UNIVERSIDAD CENTRAL DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

INSTITUTO DE POSTGRADO

MAESTRÍA EN CIENCIAS JUDICIALES

LOS DELITOS INFORMÁTICOS EN LA PROVINCIA DE IMBABURA

Trabajo de investigación para la obtención del grado de Magister en Ciencias Judiciales

AUTOR: *Dr. HUGO IMBAQUINGO N.*

TUTOR: Mgs**.** JUAN ALMENDÁRIZ

Ibarra, Abril, 2011

APROBACIÓN DEL TUTOR

En calidad de Tutor del trabajo de Grado, presentado por el Señor Dr. Hugo Salomón Imbaquingo Narváez, para optar por el grado de Magíster en Ciencias Jurídicas, doy fe de que dicho trabajo reúne los requisitos y méritos suficientes para ser sometido a presentación (pública o privada) y evaluación por parte del jurado examinador que se designe.

En la ciudad de Ibarra a los 29 días del mes de abril del 2011

_____

Mgs**.** Juan Almendáriz

CC. 1703386431

Los Delitos Informáticos en la Provincia de Imbabura

Por: *Dr. HUGO IMBAQUINGO N.*

Trabajo de Grado de Maestría aprobado en nombre de la Universidad Técnica del Norte, por el siguiente Jurado, a los 29 días del mes abril del 2011.

_____	_____
Dr. Edwin Altamirano	Dra. Yolanda Yupangui
CC:	CC:
_____	_____
DR. José García Falconi	Msc. Alberto Andrade
CC:	CC:

DEDICATORIA

Al personal docente, administrativo y sobre todo a los estudiantes de la gloriosa universidad Técnica del Norte que me incentivaron para ampliar mis conocimientos y aplicar el pensamiento del maestro Couture.

"El abogado que no estudia, será cada día menos abogado."

Dr. HUGO IMBAQUINGO N

RECONOCIMIENTO

A Dios por darme la sabiduría y la salud para la culminación de este trabajo a la Universidad Central del Ecuador y a la Universidad Técnica del Norte, por haber hecho posible que se capacite a los profesionales del derecho del Norte del país.

A mi esposa, a mis hijos que supieron impulsarme y darme ánimo en esta preparación académica.

Dr. HUGO IMBAQUINGO N

ÍNDICE GENERAL

CONTENIDOS **PAG**

LOS DELITOS INFORMÁTICOS EN LA PROVINCIA DE IMBABURA

Autor: Dr. Hugo Imbaquingo

Tutor: Mgs.Juan Almendáriz

Año: 2011

RESUMEN

El presente proyecto tiene como objetivo presentar una visión global del estado de los delitos informáticos en el Ecuador en cuanto a su tipificación, iniciativas de investigación, tecnología y formación de los especialistas que investigan dichas infracciones como también identificar los retos y brechas que deben ser superados por nuestro país para el tratamiento de los mismos. Se aborda el marco conceptual de los delitos y la criminalidad informática, así como también la normativa legal que se encuentra establecida en la legislación ecuatoriana. Asunto importante es conocer sobre los peritos que intervienen en la acción penal informática, el perfil requerido, los organismos de acreditación, requisitos para acreditarse y causales para la perdida de la acreditación. También se explican las iniciativas que convergen como propuestas iníciales y recomendaciones externas para el tratamiento y sanción de los delitos informáticos, igualmente, se da un enfoque general cómo están actuando países de Latinoamérica en el manejo de estos ilícitos relacionados con la informática. Se tratan los retos a nivel de formación, limitaciones tecnológicas, el marco legal vigente en el país para hacerle frente a estas conductas delictivas que hacen uso y abuso de las nuevas tecnologías.

LOS DELITOS INFORMÁTICOS EN LA PROVINCIA DE IMBABURA

Autor: Dr. Hugo Imbaquingo

Tutor: Mgs**.**Juan Almendáriz

Año: 2011

SUMARY

This project aims at presenting an overview of the state of cybercrime in Ecuador in their typing, research initiatives, technology and training of specialists who investigate such breaches as well as identify challenges and gaps that must be overcome for our country to treat them. Will address the conceptual framework of crime and computer crime, as well as legal regulations are established under Ecuadorian law. Will be important to know about the experts involved in the criminal information, The profile required, accreditation, accreditation requirements and grounds for the loss of accreditation. It also explains the initiatives that convert external initial proposals and recommendations for treatment and punishment of cybercrime, also will be given a general approach how Latin American countries are acting in the management of these crimes related to computer science. They were the challenges at the level of training, technological limitations, the legal framework in the country to deal with these criminal acts that use and abuse of new technologies.

INTRODUCCIÓN

Esta tesis sirve para identificar el marco legal sobre la conceptualización básica relativa a los delitos informáticos, clasificación de las infracciones informáticas, objetivos, importancia, principios, peritaje informático. Las normas legales que se aplican para la sanción de los delitos informáticos. En este trabajo investigativo se hace conocer la función específica de los peritos, técnicos que de acuerdo a la legislación ecuatoriana son los auxiliares de la justicia, pues son personas versadas en informática y en otras ramas que dan luces al juez, para el esclarecimiento de la verdad, para identificar, recoger, analizar, y reportar sobre la evidencia digital por parte del perito informático en el Ecuador para lo cual es necesario conocer los elementos, componentes, documentos, que forman parte de un proceso, en un hecho informático. Es de vital importancia transmitir las propuestas internas, Policía Judicial, Ministerio Público, Operadores de justicia, que permitan que los ilícitos informáticos, no queden en la impunidad. En cuanto a las iniciativas y propuestas externas como la OEA y otros organismos internacionales, es necesario que esta normativa se incorpore y se armonice a las legislaciones latinoamericanas, incluyendo al Ecuador, así como el resto del mundo, coordinar y aplicar sanciones a los ilícitos perpetrados por los delincuentes informáticos, que exista una regulación y tipificación de los hechos delictivos informáticos. En cuanto a la provincia de Imbabura, la sociedad, no se atreve a denunciar la serie de ilícitos informáticos que a diario se cometen, por lo que se hace necesario una difusión o socialización de los hechos delictivos de carácter informático que es víctima la población. Esta propuesta de tesis sirve para poder identificar un marco general sobre la conceptualización básica necesaria relativo a los delitos informáticos, tipos de delitos, sus objetivos, importancia, sus principios, la evidencia digital y la informática forense. En conjunto con las regulaciones existentes (leyes) para el manejo de los delitos informáticos, mediante la comprensión de los lineamientos establecidos en nuestra legislación y tener un claro entendimiento de los

criterios y medidas contempladas, haciendo imprescindible conocer cada uno de los requerimientos necesarios para el proceso de acreditación de los especialistas y los organismos que tienen la función de acreditación y renovación de credenciales para peritos informáticos y que estos puedan responder ante una designación de peritaje informático. Además, poder identificar las habilidades, preparación y pericia requerida para identificar, recoger, analizar, y reportar sobre evidencias digitales por parte del Perito Informático. Dar a conocer cuáles son los elementos, componentes, las diligencias y/o documentos (Obtención de Evidencia, Acta de Posesión de Perito, Informe de Pericia, etc.), habilitantes en el proceso de designación y realización de la Pericia Informática, así como también cuales son las implicaciones legales para el Perito informático ante un hecho jurídico informático. Conocer cuáles son las iniciativas internas (Policía Judicial, Ministerio Público) y externas (OEA.), que permitirán mejorar el manejo en la administración de justicia ante estas actividades ilícitas que se dan en nuestro medio, habilitando y definiendo aspectos legales que permitan la regulación y la tipificación de los delitos informáticos. También es importante identificar en forma general, cuáles son los aspectos contemplados en las leyes de los países a nivel latinoamericano que cuentan en su legislación con normas que regulan las infracciones informáticas. Identificar cuáles son los retos (legales, tecnológicos, etc.) que se presentan ante el manejo de un delito informático antes, durante y después de un proceso de pericia informática. Es primordial que se tenga claro que se requiere en la petición de la pericia, alcance de la misma, tipo, comprensión del informe, etc. Así como también establecer cuáles son las condiciones de los factores (educación, sistema legal, tecnología, entre otros) y que aspectos están siendo contemplados por dichos factores.

CAPITULO I

EL PROBLEMA

1.1. IDEAS INTRODUCTORIAS

Existe un alto Índice de Infracciones Informáticas en la Provincia de Imbabura.

El progreso tecnológico que ha experimentado la sociedad, supone una evolución en las formas de infringir la ley, dando lugar a la diversificación de delitos tradicionales como la aparición de nuevos actos ilícitos. El delito informático involucra acciones criminales que en primera instancia los países han tratado de insertar en figuras típicas, tales como: robo, fraudes, falsificaciones, estafa, sabotaje, entre otros; por ello, es primordial mencionar que el uso indebido de las computadoras es lo que ha creado la necesidad imperiosa de establecer regulaciones por parte de la legislación.

En nuestro medio, actualmente algunos profesionales del derecho están interesados en tener conocimiento de las normas penales que se dan en esta clase de procesos judiciales en la provincia.

1.2. ANTECEDENTES

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

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

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

1.3. SITUACIÓN ACTUAL

Hoy en día es común ver como la sociedad está siendo más dependiente de las computadoras como herramienta de trabajo en la más amplia diversidad de campos. Ya no es extraño ver que una gran parte de la población tiene acceso a este tipo de dispositivos informáticos, ni tampoco es el hecho de que puedan tener acceso a la red de redes, que es el Internet. También, muchas de las actividades que solían efectuarse manualmente, ahora pueden realizarse a través de medios informáticos, lo cual es una gran ventaja, pues se ahorra tiempo y dinero en la mayoría de los casos, pero así como se puede aprovechar la tecnología para actos lícitos, también sirve para cometer delitos. Por lo tanto, es común ver que se presentan una gran cantidad de infracciones en los que se ve involucrado algún sistema de cómputo ya sea como medio, o fin.

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

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

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

1.4. PROSPECTIVA

La presente investigación se realizó en la Provincia de Imbabura en los meses de Enero a Junio del 2010, donde se hizo un análisis de la situación actual de las infracciones informáticas.

El avance tecnológico y la necesidad de establecer mecanismos que permitan la persecución de actos ilícitos cometidos, utilizando medios tecnológicos los mismos que los profesionales en el área darán respuesta a la creciente necesidad de la sociedad de contar con asesores entendidos, y capaces de brindar sustento y respaldo legal a cada una de las actividades que se desarrollan con soporte de las tecnologías de la información. Brindar una visión global del estado de los delitos informáticos en el Ecuador en cuanto a su regulación, iniciativas de investigación, tecnología y formación de los especialistas que investigan dichos delitos, así como identificar los retos y brechas que debe ser superada por el Ecuador para el tratamiento y sanción de los mismos, es una opción que al presente y a futuro cobra sustancial importancia.

1.5. CAUSAS Y EFECTOS DEL PROBLEMA

CAUSAS	EFECTOS
• Falta de normas penales • Ambigüedad de la Ley Penal • Daños informáticos • Sabotaje informático • Pornografía infantil • Pesca de contraseña • Copias ilegales de software • Uso ilegitimo de sistemas informáticos	• Impunidad en la infracción • Incremento de delitos informáticos • Inestabilidad social. • Pérdida de confianza de la sociedad. • Inseguridad jurídica • Falta de protección al derecho de intimidad • Abusos en la manipulación de la información personal • Falta de control por parte de la autoridad pública

Tabla 1.1. Causas y Efectos del Problema
Fuente: Investigación directa

1.6. OBJETIVOS

1.6.1. Objetivo General.

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

1.6.2. Objetivos Específicos

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

2. Analizar la legislación ecuatoriana que enmarca los delitos informáticos desde un contexto nacional.

3. Realizar un diagnóstico de los Delitos Informáticos que se cometen en la Provincia de Imbabura.

4. Investigar el impacto de éstos ilícitos en la vida social y tecnológica de la sociedad.

5. Proponer reformas a la legislación penal ecuatoriana, para sancionar los delitos Informáticos, dependiendo del índice de infracciones cometidas, para conocer si existe o no vacíos jurídicos.

1.7. PREGUNTAS DIRECTRICES DE INVESTIGACIÓN

¿Cuáles son los tipos de delitos informáticos que se presenta en la Provincia de Imbabura?

¿Cuáles son los impactos que tiene el delito informático en la vida social y tecnológica de la sociedad?

¿La sociedad y los empresarios en materia del delito informático se encuentran desprotegidos debido a la ausencia de un marco jurídico adecuado?

¿Conoce la ciudadanía el procedimiento legal para denunciar a los delincuentes informáticos?

1.8. FACTIBILIDAD Y ORIGINALIDAD

1.8.1. Factibilidad

Debido a que en la actualidad la digitalización de la información se ha implementado en casi todos los países, tanto en la organización y administración de empresas públicas, como en la investigación científica, en la producción industrial, en el estudio e incluso en el ocio, el uso de la informática es, en ciertos ámbitos y contextos, indispensable. Sin embargo, junto a las incuestionables ventajas que presenta, comienzan a surgir algunas facetas negativas, como por ejemplo, lo que ya se conoce como criminalidad informática y sabotaje. Es factible realizar esta investigación debido a:

- Acceso a la información de la investigación.

- Contar con el Asesoramiento de Profesionales en Jurisprudencia e Ingenieros en Telemática quienes tienen conocimiento de este tipo de infracciones Informáticas.
- El financiamiento propio del estudiante maestrante.
- Tiempo estimado acorde a las normas de la Universidad Técnica del Norte.

1.9. JUSTIFICACIÓN

El uso fraudulento de las computadoras con el fin de obtener ganancias, la destrucción de programas, el acceso y el uso inadecuado de la información, repercute en la violación a la privacidad. La cuantía de los perjuicios así ocasionados no sólo es mayor que la obtenida por la delincuencia tradicional, sino que también es muy complicado llegar a descubrir a los autores intelectuales.

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

Por la falta de tipificación se tiene como consecuencia que las personas que cometen estos ilícitos, los delincuentes informáticos, quedan en total impunidad. De tal forma que los perjuicios que se ocasionan a las personas naturales, y a las personas jurídicas de derecho público y privado sea de gran magnitud en el Ecuador, por lo que la investigación determina cuáles delitos son sancionados en nuestra Legislación y que ilícitos deben agregarse a la misma. Necesidad manifestada por los requerimientos de los Tribunales de Justicia.

Así mismo, canalizar la búsqueda e incorporación de nuevas infracciones informáticas y en especial los que se dan en la Provincia de Imbabura, definir cuales se enmarcan en procesos judiciales actuales, cuales son los que penalizan en nuestra legislación Ecuatoriana y hechos delictivos que deberían agregarse en el futuro como infracciones penales constituye una exigencia del entorno jurídico, técnico y social de la actualidad.

CAPITULO II

MARCO TEÓRICO

2. Generalidades de los Delitos Informáticos

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

2.1 Los Delitos Informáticos

2.1.1 Antecedentes

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

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

Las víctimas del fraude informático son de preferencia del sector bancario y le siguen las grandes empresas. En piratería a los distribuidores, editores o autores del mismo.

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

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

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

2.1.2 Definición de los Delitos Informáticos

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

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

Se considera que no existe una definición formal y universal de delito informático pero se han formulado conceptos respondiendo a realidades nacionales concretas: “no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de “delitos” en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión “delitos informáticos” esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no han sido objeto de tipificación aún.

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

En 1992 la Asociación Internacional de Derecho Penal, durante el coloquio celebrado en Wurzburgo (Alemania), adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el Derecho Penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas como por ejemplo el “principio de Subsidiariedad”.

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

Finalmente la OCDE publicó un estudio sobre delitos informáticos y el análisis de la normativa jurídica en donde se reseñan las normas legislativas vigentes y se define Delito Informático como “cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos.”

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

A continuación se presenta un cuadro comparativo de las definiciones que se da al delito informático por parte de varios autores:

AUTOR	CONCEPTO
Davara Rodríguez	La realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software.
	Conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y

María de la Luz Lim	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
Carlos Sarzana	Cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo.
Jimena Leiva	Toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento automatizado de la misma
Julio Téllez Valdez	Las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin y las actitudes ilícitas en que se tienen a las computadoras como instrumento o fin.

Tabla 2.1. Conceptos de Delitos Informáticos.
Fuente: Investigación directa

Como ya se señaló anteriormente, determinados enfoques doctrinales subrayarán que el delito informático, más que una forma específica de delito, supone una pluralidad de modalidades delictivas vinculadas de algún modo con los computadores.

2.1.3 Propósitos de los delitos informáticos

Parker define a los delitos informáticos como “todo acto intencional asociado de una manera u otra a los computadores; en los cuales la víctima habría podido sufrir una pérdida. Parker establece una lista en la que se definen los delitos informáticos de acuerdo a los propósitos que se persiguen:

1. *Propósito de investigación de la seguridad:* abuso informático es cualquier acto intencional o malicioso que involucre a un computador como objeto, sujeto, instrumento o símbolo donde una víctima sufrió o podría haber sufrido una pérdida y el perpetrador obtuvo o pudo haber obtenido una ganancia.

2. *Propósito de investigación y acusación:* delito informático es cualquier acto ilegal cuya perpetración, investigación o acusación exige poseer conocimientos de tecnología informática.

3. *Propósito legal*: delito informático es cualquier acto tal como está especificado en una ley sobre delito informático en la jurisdicción en que la norma se aplica.

2.1.4 Delincuencia y criminalidad informática

Carlos Sarzana, describe en su obra “Criminalitá e Tecnología”, que los delitos por computadora comprenden “cualquier comportamiento criminógeno, en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como un simple símbolo”, entonces según esta descripción las personas que cometen delitos o crímenes informáticos, están enmarcadas dentro de lo que se conoce como criminología, y la investigación de dichos delitos, está sujeta a las ciencias de la criminalística.

Es preciso que se reconozca la diferencia entre la criminología y la criminalística; La criminología trata de investigar el por qué y qué fue lo que llevo al individuo a cometer el delito, mientras que la criminalística según Montiel Sosa, se definen como “una ciencia multidisciplinaria que reúne conocimientos generales, sistemáticamente ordenados, verificables y experimentables, a fin de estudiar explicar y predecir el cómo, dónde, cuándo, quién o quienes los cometen”, la criminalística al ser multidisciplinaria se aplica en temas de balística, medicina forense, física, química, e incluso la informática, entre otras, y se apoya de métodos y técnicas propias del trabajo de las diferentes disciplinas. Conocer el comportamiento de cómo los incidentes de seguridad, las vulnerabilidades y la criminalidad informática, es vital para el análisis de los delitos informáticos, ya que han tenido un crecimiento a lo largo de los últimos años, por ello, se requiere analizar la tendencia de dichos componentes.

El informe de Evolución de Incidentes de Seguridad que corresponde al año 2007, elaborado anualmente desde 1999 por Red IRIS, determina que el incremento de incidentes que ha habido entre el año 2006 y 2007 es el 63.32% en el que se involucran escaneo de puertos en busca de equipos vulnerables, vulnerabilidades de sistemas web, errores de programación, vulnerabilidades de navegadores más utilizados, ataques de phishing, máquinas zombis, malware y otro tipo de ataques para el cometimiento de fraudes u inhabilitación de servicios .Este mismo informe indica que el patrón de ataque continua siendo más dirigido, inteligente y silencioso con algún tipo de trasfondo que puede ser económico, religioso, político o de ansias de poder.

