomendaba una lista mínima de ejemplos de uso indebido que, los países podrían prohibir y sancionar en leyes penales (Lista Mínima), como por ejemplo el fraude y la falsificación informáticos, la alteración de datos y programas de computadora, sabotaje informático, acceso no autorizado, interceptación no

autorizada y la reproducción no autorizada de un programa de computadora protegido.

La mayoría de los miembros de la Comisión Política de Información, Computadoras y Comunicaciones recomendó también que se instituyesen protecciones penales contra otros usos indebidos (Lista optativa o facultativa), espionaje informático, utilización no autorizada de una computadora, utilización no autorizada de un programa de computadora protegido, incluido el robo de secretos comerciales y el acceso o empleo no autorizado de sistemas de computadoras.

Una vez desarrollado todo este proceso de elaboración de las normas en el ámbito continental, el Consejo de Europa aprobó la recomendación R (89)9 sobre delitos informáticos, en la que se "*recomienda a los gobiernos de los Estados miembros que tengan en cuenta cuando revisen su legislación o preparen una nueva, el informe sobre la delincuencia relacionada con las computadoras... y en particular las directrices para los legisladores nacionales*". Esta recomendación fue adoptada por el Comité de Ministros del Consejo de Europa el 13 de septiembre de 1989.

Las directrices para los legisladores nacionales incluyen una lista mínima, que refleja el consenso general del Comité, acerca de determinados casos de uso indebido de computadoras y que deben incluirse en el derecho penal, así como una lista facultativa que describe los actos que ya han sido tipificados como delitos en algunos Estados pero respecto de los cuales no se ha llegado todavía a un consenso internacional en favor de su tipificación.

Adicionalmente, en 1992, la OCDE elaboró un conjunto de normas para la seguridad de los sistemas de información, con intención de ofrecer las bases para

que los Estados y el sector privado pudieran establecer un marco de seguridad para los sistemas informáticos el mismo año.

En este contexto, se debe considerar que, si bien este tipo de organismos gubernamentales han pretendido desarrollar normas que regulen la materia de delitos informáticos, ello es resultado de las características propias de los países que los integran, quienes, comparados con Ecuador u otras partes del mundo, tienen un mayor grado de informatización y han enfrentado de forma concreta las consecuencias de ese tipo de delitos.

Por otra parte, en el ámbito de organizaciones intergubernamentales de carácter universal, debe destacarse que en el seno de la Organización de las Naciones Unidas (ONU), en el marco del Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en 1990 en la Habana, Cuba, se dijo que la delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello se había difundido la comisión de actos delictivos.

Por todo ello, en vista de que, los delitos informáticos eran un fenómeno nuevo, y debido a la ausencia de medidas que pudieran contrarrestarlos, se consideró que el uso deshonesto de las computadoras podría tener consecuencias desastrosas. A este respecto, el Congreso recomendó que se establecieran normas y directrices sobre la seguridad de las computadoras, a fin de ayudar a la comunidad internacional a hacer frente a estas formas de delincuencia.

Partiendo del estudio comparativo de las medidas que se han adoptado a escala internacional para atender esta problemática, deben señalarse los problemas que enfrenta la cooperación internacional en la esfera de los delitos informáticos y el derecho penal, a saber: la falta de consenso sobre lo que son los delitos

informáticos, falta de definición jurídica de la conducta delictiva, falta de conocimientos técnicos por parte de quienes hacen cumplir la ley, dificultades de carácter procesal, falta de armonización para investigaciones nacionales de delitos informáticos. Adicionalmente, la ausencia de la equiparación de estos delitos en los tratados internacionales de extradición.

En consecuencia, es necesario que, para solucionar los problemas derivados del incremento del uso de la informática, se desarrolle un régimen jurídico internacional donde se establezcan las normas que garanticen su compatibilidad y aplicación adecuada. Durante la elaboración de dicho régimen, se deberán considerar los diferentes niveles de desarrollo tecnológico que caracterizan a los miembros de la comunidad internacional.

Al respecto se debe considerar lo que dice el Manual de la Naciones Unidas para la Prevención y Control de Delitos Informáticos el cual señala que, cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada. Asimismo, la ONU resume de la siguiente manera a los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

- Falta de acuerdos globales acerca de qué tipo de conductas deben constituir delitos informáticos.

- Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.

- Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.

- No armonización entre las diferentes leyes procesales nacionales cerca de la investigación de los delitos informáticos.

- Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.
- Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

Considerando el valor de los bienes intangibles de la informática y las posibilidades delictivas que puede entrañar el adelanto tecnológico, se recomendó que los Estados consideraran de conformidad con sus tradiciones jurídicas y su cultura y con referencia a la aplicabilidad de su legislación vigente, la tipificación como delito punible de la conducta descrita en la "lista facultativa", especialmente la alteración de datos de computadora y el espionaje informático; así como en lo que se refiere al delito de acceso no autorizado precisar más al respecto, en virtud de los adelantos de la tecnología de la información y de la evolución del concepto de delincuencia. Además, se señala que el tráfico con contraseñas informáticas obtenidas por medios inapropiados, la distribución de virus o de programas similares deben ser considerados también como susceptibles de penalización.

En síntesis, es destacable que la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora, aunque no es el único medio. Las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente aún en países como el Ecuador, conlleva también a la posibilidad creciente de estos delitos; por eso puede señalarse que la criminalidad informática constituye un reto considerable, tanto para los sectores afectados de la

infraestructura crítica de un país, como para los legisladores, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales.

1.3.3.4. Organización de Estados Americanos

La Internet, las redes y tecnologías relacionadas se han convertido en instrumentos indispensables para los Estados Miembros de la OEA. La Internet ha impulsado un gran crecimiento en la economía mundial y ha aumentado la eficacia, productividad y creatividad en todo el Hemisferio. Individuos, empresas y gobiernos cada vez utilizan más las redes de información que integran la Internet para hacer negocios; organizar y planificar actividades personales, empresariales y gubernamentales; transmitir comunicaciones; y realizar investigaciones. Asimismo, en la Tercera Cumbre de las Américas, en la ciudad de Québec, Canadá, en 2001, nuestros líderes se comprometieron a seguir aumento la conectividad en las Américas.

Lamentablemente, la Internet también ha generado nuevas amenazas que ponen en peligro a toda la comunidad mundial de usuarios de Internet. La información que transita por Internet puede ser malversada y manipulada para invadir la privacidad de los usuarios y defraudar a los negocios. La destrucción de los datos que residen en las computadoras conectadas por Internet puede obstaculizar las funciones del gobierno e interrumpir el servicio público de telecomunicaciones y otras infraestructuras críticas. Estas amenazas a nuestros ciudadanos, economías y servicios esenciales, tales como las redes de electricidad, aeropuertos o suministro de agua, no pueden ser abordadas por un solo gobierno ni tampoco pueden combatirse utilizando una sola disciplina o práctica. Es necesario desarrollar una estrategia integral para la protección de las infraestructuras de información que adopte un enfoque integral, internacional y multidisciplinario. La OEA está comprometida con el desarrollo e implementación de esta estrategia de seguridad cibernética y en respaldo a esto, celebró una Conferencia sobre Seguridad

Cibernética (Buenos Aires, Argentina, del 28 al 29 de julio de 2003) que demostró la gravedad de las amenazas a la seguridad cibernética para la seguridad de los sistemas de información esenciales, las infraestructuras esenciales y las economías en todo el mundo, y que una acción eficaz para abordar este problema debe contar con la cooperación intersectorial y la coordinación entre una amplia gama de entidades gubernamentales y no gubernamentales.

La Estrategia Interamericana Integral de Seguridad Cibernética se basa en los esfuerzos y conocimientos especializados del Comité Interamericano contra el Terrorismo (CICTE), la Comisión Interamericana de Telecomunicaciones (CITEL), y la Reunión de Ministros de Justicia o Ministros o Procuradores Generales de las Américas (REMJA). La Estrategia reconoce la necesidad de que todos los participantes en las redes y sistemas de información sean conscientes de sus funciones y responsabilidades con respecto a la seguridad a fin de crear una cultura de seguridad cibernética.

La Estrategia también reconoce que un marco eficaz para la protección de las redes y sistemas de información que integran la Internet y para responder a incidentes y recuperarse de los mismos dependerá en igual medida de que:

- Se proporcione información a los usuarios y operadores para ayudarles a asegurar sus computadoras y redes contra amenazas y vulnerabilidades, y a responder ante incidentes y a recuperarse de los mismos.

- Se fomenten asociaciones públicas y privadas con el objetivo de incrementar la educación y la concientización, y se trabaje con el sector privado el cual posee y opera la mayoría de las infraestructuras de información de las que dependen las naciones para asegurar esas infraestructuras.

- Se identifiquen y evalúen normas técnicas y prácticas óptimas para asegurar la seguridad de la información transmitida por Internet y otras redes de comunicaciones, y se promueva la adopción de las mismas.

- Se promueva la adopción de políticas y legislación sobre delito cibernético que protejan a los usuarios de Internet y prevengan y disuadan el uso indebido e ilícito de computadoras y redes.
- Los sistemas informáticos son hoy en día el principal talón de Aquiles de los países desarrollados.
- El terrorismo informático debe ser visto como un acto similar a un acto de guerra.

De conformidad con la Declaración de Puerto España, adoptada por los Estados Miembros en el quinto período ordinario de sesiones del CICTE, el terrorismo constituye una grave amenaza a la paz y la seguridad internacionales, socava los esfuerzos continuos que fomentan la estabilidad, prosperidad y equidad en los países de la región, y viola los valores y principios democráticos consagrados en la Carta de la OEA, la Carta Democrática Interamericana y otros instrumentos regionales e internacionales, que dicha declaración está en concordancia con Declaración de Quito, en la cual se expresa por medio de sus miembros su más enérgico rechazo a toda forma de terrorismo y su respaldo al trabajo del CICTE, en el marco de la VI Conferencia de Ministros de Defensa de las Américas, celebrada en nuestro país en la ciudad de Quito del 16 al 21 de noviembre de 2004, donde se pone énfasis en la facilitación del dialogo de los países miembros de la OEA a fin de desarrollar y avanzar medidas preventivas que anticipen y enfrenten las amenazas terroristas emergentes, como son los DELITOS CIBERNÉTICOS.

1.3.3.5. La Convención de las Naciones Unidas Contra la Delincuencia Organizada Transnacional

En este contexto, la Internet y el crecimiento continuo del comercio electrónico ofrecen nuevas y enormes perspectivas de ganancias ilícitas. Es por tanto que 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 el Ecuador es parte, en dicha convención se pone de manifiesto las reglas básicas sobre la prosecución de Delincuencia Organizada Transnacional, dichas reglas hacen especial mención de 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 máxima de al menos cuatro 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.

1.3.3.6. Nuevos Retos en Materia de Seguridad

Como resultado del proceso de globalización y la difusión de la tecnología, se están produciendo cambios significativos en la naturaleza y el alcance de la delincuencia organizada. Una tendencia clave es la diversificación de las actividades ilícitas que realizan los grupos delictivos organizados, así como un aumento del número de países afectados por la delincuencia organizada.

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 adaptarse rápidamente y a aprovechar los adelantos tecnológicos debido a los inmensos beneficios que producen sus actividades ilícitas.

La apertura de nuevos mercados y las nuevas tecnologías de las comunicaciones, junto con la diversidad de actividades en las que participan, también han alimentado el crecimiento de la delincuencia organizada en los países en desarrollo. 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.

Algunos grupos terroristas, por ejemplo, han recurrido a la delincuencia organizada para financiar sus actividades. Por consiguiente, la promulgación de legislación apropiada, el fomento de la capacidad de hacer cumplir la ley y la promoción de la cooperación internacional para luchar contra las actividades de la delincuencia organizada y las prácticas corruptas conexas también fortalecen la capacidad de combatir el terrorismo.

1.3.3.7. Seguridad Informática y Normativa

A fin de evitar los ataques por parte de la Delincuencia Informática ya sea Nacional o Transnacional se debe contar con dos variables importantes que son:

1.3.3.7.1. La Seguridad Informática.

Es el conjunto de técnicas y métodos que se utilizan para proteger tanto la información como los equipos informáticos en donde esta se encuentra almacenada ya sean estos individuales o conectados a una red frente a posibles ataques accidentales o intencionados**.**

La seguridad Informática a su vez está dividida en cinco componentes a saber:

- **Seguridad Física:** Es aquella que tiene relación con la protección del computador mismo, vela por que las personas que lo manipulan tengan la autorización para ello, proporciona todas las indicaciones técnicas para evitar cualquier tipo de daños físicos a los equipos informáticos.

- **Seguridad de Datos:** Es la que señala los procedimientos necesarios para evitar el acceso no autorizado, permite controlar el acceso remoto de la información, en suma protege la integridad de los sistemas de datos.

- **Back Up y Recuperación de Datos:** Proporciona los parámetros básicos para la utilización de sistemas de recuperación de datos y Back Up de los sistemas informáticos. Permite recuperar la información necesaria en caso de que esta sufra daños o se pierda.

- **Disponibilidad de los Recursos:** Este cuarto componente procura que los recursos y los datos almacenados en el sistema puedan ser rápidamente accesados por la persona o personas que lo requieren. Permite evaluar constantemente los puntos críticos del sistema para así poderlos corregir de manera inmediata.

- **La Política de Seguridad:** Conjunto de normas y criterios básicos que determinan lo relativo al uso de los recursos de una organización cualquiera.

- **Análisis Forense:** El Análisis Forense surge como consecuencia de la necesidad de investigar los incidentes de Seguridad Informática que se producen en las entidades. Persigue la identificación del autor y del motivo del ataque. Igualmente, trata de hallar la manera de evitar ataques similares en el futuro y obtener pruebas periciales.

- **Seguridad Normativa:** Derivada de los principios de legalidad y seguridad jurídica, se refiere a las normas jurídicas necesarias para la prevención y sanción de las posibles conductas que puedan ir en contra de la integridad y seguridad de los sistemas informáticos.

En definitiva para que exista una adecuada protección a los sistemas informáticos y telemáticos se deben conjugar tanto la seguridad informática como la seguridad legal y así poder brindar una adecuada protección y tutela tanto técnica como normativa.

En resumen la Seguridad Informática y Normativa debe usarse para impedir los ataques ya sean fuera del sistema (virus, syware, adware, entre otros) y dentro del mismo, exigiendo políticas claras y precisas sobre el nivel de acceso a cierta información de carácter confidencial y una debida protección a esta.

1.3.3.8. El Delito Informático y su Realidad Procesal en el Ecuador

Desde que en 1999 en el Ecuador se puso en el tapete de la discusión el proyecto de Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, desde ese tiempo se puso de moda el tema, se realizaron cursos, seminarios, encuentros. También se conformó comisiones para la discusión de la Ley y para que formulen observaciones a la misma por parte de los organismos directamente interesados en el tema como el CONATEL (ahora CNT), la Superintendencia de Bancos, las Cámaras de Comercio y otros, que ven el Comercio Telemático una buena oportunidad de hacer negocios y de paso hacer que nuestro país entre en el boom de la llamada Nueva Economía.

Cuando la ley se presentó en un principio, tenía una serie de falencias, que con el tiempo se fueron puliendo, una de ellas era la parte penal de dicha ley, ya que las infracciones a la misma es decir los llamados Delitos Informáticos, como se los conoce, se sancionarían de conformidad a lo dispuesto en nuestro Código Penal, situación como se comprenderá era un tanto forzada, esto si tomamos en cuenta los 65 años de dicho Código, en resumen los tipos penales ahí existentes, no tomaban en cuenta los novísimos adelantos de la informática y la telemática por tanto les hacía inútiles por decirlo menos, para dar seguridad al Comercio Telemático ante el posible asedio de la criminalidad informática.

Por fin en abril del 2002 y luego de largas discusiones los diputados por fin aprobaron el texto definitivo de la Ley de Comercio Electrónico, Mensajes de

Datos y Firmas Electrónicas, y en consecuencia las reformas al Código Penal que daban la luz a los llamados Delitos Informáticos.

De acuerdo a la Constitución de la República, en su Título IV, Capitulo cuarto, sección décima al hablar de la Fiscalía General del Estado, en su Art. 195 inciso primero señala que: "La Fiscalía dirigirá, de oficio o a petición de parte, la investigación pre-procesal y procesal penal…"

Esto en concordancia con el Art. 33 del Código de Procedimiento Penal que señala que "el ejercicio de la acción pública corresponde exclusivamente a la fiscal o el fiscal". De lo dicho podemos concluir que el dueño de la acción penal y de la investigación tanto pre-procesal como procesal de hechos que sean considerados como delitos dentro del nuevo Sistema Procesal Penal Acusatorio es el Fiscal. Es por tanto el Fiscal quien deberá llevar como quien dice la voz cantante dentro de la investigación de esta clase de infracciones de tipo informático, para lo cual contara como señala el Arts.207 y 208 del Código de Procedimiento Penal con su órgano auxiliar la Policía Judicial quien realizará la investigación de los delitos de acción pública y de instancia particular bajo la dirección y control Ministerio Público, en tal virtud cualquier resultado de dichas investigaciones se incorporaran en su tiempo ya sea a la Instrucción Fiscal o a la Indagación Previa, esto como parte de los elementos de convicción que ayudaran posteriormente al representante del Ministerio Público a emitir su dictamen correspondiente.

Ahora bien el problema que se advierte por parte de las instituciones encargadas de perseguir las llamadas infracciones informáticas quienes tienen falta de preparación y experiencia en el orden técnico tanto del Ministerio Público como de la Policía Judicial, esto en razón de la falta por un lado de la infraestructura necesaria, como centros de vigilancia computarizada, las modernas herramientas de software y todos los demás implementos tecnológicos necesarios para la

persecución de los llamados Delitos Informáticos, de igual manera falta la suficiente formación tanto de los Fiscales que dirigirán la investigación como del cuerpo policial que lo auxiliara en dicha tarea, dado que no existe hasta ahora en nuestra policía una Unidad Especializada, como existe en otros países como en Estados Unidos donde el FBI cuenta con el Computer Crime Unit, o en España la Guardia Civil cuenta con un departamento especializado en esta clase de infracciones. De otro lado también por parte de la Función Judicial falta la suficiente preparación por parte de Jueces y Magistrados tratándose de estos temas, ya que en algunas ocasiones por no decirlo en la mayoría de los casos los llamados a impartir justicia se ven confundidos con la especial particularidad de estos delitos y los confunden con delitos tradicionales que por su estructura típica son incapaces de subsumir a estas nuevas conductas delictivas que tiene a la informática como su medio o fin.