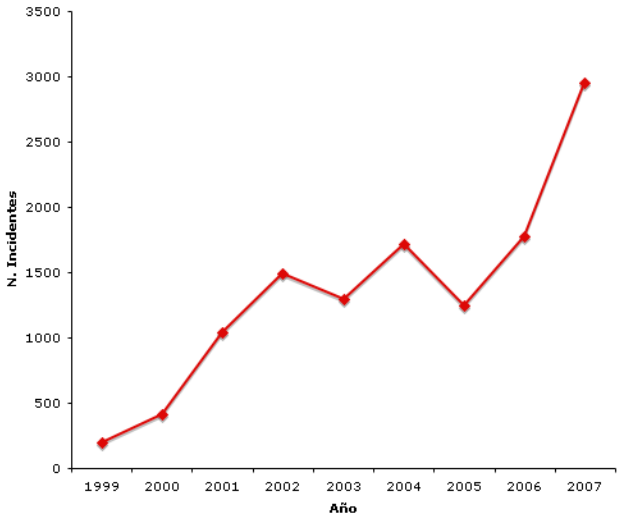


Figura. 2.1. Evolución de incidentes de seguridad
Fuente: REDIRIS – Informe de Evolución de Incidentes de Seguridad 2007

Otro organismo que realiza investigaciones de este nivel es el CERT, que publica una variedad de estadísticas relacionadas con las vulnerabilidades, que se han catalogado basados en informes de fuentes públicas y reportes que son directamente comunicados mediante sus sistemas web. Tal como se puede observar, se concluye que la tendencia sobre las vulnerabilidades tiene un crecimiento significativo a lo largo de los años que se han analizado

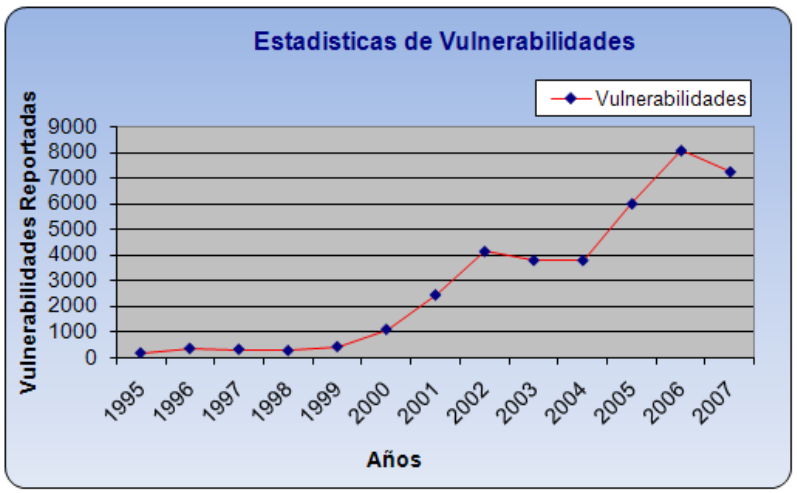


Figura. 2.2. Estadísticas de Vulnerabilidades

Fuente: CERT – Informe de vulnerabilidades reportadas 2007

Otra empresa como Computer Security Institute (CSI) en conjunto con la Oficina Federal de Investigaciones (FBI), realiza la encuesta anual de Crimen y Seguridad Computarizada, sobre los eventos potencialmente serios y costosos que se han desarrollado durante el año de la encuesta. En la encuesta se toma información que ha sido prevista por empresas de diferentes sectores como el financiero, legal, educativo, servicios de salud, transporte, manufactura, tecnologías de información, entre otros, en los que se analiza en términos de frecuencia, naturaleza y costo que han tenido dichos eventos. El perfil de las personas encuestadas es de CIOs (ChiefInformationOfficer), CEOs (ChiefExecutiveOfficer), CISOs (ChiefInformation Security Officer), Oficiales de Seguridad y Administradores de Sistemas.

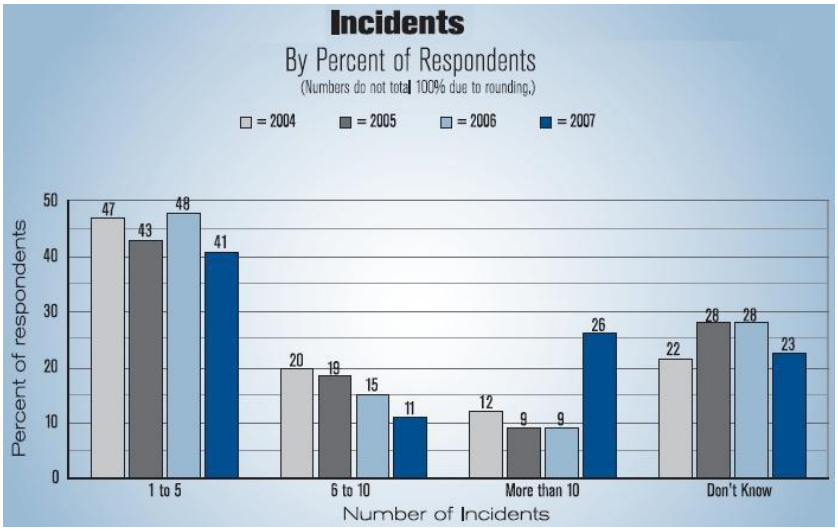


Figura. 2.3. Incidentes ocurridos en el 2007
Fuente: CSI 2007 – Computer Crime and Security Survey

En la Figura 2.3 de las estadísticas de los incidentes ocurridos durante el año 2007, comparando con respecto a años anteriores por números de incidentes, se denota un

índice creciente del más del 100%, en el grupo de incidentes reportados dentro del rango de los encuestados que han sufrido más de 10 ataques.

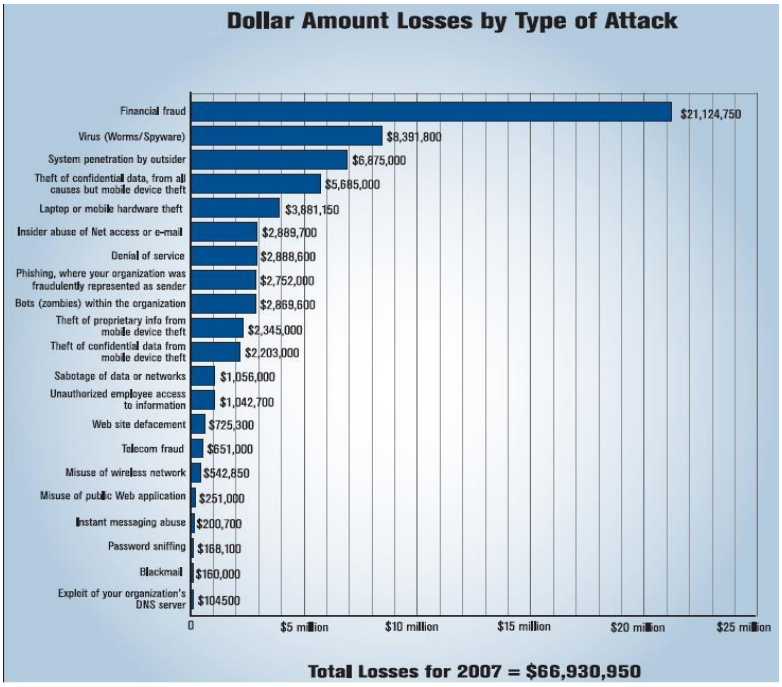


Figura. 2.4. Costos de incidentes por tipo de ataque
Fuente: CSI 2007 – Computer Crime and Security Survey

La totalidad en millones de dólares en pérdidas por tipos de ataques fue de $66,930,950 (194 encuestados) tuvo un incremento del 21 % frente al 2006, en donde se registro una pérdida de $52,494,290.00 (313 encuestados), lo que denota un crecimiento significativo para las empresas.

La criminalidad informática organizada ha crecido de manera exponencial, de acuerdo con los informes relacionados con incidentes de seguridad, vulnerabilidades reportadas y los altos costos que estos involucran para la empresa, los mismos, que son aprovechadas por los intrusos. Cabe recalcar que dichos intrusos conocen cada vez con más profundidad los detalles de las tecnologías y sus limitaciones, por ello, es cada vez más fácil desaparecer la evidencia y confundir a los investigadores, por lo cual,

constituye un reto para los sectores afectados, los legisladores, judiciales, policiales e incluso los especialistas informáticos encargados de su investigación.

2.1.5 Tipos y Clasificación de Delitos Informáticos.

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

- ✓ Las amenazas.
- ✓ Los delitos de exhibicionismo y provocación sexual.
- ✓ Los delitos relativos a la prostitución y corrupción de menores.
- ✓ Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad de domicilio: Delitos contra el honor: Calumnias e injurias, haciéndose especial mención cuando estas se realizaren con publicidad - se propaguen.
- ✓ Las estafas.
- ✓ Las defraudaciones de las redes de comunicación. Incluye de forma expresa la defraudación en telecomunicaciones siempre y cuando se utilice un mecanismo para la realización de la misma, o

alterando maliciosamente las indicaciones o empleando medios clandestinos.

- ✓ Los delitos relativos a la propiedad intelectual, cómo proteger las creaciones y proyectos que se desarrollan en la empresa.

Tipificación de delitos informáticos

Tomando como referencia la clasificación o tipificación de los delitos informáticos, éstos se clasifican de la siguiente manera:

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

- **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.

Muchos autores y organismos han clasificados de diferentes maneras los tipos de delitos informáticos según diferentes criterios, coincidiendo entre los principales los siguientes:

<table>
<tr><td>Fraudes mediante la manipulación de computadoras (programas,</td><td rowspan="2">Fraudes mediante la manipulación de computadoras:
1 Delitos contra elementos físicos-hardware (ROBO, ESTAFA)
2 Delitos contra elementos lógicos (daños, accesos ilícitos a sistemas</td></tr>
<tr><td>Falsificaciones informáticas (alteración de documentos, falsificación de documentos)</td></tr>
<tr><td>Daños o modificaciones de programas o datos computarizados (sabotaje, virus, bombas lógicas)</td><td rowspan="2">Delitos cometidos a través de sistemas informáticos:
a) Estafas
b) Apoderamiento de dinero por tarjetas de cajero
c) Uso de correo electrónico con finalidad criminal
d) Utilización de internet como medio criminal.</td></tr>
<tr><td>Accesos no autorizados a servicios y sistemas informáticos (piratas, reproducción no autorizada)</td></tr>
<tr><td>RECONOCIDOS POR LAS NACIONES UNIDAS: FUENTE ONU</td><td>ABOGADOS ESPECIALIZADOS EN DELITOS INFORMÁTICOS</td></tr>
</table>

Tabla 2.2. Delitos Informáticos comparados entre las Naciones Unidas y Abogados Especializados

Fuente: Investigación Directa

1. Fraudes:- Delitos de estafa a través de la maniobra de datos o programas para la obtención de un lucro ilícito (caballos de troya, falsificaciones, etc.).

2. Sabotaje informático:- Daños mediante la destrucción o modificación de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos (bombas lógicas, virus informáticos, malware, ataques de negación de servicio, etc.).
3. Espionaje informático:- Divulgación no autorizada de datos reservados
4. Pornografía Infantil:- Inducción, promoción, producción, venta, distribución facilitamiento de prostitución, cuando se utilizan menores con fines de exhibicionistas o pornográficos.
5. Infracciones de Propiedad Intelectual:- Copia o reproducción no autorizada de programas informáticos de protección legal.

REPORTE NACIONAL DE LOS DELITOS INFORMATICOS DE ENERO A NOVIEMBRE DEL 2010										
DELITO	NOTICIA DEL DELITO	INDAGACIÓN PREVIA	INSTRUCCIONES	DICTÁMENES			SENTENCIAS			DESESTIMACIONES
				ACUSATORIOS	ABSTENTIVOS	MIXTOS	CONDENATORIAS	ABSOLUTORIAS	MIXTAS	
APROPIACIÓN ILÍCITA UTILIZANDO MEDIOS INFORMÁTICOS	903	881	31	29	3		4	2	1	146
FALSIFICACIÓN ELECTRÓNICA	**60**	**50**	**4**	**1**		**1**				**10**
DANOS INFORMÁTICOS DE SERVICIO PUBLICO	**87**	**89**	**2**		**1**					**2**
DANOS INFORMÁTICOS DE SERVICIO PRIVADO	82	81								4
ESTAFA UTILIZANDO MEDIOS INFORMÁTICO	1									
TOTAL NACIONAL	**1133**	**1101**	**37**	**30**	**4**	**1**	**4**	**2**	**1**	**162**

Tabla 2.3. Reporte Nacional de los Delitos Informáticos de Enero a Noviembre del 2010

Fuente: Sistema Integrado Nacional de Actuaciones y Estadísticas Procesales (SINAEP)

2.1.6 La investigación tecnológica de los delitos informáticos

Los elementos de prueba dentro de un proceso son de vital importancia, ya que mediante su investigación se llega a determinar la confirmación o negación de lo que corresponde a la verdad. Es trascendental tener en consideración la formalidad y claridad de los procedimientos o técnicas de análisis utilizados en un proceso de investigación, para brindar mayor claridad y precisión a las observaciones dentro del proceso, ante un hecho delictivo informático.

Teniendo presente esa situación, se considera que es indispensable resaltar que las respuestas nacionales serán insuficientes frente a la dimensión internacional que caracteriza este problema. 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.

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 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.

2.1.7. Informática Forense

El FBI conceptualiza la informática forense “como la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y almacenados en un medio computacional”. Este mismo organismo ha desarrollado programas que permiten examinar evidencia computacional.

Esta ciencia relativamente nueva se aplica tanto para las investigaciones de delitos tradicionales tales como: fraudes financieros, narcotráfico, terrorismo, etc.; como para aquellos que están estrechamente relacionados con las tecnologías de la información y las comunicaciones, entre los que se refieren a la piratería del software, distribución pornográfica infantil, tráfico de bases de datos, etc.

El análisis forense digital, según Miguel López Delgado, en un sentido formal es definido como “el conjunto de principios y técnicas que comprende el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias digitales y que en determinados casos pueden ser aceptadas legalmente en un proceso judicial”. Para ello se establecen los pasos para realizar el descubrimiento de un acto delictivo informático y así tenemos:

2.1.7.1 Pasos para realizar una Investigación Forense

Identificación de incidentes

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

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

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

Recopilación de evidencias digitales

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

1. Generalmente la primera reacción suele ser, restablecer el sistema a su estado normal, pero se debe considerar que este paso podría resultar en que se pierdan casi todas las evidencias que aún se encuentren en la “escena del delito” e incluso puede resultar en el impedimento de llevar a cabo las acciones legales pertinentes.
2. En el caso de que se elija la segunda alternativa y el profesional se encuentra capacitado para realizarlo, se debe iniciar con el proceso de recopilar las evidencias que permitan determinar los métodos de entrada, actividades de los intrusos, identidad y origen, duración del evento o

incidente, siempre precautelando evitar alterar las evidencias durante el proceso de recolección.

Preservación de la evidencia digital

En el caso de que se inicie un proceso judicial contra los atacantes del sistema, será necesario documentar en forma precisa y clara como se ha preservado la evidencia tras su recopilación a lo largo de todo el proceso de las fases anteriores, por ello, es indispensable establecer los métodos adecuados para el almacenamiento y etiquetado de evidencias. Se recomienda la obtención de copias exactas de la evidencia obtenida utilizando mecanismos de comprobación de integridad de cada copia, las cuales deben ser documentadas y agregadas en el etiquetamiento realizado.

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

Análisis de la evidencia

Luego de que ya se han realizado los procesos de identificación, recopilación y preservación de las evidencias digitales, el siguiente paso es el análisis forense de dichas evidencias cuyo objetivo primordial es la de reconstruir con todos los datos disponibles, la línea de tiempo en que se realizó el ataque, determinando la cadena de acontecimientos desde el instante anterior al inicio del ataque, hasta su descubrimiento.

Documentación y presentación de los resultados

Durante esta última fase, el investigador o especialista debe asegurarse que cada una de las fases anteriores haya sido debidamente documentadas, esto además de permitir gestionar el incidente permite llevar un control de los procedimientos efectuados desde el descubrimiento hasta la finalización del proceso de análisis forense. Es recomendable, considerar básicamente los siguientes formularios.

1) Formulario de identificación de equipos y componentes.

2) Formulario de obtención o recolección de evidencias.

3) Formulario para el control de custodia de evidencias.

4) Formulario de incidencias tipificadas.

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

Cabe destacar en este punto y de acuerdo a lo establecido en el Art. 98 del Código de Procedimiento Penal ecuatoriano, el informe pericial debe contener lo siguiente.

1) La descripción detallada de lo que se ha reconocido o examinado, tal cual lo observo el perito en el momento de practicar el reconocimiento o examen.
2) El estado de la persona o de la cosa objeto de la pericia, antes de la comisión del delito, en cuanto fuere posible.
3) La determinación del tiempo probable transcurrido entre el momento en que se cometió la infracción y el de la práctica del reconocimiento.
4) El pronóstico sobre la evolución del daño, según la naturaleza de la pericia.

5) Las conclusiones finales, el procedimiento utilizado para llegar a ellas y los motivos en que se fundamentan.
6) La fecha del informe; y,
7) La firma y rubrica del perito.

Dicho artículo también contempla, que en el caso de que hubiesen desaparecido los vestigios de la infracción, los peritos opinarán, en forma debidamente motivada sobre si tal desaparición ha ocurrido por causas naturales o artificiales. Esta opinión deberá sujetarse a los principios del debido proceso y la presunción de inocencia. El procesado tiene derecho a conocer oportunamente el informe pericial, a formular observaciones y a solicitar aclaraciones al perito, sin perjuicio de su derecho a interrogarle en la audiencia.

2.1.8 Formas de Control Preventivo y Correctivo.

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.

También se ha producido una expansión rápida de tales actividades en esferas como la trata de personas, el tráfico ilícito de armas de fuego, vehículos robados, recursos naturales, objetos culturales, sustancias que agotan la capa de ozono, desechos peligrosos, especies amenazadas de fauna y flora silvestres e incluso órganos humanos, así como el secuestro para la obtención de un rescate.

Los adelantos en la tecnología de las comunicaciones han determinado que surjan nuevas oportunidades para la

comisión de delitos sumamente complejos, en particular un aumento significativo del fraude en el Internet. Las autoridades encargadas de hacer cumplir la ley suelen adaptarse con lentitud a las nuevas tendencias delictivas.

2.2. Legislación Ecuatoriana

La acción Constitucional de Habeas Data - 2008

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

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

interponer el habeas data y la legitimación activa que puede ser cualquier persona natural o jurídica que puede interponer esta acción constitucional.

La denominación ***Hábeas Data*** tiene sus antecedentes en la antiquísima garantía del hábeas corpus. Así, constituye la fusión de una palabra latina ***"hábeas"*** que proviene del latín habere que significa ***"téngase en posesión",*** junto con la palabra inglesa ***"data"*** que proviene de datum que significa ***dato***, información.

Por lo tanto, la frase Hábeas Data significa, literalmente, ***"traer los datos"***, es decir, traer los datos personales del actor, a fin de que éste pueda conocerlos y resolver lo pertinente acerca de ellos.

Finalidad

La finalidad del Hábeas Data es proteger a la persona de los abusos que pueda sufrir respecto del llamado *poder informático*. Se entiende por tal, la producción, almacenamiento y transferencia de información personal que pueden realizar instituciones públicas y privadas, empresas y personas en general, en base a los avances tecnológicos que hoy existen.

Tal información personal, a más de ser incorrecta o desactualizada, puede abarcar situaciones pasadas ya superadas, así como también ser de carácter *sensible*, esto es, referirse a las convicciones políticas o religiosas de la persona, a su comportamiento sexual, a su estado de salud, etc., información ésta que al ser realmente íntima no debería ser de conocimiento y manejo público, salvo que su mismo titular así lo acepte expresamente.

El riesgo que tiene la persona ante el poder informático de las instituciones es mayúsculo, no sólo por la facilidad que tienen para almacenar u obtener información, sino por la rapidez con que ella puede ser transferida a cualquier parte no solo del país sino del mundo.

Junto con lo anterior, y sin perjuicio del peligro que significa el registro de información falsa o errónea acerca de la persona, la simple manipulación de la información personal es en sí ya un grave riesgo para todos.

El poder informático es grande, tanto en el proceso de acopio como de difusión de la información que posea; ese acopio y recolección de datos puede ser realizado de manera superficial e irresponsable, sin la debida investigación y revisión; así mismo, esa difusión puede ser realizada de manera inadecuada, desmedida o fuera de contexto.

Naturaleza Jurídica

La figura del Hábeas Data es, de conformidad con la normativa constitucional y legal aplicable a la fecha en el Ecuador, una acción de garantía, de rango constitucional, la misma que protege determinados derechos constitucionales. Su naturaleza jurídica es la de ser una ***acción***, la cual genera el nacimiento de un proceso constitucional, el mismo que terminará mediante una resolución, la cual, bajo determinadas condiciones, puede ser objeto de ciertos recursos, entre ellos, el de apelación ante el superior jerárquico.

No es un recurso, como erróneamente se la ha calificado; es una acción, con un espectro de acción concreto, pues, a diferencia del amparo constitucional, el Hábeas Data protege puntuales derechos constitucionales.

Características

Es una ***ACCIÓN,*** esto es, una de las diversas manifestaciones del derecho de petición consagrado constitucionalmente y requerido para la operatividad de las garantías jurisdiccionales.

De ***GARANTÍA,*** pues los derechos no se protegen por sí solos, siendo su mecanismo de protección y de restablecimiento las garantías, pero fundamentalmente aquellas de carácter jurisdiccional, es decir, concretos mecanismos procesales que se plantean, tramitan y resuelven por parte de un juez competente y con el poder suficiente para hacer cumplir sus resoluciones.

De ***CARÁCTER AUTÓNOMA,*** pues constituye una garantía constitucional con perfil propio, regulada específicamente tanto en la Constitución como en la Ley de Garantías Jurisdiccionales y de Control Constitucional, y dotada de un procedimiento particular.

De ***RANGO CONSTITUCIONAL*** al igual que el Amparo Constitucional y el Hábeas Corpus. Que genera el nacimiento de un ***PROCESO DE CONTROL CONSTITUCIONAL.***

Proceso ***REGLADO Y NORMADO*** específicamente, tanto por la Constitución de la República y por la Ley de Garantías de Garantías Jurisdiccionales y de Control Constitucional.

Proceso de carácter ***ABREVIADO, SIMPLIFICADO*** lo cual junto con la rapidez constituyen las principales características de todo proceso de control constitucional; sin perjuicio de lo anterior, hay que aclarar que las características previamente citadas no anulan la necesaria bilateralidad, el derecho a la contradicción y, en general, el respeto al debido proceso, pues todas estas condiciones de validez se deberán cumplir, sin perjuicio de la brevedad de los plazos y el acortamiento de las diligencias, las

cuales se dan para facilitar la esencia y objetivo de una garantía constitucional, esto es, el proteger eficaz y rápidamente los derechos constitucionales conculcados de las personas.

Que funciona a ***PETICIÓN DE PARTE INTERESADA,*** pues no puede el Juez Constitucional de oficio actuar en esta clase de conflictos.

Ante la ***VULNERACIÓN EFECTIVA o AMENAZA CERTERA*** de la violación de un derecho constitucional protegido por la garantía. Recordemos que el Hábeas Data como el amparo constitucional pueden plantearse antes de que ocurra el acto ilegítimo o ya habiendo ocurrido el mismo, a fin de que en cualquiera de los dos casos, el Juez mediante un control preventivo (ante una amenaza cierta) o con un control represivo (tras la realización efectiva del acto) proceda a evitarlo, a rectificarlo o a cesarlo, etc.
De una ***ACCIÓN u OMISIÓN.***

La cual debe ser ***ILEGÍTIMA.***

Ejecutada por parte de una ***AUTORIDAD PÚBLICA*** o por un ***PARTICULAR.***
Que vulnera ***DERECHOS ESPECÍFICOS*** como son: el derecho al honor, a la buena reputación, a la buena imagen, a la intimidad o, como dicen los autores alemanes, el derecho a la autodeterminación informativa

Derechos Protegidos

Tradicionalmente se afirma que el Hábeas Data protege el derecho a la intimidad, el cual, como sabemos, no sólo es personal sino hasta familiar. Pero, además de la intimidad, también pueden ser afectados, mediante informaciones incorrectas: el honor, la buena reputación y la imagen de las personas.

Hay que aclarar que derechos como el respeto al honor, a la buena reputación y a la buena imagen1, no necesariamente son conexos o vinculados con el derecho a la intimidad personal; es decir, se puede afectar al honor, sin que necesariamente la materia de la ofensa se refiera a la intimidad de la persona.

Así, si se divulga que una persona estuvo presa, se afecta su buena reputación y la imagen pública que se tiene, pero de ninguna manera se viola su intimidad; pero, en cambio, si se divulga que cierta persona es homosexual, se afecta su intimidad personal y la buena reputación e imagen personal que, lamentablemente, una sociedad machista como la nuestra exige.

Relación con el Amparo Constitucional

Para muchos, y en especial para la doctrina argentina, el Hábeas Data no es más que un amparo especializado o una modalidad de aquel referente a los datos personales.

La vinculación se da en aquel país, más por el hecho de que el Hábeas Data consta regulado en el mismo artículo que trata acerca del amparo constitucional, que por la circunstancia de ser un procedimiento de garantía cuya esencia es la misma que la del amparo, esto es, el proporcionar algo, dejar sin efecto una situación ilegítima, etc.

Diferencias con el Recurso de Acceso a la Información Pública

Más allá de que el Hábeas Data sea una garantía de rango constitucional, a diferencia del recurso de acceso a la información pública que sólo tiene un rango legal y que los plazos son diferentes en ambos procedimientos, las diferencias fundamentales entre dichas instituciones radican en lo siguiente:

4 La **materia** de la información que se persigue o busca obtener.
5 La **relación entre el actor y la información** que se solicita.
6 La **finalidad** perseguida.
7 Las **pretensiones posteriores al acceso** que se podrían esgrimir.
8 El **requerimiento previo exigido** como condición de procesabilidad.

Así, respecto de la materia, el Hábeas Data siempre buscará el acceso a la información privada o propia del accionante; mientras que el recurso de acceso a la información pública pretenderá aquella información que es de todos los ciudadanos y que se almacena, principalmente, en las instituciones públicas.

Nociones del Hábeas Data en El Ecuador

Consecuencia de lo anterior es que en el Hábeas Data hay una relación directa entre el actor y la información que se requiere; mientras que en el recurso de acceso a la información pública aquella relación no es directa o propia, ya que no es una información personal la que se busca, sino del Estado, del Municipio al que uno pertenece.

Sobre la finalidad perseguida, el recurso de acceso a la información pública pretende ejercitar una suerte de fiscalización a la actuación pública, logrando conocer en forma clara y transparente la gestión de las instituciones y sus autoridades, las cuales están sometidas al principio de publicidad y transparencia. En cambio, el Hábeas Data no pretende fiscalizar dicha gestión pública, sino controlar que los datos personales que se tengan registrados respecto del proponente de la demanda sean correctos, actualizados y no le causen discriminación alguna.

Así mismo, en el Hábeas Data, tras la recepción de la información solicitada, el actor puede solicitar la actualización, la rectificación, la anulación y hasta la reserva de la información personal; mientras que en el recurso de acceso a la información pública aquellas pretensiones no pueden ser esgrimidas, puesto que el recurso se limita y agota simplemente con la entrega de la información pública al peticionario de la misma.

Legitimados Activos

Son todas aquellas personas cuya información personal consta en los registros o bases de datos. Dicha persona puede ser una persona natural o jurídica, debiendo existir una vinculación directa entre quién solicita la información -el actor- y el dato o información que se busca obtener, puesto que sólo se puede requerir información, como ha quedado dicho, personal o propia del actor o máximo aquella que sea de carácter familiar.

La información que se requiere debe pertenecer a una persona determinada o a lo sumo determinable. Determinada cuando se especifica que se requiere, por ejemplo, de Carlos Salmon Alvear; son personas determinables, en cambio, aquellas que no siendo identificadas por su nombre, lo son por otros datos que permiten su identificación, como por su número de cédula de identidad, su dirección domiciliaria, su número patronal ante el IESS, su número de registro único de contribuyente, etc.

Los Registros

Conocidos también como: base de datos o almacenadores de información, el registro es toda aquella institución pública o privada que posea o almacene, en la forma que fuere, información personal de terceros. Como ha quedado dicho, el registro almacena

información personal de terceros, sin que interese el medio, formato, canal o mecanismo que utilice; así, dicho registro puede ser llevado de manera manual, por escrito, en forma sonora, visual, electromagnética, gráfica, magnetofónica, a través de archivos informáticos, etc. Tal registro puede ser la persona o institución que produzca la información que posee; así mismo, puede ser la persona o institución que, recibiendo la información de otra institución, sea quien la comercializa o distribuya.

No interesa para nuestras consideraciones, si el registro tiene o no finalidades comerciales, esto es, si vende o entrega gratuitamente al público la información que posee en sus archivos.

Información Sensible

Entiéndase por *información sensible* aquella que se refiere a los antecedentes penales o judiciales que, en general, posea la persona; a los rasgos personales o sicológicos que tenga; a su situación económica, sin que interese si ésta es buena o mala; al estado de salud, padecimiento de alguna enfermedad física o psíquica, sin que importe si la misma es o no mortal o degenerativa; así mismo, se refiere a sus convicciones políticas, ideológicas, religiosas, preferencias sexuales o gustos y hábitos y demás circunstancias de su vida privada.

Pretensiones

En el proceso de Hábeas Data se pueden plantear diversas pretensiones, así tenemos:

Pretensión de Acceso

La pretensión básica o esencial del Hábeas Data es la de solicitar información **PERSONAL** y de recibirla dentro de un plazo

razonable. Esto es lo que configura el llamado DERECHO AL **ACCESO**, es decir, el derecho a acceder o conocer la información personal que el registro pueda tener respecto del demandante.

Recordemos: se accede efectivamente, cuando se recibe clara, total y oportunamente toda aquella información o dato que se busca.

Este derecho a acceder a la información personal no puede ser limitado; a lo sumo, puede ser regulado en cuanto a simples y elementales formalidades que no constituyan limitaciones que coarten el ejercicio de tal derecho.

Pretensión de Rectificación

Así mismo, mediante la acción de Hábeas Data se puede solicitar la **rectificación** de aquella información que resulte ser incorrecta.

Pretensión de Actualización

Por otro lado, tratándose de información antigua y desactualizada, a través de la acción de Hábeas Data se puede solicitar su pertinente **actualización**.

Pretensión de Reserva

En cuanto a la información que, por mandato de ley, debe constar en los registros pero que por su contenido o materia no debe ser suministrada a terceros, sino sólo a su titular y, eventualmente, a jueces, fiscales y autoridades debidamente legitimadas y solamente -resaltamos-, en los casos expresamente permitidos por la ley, se puede requerir mediante esta acción de garantía su **reserva o confidencialidad**. Insistimos, en cuanto a la reserva o la confidencialidad de la información personal, que por su materia

resulta ser especialísima y delicada como por ejemplo: las referencias financieras de una persona, dicha información solo podrá ser entregada a un Juez, Fiscal o Comisión investigadora de la Asamblea Nacional, etc.,

Pretensión de Anulación

Respecto de toda aquella información que su registro no es dispuesto por la ley, o bien cuando el contenido o materia de la información no concuerda con la finalidad perseguida por el registro para almacenarla, o bien cuando se tiene informaciones inexactas, violatorias de los derechos constitucionales de las personas o que se refieren a datos sensibles del sujeto, la pretensión sería la **anulación, exclusión o supresión** de dicha información.

Pretensión de Agregación

Otra pretensión aplicable en el hábeas data es la "de **agregar** datos al registro que se tenga, ya sea por la necesidad de que se actualicen los que se encuentran registrados, o bien con el fin de que se incluyan aquellos no registrados, pero que son necesarios para que se tenga una cabal referencia sobre la imagen e identidad de la persona afectada".

Otras pretensiones válidas

Creemos que, a través del Hábeas Data, se pueden plantear otras pretensiones válidas, sin perjuicio de que las mismas no consten expresamente en los textos constitucional y legal pertinentes.

Así, por ejemplo, la Corte Constitucional colombiana, en su sentencia de unificación de jurisprudencia identificada como la No.-SU-082/95 de fecha 01 de marzo de 1995, reconocía al Hábeas Data "como un derecho fundamental, en cuya virtud toda persona a

la cual se refieren los datos de un archivo público o privado tiene la facultad de autorizar su CONSERVACIÓN, rectificación, uso y circulación".

El Derecho al Olvido

Cuando se habla de la posibilidad de que, por intermedio del Hábeas Data, se suprima o anule información de la persona, en ciertos casos, tal información puede ser cierta, pero ya superada; tal es el caso de aquellas personas que, por ejemplo, han sido condenadas por un delito y han cumplido la pena respectiva. Ante tal situación, se sustenta la postura de que, como la persona cumplió su falta para con la sociedad, el registro de aquella información pasada ya no procedería, y de mantenerse en los archivos respectivos, su conocimiento público ocasionaría discriminaciones de todo tipo.

Etapas del Proceso

Los estudiosos del Derecho Procesal Constitucional, al estudiar el Hábeas Data, reconocen que dicho proceso tiene dos etapas claramente diferenciadas; la primera de ellas, constituye el acceso a la información personal que solicita el actor, esto es, el dueño o titular de la información requerida. El acceso involucra la entrega efectiva de la información solicitada, entrega que debiendo ser oportuna, debe ser respecto de una información y datos claros, completos y fidedignos. Obtenida dicha información y analizada ésta por el actor, procedería una segunda etapa que es la rectificación, anulación, actualización, reserva o agregación de los datos que resulten ser incorrectos, sensibles, desactualizados, privados o incompletos del actor, según la información entregada por el registro demandado.

Requerimiento Previo

A diferencia de lo previsto en otros países como el Perú, tratándose del Hábeas Data, en el Ecuador, la Constitución Política de 1998 y la Ley del Control Constitucional no han dispuesto ni exigido requerimiento previo alguno que deba formular el actor ante el registro que mantiene su información personal. Resaltamos: nuestra vigente normativa constitucional no ha previsto, como paso previo o requisito de procesabilidad para presentar la demanda de Hábeas Data, la necesidad de articular un requerimiento previo al registro que tiene la información personal del actor para que, cumplida la petición y vencido un plazo prudencial, de no haber respuesta por parte del registro o de ser la misma incompleta u oscura, recién allí, cumplido dicho paso previo, repetimos, se pueda plantear procedentemente una demanda de Hábeas Data. Esto en el Ecuador, no se aplica.

Justificación de la Petición

Ni la demanda de acceso a la información pública ni, peor aún, la acción de Hábeas Data requiere justificación que motive el por qué de su requerimiento o petición de acceso al registro que la almacena. Por otro lado, respetuosamente, criticamos lo resuelto por el Tribunal venezolano el 14 de marzo del 2001, en el Caso Insaca, cuando dispuso que, para la procedencia de la demanda de Hábeas Data, es necesario que “se demuestre la existencia del registro y la presunción sobre el asiento en él, de informaciones y datos del accionante o de sus bienes”.

Información Requerida

El actor en la demanda de Hábeas Data persigue - inicialmente- del registro el ACCESO de la INFORMACIÓN PERSONAL, esto es, el

conocer qué tiene el registro recopilado sobre él, su familia o sus bienes. Por lo tanto, no se necesita, ***como condición de procedencia de la demanda,*** el determinar la clase de información solicitada, peor aún especificarla. Claro está que, dependiendo del caso particular de que se trate, la especificación de lo que se pretende simplificará la labor de búsqueda y respuesta por parte del registro.

Juez Competente

El Juez competente en materia de Hábeas Data, de conformidad con lo prescrito en la vigente Ley del Control Constitucional, es el Juez de Primera Instancia del domicilio del registro o poseedor de la información personal requerida.

Nótese que, tratándose de la jurisdicción territorial, nuestra normativa sólo ha previsto que el Juez competente sea el de la jurisdicción territorial en donde funcione el registro o exista la base de datos; no procede, por lo tanto, demandas de Hábeas Data que hayan sido planteadas ante el domicilio del actor si es que aquel no coincide con el domicilio del titular del registro poseedor de la información personal requerida.

Excepciones y Oposición

Partamos con establecer que, en todo proceso, incluidos los de garantía constitucional, se pueden esgrimir válidamente excepciones que, de fondo o de forma, rechacen la demanda planteada. Así mismo, todo proceso constitucional, incluido el de Hábeas Data, garantiza el derecho a la contradicción, exteriorizando de esa manera la bilateralidad, es decir, la posibilidad de que frente a los argumentos del actor, el juez pueda y deba oír los del demandado, a fin de adoptar la resolución más justa y procedente en derecho.

Supuestos de Inadmisibilidad de la Acción

Será inadmitida, es decir, rechazada de plano y sin trámite alguno, la demanda de Hábeas Data en los siguientes casos, a saber:

1. Aquella que fuere planteada ante juez incompetente, sea que lo fuere por motivo de su rango o instancia o por razón del territorio;
2. Aquella en que no se alegue derecho de rango constitucional violado o, en su defecto, que se mencione un derecho constitucional diferente a aquellos que son protegidos por el Hábeas Data;
3. Aquella que no pretenda el acceso a información o datos;
4. En el caso de que la información pretendida no sea personal o propia del actor;
5. Por último, aquella que esgrima pretensiones improcedentes mediante esta vía como el resarcimiento de daños y perjuicios.

Prueba

Es obligación del actor justificar la falta de veracidad, de actualidad o de corrección de la información contenida en el registro, a fin de que el juez pueda disponer con suficientes elementos de juicio la rectificación, actualización o supresión que corresponda. Por lo tanto, si alegamos que somos casados o divorciados, deberemos adjuntar copia certificada de la partida con la razón respectiva; si decimos, por otra parte, que tenemos determinada profesión, se deberá adjuntar copia del título, etc.

Procedencia de la Demanda

La condición esencial para que se resuelva en forma favorable una demanda de Hábeas Data es que el registro posea la información

personal que es requerida. De existir la información y de ser ésta correcta y actualizada corresponde, en segundo lugar, cuestionarnos sobre el uso y la finalidad que tenga ese registro respecto de la recopilación de información personal que posea. No será legítima la finalidad de un registro que divulgue la solvencia económica de la persona, si a través de ello se considera que su seguridad y la de su familia podrían estar en riesgo.

Medidas Cautelares

Justificación de las medidas cautelares

La finalidad de toda medida cautelar es prevenir y evitar que, cuando concluya el juicio, el interés legítimo que se busca proteger, deje de existir. Es pues, la importancia del derecho en conflicto y la probable demora del pronunciamiento judicial definitivo, lo que justifica la existencia de esta clase de medidas. Una medida cautelar, decretada o no en un proceso de Hábeas Data, requiere siempre de un juicio de ponderación a cargo del juez que conoce la causa; en dicho proceso de valoración se deberá tomar en cuenta la materia litigiosa, los intereses en conflicto, los derechos afectados, la realidad de la tramitación del proceso y la coyuntura del caso particular de que se trate.

Resolución

Concedido favorablemente el Hábeas Data, debe el registro vencido entregar la información requerida. Dicha información debe tener las siguientes características, a saber: clara, completa y debidamente actualizada; por lo tanto, de ser incompleta, falsa, parcial, oscura o desactualizada deberá ser rechazada por el Juez, bajo las prevenciones de ley.