Por tanto es esencial que se formen unidades Investigativas tanto policiales como del Ministerio Público especializadas en abordar cuestiones de la delincuencia informática trasnacional y también a nivel nacional. Estas unidades pueden servir también de base tanto para una cooperación internacional formal o una cooperación informal basada en redes transnacionales de confianza entre los agentes de aplicación de la ley. Lo cual es posible aplicando la Ley de Comercio Electrónico Firmas Electrónicas y Mensajes de Datos.

De otro lado en los últimos tiempos la masificación de virus informáticos globales, la difusión de la pornografía infantil e incluso actividades terroristas son algunos ejemplos de los nuevos delitos informáticos y sin fronteras que presentan una realidad difícil de controlar. Con el avance de la tecnología digital en los últimos años, ha surgido una nueva generación de delincuentes que expone a los gobiernos, las empresas y los individuos a estos peligros.

Es por estas razones que el Ministerio Público tiene la obligación Jurídica en cumplimiento de su mandato constitucional de poseer un cuerpo especializado para combatir esta clase de criminalidad a fin de precautelar los derechos de las víctimas y llevar a los responsables a juicio, terminando así con la cifra negra de esta clase de infracciones, ya que en la actualidad esta clase de conductas ilícitas no son tratadas en debida forma por los órganos llamados a su persecución e investigación.

1.3.3.8.1. Problemas de Persecución.

Este tipo de infracciones son difícilmente descubiertas o perseguidas ya que los sujetos activos actúan sigilosamente, y poseen herramientas capaces de borrar todo rastro de intrusión o la consumación del delito, pero a pesar de eso y de no contar ni con una policía entrenada para investigar dichos hechos, ni una Fiscalía que pueda dar las directrices para la correcta indagación de dichos actos delictivos, por no contar entre otras con una Unidad Especial para la investigación y persecución de estas infracciones informáticas, existen dos problemas principales que a continuación se exponen:

1.3.3.8.2. Problemática con la concepción tradicional de tiempo y espacio.

Esta característica de transnacional de la delincuencia informática es otro de los problemas de perseguibilidad. Tradicionalmente se ha considerado que la ley penal solo se aplica en el territorio de la República, hecho que constituye el llamado "principio de territorialidad de la ley", el mismo que se encuentra tipificado como ya se mencionó en el art. 5 del Código Penal. El principio de territorialidad sostiene que la ley penal de un país es aplicable cuando la infracción ha sido cometida dentro del territorio, en el momento actual esto puede haber cambiado teniendo en cuenta que el nuevo escenario en donde mayormente se da este tipo de delitos es el Ciberespacio, un lugar donde no existen fronteras territoriales.

Por lo dicho se puede constatar de prima fase que es difícil la persecución de estos delitos y su enjuiciamiento, ya que existe la posibilidad de preparar y cometer acciones delictivas informáticas en perjuicio de terceros en tiempo y espacio lejanos.

Debido a los adelantos de las telecomunicaciones y la telemática, hace que las distancias reales o fronteras entre países no existan como ya se ha dicho, ya que una persona puede realizar un acto delictivo en un lugar distinto del lugar de los hechos, como por ejemplo los creadores de MALWARE o de los VIRUS INFORMÁTICOS.

La territorialidad de la ley es considerada como un principio de soberanía del estado y se resume al decir que no se puede aplicar al ecuatoriano delincuente otra ley que no sea la ecuatoriana, aclarando que no importa el lugar donde se encuentre el delincuente, es decir, sin importar el país en donde se haya cometido el delito.

Este principio denota algunas características como las siguientes:

- La ley penal es aplicable a los hechos punibles cometidos dentro del territorio del Estado, sin consideración a la nacionalidad del actor.
- No se toma en cuenta la nacionalidad del autor.
- Se toma en cuenta el lugar de comisión del delito. Nuestra legislación se inclina por la teoría del resultado, es decir que la INFRACCIÓN se entiende cometida en el territorio del Estado cuando los *efectos de la acción u omisión* deban producirse en el Ecuador o en los lugares sometidos a su jurisdicción.

- Se aplica al concepto jurídico de territorio por el Derecho Internacional: los límites del Estado, mar territorial. Espacio aéreo.
- Se aplica también la teoría del territorio flotante o Principio de la bandera:

Naves o aeronaves de bandera nacional ya sea que se encuentren en alta mar, en su espacio aéreo y en lugares en que por la existencia de un convenio internacional, ejerzan jurisdicción. Este principio no se aplica cuando las naves o aeronaves mercantes estén sujetas a una Ley Penal extranjera.

El ámbito de aplicación de este principio está en:

1. Territorio Continental
2. Espacio Aéreo
3. Mar Territorial
4. Naves y aeronaves ecuatorianas de guerra o mercantes.
5. Infracciones cometidas en el recinto de una Legación ecuatoriana en país extranjero.

1.3.3.9. Principios de Extraterritorialidad

Tres son los principios que constituyen el principio de extraterritorialidad y son los siguientes: el principio de la nacionalidad o personalidad, el principio de la defensa y el principio de la universalidad y justicia mundial.

a. Principio de la nacionalidad o personalidad.

Según este, se debe aplicar al delincuente únicamente la ley que corresponde a su nacionalidad, es decir, la ley del país de su origen, sea el país que sea en el que haya cometido el delito. Este principio tiene dos divisiones:

- **Principio de la Nacionalidad Activa.-** Se funda en la obediencia que se exige al súbdito ecuatoriano con respecto a su legislación. Se toma en cuenta la nacionalidad del autor del delito.

- **Principio de la Nacionalidad Pasiva.-** El alcance espacial de la ley se extiende en función *del ofendido o titular del bien jurídico protegido.* Se aplicaría cuando está en juego la protección de los bienes jurídicos individuales.

b. Principio de la defensa.

Este nos dice que es aplicable la ley del país donde los principios son atacados por el delito, sin tomar en cuenta la nacionalidad de los realizadores.
Se toma en cuenta la nacionalidad del bien jurídico protegido, es decir se aplica este principio cuando se afecta la integridad territorial. Quedando en juego la protección de los bienes nacionales. Ha sido tomado por algunos países, como por ejemplo el nuestro el cual puede pedir la extradición de una delincuente informático que haya vulnerado bienes jurídicos protegidos en nuestro país como resultado de su acción delictiva. Claro que esta norma no puede ser aplicada en todos los países ya que algunos de ellos como el nuestro prohíbe la extradición de ecuatorianos que hayan cometido una infracción en otro país, en este caso se aplica un principio de equivalencia, es decir si el delito cometido en el otro país se encuentra tipificado en el nuestro también puede seguirse el proceso penal por el cometimiento de dicho delito, pero en nuestro país.

c. Principio de la universalidad y justicia mundial.

Este principio se refiere a que es aplicable la ley del país que primero aprese al delincuente, sin considerar otro aspecto. Este principio tiene una finalidad práctica para reprimir los delitos contra la humanidad, aquellos que han sido catalogados como tales en virtud de ser considerados como ofensores de toda la humanidad. Para ello es necesario firmar convenios internacionales y unilaterales con el fin de que cada país pueda sancionar al delincuente con su propia ley, sin importar el

lugar donde el individuo haya cometido el acto ni tampoco la nacionalidad del mismo.

En doctrina penal se concede en virtud de este principio eficacia extraterritorial a la ley penal; pero en el Derecho Internacional condiciona esta eficacia extraterritorial tomando en cuenta:

- La calidad del bien jurídico protegido, como bienes culturales supranacionales.
- Cuando los autores del delito sean peligrosos para todos los estados.

En cuanto a los delitos informáticos de carácter transnacional, en especial el Ciberterrorismo es necesario aplicar este principio por cuanto la peligrosidad de este tipo de ataques puede causar más daño que el terrorismo convencional. Los delitos informáticos es la forma actual y acorde a la tecnología adoptado por los delincuentes, como un medio efectivo que sirve para evadir la justicia, estos son fenómenos delictuales que van avanzando conforme los sistemas informáticos y electrónicos adoptan nuevas medidas de seguridad para asegurar su inviolabilidad en un esfuerzo hasta ahora casi inútil, además para los encargados de las investigaciones y administración de justicia se ha vuelto un laberinto complejo ya que resulta difícil dar con el culpable de este tipo de actividad ilícita en la mayoría de casos en especial en aquellos países que no cuentan con los elementos necesarios para la persecución de estos delitos.

En materia de seguridad informática la inadecuada distribución de las asignaciones presupuestarias para contar con equipos y personal capacitado en nuestro país, es un gran inconveniente, hasta el momento la Fiscalía con los pocos elementos adecuados que cuentan tiene que tratar de realizar una investigación apropiada; obviamente al final de la investigación no se contara con

los resultados deseados o adecuados, no porque él o la Fiscal hayan hecho un mal trabajo durante la indagación previa sino porque no pueden contar con todos los elementos de convicción ya que el delito mismo puede ser cometido desde cualquier parte del país e inclusive del mundo por lo cual exige que se cuente con equipo sofisticado y personal altamente capacitado para aportar los elementos suficientes para perseguir el delito.

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

- La falta de cultura informática es un factor crítico en el impacto de los delitos informáticos en la sociedad en general, cada vez se requieren mayores conocimientos en tecnologías de la información, las cuales permitan tener un marco de referencia aceptable para el manejo de dichas situaciones.
- Nuevas formas de hacer negocios como el comercio electrónico puede que no encuentre el eco esperado en los individuos y en las empresas hacia los que va dirigido ésta tecnología, por lo que se deben crear instrumentos legales efectivos que ataquen ésta problemática, con el único fin de tener un marco legal que se utilice como soporte para el manejo de éste tipo de transacciones.
- La responsabilidad del auditor informático no abarca el dar solución al impacto de los delitos o en implementar cambios; sino más bien su responsabilidad recae en la verificación de controles, evaluación de riesgos, así como en el establecimiento de recomendaciones que ayuden a las organizaciones a minimizar las amenazas que presentan los delitos informáticos.

- La ocurrencia de delitos informáticos en las organizaciones alrededor del mundo no debe en ningún momento impedir que éstas se beneficien de todo lo que proveen las tecnologías de información (comunicación remota, Interconectividad, comercio electrónico, etc.); sino por el contrario dicha situación debe plantear un reto a los profesionales de la informática, de manera que se realicen esfuerzos encaminados a robustecer los aspectos de seguridad, controles, integridad de la información, etc. en las organizaciones.

1.3.4. 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".

En algunos casos la motivación del delito informático no es económica sino que se relaciona con el deseo de ejercitar, y a veces hacer conocer a otras personas, los conocimientos o habilidades del delincuente en ese campo.

www.es.wikipedia.org: "Muchos de los delitos informáticos encuadran dentro del concepto de "delitos de cuello blanco", término introducido por primera vez por el criminólogo estadounidense Edwin Sutherland en 1943". Esta categoría requiere que:

1. El sujeto activo del delito sea una persona de cierto estatus socioeconómico.
2. Su comisión no pueda explicarse por falta de medios económicos, carencia de recreación, poca educación, poca inteligencia, ni por inestabilidad emocional.

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

Para la labor de prevención de estos delitos es importante el aporte de los damnificados que puede ayudar en la determinación del modus operandi, esto es de las maniobras usadas por los delincuentes informáticos.

1.3.4.1. Sujeto Activo

De acuerdo al profesor chileno GARRIDO MONTT, Mario, en su obra Nociones Fundamentales de la Teoría del Delito Edit. Jurídica de Chile, (1992); "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. 23-24.

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. De esta forma, la persona que "*entra*" en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que "*desvía fondos*" de las cuentas de sus clientes.

El nivel típico de aptitudes del delincuente 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.

El Dr. ACURIO DEL PINO, Santiago en su obra Delitos Informáticos (1998) "efectivamente, señala un sinnúmero de conductas que considera como "delitos de cuello blanco", aun cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las "*violaciones a las leyes de patentes y fábrica de derechos de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios, entre otros*". Pág.16.

Dentro de poco tiempo la operación de un sistema electrónico será tan fácil como manejar una televisión, por ejemplo. De esta manera, se puede ubicar como sujeto activo de un delito cibernético a un lego en la materia o a un empleado de un área no informática que tenga un mínimo conocimiento de computación. Por no hablar del problema que se plantea con los llamados "niños genio" que son capaces no sólo de dominar sistemas electrónicos básicos, sino que pueden incluso intervenir exitosamente en operaciones de alto grado de dificultad técnica, acarreando más problemas al tambaleante concepto de la impunidad para el caso de que algunos de estos menores logre cometer estragos importantes a través de los medios computacionales que maneje.

1.3.4.2. Anonimato del Sujeto Activo

El sujeto activo de esta clase de infracciones puede ser totalmente anónimo y usar este anonimato como forma de evadir su responsabilidad, ya que este no necesariamente puede usar su propio sistema informático, sino que se puede valer

de un tercero, como por ejemplo en el caso del envión 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 crakers 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.

1.3.4.3. 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 del delito que nos ocupa, 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 activos.

La falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más,

trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada “cifra oculta” o “cifra negra”.

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

En el mismo sentido, podemos decir que mediante la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras, y alertando a las potenciales víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática, y si a esto se suma la creación de una adecuada legislación que proteja los intereses de las víctimas y una eficiente preparación por parte del personal encargado de la procuración, administración y la impartición de justicia para atender e investigar estas conductas ilícitas, se estaría avanzando mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más.

Además, se debe destacar que los organismos internacionales han adoptado resoluciones similares en el sentido de que “educando a la comunidad de víctimas y estimulando la denuncia de los delitos se promovería la confianza pública en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para detectar, investigar y prevenir los delitos informáticos”.

Este nivel de criminalidad se puede explicar por la dificultad de reprimirla en forma internacional, ya que los usuarios están esparcidos por todo el mundo y, en consecuencia, existe una posibilidad muy grande de que el agresor y la víctima

estén sujetos a leyes nacionales diferentes. Además, si bien los acuerdos de cooperación internacional y los tratados de extradición bilaterales intentan remediar algunas de las dificultades ocasionadas por los delitos informáticos.

CAPÍTULO II

2. DISEÑO DE LA PROPUESTA

2.1. Breve Caracterización del Objeto de Estudio

La presente investigación sobre Los Delitos Informáticos y su Perjuicio en la Sociedad, se materializo utilizando como medio principal la encuesta a los actores principales dentro del sistema de Administración de Justicia en la Provincia de Cotopaxi como son Jueces de la Sala Especializada de lo Penal, Tribunal y Jueces de Garantías Penales, Fiscales, y Abogados en libre ejercicio profesional, los mismos que prestaron la colaboración necesaria que esta actividad requería.

Gracias a este trabajo se logró determinar, que hace falta la inclusión de varios delitos informáticos en el Código Penal, puesto que las personas encuestadas no conocen cuales son los procedimientos que se deben seguir para el juzgamiento de las variadas formas que presentan este tipo de delitos, que no se encuentran en forma detallada en la Ley pertinente; además no existe una adecuada sociabilización y difusión de las normas Penales pertinentes para sancionar estos delitos, constatándose la necesidad de implementar de una manera más detallada dentro del Código Penal Ecuatoriano.

Los delitos informáticos en el Ecuador han sido poco estudiados y conocidos, en la actualidad a un no se ha logrado encontrar la fórmula para que todos estos sean sancionados, ya que no existen los medios necesarios para la persecución del este nuevo modo para infringir la ley, es así que el Estado debe garantizar los

derechos de sus habitantes, creando los medios suficientes y necesarios para que estos no queden en la impunidad.

2.2. Diseño de la Investigación

El presente estudio se desarrolló mediante una investigación de carácter descriptiva, ya que permitió conocer el grado de discernimiento que tienen los encuestados a cerca de los delitos informáticos y el procedimiento que se debe seguir para su juzgamiento, con el propósito de implementar un taller de capacitación referente al tema dirigido a los profesionales del derecho en libre ejercicio; la metodología que se utilizó fue el diseño no experimental de investigación, que me permitió observar la inadecuada aplicación de la norma penal establecida en los casos de delitos informáticos, donde me base en tres conceptos fundamentales:

La validez implico que la observación, la medición o la apreciación se enfocaron en la realidad que se buscó conocer y no en otra.

La confiabilidad que se refirió a los resultados estables seguros, congruentes, iguales a sí mismo en diferentes tiempos y previsibles.

La muestra, que representó el universo y se presentó como el factor crucial para generalizar los resultados.

2.3. Tipo de Investigación

Los tipos de investigación que se emplearon para llevar a cabo el presente trabajo de graduación son:

La Investigación descriptiva.- Por cuanto se debió detallar el fenómeno que produce el hecho de la violación del debido proceso y garantías en el caso de los delitos informáticos, por falta de conocimiento en las autoridades encargadas de la administración de justicia y todos los implicados en el proceso, además señalan los datos obtenidos y la naturaleza exacta de la población de donde fueron extraídos.

La investigación histórico-lógica.- Que vino a ser la construcción de los hechos en relación a los temas y formas de juzgamiento de este tipo de delitos en la provincia de Cotopaxi mediante la recolección de datos.

2.4. Metodología

Para el desarrollo del presente trabajo de Tesis, se optó por la siguiente metodología:

- Se realizó una investigación bibliográfica, de recopilación de material escrito sobre la percepción de seguridad que tienen los usuarios de Internet, y de entrevista desde el punto de vista económico, social, policial y judicial.