Apelación

Si el Juez de Primer nivel rechaza la demanda de Hábeas Data planteada por el actor, cabe la interposición del recurso de apelación a fin de que una de las Salas del Tribunal Constitucional, previo el sorteo reglamentario, resuelva de manera definitiva la causa. Si, por el contrario, el Juez de primer nivel concedió en forma favorable la demanda de Hábeas Data planteada, no puede el registro vencido interponer recurso de apelación, tal como lo ordena nuestra Constitución Política vigente desde 1998. Actualmente, la acción constitucional de habeas data se presenta ante cualquier Juez de la Función Judicial y en caso de apelación avocará conocimiento una de las Salas de la Corte Provincial de Justicia.

A inicios de 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, la Superintendencia de Bancos, las Cámaras de Comercio y otros, que ven en el comercio telemático una buena oportunidad de hacer negocios y de paso, 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 un tanto forzada, si se toma 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 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.

2.2.1. Condiciones Legales Establecidas en la Legislación Ecuatoriana

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

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

Constitución de la República del Ecuador - 2008

Personas usuarias y consumidoras

Art. 52.- Las personas tienen derecho a disponer de bienes y servicios de óptima calidad y a elegirlos con libertad, así como a una información precisa y no engañosa sobre su contenido y características. La ley establecerá los mecanismos de control de calidad y los procedimientos de defensa de las consumidoras y consumidores; y las sanciones por vulneración de estos derechos, la reparación e indemnización por deficiencias, daños o mala calidad de bienes y servicios, y por la interrupción de los servicios públicos que no fuera ocasionada por caso fortuito o fuerza mayor.

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

Art. 53.- Las empresas, instituciones y organismos que presten servicios públicos deberán incorporar sistemas de medición de satisfacción de las personas usuarias y consumidoras, y poner en práctica sistemas de atención y reparación. El Estado responderá civilmente por los daños y perjuicios causados a las personas por negligencia y descuido

en la atención de los servicios públicos que estén a su cargo, y por la carencia de servicios que hayan sido pagados.

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

Ejemplo: En la empresa eléctrica sin ningún justificativo cortan el servicio eléctrico sin previo aviso al consumidor ocasionando pérdidas económicas, se debe intentar por parte del perjudicado la correspondiente acción de daños y perjuicios.

Art. 54.- Las personas o entidades que presten servicios públicos o que produzcan o comercialicen bienes de consumo, serán responsables civil y penalmente por la deficiente prestación del servicio, por la calidad defectuosa del producto, o cuando sus condiciones no estén de acuerdo con la publicidad efectuada o con la descripción que incorpore. Las personas serán responsables por la mala práctica en el ejercicio de su profesión, arte u oficio, en especial aquella que ponga en riesgo la integridad o la vida de las personas.

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

la mala práctica en la profesión en la que se ponga en peligro inminente la vida de un ciudadano.

Ejemplo: La Empresa Municipal de Agua Potable de Ibarra**,** provee el servicio de agua potable a todo el cantón y por el cual cobra una tasa en forma mensual. Hace unos 5 años, aproximadamente, la población recibió el agua contaminada con eses fecales y otras bacterias, razón por la cual el defensor del pueblo presentó la denuncia a nombre de los ciudadanos por cuanto una cantidad considerable de ellos fueron afectados por dicho liquido vital y se solicitó las indemnizaciones dentro del campo civil, así como el enjuiciamiento penal en contra de los directivos de dicha empresa.

Art. 55.- Las personas usuarias y consumidoras podrán constituir asociaciones que promuevan la información y educación sobre sus derechos, y las representen y defiendan ante las autoridades judiciales o administrativas. Para el ejercicio de este u otros derechos, nadie será obligado a asociarse.

Comentario: De acuerdo al Art. 326 de la constitución del Ecuador todas las personas tienen derecho a asociarse y el estado está en la obligación de estimular la creación y organizaciones en especial de trabajadores, a fin de que ejerzan sus legítimos derechos ante las autoridades de la Función Judicial o ante las autoridades de tipo administrativo como son Municipios, Gobiernos Provinciales, entidades bancarias y otros.

El Art. 66 numerales 19 y 20 reconoce y garantiza a las personas el derecho a la protección de datos de carácter personal, que incluye el acceso y l decisión sobre información

y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley. Así también se reconoce al individuo el derecho a la intimidad personal y familiar, en esta carta constitucional se reconoce a los ciudadanos su derecho a la protección de sus datos, es decir nadie puede invadir la vida privada de los individuos.

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

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

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

2.2.3 Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

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

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

2.2.4 Ley de Propiedad Intelectual

La Ley de Propiedad Intelectual (LPI.) publicada en el Registro Oficial N° 320 del 19 de Mayo de 1998, nace con el objetivo de brindar por parte del Estado una adecuada protección de los derechos intelectuales y asumir la defensa de los mismos, como un elemento imprescindible para el desarrollo tecnológico y económico del país.

El organismo nacional responsable por la difusión, y aplicación de las leyes de la Propiedad Intelectual en el Ecuador es el INSTITUTO ECUATORIANO DE PROPIEDAD INTELECTUAL (IEPI), el mismo que cuenta con oficinas en Quito, Guayaquil y Cuenca. Es una persona jurídica de derecho público, con patrimonio propio, autonomía administrativa, económica, financiera, y operativa, con sede en la ciudad de Quito.

2.2.5 Ley Especial de Telecomunicaciones

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

2.2.6 Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional

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

Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, en su Capítulo III Articulo 49, Acción de Habeas Data establece que “la acción de habeas data tiene objeto garantizar judicialmente a toda persona el acceso a los documentos, datos genéticos, bancos o archivos de datos personales e informe que por sí misma, o sobre sus

bienes, estén en poder de entidades públicas o de personas naturales o jurídicas privadas en soporte material o electrónico. Asimismo, toda persona tiene derecho a conocer el uso que se haga de dicha información, su finalidad, el origen y destino, y el tiempo de vigencia del archivo o banco de datos".

En la Constitución Política del Ecuador vigente (2008), en su capítulo tercero de las Garantías Jurisdiccionales de su sección quinta Art. 92 sobre la acción de Habeas Data, también se establece recurso jurídico de Habeas Data.

De acuerdo a la especificación contemplada en la Ley de Comercio Electrónico, Firmas Digitales y Mensajes de Datos, en su título quinto de las infracciones informáticas, los delitos informáticos que se tipifican, mediante reformas al Código Penal. Hemos visto la definición de los delitos informáticos, su principal insumo que es la evidencia digital y las técnicas o mecanismos con los procedimientos existentes para su investigación, vale destacar, entonces que los profesionales dedicados a la persecución de actos ilícitos en los que se utilizan medios tecnológicos, se mantengan a la vanguardia de conocer los avances que se den de ésta índole, y de esta manera mantenerse preparados y reaccionar de manera adecuada ante los actos cometidos por la delincuencia informática.

Ecuador ha dado sus primeros pasos con respecto a las leyes existentes, en las que se contemplan especificaciones de la información y la informática, lo que se considera un avance importante ante el desarrollo tecnológico que se ha tenido en los últimos años en el país, pero es evidente que aún falta mucho por legislar, para asegurar que no queden

en la impunidad los actos que se comentan relacionados con las tecnologías.

2.3 El Perito y el Peritaje Informático

La conceptualización que brinda Juan Carlos Riofrío, es que “los peritos en general, para la administración de justicia, son personas expertas en una materia, capaces de aportar al juez conocimientos que no posee, con el fin se servir de lentes de aumento para la justicia con el fin de aclarar el asunto litigiosos en revisión.”, entonces, bajo esta conceptualización, el perito es un auxiliar de la justicia, que no persigue como objetivo resolver un problema operativo, sino revelar y/o explicar la causa y el porqué de dichos problemas, luego de un análisis y profundo estudio.

2.3.1. Definiciones

Para poder iniciar el tema de peritaje informático es necesario que diferenciemos perito y perito informático:

Perito: Experto en una materia, capaz de aportar al juez conocimientos que no posee, con el fin de servir de lentes de aumento para la justicia con el fin de aclarar el asunto litigioso en revisión.

Perito informático: perito especializado en el área de las tecnologías de la información que de acuerdo con el tema requerido puede ser seleccionado según su competencia y experiencia para una labor de análisis.

De acuerdo a lo contemplado en nuestra legislación en el Art. 94 del Código de Procedimiento Penal (CPP), “son peritos los profesionales especializados en diferentes

materias que hayan sido acreditados como tales, previo proceso de calificación del Ministerio Público".

2.3.2 Perfil del perito informático

De acuerdo a Jeimy Cano, un perito informático, requiere de una formación exigente y detallada no solo en la materia en la que se requiere de su conocimiento sino también de procedimientos legales, legislación nacional e internacional, fundamentos de criminalística y psicología que le permitan un conocimiento más profundo de los casos analizados, ya que como perito es un garante de la verdad en un proceso. Por lo expuesto, es clave que el perito acredite experiencia

El perfil del perito informático debe cumplir con algunas de las funciones que se destacan a continuación:

1. Identificación y recolección de evidencias en medios magnéticos.
2. Comprensión y práctica en procedimientos de revisión y análisis forenses.
3. Comprensión y práctica de los estándares de ética que rigen las ciencias forenses en informática.
4. Comprensión de los aspectos legales y de privacidad asociados con la adquisición y revisión de medios magnéticos.
5. Comprensión y práctica de mantenimiento de la cadena de custodia de la evidencia cuando se realiza una investigación informática.
6. Comprensión de los diferentes sistemas de archivos asociados con sistemas operativos, acceso a archivos temporales, de cache, de correo electrónico, de Web, etc.
7. Conducir de manera detallada, recuperación de datos de todas las porciones de un disco.

8. Comprensión de aspectos de Internet.
9. Comprensión de técnicas de rompimiento de contraseñas y claves de seguridad.
10. Comprensión general de los temas relacionados con investigaciones forenses.

Las investigaciones forenses aplicables a la informática, requieren de profesionales con altos conocimientos en tecnologías de la información, que se ajusten a la aplicación de procedimientos científicamente probados válidos y reconocidos sobre las evidencias que vulneran o comprometen sistemas de tipo informático, para ellos existen certificaciones u avales profesionales, que pueden ser obtenidos por los profesionales en las ramas de informática.

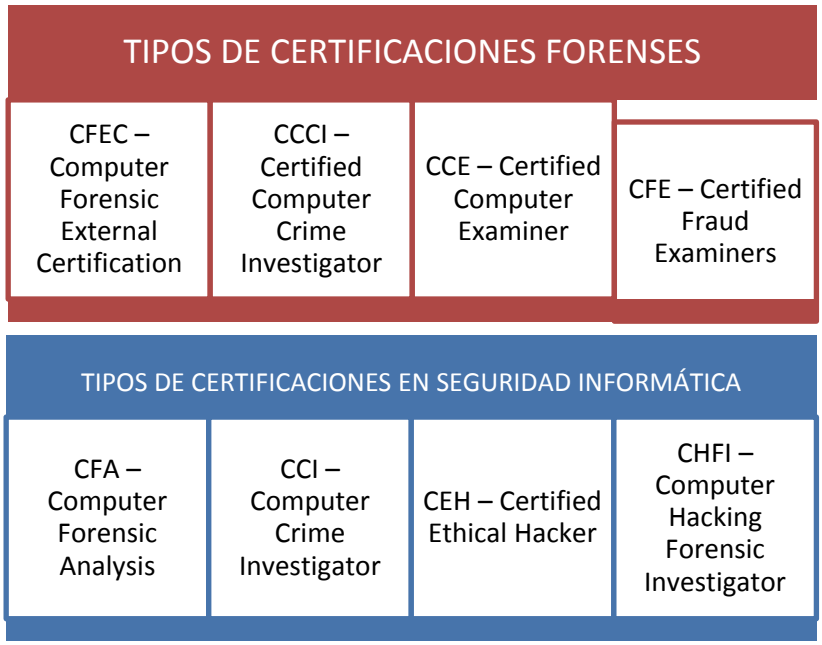


Tabla 2.4. Tipos de Certificaciones Forenses
Fuente: Investigación Directa

Es menester recalcar, que el perito debe contar, además de sus vastos conocimientos, con altos **valores éticos morales y profesional** que acredite la seriedad de su diligencia ante un proceso legal en que se hayan requerido sus conocimientos y habilidades para la investigación de un acto ilícito que se haya cometido.

2.3.3 Implicaciones legales para el perito

El profesional que se encuentre acreditado y se desempeñe en calidad de perito, debe conocer las implicaciones legales que pudieran tener sus intervenciones en un proceso de investigación de un acto ilícito. Los motivos de inhabilidad o excusa, contemplados en el Art. 67 del Código de Procedimiento Penal, incluyen:

1) Cuando el sospechoso, el imputado, el acusado, el agraviado, el denunciante, el acusador, o el abogado

defensor de cualquiera de ellos sea su cónyuge o conviviente, o tenga con él parentesco dentro del cuarto grado de consanguinidad y segundo de afinidad.

2) Cuando hubiera sido abogado de alguna de las partes.

3) Cuando tenga parentesco hasta el cuarto grado de consanguinidad o segundo de afinidad con el juez o con los miembros del tribunal.

4) Cuando esté ligado con cualquiera de las personas mencionadas en el inciso uno, por intereses económicos o de negocios de cualquier índole.

Otra disposición con implicación legal para los peritos, la constituye el Reglamento del Sistema de Acreditación de Peritos del Ministerio Público, en el cual consta según el Art. 9 que “el perito está obligado a practicar todo acto o diligencia propios de su experticia con el celo, esmero, prontitud, sigilo y reserva que la naturaleza del caso exija”, esto dará a lugar a enjuiciamiento penal y a la pérdida de su acreditación como perito, en caso por ejemplo: según el Art. 215 del CPP se establece que “sin perjuicio de las garantías del debido proceso, las actuaciones del Ministerio Público y de la Policía Judicial para el esclarecimiento del delito durante la indagación previa, se mantendrán en reserva…” si durante esta fase del proceso se contrapone dicha disposición por parte del perito esta actuación es sancionada conforme lo previsto en el Código de Procedimiento Penal.

2.3.4 Acreditación de peritos.

El Reglamento Sustitutivo del Reglamente para el Sistema de Acreditación de Peritos, el cual es definido por el Ministerio Público del Ecuador, publicado en el Registro

oficial N° 177, del 30 de diciembre del 2005, mediante Decreto Ejecutivo 977, establece que “el sistema de acreditación de peritos en las diferentes disciplinas de la ciencia y del arte, rige para todos aquellos profesionales y técnicos que posean conocimientos académicos y técnicos especializados y que tengan la experiencia suficiente y necesaria para intervenir en calidad de peritos en las causas penales, en las investigaciones pre procesales y procesales penales”. Dicho reglamento fue reformado mediante Decreto Ejecutivo 529, publicado en el registro oficial N° 151, del 20 de Agosto del 2007, reformando el sistema, en el cual, se agrupan las especialidades de los peritos y se modifican los requisitos de acreditación.

2.3.5 Organismos facultados para la acreditación de peritos

El Ministerio Público es la única entidad que puede acreditar y nombrar peritos, según lo establecido en el Reglamento para el Sistema de Acreditación de Peritos. La acreditación otorgada por los Ministerios Fiscales Distritales tiene validez en todo el territorio nacional y la acreditación es válida por dos años consecutivos, las renovaciones de credenciales se las realiza por igual periodo.

El Consejo Nacional de la Judicatura, establece requisitos de acreditación, en la que los profesionales acreditados pueden actuar previa designación en los juicios penales, laborales, civiles de la Corte Suprema de Justicia, en este organismo, de la misma manera, pueden ser nombrados los peritos que han sido acreditados por el Ministerio Público.

2.3.6. Requisitos de acreditación de peritos por el Ministerio Público.

Para ser acreditado como perito al Ministerio Público, se requieren presentar varios requisitos, los requerimientos solicitados son los siguientes:

1 Solicitud dirigida al Señor Ministro Fiscal General, especificando la especialidad pericial.
2 Cedula de Identidad y papeleta de votación, en original y copia.
3 Record Policial.
4 Hoja de Vida.
5 Copia notariada del Título legalizado y registrado en la SENESCYT, que acredite la formación académica en las ciencias de la especialidad cuya acreditación se solicita.
6 Copia notariada del certificado de la SENESCYT.
7 Inscripción en el correspondiente colegio profesional y credencial vigente.
8 Certificación de cumplimiento de obligaciones y de no haber sido sancionado por el colegio profesional.
9 Tres certificados de honorabilidad, probidad notoria e idoneidad.
10 Declaración juramentada notariada de tener más de 3 años de experiencia en peritajes, o en el área en que solicita la acreditación.
11 Una vez aprobada la carpeta anexar.
12 Comprobante de depósito.
13 Originales de la cedula de ciudadanía y certificado de votación.
14 Para los señores miembros de la Policía Nacional, Hoja de vida Policial con firma y sello de la Dirección General de Personal de la Policía Nacional.

2.3.7 Renovación en el Ministerio Público

En el proceso de renovación de credenciales de peritos, los requerimientos que se solicitan por el Ministerio Público son:

1. Solicitud dirigida al Señor Ministro Fiscal General.
2. Hoja de Vida actualizada.
3. Tres certificados de los Agentes Fiscales del Distrito, del área específica de la acreditación, sobre el cumplimiento de sus funciones y asistencia a las audiencias y de no tener denuncias ni quejas en contra.
4. Copia notariada del certificado del SENESCYT.
5. Actualización del record policial.
6. Nuevos certificados o diplomas de cursos o seminarios que haya realizado.
7. Una vez aprobada la carpeta anexar.
    a. Comprobante de depósito.
    b. Originales de la cedula de ciudadanía y certificado de votación.
8. Para los señores miembros de la Policía Nacional, Hoja de vida Policial con firma y sello de la Dirección General de Personal de la Policía Nacional.

2.3.8 Peritos Acreditados en el Consejo Nacional de la Judicatura

Los requisitos establecidos para el registro e inscripción de peritos por el Consejo Nacional de la Judicatura son:

1. Solicitud dirigida al Director Provincial del Consejo de la Judicatura, especificando la especialidad pericial
2. Hoja de Vida.
3. Cédula de Identidad y certificado de votación.
4. Record policial actualizado.

5. Documentos que acreditan capacitación y experiencias en las materias
6. Comprobante de pago de servicios administrativos e n el caso de peritos profesionales
7. Titulo registrado en el SENESCYT, en original y copia que acredite la formación académica en la especialidad que postula

2.3.9 Peritos acreditados en los Centros de Conciliación y Arbitraje

Centros de Conciliación y Arbitraje también establecen requisitos para la inscripción de peritos, los cuales son establecidos es sus respectivos Reglamento de Funcionamiento, a continuación se detalla por ejemplo los requisitos establecidos, según el Reglamento de Funcionamiento del Centro de Arbitraje y Mediación de la Cámara de Comercio Ecuatoriano Americana:

1. Tener al menos 30 años de edad.
2. Poseer título profesional.
3. Acreditar suficientes conocimientos en la materia sobre la que versará el informe pericial.
4. Acreditar idoneidad profesional y ética.
5. De preferencia, dominar el idioma inglés.

El proceso y los requisitos para ser acreditado como perito, como pudimos observar, no son complicados ni rigurosos, es un proceso sencillo en el que pueden aplicar los profesionales dentro de los organismos que contemplan sus sistemas de acreditación, sin embargo, dichos profesionales deben tener el conocimiento de sus implicaciones más allá de la rama en que se acrediten, es decir, que conozcan y tengan la preparación necesaria para rendir declaración ante un tribunal, capacidad de trabajar en un ambiente bajo presión, facilidad de comunicación, entre otras.

2.3.10 Causales para pérdidas de credenciales de peritos

El Reglamento Sustitutivo del Reglamento para el Sistema de Acreditación de Peritos, dispone que, el Ministerio Público del Ecuador esté facultado a retirar la acreditación del perito en cualquier momento en los siguientes casos:

1) Por falsedad en los datos entregados para la acreditación o renovación.
2) Por manifiesto desconocimiento de la disciplina en que se halla acreditado.
3) Por incumplimiento de la ética profesional.
4) Por hechos de corrupción en el ejercicio de las funciones de perito.
5) Por denuncias y quejas presentadas en su contra.
6) Por cobros indebidos a las partes procesales.
7) Por la emisión de informes parcializados plenamente justificados.

En el caso de hechos de corrupción, las denuncias y quejas y la emisión de informes parcializados, deben ser suficientemente comprobadas para que se retire la acreditación al profesional.

2.3.11. Peritos acreditados en el Ecuador

El Ministerio Público del Ecuador, mantiene el registro de los peritos acreditados a nivel nacional en el cual existen alrededor de 1433 peritos acreditados en diferentes ramas como: la medicina, química, criminalística, documentología, traducciones, financieros, contables, avalúos, entre otras, incluidos peritos en la rama de informática y

telecomunicaciones. La siguiente gráfica muestra porcentualmente por especialidades los peritos acreditados que constan en los registros.

En lo que corresponde a los especialistas de la rama de informática y telecomunicaciones en el Ecuador, al mes de agosto del 2008, se encuentran acreditados 31 profesionales como peritos (25 profesionales de la rama de informática y 6 profesionales de la rama de Telecomunicaciones), los cuales representan el 2% del total de especialistas acreditados a nivel nacional, los peritos informáticos se encuentran distribuidos geográficamente de la siguiente manera:

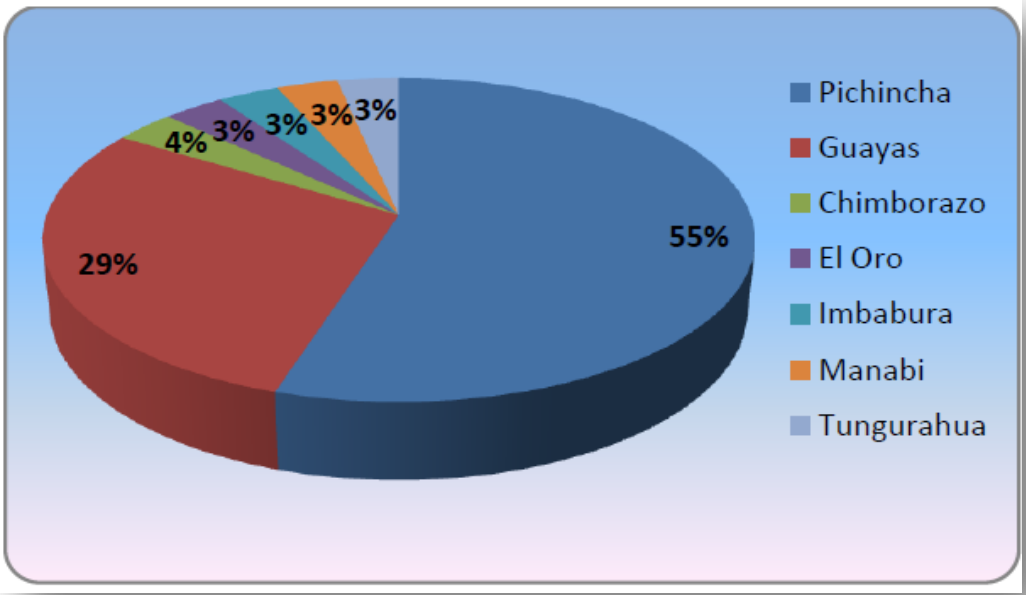


Figura. 2.5. Distribución geográfica de peritos informáticos por provincia.
Fuente: Nómina de Peritos del Ministerio Público de Ecuador – Agosto 2008

Metodología de la Auditoria Informática Forense

El auditor forense para poder iniciar su trabajo, determinando los hallazgos de irregularidades, fraude y corrupción en las empresas del

sector comercial, deben establecer una metodología que este, acorde con las irregularidades encontradas.

1. **Reconocimiento del Problema:** En esta fase se determinar si hay suficientes motivos o indicios, para investigar los síntomas de un posible fraude.
2. **Recopilación de evidencias de fraude:** Después del reconocimiento del problema, comenzamos a buscar las evidencias relacionadas al fraude, siniestro o ataque, estas evidencias deben ser suficientes para que garanticen el éxito de la investigación. Las principales técnicas que se aplican son: Indagación, Observación, Inspección, Confirmación, Análisis y recálculo.

   Ejemplos de evidencia digital: Email, Imágenes, Chat rooms, File contents, System logs, Network packets.
3. **Evaluación de las evidencias recolectadas o análisis:** Esta fase sirve para determinar si son suficientes y válidas las evidencias recolectadas como para comenzar a reportar eficazmente el fraude. La evidencia deber ser evaluada para determinar si es completa y precisa, si es necesario seguir recolectando más evidencias. De la evidencia recolectada surgirá la respuesta de que acciones judiciales se pueden realizar por parte de la Organización.

2.4. Los Delitos Informáticos en el Derecho Comparado

2.4.1. Generalidades

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.

2.4.2. Contemplaciones de la Organización de Estados Americanos (OEA)

La Organización de Estados Americanos (OEA), está conformada por 35 países independientes de las Américas, de Norte, Sur y Centroamérica y el Caribe que han ratificado la carta de la OEA y pertenecen a la Organización.

En el mes de marzo del año 1999, los Ministros de Justicia de las Américas que pertenecen a la OEA, encomendaron establecer un Grupo de Expertos Intergubernamentales en Materia de Delitos Cibernéticos, que les permita:

- Realizar un diagnóstico de la actividad delictiva vinculada a las computadoras y la información de los Estados miembros.
- Realizar un Diagnóstico de la legislación, las políticas y las prácticas nacionales con respecto a dicha actividad.
- Identificar las entidades nacionales e internacionales que tienen experiencia en la materia; y
- Identificar mecanismos de cooperación dentro del sistema interamericano para combatir el delito cibernético.

2.4.3 Legislación de la Comunidad Económica Europea

En Alemania, para hacer frente a la delincuencia relacionada con la informática, el 15 de mayo de 1986 se adoptó la Segunda Ley contra la Criminalidad Económica. Esta ley

reforma el Código Penal (art. 148 del 22 de diciembre de 1987) para contemplar los siguientes delitos:

1. Espionaje de datos (202a).
2. Estafa informática (263a).
3. Falsificación de datos probatorios (269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos (270, 271, 273).
4. Alteración de datos (303a) es ilícito cancelar, inutilizar o alterar datos e inclusive la tentativa es punible.
5. Sabotaje informático (303b).
6. Destrucción de datos de especial significado por medio de deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.
7. Utilización abusiva de cheques o tarjetas de crédito (266b).

2.4.4 Regulaciones Existentes en Latinoamérica

A nivel de Latinoamérica algunos países como Chile, Argentina, Venezuela, Perú, cuentan con regulación, a nivel legislativo que tipifica los delitos informáticos, mientras que en otros países se ha procedido a la reforma de los Códigos de Procedimiento Penal para la aplicación de las sanciones, ante las infracciones informáticas cometidas. Además de las reformas concernientes al Código de Procedimiento Penal se mantienen leyes como: Ley de Propiedad Intelectual, Ley de Comercio Electrónico, Ley de Habeas Data, Ley de Firmas Digitales, entre otras, que establecen especificaciones que conciernen a lo información e informática.

Legislación de Países Latinoamericanos	Ley de Propiedad Intelectual	Ley de Habeas Data	Ley de Comercio Electrónico, Mensajes de Datos y	Ley de Delitos Informáticos	Ley de Transparencia y Acceso a la Información	Ley de Pornografía Infantil	Ley Uso de correo electrónico (SPAM)
Argentina	▼	◆	●	▲			
Bolivia					D		
Brasil		◆	●				
Chile	▼		●	▲		✹	
Colombia			●	▲	■		
Costa Rica				▲			
Ecuador	▼	◆	●		■		
Guatemala			●				
México				Proy.	■		
Panamá			●				
Paraguay					■		
Perú			●	▲	■		▼
República Dominicana			●				
Uruguay							Proy.
Venezuela			●	▲			

Tabla 2.4. Leyes en países Latinoamericanos

Fuente: Retos a superar en la administración de justicia ante los delitos informáticos en el Ecuador.

2.4.5. Legislación de la República de Chile

Chile fue el primer país latinoamericano en sancionar la ley contra delitos informáticos en donde se legisla aspecto que conciernen a la información y a la informática, a continuación la siguiente tabla lista las leyes, decretos y normas que han incorporado ésta figuras bajo el contexto legal.

Ley de Delitos Informáticos - Chile), establece figuras penales sobre los delitos informáticos en los que se incluyen los siguientes tipos de actos ilícitos de acuerdo a lo que establecen sus articulados:

1) Sabotaje.
2) Espionaje informático.
3) Destrucción maliciosa de la información.
4) Divulgación de información no autorizada.

Para la investigación de los delitos informáticos, Chile cuenta con la Brigada Investigadora del Ciber Crimen, que pertenece como Unidad departamental a la Policía de Investigaciones de Chile, cuya creación fue en el año 2000, a pesar de contar con la Ley desde 1993, que se especializa en los delitos cometidos vía Internet, tales como amenazas, estafas, falsificación, pornografía infantil en Internet, entre otros.

Las actividades que cumplen los departamentos de la brigada, están dadas de acuerdo a lo siguiente:

- Investigación de Pornografía Infantil:- Orientada a las investigaciones en Internet, en lo que concierne a la mantención, distribución y creación de material pornográfico infantil, además identificar comunidades y movimientos relacionados con este tipo de delitos.

- Agrupación de Delitos Financieros e Investigaciones Especiales en Internet:- Investigación de los delitos financieros con apoyo de alta tecnología, se especializa entre otros, en la clonación de tarjetas de crédito y débito, traspasos no autorizados vía web. Además de todas las investigaciones de carácter especial, tales como, amenazas vía internet, Infracción a la Ley 19.223, Infracción a la Ley de propiedad Intelectual e industrial.

- El Grupo de Análisis Informático:- Busca, recupera, y analiza información y evidencias, de los equipos que son atacados o

utilizados para la comisión de diversos delitos, trabajan en conjunto con las dos agrupaciones del inciso 1 y 2.

2.4.6 Legislación de la República de Argentina

Argentina es uno de los países que a nivel de legislación ha desarrollado el tema sobre los delitos informáticos y los ha presentado en debate desde el año 2006, logrando en Junio del 2008 que La Cámara de Senadores del Congreso Nacional apruebe la Ley 26388 en la que se penalizan los delitos electrónicos y tecnológicos. La siguiente tabla muestra las leyes y decretos que mantiene Argentina y que contemplan especificaciones de informática e información:
La Ley 26388, dio paso a que se incorpore importantes cambios en el Código Penal Argentino sobre el uso de las tecnologías de la información, en la cual se sanciona:

1) Pornografía infantil.

2) Destrucción maliciosa y accesos no autorizados a la información y sistemas de información.

3) Intercepción e interrupción de las comunicaciones electrónicas y de telecomunicaciones.

4) Divulgación de información no autorizada.

Desde el año 2001 la justicia argentina, conformó un equipo de peritos expertos en delitos informáticos, los mismos que asisten a las cámaras y juzgados del país.

1) Peritos oficiales o judiciales:- Son aquellos que pertenecen a algún organismo oficial como la policía federal o gendarmería

2) Peritos de parte:- Son aquello que son proveídos, como su nombre lo indica por una de las partes contratados por abogados en un caso litigioso.

3) Peritos de oficio o dirimentes:- También reconocidos como tercero en discordia y son llamados a evaluar informes previos de otros peritos, o cuando los informes presentados guardan una discordancia.

2.4.7 Legislación de la República de Colombia.

Colombia ha implementado iniciativas que le permiten en diferentes espacios, establecer mecanismos que le permiten controlar los delitos relacionados con las tecnologías.

Colombia ha tenido un desarrollo particular con respecto a la investigación de delitos de índole informático, factores como el narcotráfico, lavado de dinero, falsificación y terrorismo, ha incentivado que este país implemente unidades de investigación que les colabore en los procesos de indagación de actos ilícitos en los que se utilizan medios tecnológicos o que afectan sistemas de tecnología o de información.

El Código Penal Colombiano expedido con la Ley 599 de 2000, no hace referencia expresa a los delitos informáticos como tales; no obstante, en varias de sus normas recoge conductas que podrían entenderse incorporadas al concepto que la doctrina ha elaborado a este respecto.

En Colombia con la expedición de la Ley 527 de 1999 y su decreto reglamentario 1747 de 2000, se reconoció

fuerza probatoria como documentos a los mensajes de datos. El artículo 10º de la Ley 527/99 regla:

> Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de procedimiento Civil.

La Corte Constitucional en sentencia C-662 de junio 8 de 2000, con ponencia del Magistrado Fabio Morón Díaz, al pronunciarse sobre la constitucionalidad de la Ley 527 de 1999, hizo las siguientes consideraciones:

> El mensaje de datos como tal debe recibir el mismo tratamiento de los documentos consignados en papel, es decir, debe dársele la misma eficacia jurídica, por cuanto el mensaje de datos comporta los mismos criterios de un documento.

El proyecto de ley establece que estos crímenes tendrán penas de prisión de 4 a 8 años para los delincuentes informáticos y multas de 100 a 1.000 salarios mínimos mensuales, es decir de 46,1 a 461,5 millones de pesos.

Entre las conductas tipificadas como delito están el acceso abusivo a sistemas informáticos, la obstaculización ilegítima de sistemas computacionales o redes de telecomunicaciones, la interceptación de datos informáticos, el uso de software malicioso, la violación de datos personales y la suplantación de portales de Internet para capturar datos personales, entre otras.

- **Acceso abusivo a un sistema informático.** Será sancionado quien sin autorización acceda a un sistema informático protegido o se mantenga dentro del mismo

en contra de la voluntad de quien tenga el legítimo derecho a excluirlo.

- Obstaculización ilegítima de sistema informático o red de telecomunicación. Se penalizará a quien impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones.

- Interceptación de datos informáticos. Bajo este delito serán castigadas las personas que, sin orden judicial previa, intercepten datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte.

- Daño informático. Se sancionará a quien, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos.

- Uso de software malicioso. El proyecto de ley señala que serán castigadas las personas que, sin estar facultadas para ello, produzcan, trafiquen, adquieran, distribuyan, vendan, envíen, introduzcan o extraigan del territorio nacional software malicioso u otros programas de computación de efectos dañinos.

- Violación de datos personales. Este delito cobijará a quienes, sin estar facultados para ello, con provecho propio o de un tercero, obtengan, compilen, sustraigan, ofrezcan, vendan, intercambien, envíen, compren, intercepten, divulguen, modifiquen o empleen códigos

personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes.

- Suplantación de sitios web para capturar datos personales. Será sancionado quien, con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes. También quien modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

2.4.8 Legislación de la República del Perú.

La reforma del Código Penal en materia de delitos informáticos es la más reciente puesto que data de fines del año 2000.
Entre las figuras más salientes se encuentran:

1. El ingreso o uso indebido, a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos (art. 207 A).

2. El uso, ingreso o interferencia indebida de una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos (art. 207 B).

3. Agravantes cuando se accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función del cargo; o sí el autor pone en peligro la seguridad nacional (art. 207 c).

Delitos Informáticos Contemplados en la Legislación Peruana:

Delitos Informáticos	Código Penal
Acceso no autorizado a servicios y sistemas informáticos y telemáticos	Artículo 207-A.-
Base de datos público y privado.	Artículo 207-A.-
Manipulación de programas informáticos.	Artículo 207-B. Artículo 207-C.
Manipulación de los datos bancarios personales(Uso indebido de tarjetas de crédito y de cajeros automáticos)	Artículo 186
Falsificación electrónica de documentos.	Artículo 427
Suplantación (e-mail)	Artículo 161
Pornografía infantil	Artículo 183 - A
Propiedad intelectual	Artículo 216. Artículo 217 Artículo 218 Artículo 219 Artículo 220
Propiedad industrial: marcas, patentes	Artículo 222. Artículo 223 Artículo 224
Pánico Financiero	Artículo 249
Apología	Artículo 316

Difamación	Artículo 132
Espionaje	Artículo 331
Manipulación y/o falsificación de datos.	Artículo 427

2.4.9 Legislación de La República de Venezuela.

En la Ley sobre Delitos Informáticos, cuyo objetivo es proteger los sistemas que utilicen tecnologías de información, así como prevenir y sancionar los delitos cometidos contra o mediante el uso de tales tecnologías (Gaceta Oficial N° 37.313 del 30 de octubre de 2001). Se trata de una ley especial que descodifica el Código Penal y profundiza aún más la incoherencia y falta de sistematicidad de la legislación penal, con el consecuente deterioro de la seguridad jurídica.

La Ley define los términos tecnología de la información, sistema, data, documento, computadora, hardware, firmware, software, programa, procesamiento de datos o de información, seguridad, virus, tarjeta inteligente, contraseña y mensaje de datos.

La ley presenta varias deficiencias y problemas, entre los que podemos mencionar los siguientes:

(i) Utiliza términos en el idioma inglés, cuando la Constitución solo autoriza el uso del castellano o lenguas indígenas en documentos oficiales;

(ii) No tipifica delito alguno relativo a la seguridad e integridad de la firma electrónica y a su registro;

(iii) La terminología utilizada es diferente a la de la Ley de Mensaje de Datos y Firmas Electrónicas, tal como se observa en la definición que hace del mensaje de datos con lo que se propicia un desorden conceptual de la legislación en materia electrónica;

(iv) Repite delitos ya existentes en el Código Penal y en otras leyes penales, a los cuales les agrega el medio empleado y la naturaleza intangible del bien afectado;

(v) Tutela los sistemas de información sin referirse a su contenido ni sus aplicaciones;

(vi) No tutela el uso debido de Internet; y

(vii) Establece principios generales diferentes a los establecidos en el libro primero del Código Penal, con lo cual empeora la descodificación.

La Ley, que pretende ser un Código Penal en miniatura, pero carece de la sistematicidad y exhaustividad propias de tal instrumento, elabora cinco clases de delitos:

1) Contra los sistemas que utilizan tecnologías de información;

2) Contra la propiedad;

3) Contra la privacidad de las personas y de las comunicaciones;

4) Contra niños y adolescentes y;

5) Contra el orden económico.

Además de las penas principales indicadas anteriormente, se impondrán, sin perjuicio de las establecidas en el Código Penal, las siguientes penas accesorias:

(i) El comiso de equipos, dispositivos, instrumentos, materiales, útiles, herramientas y cualquier otro objeto que haya sido utilizado para la comisión de los delitos previstos en los artículos 10 y 19 de la Ley (posesión de equipos o prestación de servicios de sabotaje y posesión de equipos para falsificaciones).

(ii) Trabajo comunitario por el término de hasta tres años en los casos de los delitos previstos los artículos 6 y 8 de la Ley (acceso indebido y favorecimiento culposo del sabotaje o daño).

(iii) La inhabilitación para el ejercicio de funciones o empleos públicos; para el ejercicio de la profesión, arte o industria; o para laborar en instituciones o empresas del ramo por un período de hasta tres años después de cumplida o conmutada la sanción principal, cuando el delito se haya cometido con abuso de la posición de acceso a data o información reservadas, o al conocimiento privilegiado de contraseñas, en razón del ejercicio de un cargo o función público, del ejercicio privado de una profesión u oficio, o del desempeño en una institución o empresa privada.