- Con los datos obtenidos, se realizó una selección de material escrito, emanado de diversas fuentes externas a nuestro país, provenientes de países con mayor desarrollo y experiencias en esta área del crimen tecnológico o delitos informáticos.

El estudio que se plantea está enfocado en un diseño no experimental de investigación; por cuanto no se realiza la manipulación de variables; tan solo se observa la inadecuada aplicación de la Ley Penal en cuanto al procedimiento sobre Delitos Informáticos y como afecta a la sociedad en general.

Esta investigación aplicará un diseño no experimental de tipo transaccional por cuanto se recolectarán los datos en un solo momento o en un tiempo único a la población que será objeto de la misma.

2.4.1. Unidad de Estudio

Para realizar este trabajo de investigación se consideró a la población como un universo de individuos y objetos con ciertas características y cualidades en razón del objeto de estudio, la misma que se describe a continuación.

El universo total de la investigación se remitió al Tribunal de Garantías Penales, Jueces de Garantías Penales de Cotopaxi, Fiscales y abogados en libre ejercicio de la provincia de Cotopaxi.

SUJETOS DE LA INVESTIGACIÓN	**N°**
Jueces de la sala especializada, miembros del Tribunal y Jueces de Garantías Penales de Cotopaxi	9
Fiscales	8
Abogados en libre ejercicio	236
TOTAL	**253**

2.4.2. Muestra

Se realizó la presente investigación a través de la aplicación de una muestra en base a la siguiente fórmula:

$$n = \frac{N}{E^2 (N-1)+1}$$

De donde:

N = Población total

n = Muestra

E = error máximo admitido = 0.05

Cálculo de la muestra:

$$n = \frac{571}{(0.05)^2(571-1)+1} n = \frac{571}{(0.0025)(570)+1}$$

$$n = \frac{571}{(1.44)+1} n = \frac{571}{2.44} \boldsymbol{n = 236}$$

En este sentido se considera trabajar con un número de 236 sujetos a investigar, con respecto al Tribunal de Garantías Penales, Jueces de Garantías Penales de Cotopaxi, Fiscales y abogados en libre ejercicio de la provincia.

Finalmente para seleccionar a los sujetos que serán investigados, se aplicará un método de muestreo no probabilístico.

2.4.2. Métodos

Para llevar a cabo la presente investigación sobre los delitos informáticos, el participante ha visto necesario la utilización del método no experimental porque se lo realizará sin manipular las variables, simplemente se observará el fenómeno tal y como se da en su contexto natural.

Los métodos a emplear en esta investigación son los siguientes:

Método Histórico.- Se utilizó para desentrañar la evolución del fenómeno a investigarse desde sus orígenes hasta la actualidad y conocer sus elementos constitutivos primarios fundamentales.

Método Inductivo.- Para el descubrimiento de la verdad científica, se usaron procedimientos partiendo del estudio de los elementos particulares conocidos que se proyectan a la generalidad o totalidad por descubrirse.

Método Deductivo.- Conociendo las leyes generales y principios universales del derecho, posibilitó detallar y analizar las características del problema para poder establecer los comportamientos de las variables y sus relaciones.

Método Analítico-Sintético.- Permitió partir del estudio del casos o fenómenos particulares para llegar a los cubrimientos de un principio o ley general.

Método Dialéctico.- Proporciono la posibilidad de comprender los más diversos fenómenos de la realidad, al analizar los fenómenos de la naturaleza, de la sociedad y del pensamiento permitió descubrir sus verdaderas leyes y las fuerzas motrices del desarrollo de la realidad.

Método Documental.- La investigación documental es parte fundamental de un proceso de investigación científica, constituyó en una estrategia donde se observó y reflexionó sistemáticamente sobre distintas realidades, usando para ello diferentes tipos de documentos. Indagación, interpretación, presenta datos e informaciones sobre un tema determinado de cualquier ciencia.

2.4.3. Técnicas

Encuesta.- Se usó para recolectar información, conocer la realidad de la problemática y tratar de dar soluciones a las mismas. Se la realizó por medio de cuestionarios elaborados con anticipación.

Observación Directa.- Estuvo sujeta a la intervención de varios factores subjetivos que incidirán en el acto cognoscitivo, tales como el lugar, los hábitos que se repiten en forma reiterativa cuyos elementos inferirán directamente en la facilidad o dificultad de la realidad objetiva a observar los mismos que serán consignados en un cuadernos de notas. Gracias a esta técnica se ha podido apreciar la naturaleza misma de la investigación.

2.4.4. Instrumentos de la investigación

Fichas Bibliográficas.- Se usó para apuntar los diferentes datos de investigación de distintos documentos como revistas, diarios, obras, etc. Estas sirvieron para indagar sobre el tema de análisis por lo que se realizó un registro de elementos para el estudio.

Fichas Nemotécnicas.- Se tomaron todo tipo de nota de los diferentes documentos o elemento que se han consultado o de personas quienes conocían sobre el objeto materia de la investigación.

2.5. Análisis e Interpretación de Datos

2.5.1. Encuesta Efectuada a los Señores Jueces de la Sala Especializada de lo Penal y Miembros del Tribunal y Jueces de Garantías Penales de Cotopaxi

1. ¿Conoce usted, que es un delito informático?

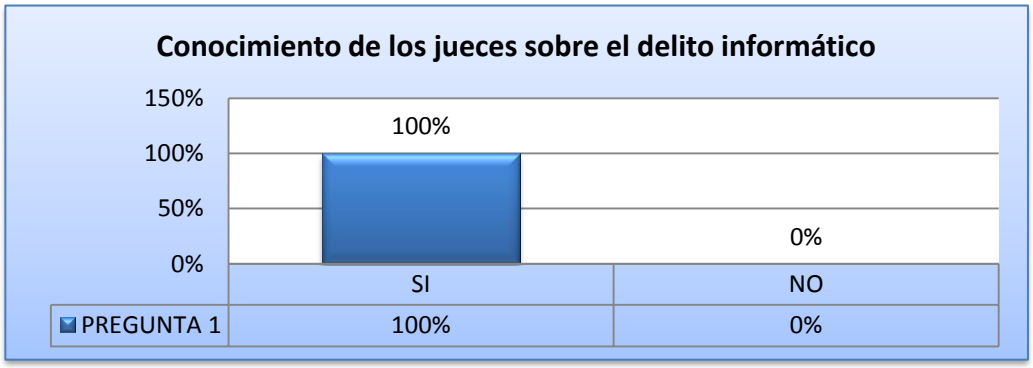
Cuadro Nº 1

Conocimiento de los jueces sobre el delito informático

Opción	No.	Porcentaje
Si	9	100%
No	0	0%
TOTAL	9	100%

Fuente: Encuestas
Elaborado por: Investigador

Gráfico Nº 1



Fuente: Encuestas
Elaborado por: Investigador

ANÁLISIS E INTERPRETACIÓN

De lo investigado se desprende que los 9 encuestados que corresponden a un 100% tienen conocimiento de lo que es el Delito Informático.

2. ¿Usted considera, que todos los delitos informáticos están tipificados en el Código Penal?

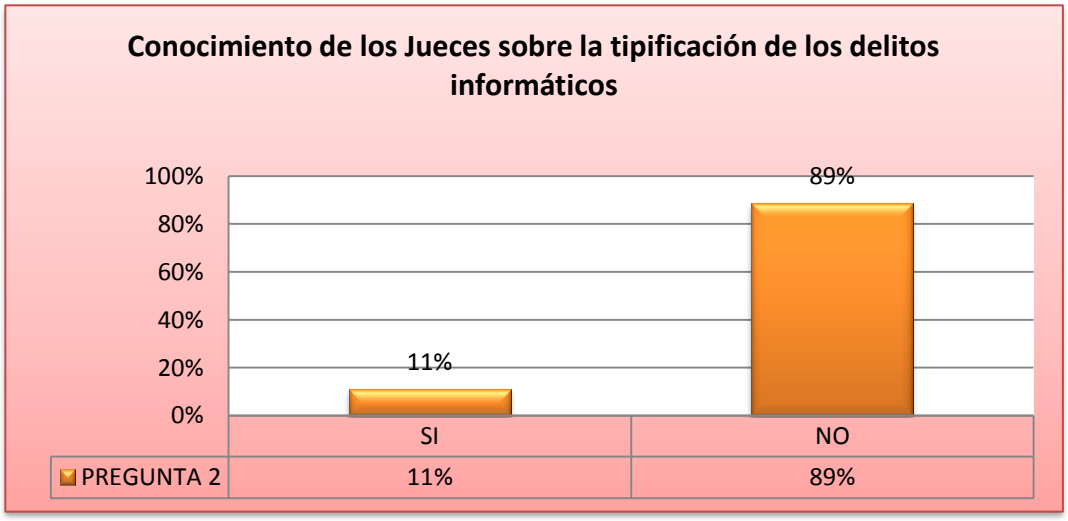
Cuadro N° 2

Conocimiento de los Jueces sobre la tipificación de los delitos informáticos

Cuestión	No.	Porcentaje
Si	1	11%
No	8	89%
TOTAL	**9**	**100%**

Fuente: Encuestas
Elaborado por: Investigador

Gráfico Nº 2



Fuente: Encuestas
Elaborado por: Investigador

ANÁLISIS E INTERPRETACIÓN

Para los investigados, 8 que corresponde a un 89% dicen que No; consideran que todos los delitos de carácter informático se encuentren tipificados en el Código de Procedimiento Penal Ecuatoriano vigente. Mientras tanto 1 que es equivalente al 11% dice no conocer que es el delito informático.

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

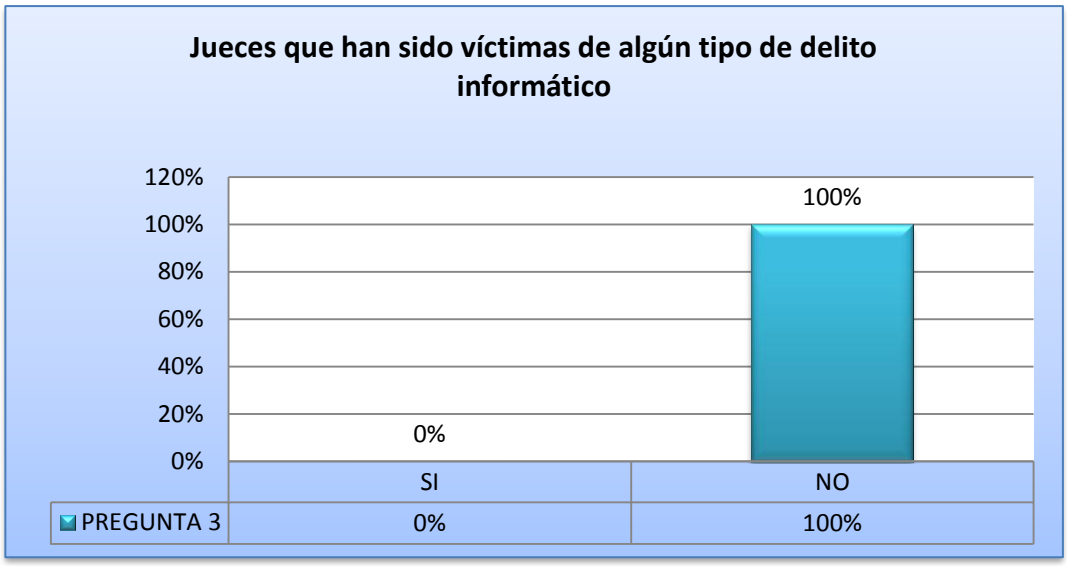
Cuadro Nº 3

Jueces que han sido víctimas de algún tipo de delito informático

Cuestión	No.	Porcentaje
Si	0	0%
No	9	100%
TOTAL	**9**	**100%**

Fuente: Encuestas
Elaborado por: Investigador

Gráfico Nº 3



Fuente: Encuestas
Elaborado por: Investigador

ANÁLISIS E INTERPRETACIÓN

Como indican los datos del cuadro y gráfico que anteceden los 9 profesionales encargados de la administración de justicia encuestados que corresponde al 100 % indican que hasta el momento no han sido víctimas de algún tipo de delito informático.

4. ¿Considera usted, que su derecho a la intimidad es violentada en las comunicaciones utilizando el internet u otro mecanismos de sistema informático?

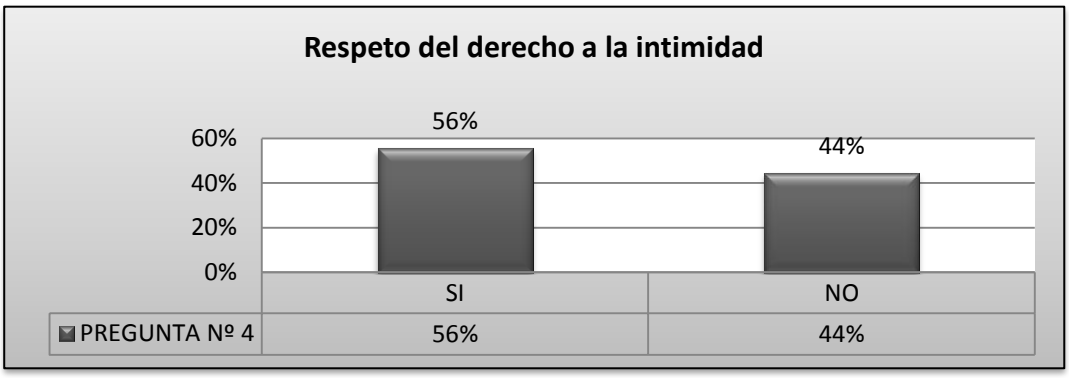
Cuadro Nº 4

Respeto del derecho a la intimidad

Cuestión	No.	Porcentaje
Si	5	56%
No	4	44%
TOTAL	**9**	**100%**

Fuente: Encuestas
Elaborado por: Investigador

Gráfico Nº 4



Fuente: Encuestas
Elaborado por: Investigador

ANÁLISIS E INTERPRETACIÓN

De los investigados los 5 que corresponden al 56% opinan que SI, que el derecho a la intimidad es violentada en las comunicaciones utilizando el internet u otro mecanismo de sistema informático. Mientras que los otros 4 que es equivale al otro 44% opinan que NO, que su derecho a la intimidad no es vulnerado de ninguna manare al utilizar medios o sistemas informáticos.

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

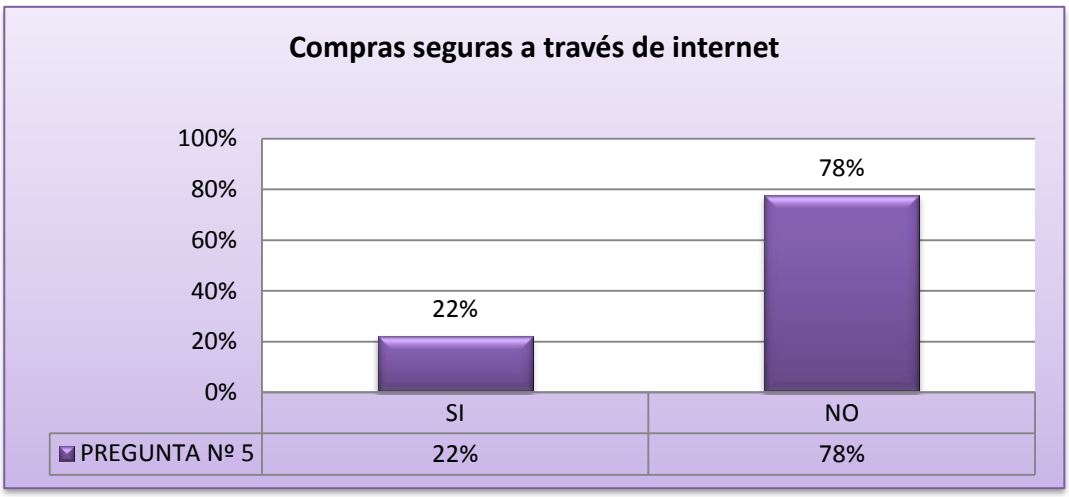
Cuadro Nº 5

Compras seguras a través de internet

Cuestión	No.	Porcentaje
Si	2	22%
No	7	78%
TOTAL	**9**	**100%**

Fuente: Encuestas
Elaborado por: Investigador

Gráfico Nº 5



Fuente: Encuestas
Elaborado por: Investigador

ANÁLISIS E INTERPRETACIÓN

Según las opiniones de los encuestados al referirse a la pregunta, obtenemos que 2 de ellos que equivale al 22%, opina que las compras a través del internet son seguras, y no representan ningún tipo de riesgo o modo de cometer algún ilícito. No así los 7 igual al 78% quienes dicen que las compras mediante el internet no son confiables ya que es muy probable que a través de este medio se cometa algún tipo de delito.

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

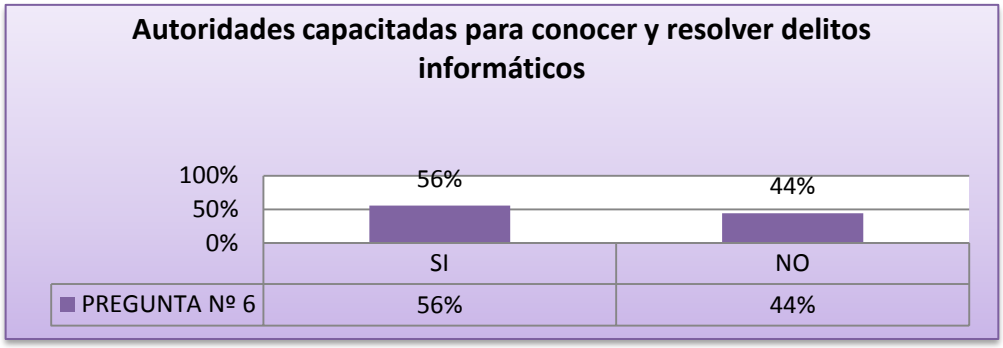
Cuadro Nº 6

Autoridades capacitadas para conocer y resolver delitos informáticos

Cuestión	No.	%
Si	5	56%
No	4	44%
TOTAL	**9**	**100%**

Fuente: Encuestas
Elaborado por: Investigador

Gráfico Nº 6



Fuente: Encuestas
Elaborado por: Investigador

ANÁLISIS E INTERPRETACIÓN

Según la opinión de 5 encuestados que representa el 56% dicen que SI, consideran que las autoridades encargadas de la administración de justicia están plenamente capacitadas para conocer y resolver casos sobre delitos informáticos. Los 4 restantes que corresponde al 44 % dice que NO, consideran que las autoridades estén plenamente preparadas para conocer y resolver debidamente estos casos ya que al ser un delito nuevo en nuestro país necesitan capacitación, personal y equipos adecuados.

7. ¿Según su propia experiencia considera usted, que en el juzgamiento de los delitos informáticos existe algún problema?

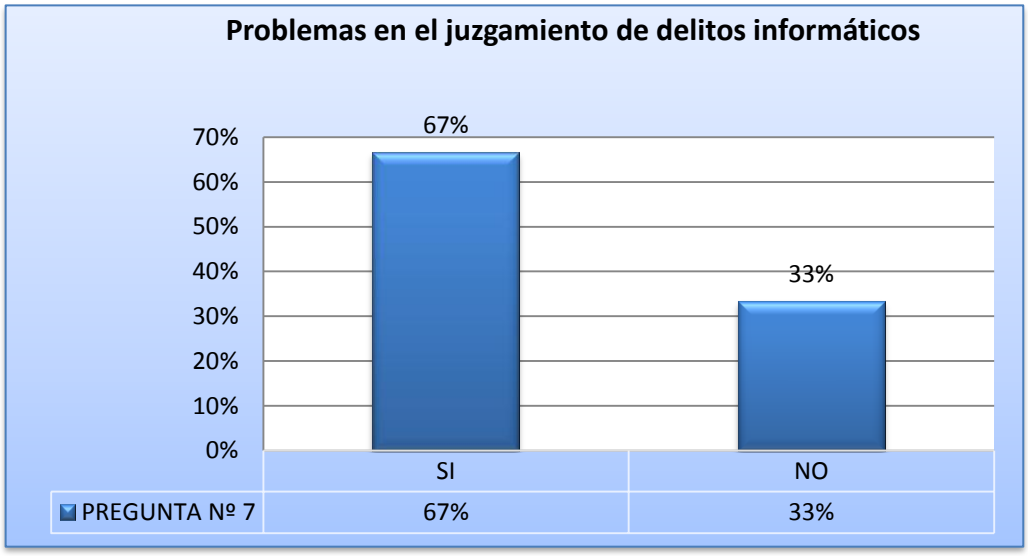
Cuadro Nº 7

Problemas en el juzgamiento de delitos informáticos

Cuestión	No.	Porcentaje
Si	6	67%
No	3	33%
TOTAL	**9**	**100%**

Fuente: Encuestas
Elaborado por: Investigador

Gráfico Nº 7



Fuente: Encuestas
Elaborado por: Investigador

ANÁLISIS E INTERPRETACIÓN

Los investigados responden; 6 que es igual al 67% que según su propia experiencia en el juzgamiento de casos sobre delitos informáticos existe algún tipo de problema, 3 correspondiente al 33% opinan que NO, existe ningún inconveniente en el juzgamiento de este tipo de delitos.

8. ¿Considera que es necesario la ampliación de un Capítulo en el Código Adjetivo Penal exclusivo para la tipificación de los delitos informáticos?

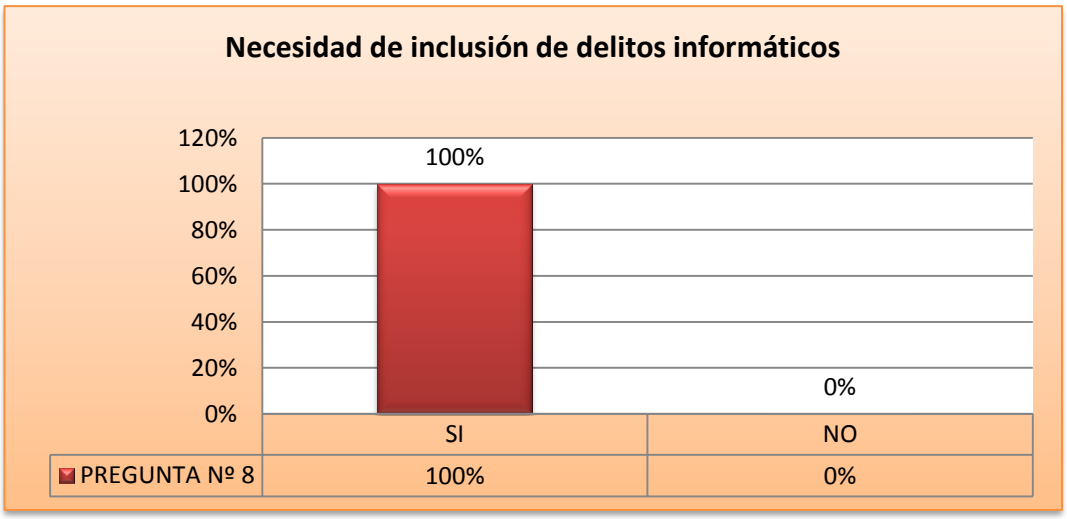
Cuadro Nº 8

Necesidad de inclusión de delitos informáticos

Cuestión	No.	Porcentaje
Si	9	100%
No	0	0%
TOTAL	**9**	**100%**

Fuente: Encuestas
Elaborado por: Investigador

GRÁFICO Nº 8



Fuente: Encuestas
Elaborado por: Investigador

ANÁLISIS E INTERPRETACIÓN

Los encuestados responde de la siguiente manera: 9 igual al 100% dicen considerar necesario la inclusión de delitos informáticos en el Código Penal.

9. ¿Apoyaría usted, la implementación de un Capítulo exclusivo sobre los delitos informáticos en el Código Adjetivo Penal Ecuatoriano?

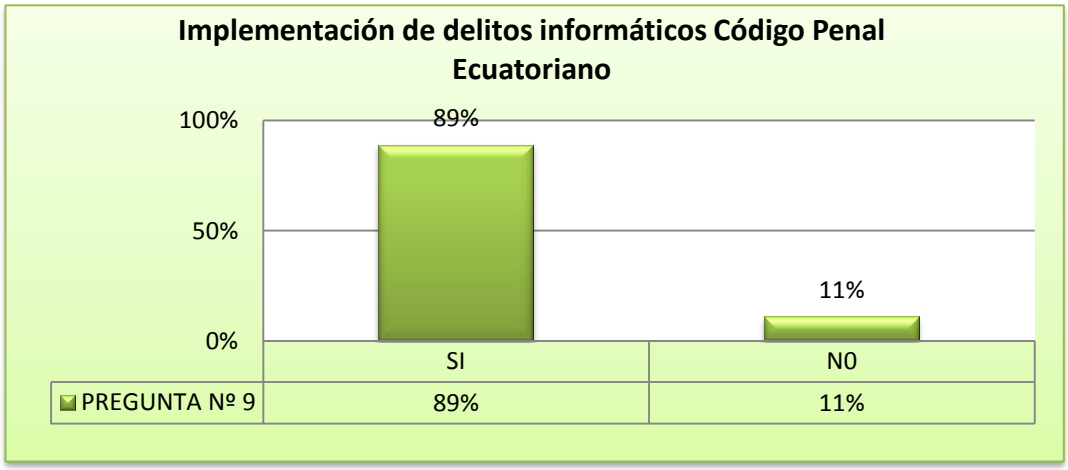
Cuadro Nº 9

Implementación de delitos informáticos Código Penal Ecuatoriano

Cuestión	No.	Porcentaje
Si	8	89%
No	1	11%
TOTAL	**9**	**100%**

Fuente: Encuestas
Elaborado por: Investigador

GRÁFICO Nº 9



Fuente: Encuestas
Elaborado por: Investigador

ANÁLISIS E INTERPRETACIÓN

Opinan 8 de los investigados que corresponden al 89% que si apoyarían la implementación de delitos informáticos en el Código Penal Ecuatoriano. Mientras tanto 1 de ellos equivalente al 11% no está de acuerdo con apoyar esta propuesta.

2.5.2. Encuesta Efectuada a los Señores Fiscales de Cotopaxi

1. ¿Conoce usted, que es un delito informático?

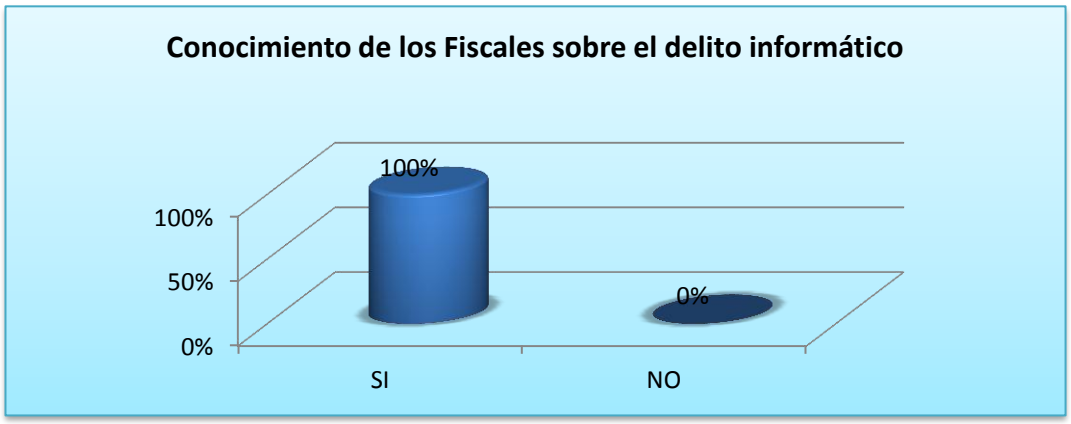
Cuadro Nº 1

Conocimiento de los Fiscales sobre el delito informático

Opción	No.	Porcentaje
Si	8	100%
No	0	0%
TOTAL	8	100%

Fuente: Encuestas
Elaborado por: Investigador

Gráfico Nº 1



Fuente: Encuestas
Elaborado por: Investigador

ANÁLISIS E INTERPRETACIÓN

De los 8 Fiscales Distritales de la Provincia de Cotopaxi, encuestados que equivalen al 100% se desprende que todos tienen conocimiento de lo que es el Delito Informático.

2. ¿Usted considera, que todos los delitos informáticos están tipificados en el Código Penal?

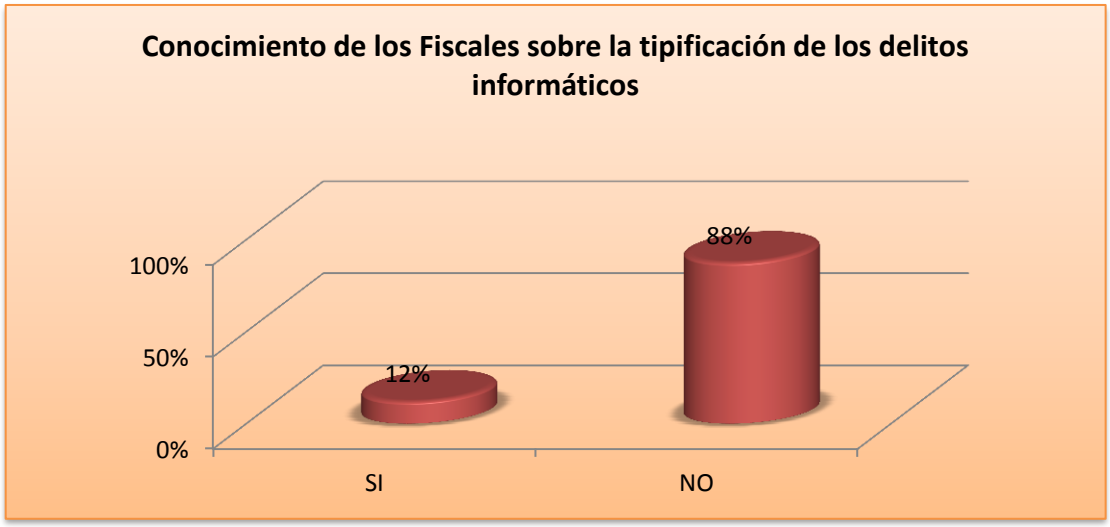
Cuadro N° 2

Conocimiento de los Fiscales sobre la tipificación de los delitos informáticos

Cuestión	No.	Porcentaje
Si	1	12%
No	7	88%
TOTAL	**8**	**100%**

Fuente: Encuestas
Elaborado por: Investigador

Gráfico Nº 2



Fuente: Encuestas
Elaborado por: Investigador

ANÁLISIS E INTERPRETACIÓN

Para los investigados, 1 Fiscal correspondiente al 12% considera que todos los delitos informáticos se encuentren tipificados en el Código Penal. Mientras que 7 de ellos equivalente al 88% refieren que la totalidad de delitos informáticos no se encuentren tipificados y sancionados en el Código Penal Ecuatoriano.

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

Cuadro Nº 3

Fiscales que han sido víctimas de algún tipo de delito informático

Cuestión	No.	Porcentaje
Si	0	0%
No	8	100%
TOTAL	**8**	**100%**

Fuente: Encuestas
Elaborado por: Investigador

Gráfico Nº 3

Fuente: Encuestas
Elaborado por: Investigador

ANÁLISIS E INTERPRETACIÓN

Según los datos recopilados los 8 Fiscales encuestados correspondiente al 100% indican que nunca han sido víctimas de algún tipo de delito informático.

4. ¿Considera usted, que su derecho a la intimidad es violentada en las comunicaciones utilizando el internet u otro mecanismos de sistema informático?

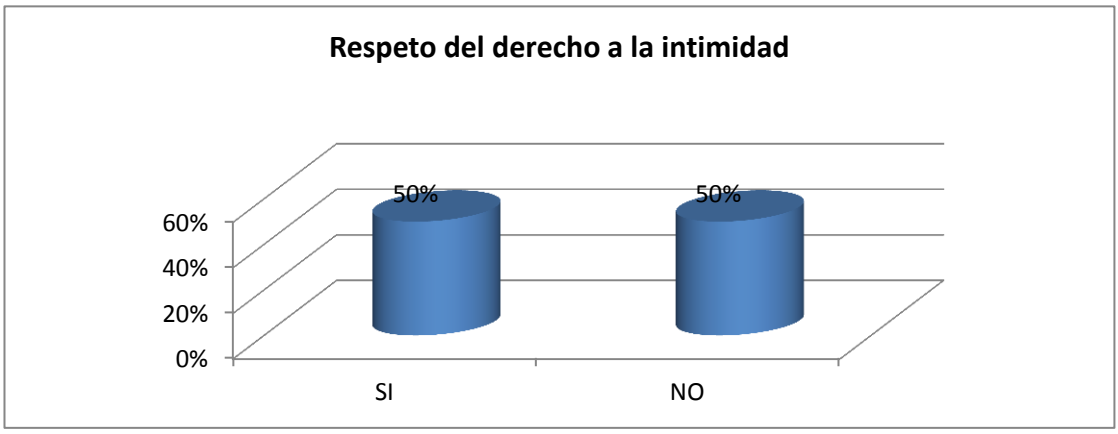
Cuadro Nº 4

Respeto del derecho a la intimidad

Cuestión	No.	Porcentaje
Si	4	50%
No	4	50%
TOTAL	**8**	**100%**

Fuente: Encuestas
Elaborado por: Investigador

Gráfico Nº 4



Fuente: Encuestas
Elaborado por: Investigador

ANÁLISIS E INTERPRETACIÓN

De los investigados 4 Fiscales que equivale al 50% opinan, que su derecho a la intimidad es violentada en las comunicaciones utilizando el internet u otro mecanismos de sistema informático. Mientras que el otro 50% dice que su derecho a la intimidad esta salvaguardado por los mecanismos informáticos.

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

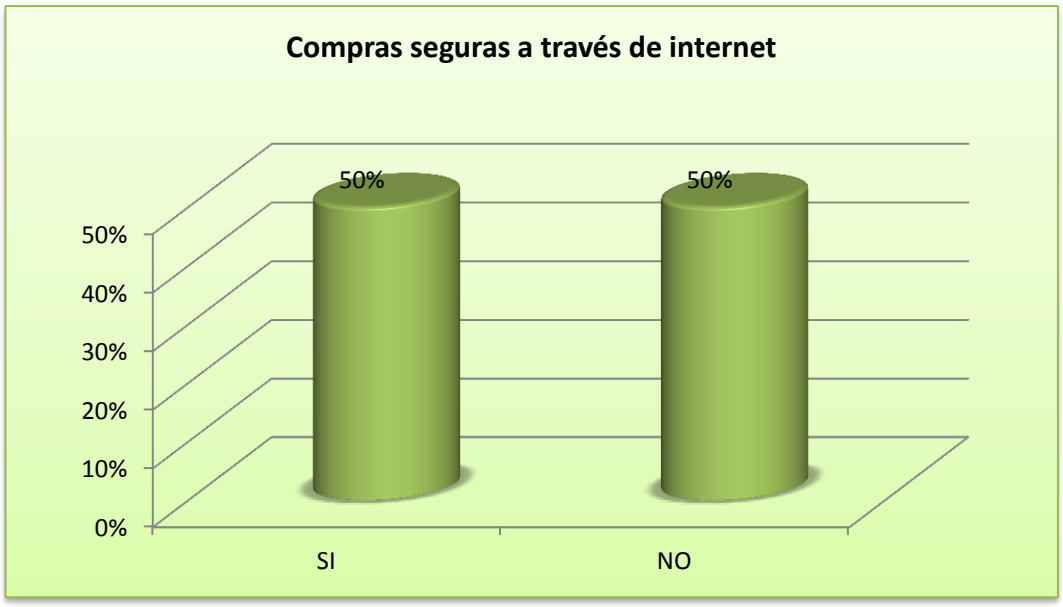
Cuadro Nº 5

Compras seguras a través de internet

Cuestión	No.	Porcentaje
Si	4	50%
No	4	50%
TOTAL	**8**	**100%**

Fuente: Encuestas
Elaborado por: Investigador

Gráfico Nº 5



Fuente: Encuestas
Elaborado por: Investigador

ANÁLISIS E INTERPRETACIÓN

Según las opiniones de los encuestados al referirse a la pregunta, responden 4 Fiscales que es el 50% que las compras a través de internet son seguras y confiables. No así los 4 restantes igual al 50% dicen que las compras a través de internet no son seguras.