(iv) La suspensión del permiso, registro o autorización para operar o para ejercer cargos directivos y de representación de personas jurídicas vinculadas con el uso de tecnologías de información, hasta por el período de tres años después de cumplida o conmutada la sanción principal, si para cometer el delito el agente se valió de o hizo figurar a una persona jurídica.

(v) Además, el tribunal podrá disponer la publicación o difusión de la sentencia condenatoria por el medio que considere más idóneo.

GLOSARIO

ACCESO ALEATORIO.- Operación de almacenamiento y recuperación de la información en la que el sistema accede directamente a la memoria en base a un parámetro preestablecido.

ACCESO DIRECTO.- Técnica por la cual los diferentes periféricos del ordenador acceden a la memoria de éste sin control de la CPU.

ADMINISTRACIÓN DE MEMORIA.- Se refiere a una variedad de métodos utilizados para almacenar datos y programas en memoria, hacer un seguimiento de ellos y recuperar el espacio de memoria cuando ya no se necesitan. En los mini computadores y mainframes tradicionales, la administración de memoria incluye la memoria virtual, la conmutación de bancos y las técnicas de protección de memoria.

APLICACIÓN.- En informática las aplicaciones son los programas con los cuales el usuario final interactúa, es decir, son aquellos programas que permiten la interacción entre el usuario y la computadora. Esta comunicación se lleva acabo cuando el usuario elige entre las diferentes opciones o realiza actividades que le ofrece el programa. Que generalmente le decimos software. Es por definición un programa diseñado con un objetivo específico y que lleva a cabo alguna tarea útil.
Algunos ejemplos son: planilla de cálculo, procesador de textos, editor gráfico, creador de presentaciones o administrador de bases de datos. También existen los denominados paquetes de aplicaciones, que contienen varios programas que, generalmente, son capaces de interactuar entre sí. El ejemplo más común es el de los paquetes Office.

ARCHIVO.- Datos estructurados que pueden recuperarse fácilmente y usarse en una aplicación determinada. Se utiliza como sinónimo de fichero. El archivo no contiene elementos de la aplicación que lo crea, sólo los datos o información con los que trabaja el usuario.

BASE DE DATOS.- (DataBase). Conjunto de datos relacionados que se almacenan de forma que se pueda acceder a ellos de manera sencilla, con la posibilidad de relacionarlos, ordenarlos en base a diferentes criterios, etc. Las bases de datos son uno de los grupos de aplicaciones de productividad personal más extendidos. Entre las más conocidas pueden citarse dBase, Paradox, Access y Aproach, para entornos PC, y Oracle, ADABAS, DB/2, Informix o Ingres, para sistemas medios y grandes

BANNER.- Son espacios publicitarios en las páginas los cuales describen un web o sólo te dan una idea de lo que hay al otro lado si te atreves a pinchar en ellos.

BLOQUEOS.- Toda acción que impide que las interrupciones u otro agente interrumpan o alteren el funcionamiento correcto de la sección critica de un proceso.

CACHÉ (RAM CACHÉ).- Un caché es un sistema especial de almacenamiento de alta velocidad. Puede ser tanto un área reservada de la memoria principal como un dispositivo de almacenamiento de alta velocidad independiente. Hay dos tipos de caché frecuentemente usados en las computadoras personales: memoria caché y caché de disco. Una memoria caché, llamada tambien a veces almacenamiento caché ó RAM caché, es una parte de memoria RAM estática de alta velocidad (SRAM) más que la lenta y barata RAM dinámica (DRAM) usada como memoria principal. La memoria caché es efectiva dado que los programas acceden una y otra vez a los mismos datos o instrucciones. Guardando esta información en SRAM, la computadora evita acceder a la lenta DRAM. Cuando un dato es encontrado en el caché, se dice que se ha producido un impacto (hit), siendo un caché juzgado por su tasa de impactos (hit rate). Los sistemas de memoria caché usan una tecnología conocida por caché inteligente en el cual el sistema puede reconocer cierto tipo de datos usados frecuentemente. Las estrategias para determinar qué

información debe de ser puesta en el caché constituyen uno de los problemas más interesantes en la ciencia de las computadoras. Algunas memorias caché están construidas en la arquitectura de los microprocesadores. Por ejemplo, el procesador Pentium II tiene una caché L2 de 512 Kbytes.

CLASIFICACIÓN.- Distribución de un conjunto de acuerdo con un principio de jerarquía lógica. Cuando se trata de libros o documentos se llama clasificación bibliográfica o documental. // Técnica que se utiliza para la identificación, agrupación y distribución sistemática de documentos o cosas semejantes, con características comunes o sistema determinado y que pueden ser con posterioridad diferenciadas según su tipología fundamental. Dicho proceso se aplica de acuerdo a un esquema lógico predeterminado para señalar su ubicación. Tratándose de documentos, permite además, definir los temas contenidos en ellos.

COMPUTACIÓN.- Ciencia que estudia el tratamiento automático de la información, mediante máquinas diseñadas para ese propósito

COMPUTADORA.- Ordenador. En Hispanoamérica se utiliza la palabra computadora, derivada del inglés computer, para designar a los ordenadores.

COMUNICACIÓN.- (Communications). Transferencia electrónica de información de un lugar a otro. Las comunicaciones de datos se refieren a las transmisiones digitales, y las telecomunicaciones, a transmisión análoga y digital, incluyendo voz y video.

COOKIE.- Cuando se visita una página Web, es posible recibir una Cookie. Este es el nombre que se da a un pequeño archivo de texto, que queda almacenado en el disco duro del ordenador. Este archivo sirve para identificar al usuario cuando se conecta de nuevo a dicha página Web.

CONTRATOS INFORMÁTICOS.- Es todo acuerdo en virtud del cual se crean conservan, modifican o extinguen obligaciones relativas a sistemas, subsistemas o elementos destinados al tratamiento sistematizado de la información CPU (Central Processing Unit).- Unidad Central de Proceso

DERECHO INFORMÁTICO.- el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática.

ELECTRONIC MAIL (EMAIL).- (correo electrónico) Sistema mediante el cual un ordenador puede intercambiar mensajes con otros usuarios de ordenadores (o grupos de usuarios) mediante redes de comunicación. El correo electrónico es uno de los usos más populares de Internet.

E-MAIL (MESSAGE).- Mensaje (electrónico)

FORMATO.- Estructura de un archivo que define la forma en que se guarda y representa en pantalla o en impresora. El formato puede ser muy simple y común, como los archivos guardados como texto ASCII puro, o puede ser muy complejo e incluir varios tipos de instrucciones y códigos de control utilizados por programas, impresoras y otros dispositivos. En MS-DOS la extensión del nombre del archivo suele indicar el formato del archivo. Entre los ejemplos se cuentan el formato RTF (Rich Text Format), DCA (Document Content Architecture), PICT, DIF (Data Interchange Format), DXF, TIFF (Tag Image File Format) y EPSF (Encapsulated PostScript Format). Se refiere al formato de archivo que una aplicación utiliza para producir sus propios archivos. Forma preestablecida que se le da a un documento tomando como base o referencia otro con la forma deseada.

HARDWARE.- Conjunto de los componentes que integran la parte material de una computadora.

INTERNET.-. Red informática mundial, descentralizada, formada por la conexión directa entre computadoras u ordenadores mediante un protocolo especial de comunicación

INTERNET ADDRESS.- (Dirección internet) Dirección IP que identifica de forma inequívoca un nodo en una red internet. Una dirección Internet (con "I" mayúscula) identifica de forma inequívoca un nodo en Internet. Ver también: "internet", "Internet", "IP address".

INTERNET RELAY CHAT (IRC).- (Charla Interactiva Internet) Protocolo mundial para conversaciones simultáneas ("party line") que permite comunicarse por escrito entre sí a través de ordenador a varias personas en tiempo real. El servicio IRC está estructurado mediante una red de servidores, cada uno de los cuales acepta conexiones de programas cliente, uno por cada usuario.

INTERNET SOCIETY (ISOC).- Sociedad Internet) La Internet Society es una organización profesional sin ánimo de lucro que facilita y da soporte a la evolución técnica de Internet, estimula el interés y forma a las comunidades científica y docente, a las empresas y a la opinión pública acerca de la tecnología, usos y aplicaciones de Internet y promueve el desarrollo de nuevas aplicaciones para el sistema. Esta sociedad ofrece un foro para la discusión y la colaboración en el funcionamiento y uso de la infraestructura global. La Internet Society publica un boletín trimestral (On The Net) y convoca una conferencia anual (INET). El desarrollo de estándares técnicos de Internet tiene lugar bajo los auspicios de Internet Society con un importante apoyo de la Corporation for National Research Initiatives mediante un acuerdo de cooperación con la Administración Federal de los Estados Unidos de América.

PASSWORD.- Contraseña

SOFTWARE.- Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

VIRTUAL.- Esta palabra se suele usar para referirse a algo que no existe realmente, sino sólo dentro del ordenador. Las dos acepciones más habituales son \"Realidad virtual\", referida a un espacio en 3 dimensiones creado dentro del ordenador, por el que el usuario puede desplazarse (normalmente con la ayuda de dispositivos auxiliares, como gafas estereoscópicas, guantes o joysticks), y \"Memoria virtual\", que consiste en que un ordenador aparente tener más memoria de la que físicamente tiene, gracias a que parte del disco duro se utiliza como zona de almacenamiento intermedio, en la que se va volcando información cuando la memoria real se satura (de forma transparente, sin que el usuario tenga que hacer nada).

VIRUS.- Un virus es un programa informático que se ejecuta en el ordenador sin previo aviso y que puede corromper el resto de los programas, ficheros de datos e, incluso el mismo sistema operativo. Afortunadamente, los virus no provocan daños en el hardware del ordenador. Sin embargo si que pueden borrar los datos del disco duro. Éste podrá volver a utilizarse, una vez eliminado el virus del ordenador.

Los virus se transmiten, normalmente, a través de disquetes o de los archivos enviados a través de Internet. El intercambio de documentos entre usuarios provoca la entrada de estos "inquilinos" en el ordenador. Los virus suelen esconderse en un programa de aspecto inocente, de manera que, al ejecutarlos, el virus se activa. En ese momento, quedan residentes en la memoria del ordenador.

WEB.- Por éste término se suele conocer a WWW (World Wide Web), creado por el Centro Europeo de Investigación Nuclear como un sistema de intercambio de información y que Internet ha estandarizado. Supone un medio cómodo y elegante, basado en multimedia e hipertexto, para publicar información en la red.

Inicial y básicamente se compone del protocolo http y del lenguaje html. Un ejemplo de páginas de éste tipo, es la que tienes delante en estos momentos.

CAPITULO III

METODOLOGÍA

3.1. Tipo de Investigación

Esta investigación se refiere a la búsqueda de nuevas infracciones informáticas y en especial los que se dan en la Provincia de Imbabura, definir cuáles se enmarcan en procesos judiciales actuales, cuáles son las que se penalizan en nuestra legislación Ecuatoriana y cuáles deberían integrarse. Está enfocada en los siguientes tipos de investigación:

- Es una Investigación Bibliográfica y Documental, debido especialmente en la construcción de marcos teóricos y marcos contextuales.

- Es una Investigación Descriptiva: Se realiza una recopilación de información y datos que se dan en los actuales momentos sobre las infracciones informáticas en la Provincia de Imbabura, y basado en esta información se desarrollara el diseño y propuesta de las reformas a la Normativa Legal que penalicen los tipos de delitos investigados.

- Es una Investigación de campo: Ya que se apoya en informaciones que provienen entre otras, de encuestas y observaciones.

3.2. Diseño de Investigación.

Es una Investigación no Experimental, porque no se van a manipular ni a experimentar con los sujetos motivo de la investigación.

3.3. Selección de Variables

En la presente investigación en base a la “Falta de leyes y penalizaciones en nuestra legislación acerca de los Delitos Informáticos; hace que exista delito por el simple hecho de copiar o pegar o de usar datos sin autorización alguna del dueño; sin penalizar algunos delitos importantes que ya se encuentran vigentes en la mayoría de países de Latinoamérica y del resto del mundo. Se determina las siguientes variables:

3.3.1 Independiente: Leyes y Reglamentos Ecuatorianos relacionados a infracciones informáticas.

3.3.2 Dependiente: Impacto de las infracciones informáticas en las organizaciones y sociedad en general.

3.4. Definición conceptual de las Variables

VARIABLE	DEFINICIÓN OPERACIONAL	INDICADORES	TÉCNICAS	INSTRUMENTOS
Leyes y Reglamentos Ecuatorianos	Actividad Científica: Proponer leyes y reglamentos que legislan estos delitos para que se juzgue las infracciones informáticos en nuestro país y por ende en la provincia de Imbabura	Diversidad Actualidad Aplicabilidad	Observación directa de entrevistas y encuestas. Análisis de información.	Cuestionarios
Impacto de las infracciones informáticas en las organizaciones y sociedad en general.	organización, planificación para reestructurar leyes y reglamentos ecuatorianos	Consecuencias morales Consecuencias económicas Consecuencias sociales	Observación directa de entrevistas y encuestas	Cuestionarios

Tabla 3.1. Definición conceptual de las Variables

Elaboración: Dr. Hugo Imbaquingo

Fuente: Investigación directa

3.5 Población y muestra

Población:

La presente investigación se desarrolló en la provincia de Imbabura. Tomando como población a los Jueces Penales, Tribunales Penales de la Corte Provincial de Justicia de Imbabura, esto con la finalidad de contar con un criterio confiable sobre la importancia de una sanción a cada delito que ayudó a una validación de la propuesta a la Legislación.

Los Abogados en libre ejercicio, Comandancia de Policía de Imbabura, Profesionales Informáticos, Universidades, Empresas e Instituciones, para recopilar datos que ha sido sujeto a un tipo de Delito Informático en la Provincia de Imbabura.

Muestra de Juicio.

Una muestra de juicio es llamada una muestra no probabilística, puesto que este método está basado en los puntos de vista del Investigador. Las principales ventajas de una muestra de juicio son la facilidad de obtenerla y que el costo usualmente es bajo.

En el caso de las encuestas se escogió el asesoramiento de los profesionales del derecho por haber sido ex-Presidente de Colegio de Abogados de Imbabura, de la misma manera se recogió el criterio de los Ingenieros en Sistemas y Computación, y estudiantes de las Universidades de Provincia de Imbabura ser Docente de las especialidades tecnológicas, así como empresas públicas y privadas por el ejercicio profesional y por ser las más vulnerables ser víctimas de los delitos informáticos.

La muestra se describe en el siguiente cuadro:

NOMBRE	ORIGEN
Abogados de libre ejercicio (70)	Colegio de Abogados de Imbabura
Ingenieros Informáticos (20)	Colegio de Ingenieros en Informática, Sistemas y Computación de Imbabura
Comandancia de Policía de Imbabura (10)	Policías
Universidades (40)	UTN, PUCE,UCL,ANIANDES,UNITA,UTPL,UTPO
Empresas/Instituciones (10)	Empresas/Instituciones de la Provincia de Imbabura

3.6 MÉTODOS Y TÉCNICAS

3.6.1 Métodos

Los métodos que fueron empleados son:

a**) Deductivo**. Es el método el que presenta el conjunto de afirmaciones usado para describir los Delitos Informáticos actuales, que servirá de base para deducir conclusiones y consecuencia de cada delito.

b) Inductivo. Este método es usado para obtener, describir, principios generales de la Legislación Ecuatoriana aplicado a sanción de cada uno de los delitos informáticos, en base al análisis de los diferentes casos particulares en la Provincia de Imbabura.

c) Analítico. Es usado para presentar conceptos como una totalidad para luego ir descomponiendo en capítulos y subcapítulos, temas y subtemas.

d) Sistemático. Permite conocer los delitos en la Provincia de Imbabura, desde cuales son y sus sanciones, en un proceso de secuencia lógica.

3.6.2. Técnicas.

Entre las técnicas de investigación que se aplicaron están:

Fuentes de Información Primarias.

Las fuentes de información primarias, usada para recolectar los datos de las fuentes de origen, se aplica los siguientes instrumentos:

a) Encuesta. Se aplicó esta técnica a: Abogados en libre ejercicio, Comandancia de Policía de Imbabura, Profesionales Informáticos, Universidades a través de los cuestionarios o llamados también instrumentos. Para

recopilar datos de la muestra seleccionada de la población que conoce y ha sido sujeto a un tipo de Delito Informático en la Provincia.

Fuentes de Información Secundaria.

Esta técnica se aplicó para tener datos de textos, manuales y otros referentes a la investigación y que fue usada para el desarrollo teórico práctico.

3.6.3 Instrumentos.

Los instrumentos que fueron aplicados en la investigación son los cuestionarios para las encuestas y entrevistas indicados en ANEXOS.

3.6.4 Procedimiento de la Investigación.

Los pasos para la investigación de manera lógica y cronológica

En esta investigación se aplicó un diseño estadístico en función al tipo de investigación, del tamaño de la muestra que representa a toda la población, el tipo de relaciones que establecieron entre la variable dependiente e independiente y el número de indicadores que se relacionan.

Codificación.

La codificación es el reemplazo de respuestas de las encuestas ubicado en las diferentes matrices de datos codificados.

Cuadro de Resultados.

Después de haber concluido con la investigación y determinado las codificaciones de los indicadores,

porcentuales, datos parciales y totales se realizaron cuadros de salida de los resultados que permitan interpretar los resultados finales.

Análisis e Interpretación de Resultados.

Se realizó el análisis e interpretación de resultados una vez que se recopiló toda la información a través de la aplicación de las técnicas de investigación como son las encuestas. Estos resultados se presentan en cuadros.

3.7. Proceso de construcción de la propuesta de solución.

1. Se formuló el problema
2. Se formularon los objetivos
3. Se realizaron las preguntas de investigación,
4. Se elaboró el marco teórico.
5. Se comparó la teoría científica con la práctica mediante encuestas y entrevistas, lo que permitió el análisis, interpretación y discusión de resultados,
6. Finalmente sirvió para elaborar la Propuesta de Reformas Código Penal respecto a los Delitos Informáticos.

CAPITULO IV

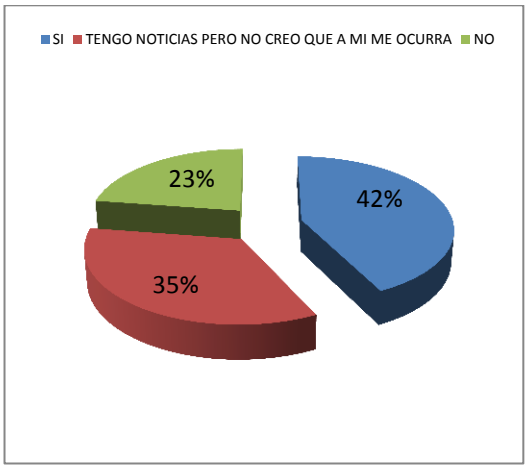
INFORMACIÓN Y RESULTADOS

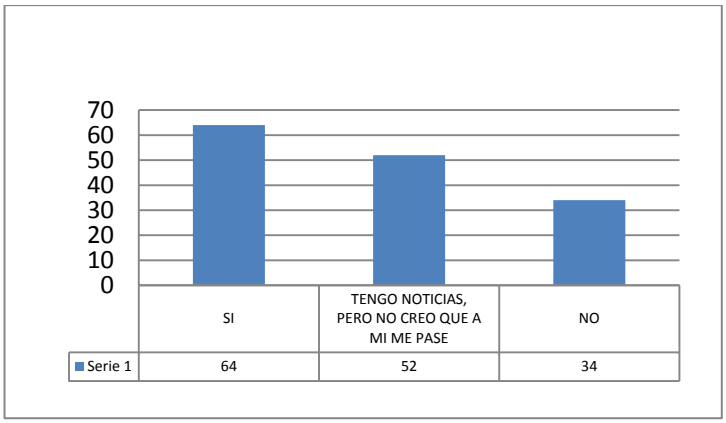
4. 1 Presentación y análisis de la información

La investigación realizada acerca de los Delitos Informáticos en la provincia de Imbabura, dio como resultados altos índices en lo que tiene que ver a algunos tipos de delitos como por ejemplo violación a los datos personales, virus informáticos.