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

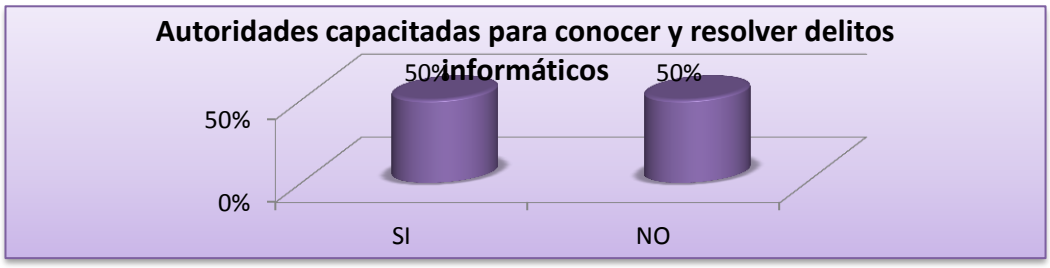
Cuadro Nº 6

Autoridades capacitadas para conocer y resolver delitos informáticos

Cuestión	No.	Porcentaje
Si	4	50%
No	4	50%
TOTAL	**8**	**100%**

Fuente: Encuestas
Elaborado por: Investigador

Gráfico Nº 6



Fuente: Encuestas
Elaborado por: Investigador

ANÁLISIS E INTERPRETACIÓN

Como resultado de los datos de investigación se conoce que 4 Fiscales equivalente al 50% consideran que las autoridades encargadas de la administración de justicia están capacitadas para conocer y resolver plenamente los casos de delitos informáticos. Y 4 de ellos equivalente al 50% restante considera que las autoridades encargadas de la administración de justicia no se encuentran capacitadas para conocer y resolver plenamente este tipo de delitos.

7. ¿Según su propia experiencia considera usted, que en el juzgamiento de los delitos informáticos existe algún problema?

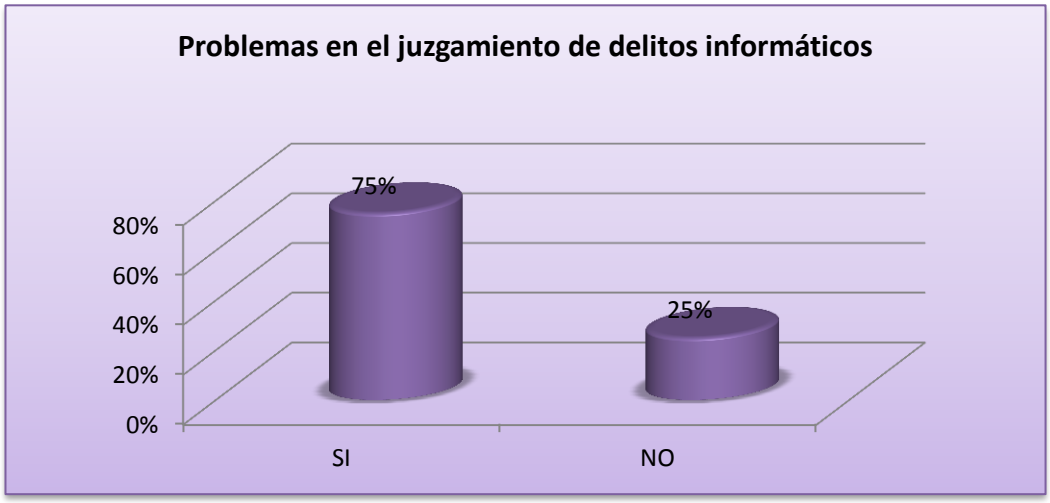
Cuadro Nº 7

Problemas en el juzgamiento de delitos informáticos

Cuestión	No.	Porcentaje
Si	6	75%
No	2	25%
TOTAL	**8**	**100%**

Fuente: Encuestas
Elaborado por: Investigador

GRÁFICO Nº 7



Fuente: Encuestas
Elaborado por: Investigador

ANÁLISIS E INTERPRETACIÓN

Los resultados que arroja la encuesta indican que 6 Fiscales correspondiente al 75% opinan que en el juzgamiento de los delitos informáticos existe algún problema. Mientras que 2 Fiscales correspondiente al 25% consideran que en el juzgamiento de este tipo de delitos existen problemas de acuerdo a su propia experiencia.

8. ¿Considera que es necesario la ampliación de un Capítulo en el Código Adjetivo Penal exclusivo para la tipificación de los delitos informáticos?

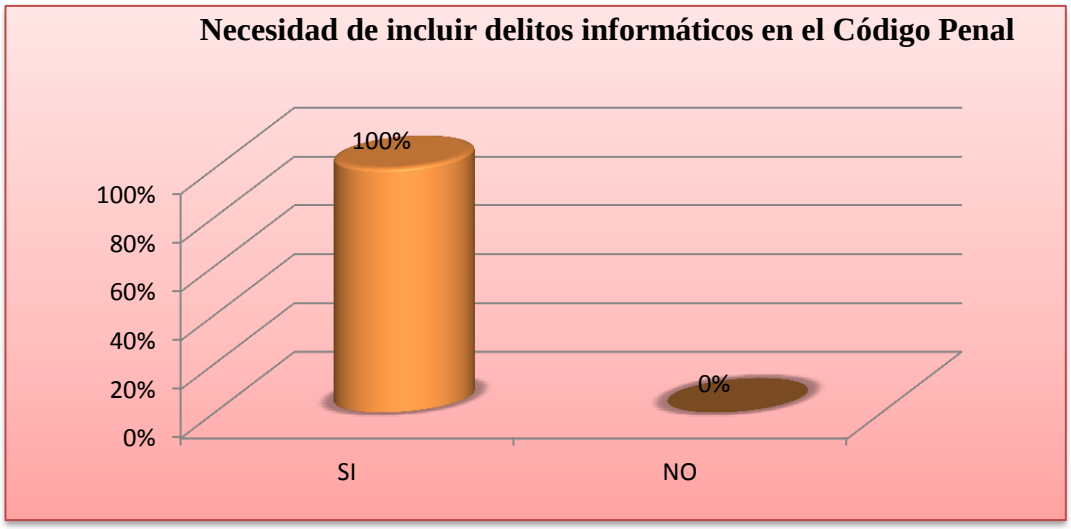
Cuadro Nº 8

Necesidad de incluir delitos informáticos en el Código Penal

Cuestión	No.	Porcentaje
Si	8	100%
No	0	0%
TOTAL	**8**	**100%**

Fuente: Encuestas
Elaborado por: Investigador

Gráfico Nº 8



Fuente: Encuestas
Elaborado por: Investigador

ANÁLISIS E INTERPRETACIÓN

Los 8 Fiscales encuestados que es el 100% considera necesario incluir en el Código Penal delitos informáticos.

9. ¿Apoyaría usted, la implementación de un Capítulo exclusivo sobre los delitos informáticos en el Código Adjetivo Penal Ecuatoriano?

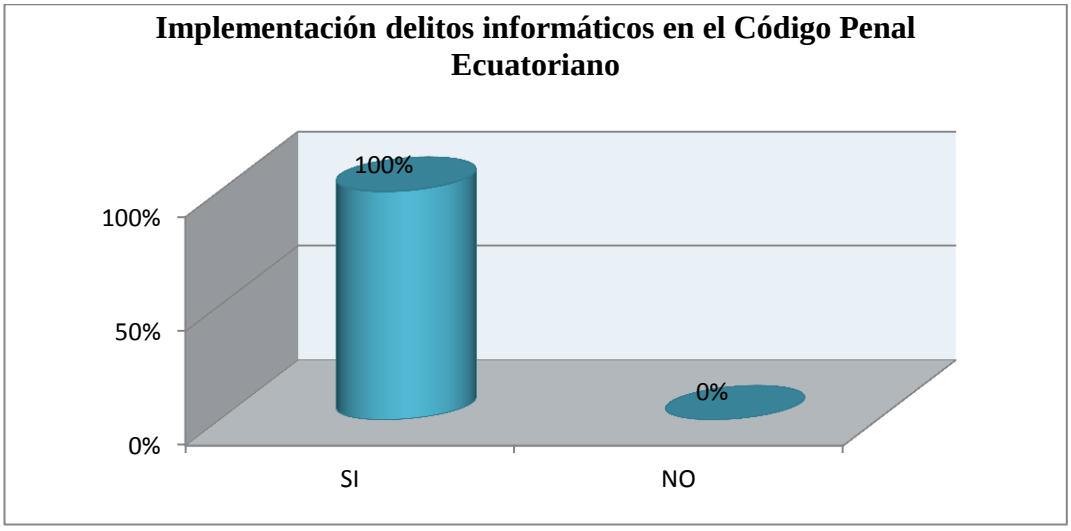
TABLA Nº 9

Implementación delitos informáticos en el Código Penal Ecuatoriano

Cuestión	No.	Porcentaje
Si	8	100%
No	0	0%
TOTAL	**8**	**100%**

Fuente: Encuestas
Elaborado por: Investigador

GRÁFICO Nº 9



Fuente: Encuestas
Elaborado por: Investigador

ANÁLISIS E INTERPRETACIÓN

Los 8 encuestados que corresponde al 100% manifiestan que apoyarían, la inclusión de delitos de carácter informático en el Código Penal Ecuatoriano...

2.5.3. Encuesta Efectuada a los Señores Abogados en Libre Ejercicio de la Provincia de Cotopaxi

1. ¿Conoce usted, que es un delito informático?

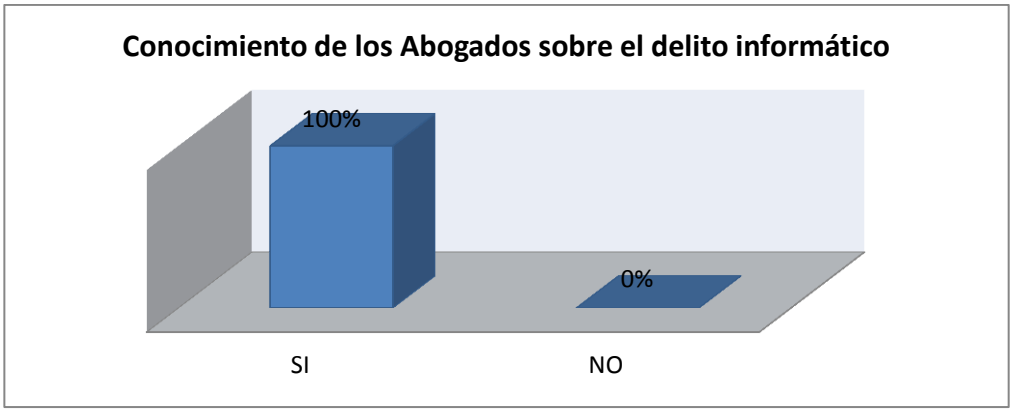
Cuadro Nº 1

Conocimiento de los Abogados sobre el delito informático

Opción	No.	Porcentaje
Si	236	100%
No	0	0%
TOTAL	236	100%

Fuente: Encuestas
Elaborado por: Investigador

Gráfico Nº 1



Fuente: Encuestas
Elaborado por: Investigador

ANÁLISIS E INTERPRETACIÓN

Los 236 abogados encuestados sobre el tema equivalente al 100% determinan que conocen que es el Delito Informático.

2. ¿Usted considera, que todos los delitos informáticos están tipificados en el Código Penal?

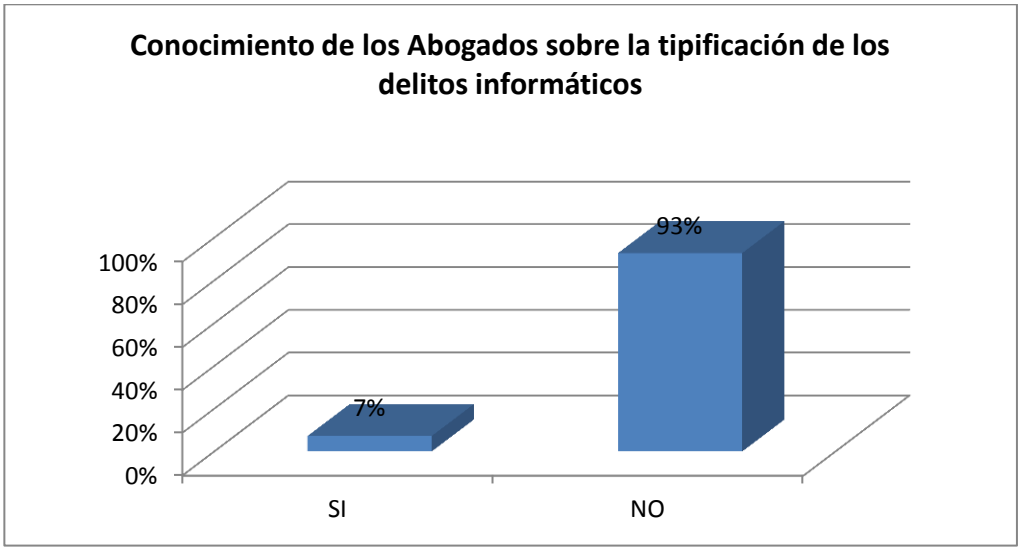
Cuadro N° 2

Conocimiento de los Abogados sobre la tipificación de los delitos informáticos

Cuestión	No.	Porcentaje
Si	17	7%
No	219	93%
TOTAL	**236**	**100%**

Fuente: Encuestas
Elaborado por: Investigador

Gráfico Nº 2



Fuente: Encuestas
Elaborado por: Investigador

ANÁLISIS E INTERPRETACIÓN

De los 236 abogados en libre ejercicio encuestados 17 de ellos equivalente al 7% opinan que todos los delitos informáticos están tipificados en el Código Penal. Mientras tanto que 219 que son el 93% señalan que no todos los delitos se encuentran tipificados.

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

Cuadro Nº 3

Abogados que han sido víctimas de algún tipo de delito informático

Cuestión	No.	Porcentaje
Si	5	2%
No	231	98%
TOTAL	**236**	**100%**

Fuente: Encuestas
Elaborado por: Investigador

Gráfico Nº 3

Fuente: Encuestas
Elaborado por: Investigador

ANÁLISIS E INTERPRETACIÓN

Según las opiniones vertidas en la encuesta 5 de los encuestados cuya equivalencia es del 2% determinan haber sido víctimas de algún delito de naturaleza informática. Y 231 de ellos que son el 98% establecen que nunca han sido víctima de algún tipo de delito informático.

4. ¿Considera usted, que su derecho a la intimidad es violentada en las comunicaciones utilizando el internet u otro mecanismos de sistema informático?

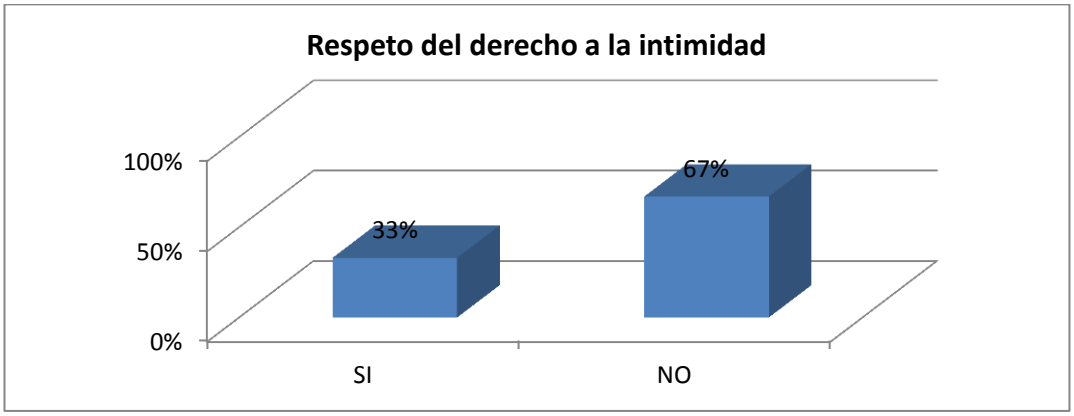
Cuadro Nº 4

Respeto del derecho a la intimidad

Cuestión	No.	Porcentaje
Si	78	%
No	158	%
TOTAL	**236**	**100%**

Fuente: Encuestas
Elaborado por: Investigador

Gráfico Nº 4



Fuente: Encuestas
Elaborado por: Investigador

ANÁLISIS E INTERPRETACIÓN

78 de los encuestados que son el 33% opinan que su derecho a la intimidad es violentada en las comunicaciones utilizando el internet u otro mecanismos de sistema informático. Mientras que 158 correspondiente al 67% consideran que no es violentada en las comunicaciones utilizando el internet u otro mecanismo de sistema informático.

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

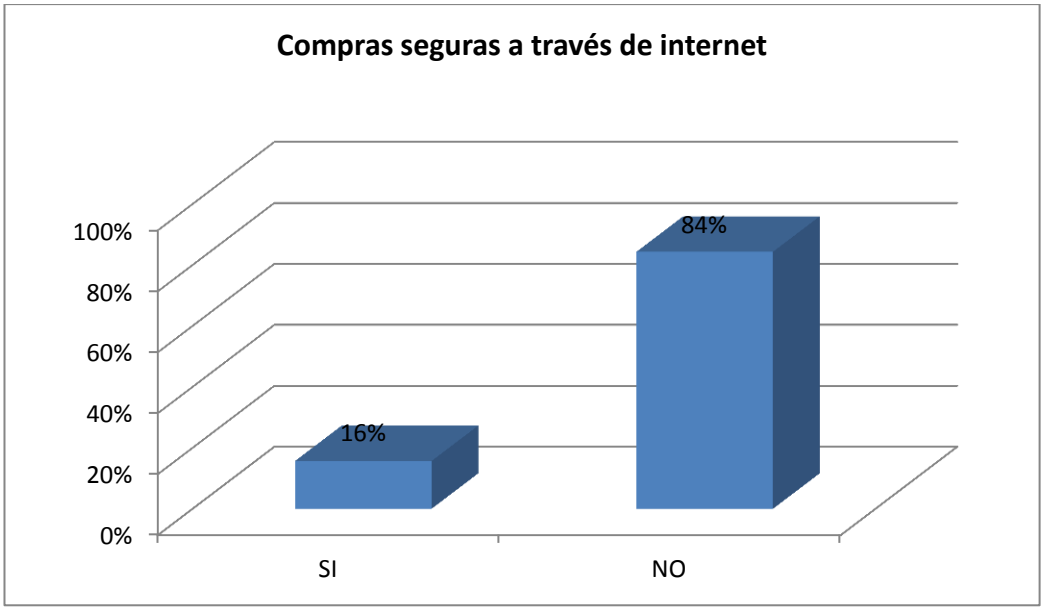
Cuadro Nº 5

Compras seguras a través de internet

Cuestión	No.	Porcentaje
Si	37	16%
No	199	84%
TOTAL	**236**	**100%**

Fuente: Encuestas
Elaborado por: Investigador

Gráfico Nº 5



Fuente: Encuestas
Elaborado por: Investigador

ANÁLISIS E INTERPRETACIÓN

De los encuestados 37 equivalentes al 16% consideran, que las compras a través de internet son seguras. Y por otro lado 199 que son el 84% asumen que las compras a través de internet no son seguras.

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

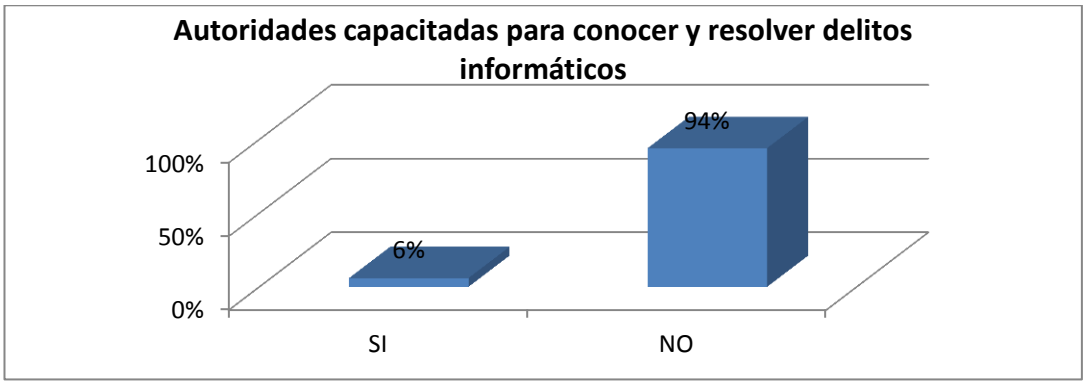
Cuadro Nº 6

Autoridades capacitadas para conocer y resolver delitos informáticos

Cuestión	No.	Porcentaje
Si	14	6%
No	222	94%
TOTAL	**236**	**100%**

Fuente: Encuestas
Elaborado por: Investigador

Gráfico Nº 6



Fuente: Encuestas
Elaborado por: Investigador

ANÁLISIS E INTERPRETACIÓN

14 de los encuestados correspondientes al 6% opinan que las autoridades encargadas de la administración de justicia están capacitadas para conocer y resolver plenamente los delitos de carácter informático. Mientras 222 equivalente al 84% determinan que las autoridades no se encuentran capacitadas para resolver sobre estos delitos.

7. ¿Según su propia experiencia considera usted, que en el juzgamiento de los delitos informáticos existe algún problema?

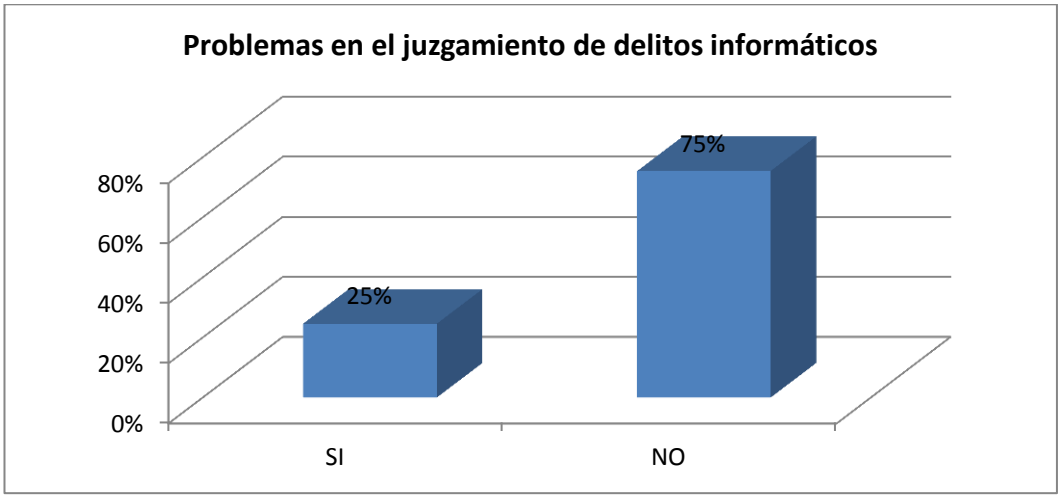
Cuadro Nº 7

Problemas en el juzgamiento de delitos informáticos

Cuestión	No.	Porcentaje
Si	58	25%
No	178	75%
TOTAL	**236**	**100%**

Fuente: Encuestas
Elaborado por: Investigador

Gráfico Nº 7



Fuente: Encuestas
Elaborado por: Investigador

ANÁLISIS E INTERPRETACIÓN

De los datos obtenidos se puede concluir que 58 de los encuestados que son el 25% asumen que según su propia experiencia considera que en el juzgamiento de los delitos informáticos si existe algún problema. Mientras que 178 de ellos que equivalen al 75% restante dicen que no existen problemas en el juzgamiento de este tipo de delitos.

8. ¿Considera que es necesario la ampliación de un Capítulo en el Código Adjetivo Penal exclusivo para la tipificación de los delitos informáticos?

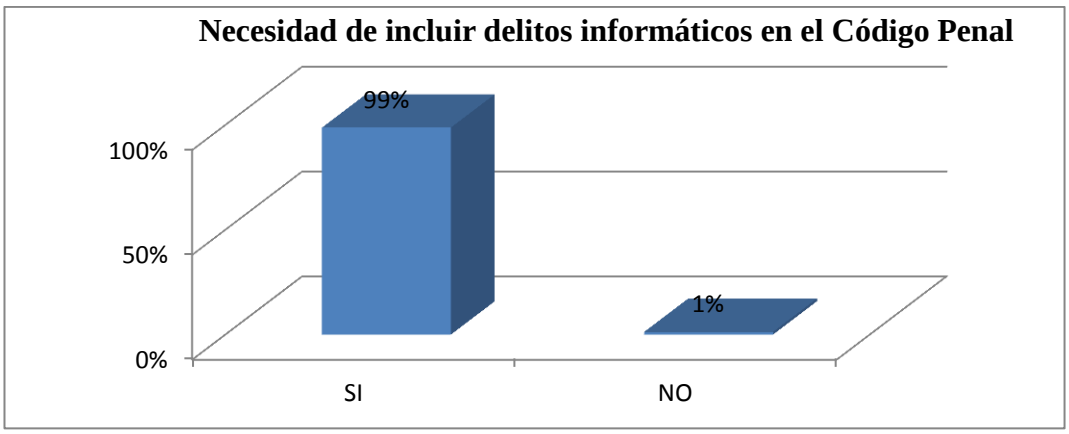
Cuadro Nº 8

Necesidad de incluir delitos informáticos en el Código Penal

Cuestión	No.	Porcentaje
Si	233	99%
No	3	1%
TOTAL	**236**	**100%**

Fuente: Encuestas
Elaborado por: Investigador

Gráfico Nº 8



Fuente: Encuestas
Elaborado por: Investigador

ANÁLISIS E INTERPRETACIÓN

Según los datos obtenidos los encuestados manifiestan su opinión de la siguiente manera 233 que es igual al 99% piensan que es necesario incluir delitos informáticos en el Código Penal. Y los 3 restantes que es el 1% asumen que no es necesario.

9. ¿Apoyaría usted, la implementación de un Capítulo exclusivo sobre los delitos informáticos en el Código Adjetivo Penal Ecuatoriano?

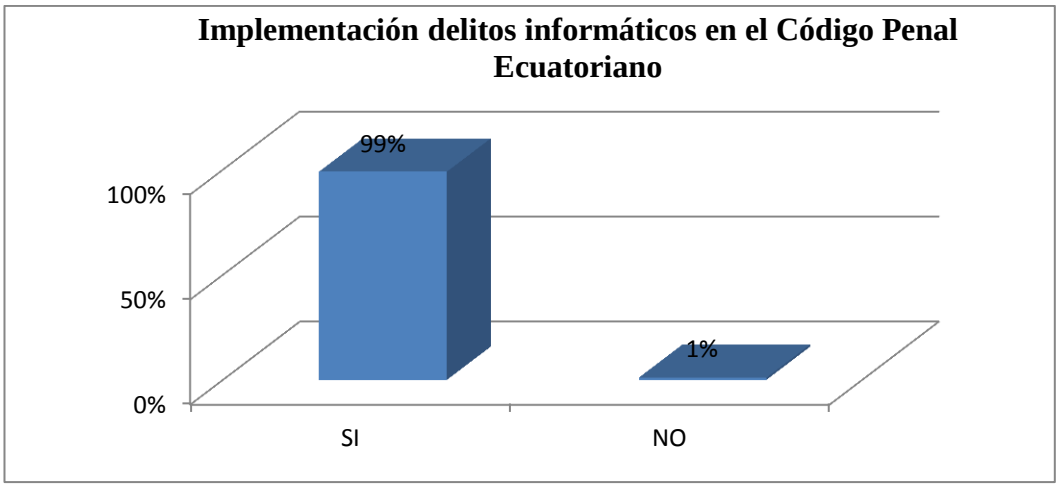
Cuadro Nº 9

Implementación delitos informáticos en el Código Penal Ecuatoriano

Cuestión	No.	Porcentaje
Si	233	99%
No	3	1%
TOTAL	**236**	**100%**

Fuente: Encuestas
Elaborado por: Investigador

Gráfico Nº 9



Fuente: Encuestas
Elaborado por: Investigador

ANÁLISIS E INTERPRETACIÓN

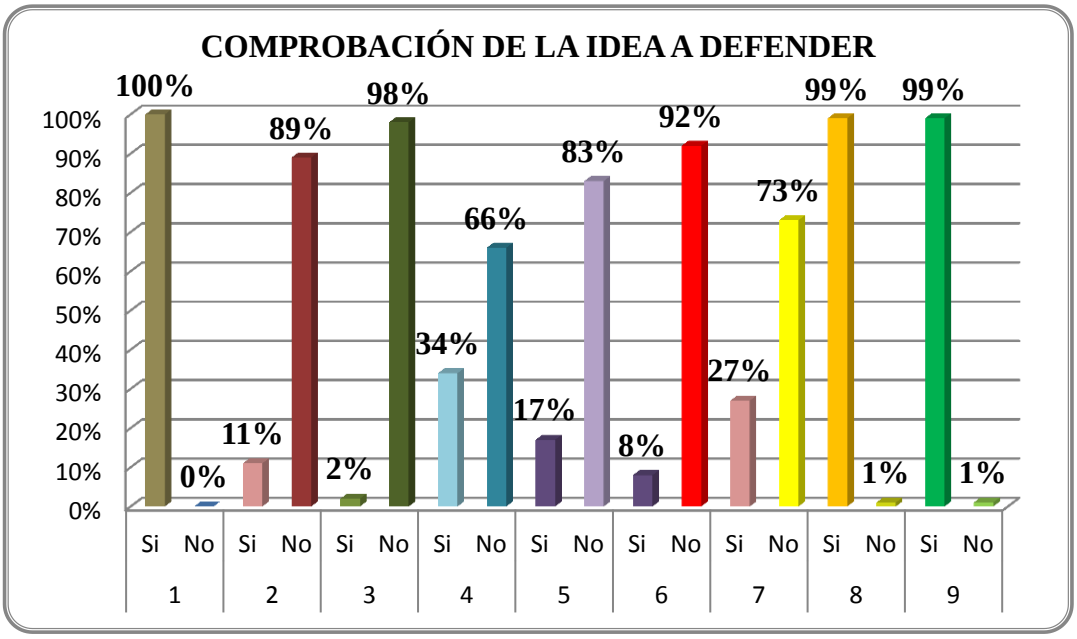
De los 236 encuestados 233 equivalentes al 99% según su opinión dicen que apoyarían, un taller de capacitación dirigido a los abogados en libre ejercicio, en el cual se determine los problemas dentro de los procesos de juzgamiento en los casos de delitos informáticos. Mientras tanto que 3 que es el 1% dicen no estar de acuerdo con esta capacitación.

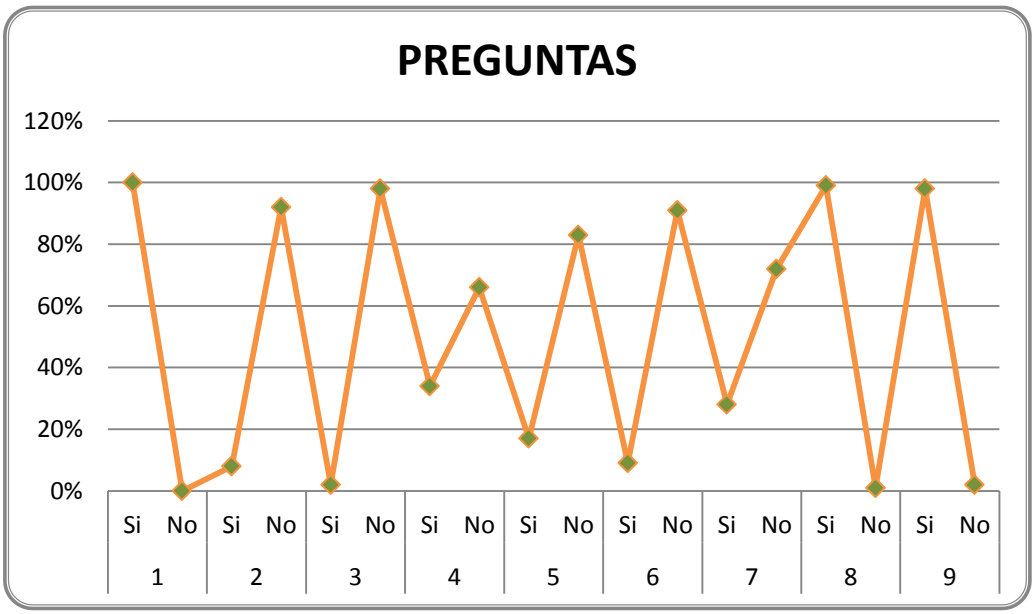
2.6. Verificación de la Idea a Defender

PREG. / RESP	1		2		3		4		5		6		7		8		9	
	N	%	N	%	N	%	N	%	N	%	N	%	N	%	N	%	N	%
SI	253	100																
NO	0	0																
SI			19	8														
NO			234	92														
SI					5	2												
NO					248	98												
SI							87	34										
NO							166	66										

SI									43	17								
NO									210	83								
SI											23	9						
NO											230	91						
SI													70	28				
NO													183	72				
SI															250	99		
NO															3	1		
SI																	249	98
NO																	4	2
TOTAL	253	100	253	100	253	100	253	100	253	100	253	100	253	100	253	100	253	100

2.7. Comprobación de la Idea a Defender





2.8. Conclusiones

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

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

- Se ha determinado que los en cargados de la administración de justicia y profesionales en libre ejercicio, tienen la necesidad de conocer la normativa penal vigente en materia referente a delitos informáticos, para acceder a los beneficios y saber cuáles son las limitantes que la ley impone a los ciudadanos sobre el tema de los delitos informáticos.

- Existe la aceptación respecto de la posibilidad de que se implemente un Capítulo exclusivo sobre los delitos informáticos en el Código Adjetivo Penal.

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

2.8.1. Recomendaciones

- Con el fin de agilizar los trámites y evitar controversias en la administración de justicia en estos casos, por desconocimiento en materia de Delitos Informáticos por parte del sistema relacionado con la Administración de Justicia, Abogados en libre ejercicio profesional, acusadores y defensores, se debe capacitar a los profesionales del derecho.

- Incentivar a los profesionales del derecho para su formación sobre el tema de los Delitos Informáticos, dando a conocer sus ventajas y limitaciones, para lo cual el respectivo Colegio de Abogados, deberá socializar mediante capacitaciones motivadoras a todos los profesionales del derecho y administradores de justicia.

- Proponer la implementación en el Código Adjetivo Penal, sobre un Capítulo exclusivo que establezca con claridad los tipos de Delitos informáticos existentes.

- Enviar una propuesta ampliatoria al Código Adjetivo Penal; a la Asamblea Nacional, con la implementación de un Capítulo exclusivo sobre los Delitos Informáticos.

- Es recomendable que los funcionarios judiciales y todos los profesionales que se encuentran íntimamente ligados con la administración de la justicia, se encuentren continuamente capacitando, en razón a la evolución del Derecho en General.

CAPÍTULO III

3. MARCO PROPOSITIVO

3.1. Documento Crítico

La legislación ecuatoriana brinda todas las garantías basadas en principios constitucionales sobre la protección en los casos de delitos de carácter informático, además se encuentran contenidos y sancionados por los tratados y convenios internacionales, el gran problema que se presenta en estos casos es que al momento de ser aplicados en el Código Adjetivo Penal Ecuatoriano existen vacíos en las normas para el juzgamiento de casos sobre delitos informáticos, ya que los mismos son abordados en una manera muy generalizada que tiende a limitar la validación de derechos de las víctimas de los este tipo de delitos, pues existen muchas fallas dentro de nuestro sistema jurídico y de administración de justicia.