En cuanto a la encuesta dirigida a profesionales en el área informática, estudiantes informáticos, y profesionales en la rama del derecho se presentan los siguientes resultados:

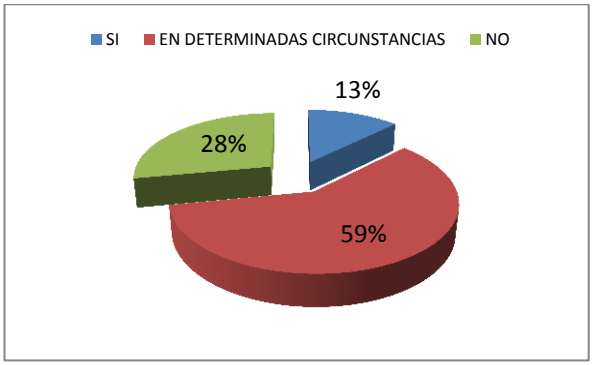
1.- ¿SIENTE SU DERECHO A LA INTIMIDAD VIOLADO EN LAS COMUNICACIONES A TRAVÉS DE INTERNET?

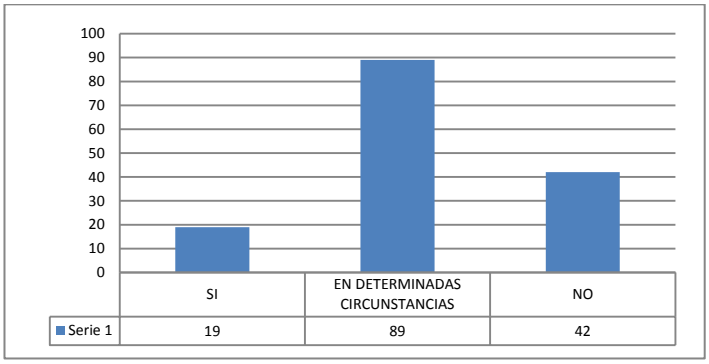




COMENTARIO: De un total de 150 entrevistados el 42% siente que su intimidad ha sido violado por lo que creen que es necesario que se impongan sanciones y que se aplique la Ley como debe ser de igual forma parece que los profesionales en Derecho de la Provincia muy pocos están informados de este tipo de delitos y no saben cómo actuar ni como presentar pruebas si no se cuenta con peritos acreditados en la provincia.

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

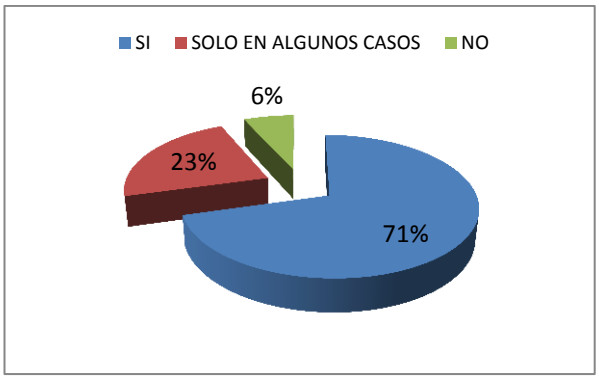


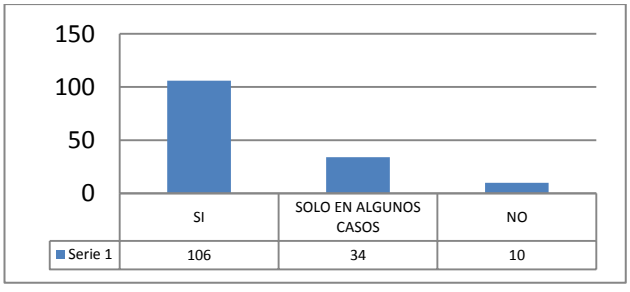


COMENTARIO: Con respecto a esta pregunta si se cree que las compras a través de internet son seguras el 59% creen que en determinadas circunstancias, ya sea por comentarios o noticias que ven en internet o saben que algunas de estas páginas si son seguras ya que poseen códigos de encriptación o métodos de seguridad para que sus transacciones no se vean afectadas pero en la provincia son pocas las personas que han realizado compras por internet.

Por estos antecedentes se puede decir que las personas en la provincia de Imbabura casi no realizan transacciones o envió de información verdadera ya que pueden ser expuestos a algún tipo de violación de la seguridad informática.

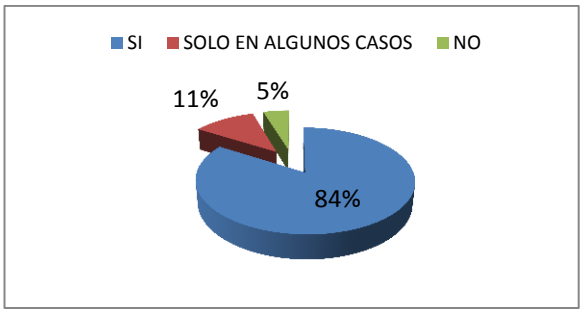
3.- ¿CREE NECESARIA UNA REGULACIÓN PARA INTERNET?

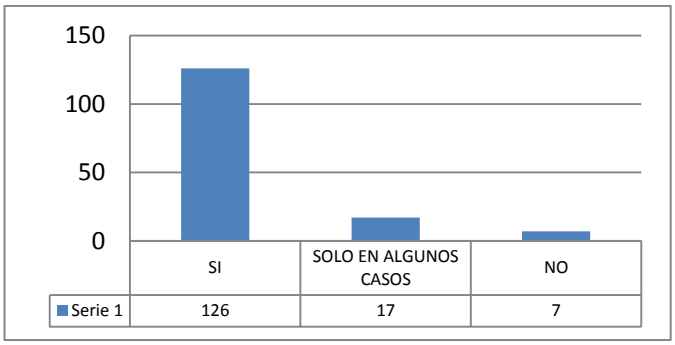




COMENTARIO: La mayoría de las personas opinan que es necesaria una regulación, pero más que eso la aplicabilidad de las leyes existentes creen que sería una buena táctica para sancionar estos delitos.

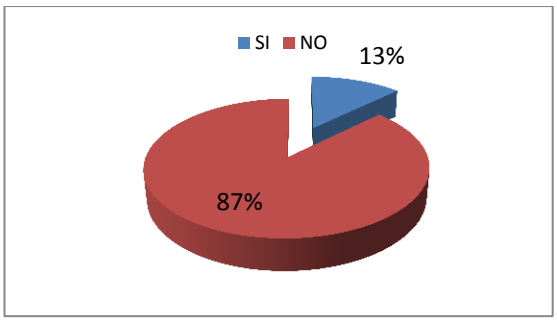
4.- ¿CONSIDERA USTED QUE LA SEGURIDAD A LOS DATOS PESONALES ES UNA CUESTIÓN ALTA PRIORIDAD?

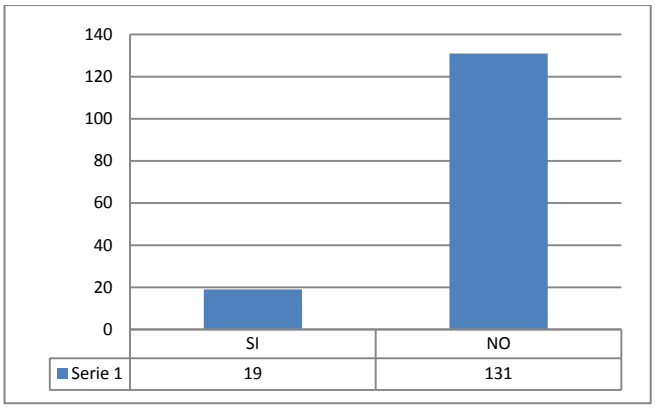




Comentario: según las encuestas realizadas la ciudadanía opina que la seguridad de los personales es de extrema prioridad y que se debe mantener en absoluta reserva cada uno de estos bancos o bases de datos.

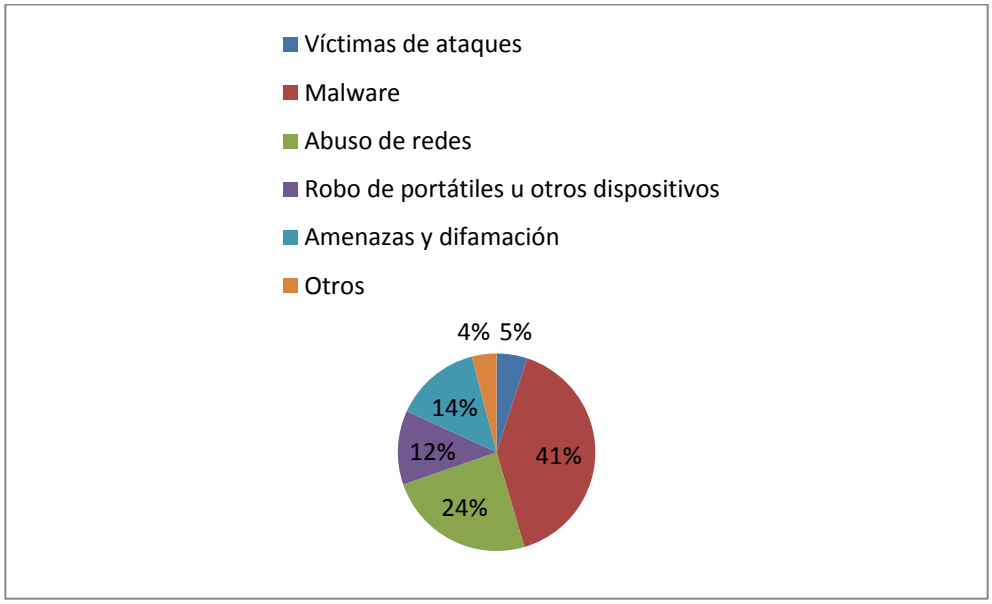
5.- ¿USTED HA SIDO VÍCTIMA DE VIOLACIONES DE LA SEGURIDAD INFORMÁTICA?

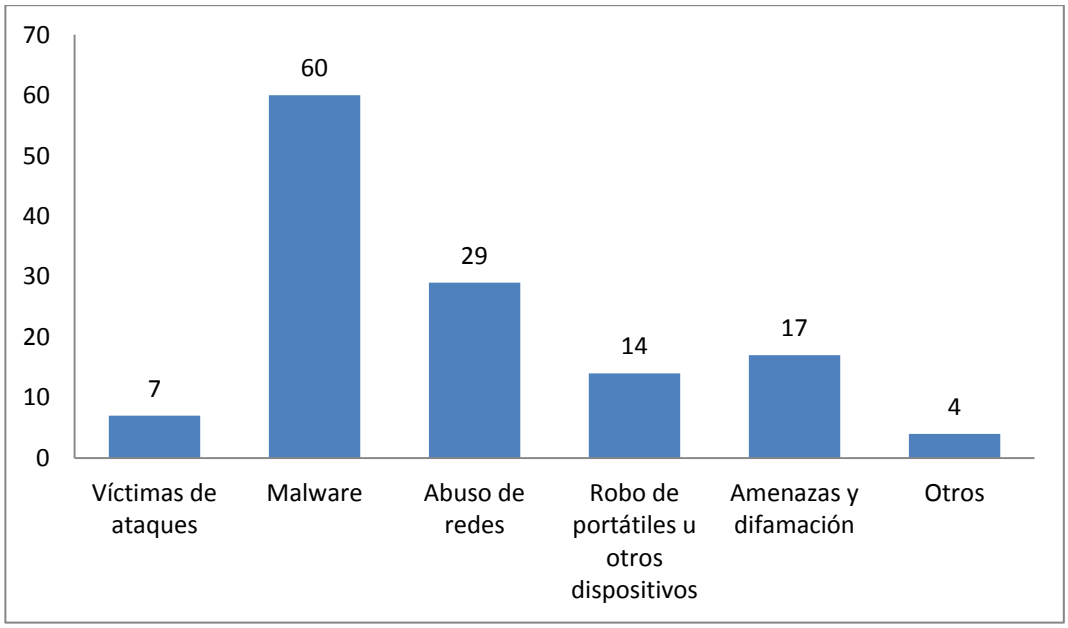




Comentario: en la provincia de Imbabura tenemos aún un porcentaje alto de las personas que no han sufrido de ataques informáticos pero esta, tal vez se da porque no toda la ciudadanía utiliza el internet para realizar transacciones financieras.

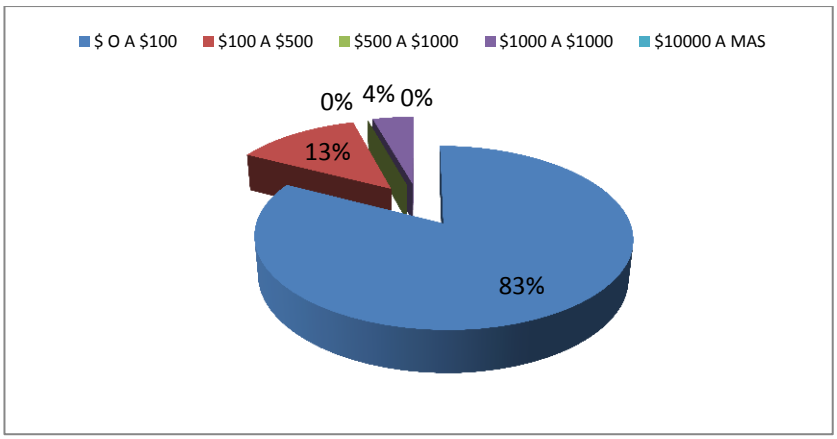
6.- Si la respuesta a la pregunta anterior es Si, ¿Cuáles fueron los efectos de esas violaciones?

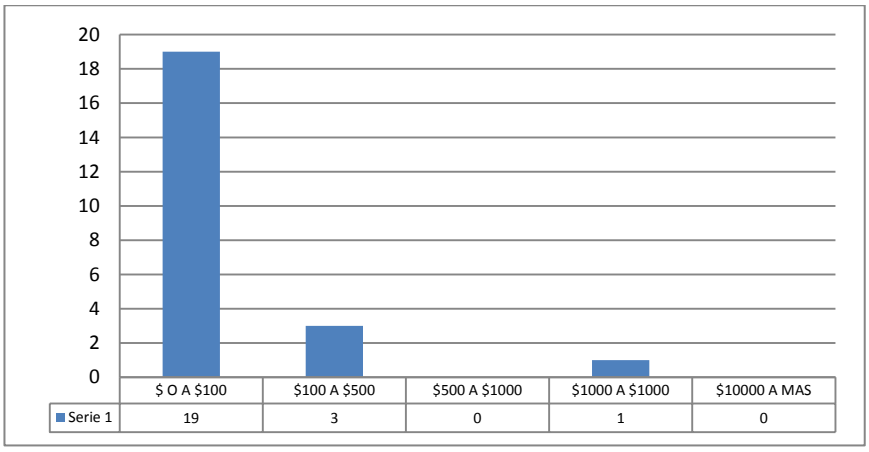




En donde más se encontró violación se la seguridad informática se vio un alto porcentaje en las víctimas de los virus informáticos más novedosos por el hecho de descargar programas que esconden detrás de los programas y búsqueda de información.

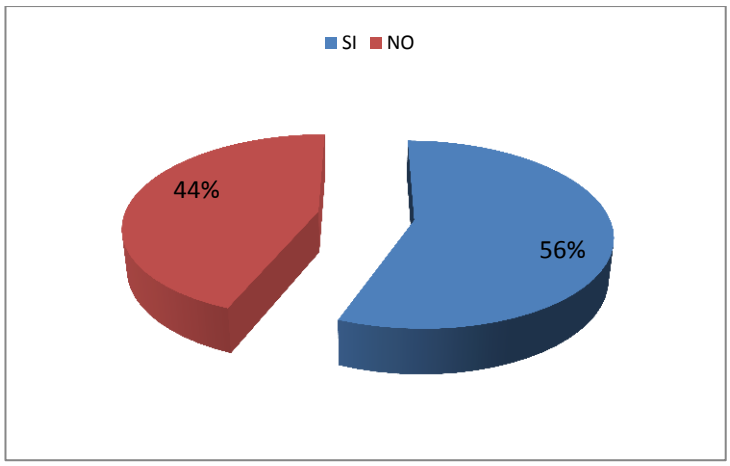
7.- SI, ENTRE LOS EFECTOS ANOTADOS EN LA PREGUNTA 6 SE MENCIONA PÉRDIDAS FINANCIERAS, ¿CUÁL ES EL MONTO APROXIMADO?

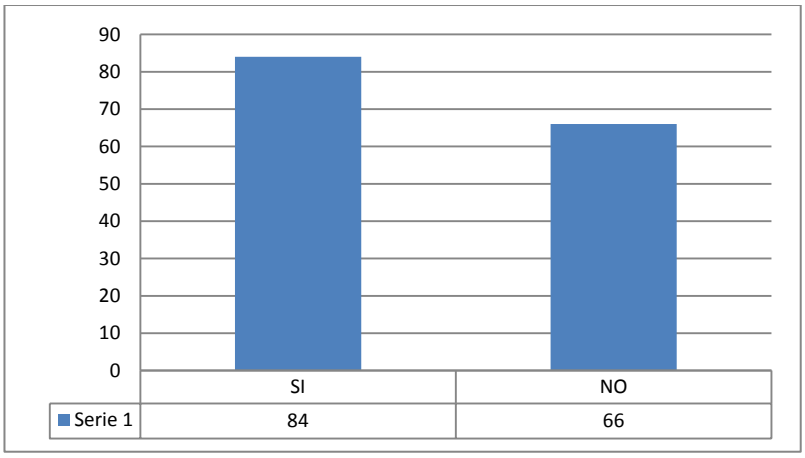




Comentario: De las personas que respondieron Si en la pregunta 6, las pérdidas económicas en nuestra provincia no son tan altas comparadas como las de otras ciudades como Quito y Guayaquil que son las ciudades más grandes de nuestro país.

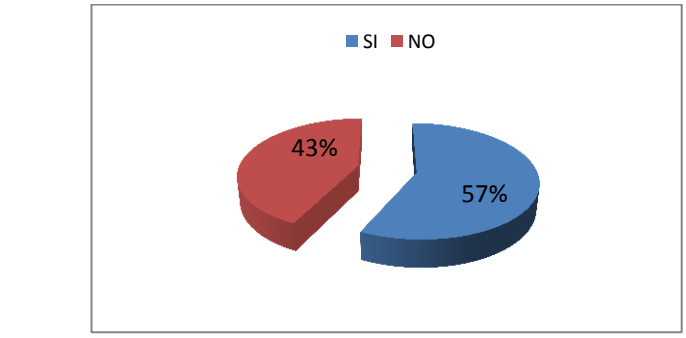
8.- ¿EN LA EMPRESA O ENTIDAD DONDE TRABAJA, SE PRESENTA INCIDENTES DE CARÁCTER INFORMÁTICO?