El Código Adjetivo Penal Ecuatoriano tipifica varios tipos de delitos de carácter informático en los cuales se deben seguir procesos para una correcta aplicación de justicia, todo esto para garantizar el justo proceso y que tanto la parte ofendida y procesada, llamados en los casos de los delitos informáticos sujeto pasivo y sujeto activo puedan lograr que se cumplan con eficacia la correcta aplicación de las normas constitucionales y penales vigentes.

Todo esto estaría muy bien si se cumplieran correctamente con las normas establecidas, pero que sucede si al momento de que los encargados de la

administración de justicia desconocen sobre este tipo de delitos, y peor aún no conocen el procedimiento que hay que seguir para su aplicación; puede ocasionar problemas graves al momento de garantizar derechos ciudadanos por la falta de experiencia y el modos operandi del sujeto activo en este tipo de delitos lo cual puede crear confusión y la mala administración de justicia, pudiendo condenar a inocentes y absolver a culpables.

En consecuencia los Delitos Informáticos se han convertido en un medio efectivo para los delincuentes para cometer actos atípicos y no ser sancionados conforme a derecho, provocando así un gran perjuicio, la inseguridad jurídica en el presente caso y daño en la sociedad en forma general, del Derecho Penal que va íntimamente ligado a la humanidad de la persona en razón del ejercicio y goce de sus derechos debe garantizar que estos se hagan efectivos.

En consecuencia la propuesta al tema investigado permite de una u otra forma fortalecer los conocimientos ya obtenidos por funcionarios del derecho y los encargados de la administración de justicia de cumplir y hacer cumplir las normas legales establecidas en nuestra sociedad y además cubriría los vacíos existentes en el Código Adjetivo Penal Ecuatoriano referente a los Delitos Informáticos.

3.2. Diseño de la Propuesta

3.2.1. Título de la propuesta

"ELABORACIÓN DE UN ANTEPROYECTO DE LEY AMPLIATORIO AL CODIGO ADJETIVO PENAL CON LA INCLUSIÓN DE UN CAPÍTULO EXCLUSIVO PARA LA TIPIFICACIÓN DE LOS DELITOS INFORMÁTICOS"

3.2.2. Fundamentación

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.

Nos enfrentamos a un gran problema ya que estos delitos que no pueden ser investigados de forma eficaz presentan problemas en todas sus etapas por falta de eficacia probatoria en algunos casos y lo que es aún más grave en otros por falta de conocimiento, experiencia y un vacío en la Ley pertinente que dificulta la aplicabilidad por parte de las autoridades encargadas de la administración de justicia para este tipo de delitos, que en nuestro país es una forma de delinquir sumamente nueva.

Para respaldar con base legal la inclusión exclusiva de un Capítulo referente a los delitos informáticos en el Código Adjetivo Penal vigente en el Estado Ecuatoriano.

Para evitar que la cultura de incumplimiento de las normas establecidas dentro de la sociedad ecuatoriana sigan siendo un hecho que actúen como factor multiplicador de la impunidad en los casos sobre delitos informáticos.

Para garantizar el pleno ejercicio de los derechos de todas las personas y la seguridad jurídica que debe ofrecer el Estado Ecuatoriano a la sociedad, es necesario la implementación de delitos informáticos en el Código Penal Ecuatoriana, que garanticen una administración de justicia eficiente.

3.2.3. Justificación

Con el pasar del tiempo el derecho ha ido evolucionado constantemente para acoplarse a eventos atípicos que necesitan reglamentarse de manera moderna y aplicar principios basados en la esencia misma del ser humano. El motivo por el cual se ha seleccionado el presente tema es porque la informática en la actualidad es una de las herramientas básicas que se encuentran en el mercado y es el eje mediante el cual se mueve la economía a nivel mundial, lo cual siempre me ha llamado la atención, además porque los delitos informáticos están estrechamente relacionados con la informática y con el derecho.

Una de las causas principales que han motivado la presente investigación es la satisfacción personal pero también porque los delitos informáticos son una forma de criminalidad novedosa que están ocasionando graves problemas y se necesita buscar soluciones ya que hoy en día no hay suficientes formas de combatirlos.

El propósito de la presente investigación es analizar el concepto de delito informático así como sus diferentes tipos, tipificación, estadística, seguridad, legislación de estos, y muchas otras cosas importantes relacionadas con el crimen informático.

Este tipo de delitos por ser de reciente aparición en nuestro medio y en general en nuestro país aún no han sido investigados en forma amplia y detallada haciendo de esta manera que exista cierto tipo de desconocimiento por parte de la sociedad en general y por los encargados para administrar justicia, convirtiéndose en un tema novedoso y de interés para toda la colectividad y para los estudiosos del derecho en particular.

La presente investigación aportará con una amplia información para garantizar la defensa de los derechos de las personas a las que se han vulnerado sus garantías por este tipo de delitos, pues ningún delito puede quedar en la impunidad por falta de ley, norma o desconocimiento según lo manifiesta la Carta Magna del Estado; además servirá de guía para los futuros estudiantes de derecho, abogados, jueces, fiscales y todos aquellos que conforman la Función Judicial en nuestro país, para que se efectué nuevos estudios sobre el tema en forma más amplia, cuando se cuente con los recursos necesarios.

Con la elaboración del presente proyecto se beneficiará a la sociedad en general, ya que se le permite obtener información sobre el tema que quizá no ha sido difundido en forma debida, o no sea creado eco dentro de ella, al ser un nuevo modo de quebrantar las leyes sin obtener ningún tipo de sanción por parte del infractor es necesario que nos mantengamos informados sobre este tipo de hechos; de forma particular se beneficiaran los estudiosos del derecho que tienen en el presente, un material de información y apoyo de estudios sobre el caso.

Existe la factibilidad para lograr la investigación y aplicación del tema ya que existen antecedentes sobre estos hechos en otros países del mundo los mismos que han desarrollado medios eficaces para su estudio y sobre todo para que estos sean sancionados con todo el peso y rigor de la ley que se merecen, hay la información necesaria para el desarrollo del tema en libros, revistas, e incluso codificaciones de otros países del mundo entero que tienen avanzado su estudio sobre el tema.

El estudiante ha identificado como limitación para la elaboración del proyecto en nuestro país no se cuenta con todos los recursos necesarios tanto económicos, humanos y de investigación que esta demanda; además dentro de la administración de justicia aún no se ha logrado la creación de oficinas equipadas, con personal especializado para verificar la existencia del delito, y que los responsables sean juzgados conforme a derecho tal como la ley lo demanda.

La Constitución de la República del Ecuador en su Artículo N°3, numeral 8 dispone al Estado como uno de sus deberes primordiales garantizar a sus habitantes el derecho a la seguridad integral.

En el artículo 82 se establece el derecho a la seguridad jurídica se fundamenta en el respeto a la Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicadas por las autoridades competentes.

De igual manera en el artículo N° 84 se determina que la Asamblea Nacional y todo órgano con potestad normativa tendrá la obligación de adecuar, formal y materialmente, las leyes y demás normas jurídicas a los derechos previstos en la Constitución y los tratados internacionales, y los que sean necesarios para garantizar la dignidad del ser humano o de las comunidades, pueblos y nacionalidades.

Por lo tanto es menester la elaboración de un Anteproyecto de Ley Ampliatorio al Código Adjetivo Penal con inclusión de un Capítulo para la tipificación de los delitos informáticos.

3.3. Objetivos:

3.3.1. Objetivo General:

- ✓ Tipificar los delitos informáticos en el Código Adjetivo Penal, con la inclusión de un capítulo exclusivo para este fin.

3.3.2. Objetivos Específicos:

- ✓ Analizar los contenidos doctrinarios en relación a los delitos informáticos.

- ✓ Revisar los artículos en relación a las penas peculiares del delito a fin de determinar las sanciones para los delitos informáticos.

- ✓ Redactar el Anteproyecto con la inclusión de aportes teóricos y legales en relación a los delitos informáticos.

3.4. Desarrollo de la Propuesta

3.4.1. Exposición de Motivos

REPÚBLICA DEL ECUADOR

LA ASAMBLEA NACIONAL

CONSIDERANDO:

QUE: Es obligación del Estado ecuatoriano garantizar el ejercicio de la administración de justicia eficaz y eficiente establecida en la Constitución de la República.

QUE: Es obligación del Estado ecuatoriano evitar que siga incrementando el número de delitos informáticos, por falta de tipificación en el Código Adjetivo Penal ecuatoriano vigente.

QUE: El desarrollo tan amplio de las tecnologías informáticas ofrece un aspecto negativo: ha abierto la puerta a conductas antisociales y delictivas que se manifiestan de formas que hasta ahora no era posible imaginar. Los sistemas de computadoras 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.

QUE: En los últimos tiempos, ha sido evidente que la sociedad ha utilizado de manera benéfica los avances derivados de la tecnología en diversas actividades; sin embargo, es necesario que se atiendan y regulen las cada vez más frecuentes consecuencias del uso indebido de las computadoras y los sistemas informáticos en general.

EN USO DE SUS ATRIBUCIONES QUE LE CONCEDE LA LEY EXPIDE:

Las siguientes reformas ampliatorias al Código Adjetivo Penal:
Luego del Capítulo IX, agréguese el Capítulo X que diga:

CAPÍTULO X

DE LOS DELITOS INFORMÁTICOS

Agréguese los siguientes artículos inumerados:

Art… Acceso indebido.- El que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información; con fines delictivos, será penado con prisión de uno a cinco años y multa de cien a quinientos dólares de los Estados Unidos de Norteamérica.

Art… Sabotaje o daño a sistemas.- El que destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que emplee tecnologías de información o cualquiera de los componentes que lo conforman, será penado con prisión de dos a cinco años y multa de quinientos a cuatro mil dólares de los Estados Unidos de Norteamérica.

Incurrirá en la misma pena quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualquiera de sus componentes.

La pena se aumentará hasta dos años, si los efectos indicados en el presente artículo se realizaren mediante la creación, introducción o transmisión, por cualquier medio, de un virus o programa análogo.

Art… Sabotaje o daño culposo.- Si el delito previsto en el artículo anterior se cometiere por imprudencia, negligencia, impericia o inobservancia de las normas establecidas, se aplicará la pena correspondiente según el caso, con una reducción entre la mitad y dos tercios.

Art… Acceso indebido o sabotaje a sistemas protegidos.- Las penas previstas en los artículos anteriores se aumentarán entre una tercera parte y la mitad cuando los hechos allí previstos o sus efectos recaigan sobre cualquiera de los componentes de un sistema que utilice tecnologías de información protegido por medidas de seguridad, que esté destinado a funciones públicas o que contenga información personal o patrimonial de personas naturales o jurídicas

Art… Posesión de equipos o prestación de servicios de sabotaje.- El que, con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información, importe, fabrique, posea, distribuya, venda o utilice equipos, dispositivos o programas; o el que ofrezca o preste servicios destinados a cumplir los mismos fines, será reprimido con prisión de seis a cuatro años y multa de trescientos a dos mil dólares de los Estados Unidos de Norteamérica.

Art… Espionaje informático.- El que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de

información o en cualquiera de sus componentes, será reprimido con prisión de seis meses a un año y multa de quinientos a dos mil dólares de los Estados Unidos de Norteamérica.

Si se cometiere con el fin de obtener algún tipo de beneficio para sí o para otra persona, la pena será de uno a tres años de prisión.

Si la información obtenida se refiere o pone en peligro la seguridad nacional, la confiabilidad de las operaciones de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas como consecuencia de la revelación de las informaciones de carácter reservado, será sancionado con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Art… Falsificación de documentos.- El que a través de cualquier medio, cree, modifique o elimine un documento que se encuentre incorporado a un sistema que utilice tecnologías de información; o cree, modifique o elimine datos del mismo; o incorpore a dicho sistema un documento inexistente, será reprimido con prisión de seis a tres años y multa de trescientos a seiscientos dólares de los Estados Unidos de Norteamérica.

La pena se aumentará hasta un año, cuando el agente hubiere actuado con el fin de procurar para sí o para otro algún tipo de beneficio.

El aumento será de dos años si del hecho resultare un perjuicio para otro.

Art… Hurto.- El que a través del uso de tecnologías de información, acceda, intercepte, interfiera, manipule o use de cualquier forma un sistema o medio de

comunicación para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolos a su tenedor, con el fin de procurarse un provecho económico para sí o para otro, será reprimido con prisión de un mes a tres años, tomando en cuenta el valor de las cosas hurtadas doscientos a dos mil dólares de los Estados Unidos de Norteamérica, tomando en cuenta el valor de las cosas hurtadas.

Art… Fraude.- El que, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes o en la data o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno, será reprimido con prisión de seis meses a cinco años y multa de trescientos a cinco mil dólares de los Estados Unidos de Norteamérica.

Art… Obtención indebida de bienes o servicios.- El que, sin autorización para portarlos, utilice una tarjeta inteligente ajena o instrumento destinado a los mismos fines, o el que utilice indebidamente tecnologías de información para requerir la obtención de cualquier efecto, bien o servicio o para proveer su pago sin erogar o asumir el compromiso de pago de la contraprestación debida, será castigado con prisión de seis meses a un año y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica.

Art… Manejo fraudulento de tarjetas inteligentes o instrumentos análogos.- El que por cualquier medio, cree, capture, grabe, copie, altere, duplique o elimine

la data o información contenidas en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines; o el que, mediante cualquier uso indebido de tecnologías de información, cree, capture, duplique o altere la data o información en un sistema con el objeto de incorporar usuarios, cuentas, registros o consumos inexistentes o modifique la cuantía de éstos, serán reprimidos con prisión de dos a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

En la misma pena incurrirá quien, sin haber tomado parte en los hechos anteriores, adquiera, comercialice, posea, distribuya, venda o realice cualquier tipo de intermediación de tarjetas inteligentes o instrumentos destinados al mismo fin, o de la data o información contenidas en ellos o en un sistema.

Art… Apropiación de tarjetas inteligentes o instrumentos análogos.- El que se apropie de una tarjeta inteligente o instrumento destinado a los mismos fines, que se hayan perdido, extraviado o hayan sido entregados por equivocación, con el fin de retenerlos, usarlos, venderlos o transferirlos a persona distinta del usuario autorizado o entidad emisora, será reprimido con prisión de seis meses a cinco años y multa de veinticinco a doscientos dólares de los Estados Unidos de Norteamérica.

La misma pena se impondrá a quien adquiera o reciba la tarjeta o instrumento a que se refiere el presente artículo.

Art… Provisión indebida de bienes o servicios.- El que a sabiendas de que una tarjeta inteligente o instrumento destinado a los mismos fines, se encuentra vencido, revocado, se haya indebidamente obtenido, retenido, falsificado,

alterado, provea a quien los presente de dinero, efectos, bienes o servicios o cualquier otra cosa de valor económico, será reprimido con prisión de seis meses a cinco años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica.

Art… Posesión de equipo para falsificaciones.- El que sin estar debidamente autorizado para emitir, fabricar o distribuir tarjetas inteligentes o instrumentos análogos, reciba, adquiera, posea, transfiera, comercialice, distribuya, venda, controle o custodie cualquier equipo de fabricación de tarjetas inteligentes o de instrumentos destinados a los mismos fines o cualquier equipo o componente que capture, grabe, copie o transmita la data o información de dichas tarjetas o instrumentos, será reprimido con prisión de seis meses a cuatro años , decomiso de los artículos y multa de trescientos a seiscientos dólares de los Estados Unidos de Norteamérica.

Art… Violación de la privacidad de la data o información de carácter personal.- El que por cualquier medio se apodere, utilice, modifique o elimine, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será reprimido con prisión de dos meses a un año.

La pena se incrementará hasta en un año si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero.

Art… Violación de la privacidad de las comunicaciones.- El que mediante el uso de tecnologías de información, acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, será reprimidos con prisión de seis meses a dos años y multa de doscientas a seiscientos dólares de los Estados Unidos de Norteamérica.

Art… Revelación indebida de data o información de carácter personal.- El que revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los artículos precedentes, aun cuando el autor no hubiese tomado parte en la comisión de dichos delitos, será sancionado con prisión de dos meses a dos años y multa de cuatrocientos a dos mil dólares de los Estados Unidos de Norteamérica.

Si la revelación, difusión o cesión se hubieren realizado con un fin de lucro o si resultare algún perjuicio para otro, la pena será de seis meses a tres años y multa de quinientos a tres mil dólares de los Estados Unidos de Norteamérica.

Art… Apropiación de propiedad intelectual.- El que sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un software u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información, será reprimido con prisión de seis meses a tres años y multa de cien a quinientos dólares de los Estados Unidos de Norteamérica.

Art… Oferta engañosa.- El que ofrezca, comercialice o provea de bienes o servicios mediante el uso de tecnologías de información y haga alegaciones falsas o atribuya características inciertas a cualquier elemento de dicha oferta de modo que pueda resultar algún perjuicio para los consumidores, será sancionado con prisión de dos meses a dos años y multa de cien a quinientos dólares de los Estados Unidos de Norteamérica.

Dado y firmado en la ciudad de San Francisco de Quito, Distrito Metropolitano a los días……del mes de……del……

REFERENCIAS BIBLIOGRÁFICAS

BIBLIOGRAFÍA CITADA

- ✓ CUERVO, José; Tema: "Delitos Informáticos y Protección Penal a la Intimidad" (Pág.32).
- ✓ CARRASCOSA, Valentín; POZO, María; RODRIGUEZ, E. P., (1999) Tema: "La contratación Informática: El Nuevo Horizonte Contractual" (Pág.17).
- ✓ GARRIDO MONTT, Mario; (1998) Tema: "Contratación Electrónica y Firma Digital" (Pág.27).
- ✓ ILLESCAS ORTIS, Rafael; (2001) Tema: "Derecho de la Contratación Electrónica" (Pág. 21).
- ✓ LARA RIVERA, Jorge; (2001)Tema: "Derecho de Internet" (Pág.13)
- ✓ TEMBOURY REDONDO, Miguel; (2000) Tema: "La Prueba de los Documentos Electrónicos en los distintos Órdenes Jurisdiccionales, en Derecho de Internet" (Pág.66)

BIBLIOGRAFÍA CONSULTADA

- ✓ AVILA C, Luis A; (2006) "Delitos Informáticos".
- ✓ ACURIO DEL PINO, Santiago; "Delitos Informáticos, Manual de docencia sin lugar ni fecha".
- ✓ BICCARI, César; (2002) "De los delitos y las penas".
- ✓ BODERO, René E; (1993) "Derecho Penal Básico".
- ✓ ACURIO DEL PINO, Santiago; (2004) "Delitos Informáticos"
- ✓ CAÑAR L, Luis; (2004) "Comentarios de Código Penal de la República del Ecuador".
- ✓ DAVARA R, Miguel A; (1997) "Manual de Derecho Informático".
- ✓ DEL PESO N, Emilio; (2000) "Ley de Protección de Datos".
- ✓ LORENZETTI, Ricardo; (2001) "Comercio Electrónico".

- ✓ NIEVES GALARZA, Ricardo E; (2009) "Derecho Informático, Los Documentos Electrónicos".
- ✓ PEREZ MERAYO, Augusto; (1999) "Derecho, Tecnología y Cambio, Revista Electrónica del Derecho Informático".
- ✓ REBOLLO D, Lucrecia; (2004) "Derechos Fundamentales y Protección de Datos".
- ✓ TORRES CH, Efraín, (2001) "Breves Comentarios al Código Penal".
- ✓ VALLEGO DELGADO, Vicente E; (2010) "El delito Informático en la Legislación Ecuatoriana".
- ✓ ZABALA B, Jorge E; (2005) "Tratado de Derecho Procesal Penal".

LINKCOGRAFÍAS

- ✓ http://es.wikipedia.org/wiki/Delito_inform%C3%Altico Tema: "El Delito Informático".
- ✓ http://www.alegsa.com.ar/Dic/delito%20informatico.php Tema: "El Delito Informático".
- ✓ http://eva.utpl.edu.ec/oprnutpl/delito%20informatico.php Tema: "La Cibercriminalidad"
- ✓ http://www.eff.org/pub/publications/John perry barlow/barlow0296 Tema: "La declaración de independencia del ciberespacio".
- ✓ http://www.delitosinformaticos.com/tesis.htm Tema: "Presupuestos Para la Punibilidad del Hacking".
- ✓ http://www.http://www.vecam.org/article659.html. Tema: "Delito Informático".
- ✓ http://www.legistdf.gov.ar/sitio/documentos/firmadigital.
- ✓ http://www.delitosinformaticos.com/tesis.htm.
- ✓ http://www.uncintral.org.
- ✓ http://www.un.org.
- ✓ http://vlex.com/cl.
- ✓ www.derechoecuador.com

- ✓ www.google.com

TEXTOS LEGALES

- ✓ CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR; 2008, Publicación Oficial de la Asamblea Constituyente.
- ✓ CÓDIGO PENAL; 2010, Corporación de Estudios y Publicaciones.
- ✓ CÓDIGO DE PROCEDIMIENTO PENAL; 2010, Corporación de Estudios y Publicaciones.
- ✓ CÓDIGO DE PROCEDIMIENTO CIVIL ECUATORIANO; 2010, Corporación de Estudios y Publicaciones.
- ✓ LEY DE PROPIEDAD INTELECTUAL; 2010, Corporación de Estudios y Publicaciones.
- ✓ LEY ORGÁNICA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA; 2010, Corporación de Estudios y Publicaciones.
- ✓ LEY DE COMERCIO ELECTRÓNICO FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS; 2010, Corporación de Estudios y Publicaciones.
- ✓ LEY ESPECIAL DE TELECOMUNICACIONES; 2010, Corporación de Estudios y Publicaciones.

ANEXOS

UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS ADMINISTRATIVAS Y HUMANISTICAS

Latacunga-Ecuador

ENCUESTA N° 1

Objetivo: Determinar los problemas existentes dentro de los procesos de juzgamiento en los casos de delitos informáticos.

Esta encuesta es anónima y está dirigida a los Abogados en libre ejercicio de la Provincia de Cotopaxi; marque con una X la respuesta que usted considera acertada.

1. ¿Conoce usted, que es un delito informático?

   Si ☐ No ☐

2. ¿Usted considera, que todos los delitos informáticos están tipificados en el Código Penal?

   ☐

   Si ☐ No

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

   Si ☐ No ☐

4. ¿Considera usted, que su derecho a la intimidad es violentada en las comunicaciones utilizando el internet u otro mecanismos de sistema informático?

   Si ☐ No ☐

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

   Si ☐ No ☐

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

   Si ☐ No ☐

7. ¿Según su propia experiencia considera usted, que en el juzgamiento de los delitos informáticos existe algún problema?

   Si ☐ No ☐

8. ¿Considera que es necesario la ampliación de un Capítulo en el Código Adjetivo Penal exclusivo para la tipificación de los delitos informáticos?

   Si ☐ No ☐

9. ¿Apoyaría usted, la implementación de un Capítulo exclusivo sobre los delitos informáticos en el Código Adjetivo Penal Ecuatoriano?

   Si ☐ No ☐

Gracias por su colaboración

UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS ADMINISTRATIVAS Y HUMANISTICAS

Latacunga-Ecuador

ENCUESTA N° 2

Objetivo: Determinar los problemas existentes dentro de los procesos de juzgamiento en los casos de delitos informáticos.

Esta encuesta es anónima y está dirigida a los Fiscales de la Provincia de Cotopaxi; marque con una X la respuesta que usted considera acertada.

1. ¿Conoce usted, que es un delito informático?

   Si ☐ No ☐

2. ¿Usted considera, que todos los delitos informáticos están tipificados en el Código Penal?

   ☐

   Si ☐ No

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

   Si ☐ No ☐

4. ¿Considera usted, que su derecho a la intimidad es violentada en las comunicaciones utilizando el internet u otro mecanismos de sistema informático?

   Si ☐ No ☐

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

   Si ☐ No ☐

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

Si ☐ No ☐

7. ¿Según su propia experiencia considera usted, que en el juzgamiento de los delitos informáticos existe algún problema?

Si ☐ No ☐

8. ¿Considera que es necesario la ampliación de un Capítulo en el Código Adjetivo Penal exclusivo para la tipificación de los delitos informáticos?

Si ☐ No ☐

9. ¿Apoyaría usted, la implementación de un Capítulo exclusivo sobre los delitos informáticos en el Código Adjetivo Penal Ecuatoriano?

Si ☐ No ☐

Gracias por su colaboración

UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS ADMINISTRATIVAS Y HUMANISTICAS

Latacunga-Ecuador

ENCUESTA N° 3

Objetivo: Determinar los problemas existentes dentro de los procesos de juzgamiento en los casos de delitos informáticos.

Esta encuesta es anónima y está dirigida a los Jueces de la Sala Especializada de lo Penal, Tribunal y Jueces de Garantías Penales de la Provincia de Cotopaxi; marque con una X la respuesta que usted considera acertada.

1. ¿Conoce usted, que es un delito informático?

   Si ☐ No ☐

2. ¿Usted considera, que todos los delitos informáticos están tipificados en el Código Penal?

   ☐

   Si ☐ No

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

   Si ☐ No ☐

4. ¿Considera usted, que su derecho a la intimidad es violentada en las comunicaciones utilizando el internet u otro mecanismos de sistema informático?

   Si ☐ No ☐

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

   Si ☐ No ☐

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

Si ☐ No ☐

7. ¿Según su propia experiencia considera usted, que en el juzgamiento de los delitos informáticos existe algún problema?

Si ☐ No ☐

8. ¿Considera que es necesario la ampliación de un Capítulo en el Código Adjetivo Penal exclusivo para la tipificación de los delitos informáticos?

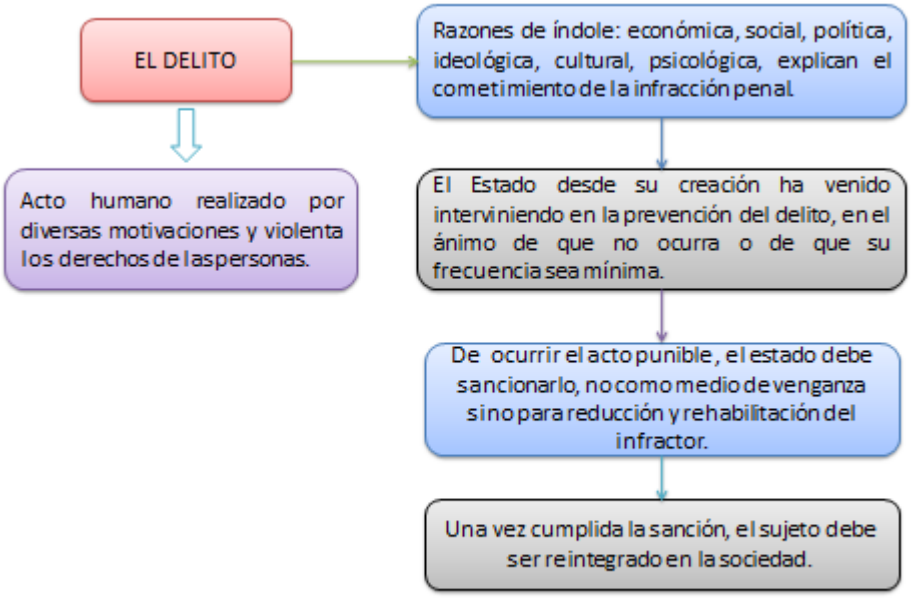
Si ☐ No ☐

9. ¿Apoyaría usted, la implementación de un Capítulo exclusivo sobre los delitos informáticos en el Código Adjetivo Penal Ecuatoriano?

Si ☐ No ☐

Gracias por su colaboración

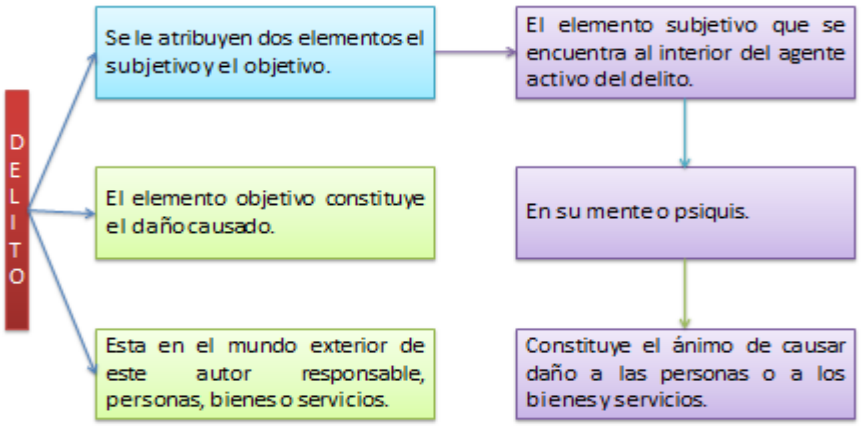
GRÁFICO N° 1



FUENTE: Power Point

DISEÑADO POR: El Investigador

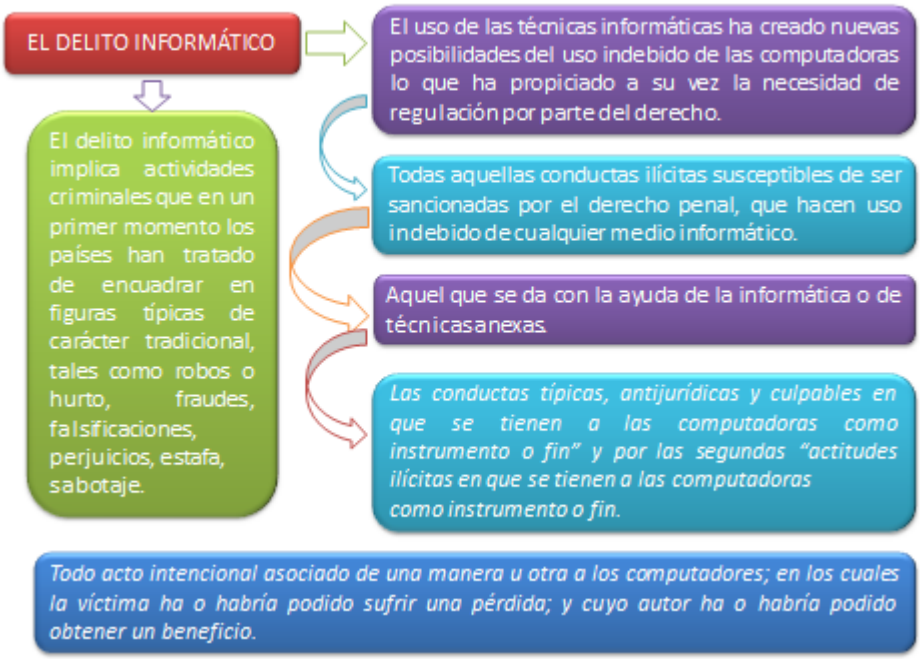
GRÁFICO N° 2



FUENTE: Power Point

DISEÑADO POR: El Investigador

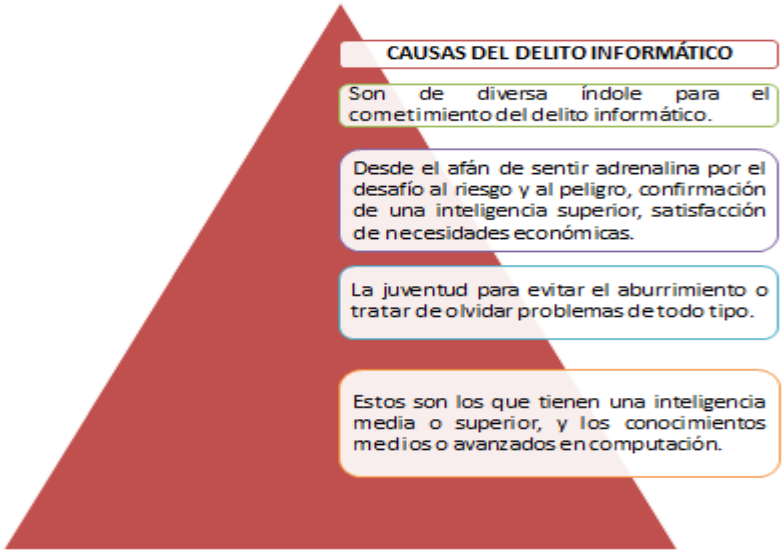
GRAFICO N° 3



FUENTE: Power Point

DISEÑADO POR: El Investigador

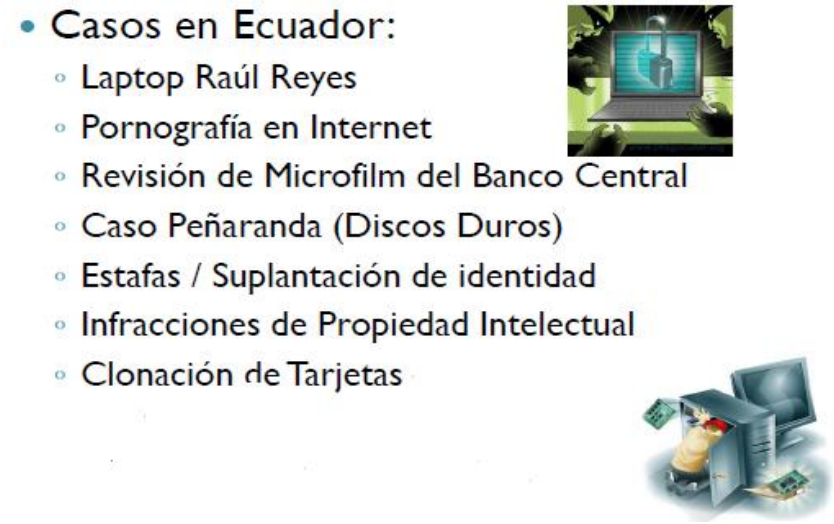
GRAFICO N° 4



FUENTE: Power Point

DISEÑADO POR: El Investigador

GRAFICO N° 5



FUENTE: Internet

DISEÑADO POR: El Investigador

GRAFICO N° 6

FUENTE: Internet

DISEÑADO POR: El Investigador

GRAFICO N° 7

FUENTE: Power Point

DISEÑADO POR: El Investigador

GRAFICO N° 8

Infracciones Informáticas (CPP)

INFRACCIONES INFORMATICAS	REPRESION	MULTAS
Delitos contra la información protegida (CPP Art. 202) 1. Violentando claves o sistemas 2. Seg. nacional o secretos comerciales o industriales 3. Divulgación o utilización fraudulenta 4. Divulgación o utilización fraudulenta por custodios 5. Obtención y uso no autorizados	 6 m. - 1 año 3 años 3 a 6 años 9 años 2 m. - 2 años	 $500 a $1000 $1.000 - $1500 $2.000 - $10.000 $2.000 - $10.000 $1.000 - $2.000
Destrucción maliciosa de documentos (CCP Art. 262)	6 años	---
Falsificación electrónica (CPP Art. 353)	6 años	---
Daños informáticos (CPP Art. 415) 1. Daño dolosamente 2. Serv. público o vinculado con la defensa nacional 3. No delito mayor	 6 m. - 3 años 5 años 8 m. - 4 años	 $60 – $150 $200 - $600 $200 - $600
Apropiación ilícita (CPP Art. 553) 1. Uso fraudulento 2. Uso de medios (claves, tarjetas magnéticas, etc.)	6 m. - 5 años 5 años	$500 - $1000 $1.000 - $2.000
Estafa (CPP Art. 563)	5 años	$500 - 1.000

FUENTE: Internet

DISEÑADO POR: El Investigador