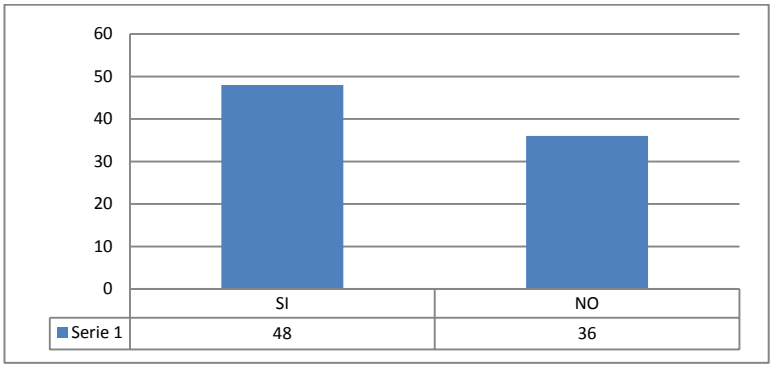




COMENTARIO: A las personas que se les aplico esta encuesta acerca de las entidades donde trabajan si han presentado incidentes de carácter informático casi que la mitad de la población los ha tenido pero esto se debe a la poca información que poseen en unos casos y en otros al abuso del internet por parte de los mismos empleados.

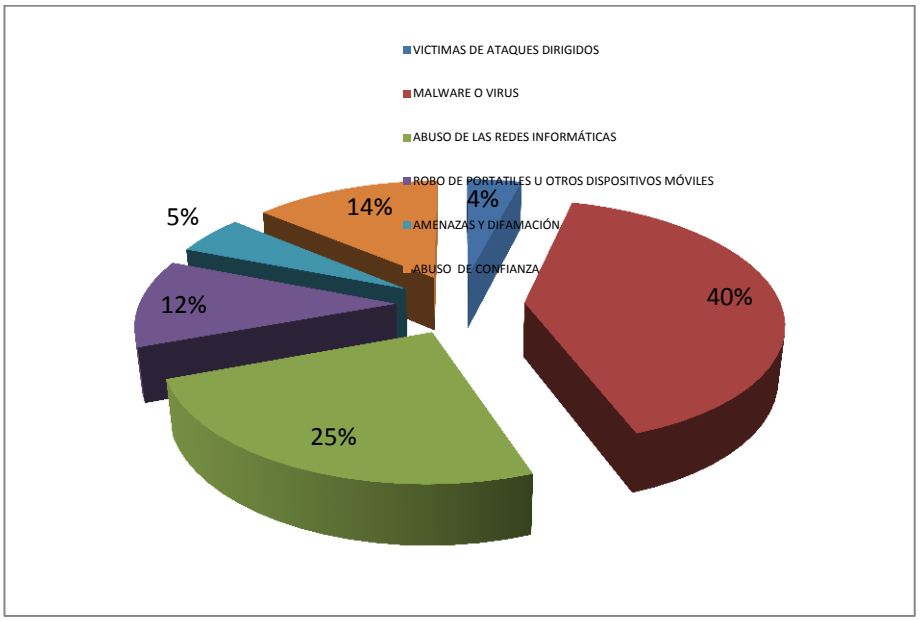
9.- ¿EN CASO DE HABER RESPONDIDO SI EN LA PREGUNTA ANTERIOR, LOS INCIDENTES HAN SIDO PROVOCADOS POR EMPLEADOS INTERNOS DE LA ENTIDAD?

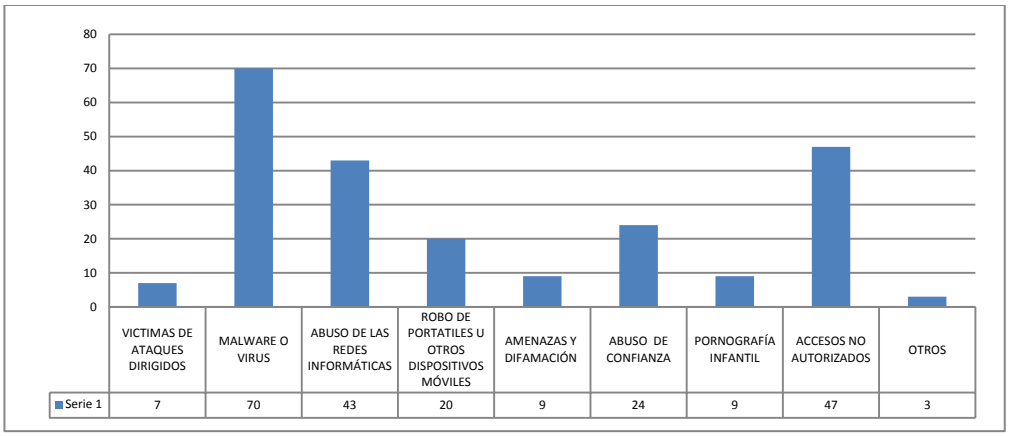




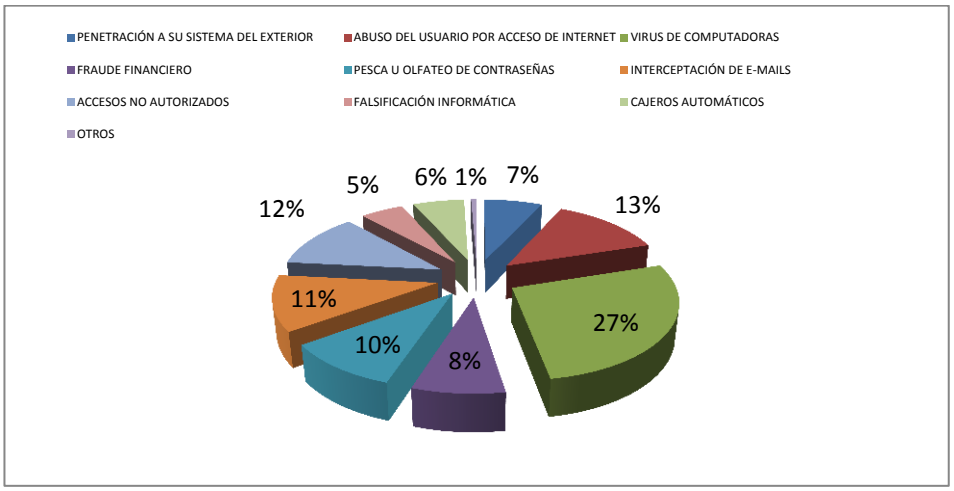
Comentario: De las personas que respondieron Si en la pregunta 8 la mayoría de este tipo de incidentes si han sido provocados por los usuarios de la empresa misma por motivos de desconocimiento y por la facilidad que ahora todo mundo tiene para el uso del internet.

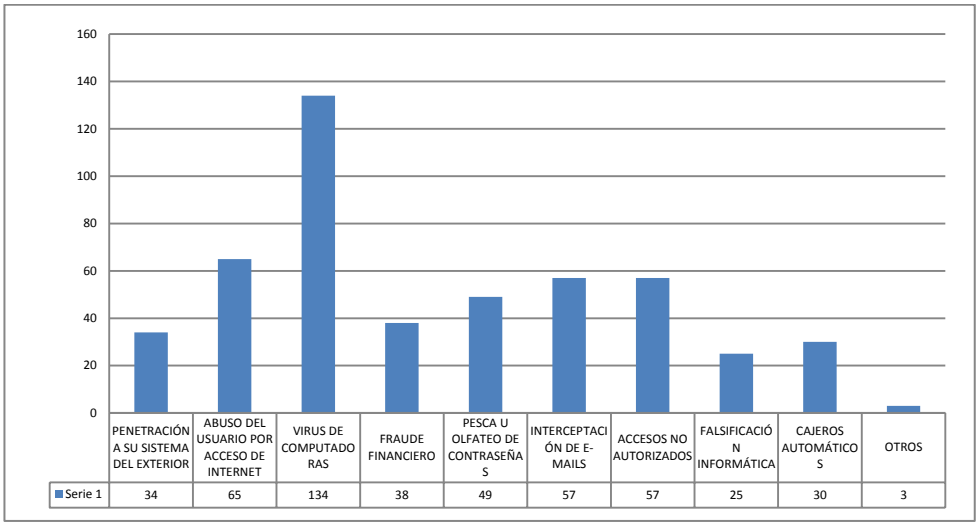
10.- SI SU RESPUESTA A LA PREGUNTA 8, HA SIDO SI, ¿CUÁLES INCIDENTES SE HA PRESENTADO? (SEÑALE LA MÁS IMPORTANTES Y/O FRECUENTES)



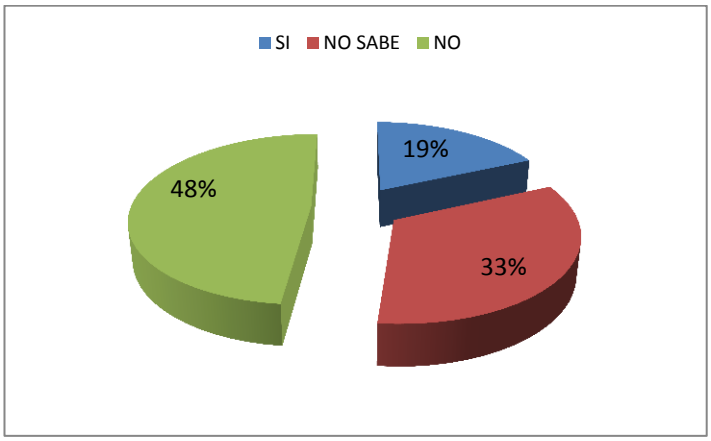


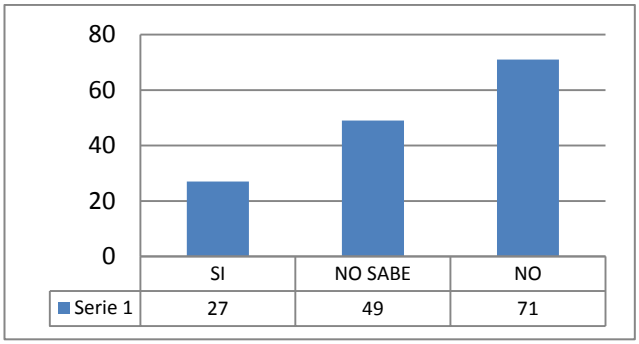
11.- BASADO EN SU EXPERIENCIA CUÁLES SON LOS ATAQUES INFORMÁTICOS MÁS COMUNES. SEÑALE LA MÁS IMPORTANTES Y /O FRECUENTES (Selección Múltiple).



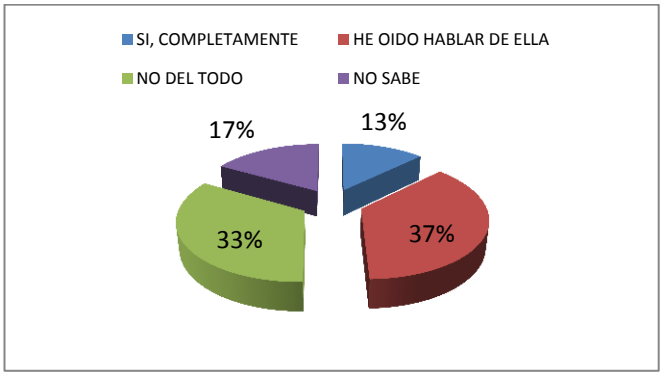


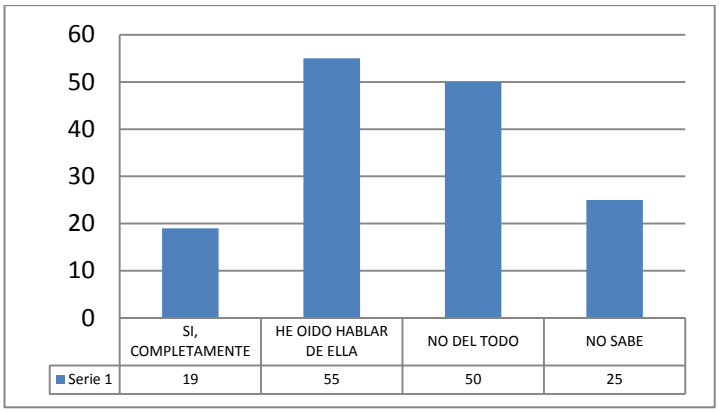
12.- ¿HA SUFRIDO SU ORGANIZACIÓN O SU HOGAR DURANTE EL ÚLTIMO AÑO ALGÚN DELITO INFORMÁTICO?





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





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

4.2. Comprobación de preguntas de investigación.

¿Cuáles son los tipos de delitos informáticos que se presenta en la Provincia de Imbabura?

En la provincia de Imbabura tenemos aún un porcentaje alto de las personas que no han sufrido de ataques informáticos pero ésta tal vez se da porque no toda la ciudadanía utiliza el internet para realizar transacciones. Los delitos informáticos que más se cometen en la provincia de Imbabura son:

Malware o virus: Tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario.

Abuso de las redes informáticas: Mal uso de las redes informáticas de las organizaciones conectadas entre sí por intereses comunes.

Robo de portátiles u otros dispositivos móviles: Los lugares preferidos por los desconocidos para el robo de computadoras portátiles y dispositivos móviles son las afueras de las oficinas y universidades.

Abusos de confianza: Vemos al Internet y a los medios informáticos como si fuera un medio confiable, cuando realmente no lo es.

Accesos no Autorizados: La confianza depositada por un tercero (ingreso indebido), o mediante maquinaciones maliciosas (dolo) que ingresare a un sistema o computadora utilizando una contraseña ajena.

¿Cuáles con los impactos que tiene el delito informático en la vida social y tecnológica de la sociedad?

La seguridad informática de las personas es de extrema prioridad y que se debe mantener en absoluta reserva de cada uno en bancos o bases de datos.

Los impactos sufridos de los delitos informáticos han sido las pérdidas económicas aunque no son tan altas porque oscilan entre 100 y 1000 dólares, y en ellos incluyendo las perdidas físicas entre portátiles y medios digitales.

Los ciudadanos han presentado incidentes de carácter informático porque ha tenido poca información sobre el abuso del internet y de los medios informáticos, los delincuentes han utilizado el correo electrónico y las salas de chat de la Internet para buscar presas vulnerables. Por ejemplo, los aficionados a la pedofilia se han ganado la confianza de niños online y luego concertado citas reales con ellos para explotarlos o secuestrarlos.

Uno de los mayores problemas son los virus por la rápida propagación de los mismos a través de archivos infectados y con el objetivo de alterar el correcto funcionamiento del sistema y, en la inmensa mayoría de los casos, corromper o destruir parte o la totalidad de los datos almacenados en el disco, generalmente se distribuyen a través del correo electrónico, estos suele desconocer la existencia del virus en el archivo que transmite e, incluso, en las

nuevas generaciones de virus, el usuario incluso desconoce que el virus aprovecha su libreta de direcciones y su programa de correo para autorrenviarse.

¿La sociedad y los empresarios en materia del delito informático se encuentran desprotegidos debido a la ausencia de un marco jurídico adecuado?

La legislación ecuatoriana no contiene suficiente jurisprudencia relativa a la tipificación y tratamiento del delito informático. No se tienen muchas noticias y tampoco casos denunciados sobre este tipo de delito, hace que nuestro estudio se encuentra en el rubro de interesante y vital para un mejoramiento de la legislación informática.

Es necesaria una regulación a la legislación, pero más que eso la aplicabilidad de las leyes, que permitan tener una mejor visión del delito informático y los aportes de un modelo jurídico para su tratamiento que serán de gran utilidad, sobre todo hoy en día, cuando la comunicación mediante las redes de la Internet y la computadora se ha vuelto parte de la vida social, publica, económica, cultural y política.

¿Conoce la sociedad los procedimientos para denunciar a los delincuentes informáticos?

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

Es imposible conocer la verdadera magnitud de los delitos informáticos, ya que la mayor parte no son descubiertos o no son denunciados a las autoridades responsables y si a esto se suma la

falta de leyes que protejan a las víctimas de estos delitos; la falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado; 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

CAPITULO V

PROPUESTA

5.1. Situación Actual en la Provincia de Imbabura.

Es preciso considerar que el internet brinda grandes beneficios a los usuarios, pero su fácil acceso también podría perjudicarlos. Según las estadísticas del mes de Junio de 2010de la Superintendencia de Telecomunicaciones en Ecuador, hay alrededor de 2,359,710 usuarios Internet, es decir el 16% de la población, los cuales corren un alto riesgo de ser perjudicados mediante actos delictivos como la ingeniería social, estafa, un ataque de phishing u otros, relacionados con las tecnologías.

Las cifras sobre los delitos informáticos, en Ecuador también son inciertas, las pocas denuncias que se presentan, ya sea por la falta de conocimiento o interés impide la lucha contra este tipo de delitos, y más en una provincia como la nuestra Imbabura, que por el desconocimiento de leyes y reglamentos si son presa de uno de estos delitos no saben que trámite seguir y si hay sanción para cualquiera de los delitos informáticos citados anteriormente, y cabe considerar también que ni los profesionales en área del derecho tienen conocimiento de estas leyes.

De la investigación realizada ha llegado a tener conocimiento la fiscalía de un caso de infracción informática de comercialización de pornografía infantil a través del internet realizado por un individuo conocedor de la informática jurídica ya que de acuerdo al proceso se trata de una Ingeniero en Sistemas, quien ha sido procesado por la Fiscalía y luego se le ha llamado a juicio dentro de la instrucción fiscal seguida en contra de este sujeto, llegando a dictar el Tribunal Segundo de Garantías Penales sentencia en la cual se le impone la pena de 6 años de reclusión menor ordinaria, se dispone la

inhabilitación del sentenciado para el desempeño de todo empleo, profesión u oficio y de conformidad lo dispuesto por el Art.60 del código penal se suspende los derechos de ciudadanía por un tiempo igual al de la condena, debiendo para ellos oficiarse a la dirección provincial de Imbabura, del consejo nacional electoral, una vez ejecutoriada la sentencia, la misma que ha sido apelada a la sala de lo penal de la Corte Provincial de Justicia, quien dicta la sentencia el 17 de noviembre del 2010 confirmando la resolución expedida por el Tribunal de Primer Nivel, actualmente el caso se halla en una de las Salas de lo Penal de la Corte Nacional de Justicia, por haber interpuesto el imputado el recurso de Casación.

También cabe tomar en cuenta que en la Provincia de Imbabura, y específicamente en la ciudad de Ibarra, no cuenta con peritos informáticos acreditados, ya que para este tipo de delito se ha tenido que llamar a peritos de la ciudad de Quito ya que en esta provincia a pesar de contar con profesionales calificados no se han llegado acreditar; y todo esto por el desconocimiento en la parte legal y desinformación.

Es importante considerar los retos particulares que están latentes a todo nivel e incluso para los actores involucrados, en el manejo de los Delitos Informáticos, sean estos el Ministerio Público, la Policía Judicial, la Función Judicial y hasta la misma sociedad.

5.2. Propuesta de Reforma a la Legislación Ecuatoriana que contempla los delitos informáticos.

Debemos considerar la problemática Jurídica, ya que si bien es cierto Ecuador ha iniciado los primeros pasos en la generación de Leyes y Normativas Legales que contemplan aspectos significativos de las nuevas tecnologías y también se han establecido penas en el Código Penal y de Procedimiento Penal,

aún se siente la ausencia de legislación, por parte de la sociedad, que sea precisa y coherente, para el tratamiento de esta nueva modalidad de delincuencia, por ello es necesaria la incorporación de un marco legal que contemple a los delitos informáticos de una manera integral.

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

De allí que consideramos conveniente incluir dentro de este trabajo algunas propuestas con el fin de dar posibles soluciones o respuestas a este grave problema que nos aqueja día a día.

NORMA LEGAL VIGENTE	PROPUESTA DE REFORMA
ARTICULO 202.1 DELITOS CONTRA LA INFORMACION PROTEGIDA.- "El que empleando cualquier medio electrónico, informático o a fin, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto confidencialidad y reserva o simplemente vulnerar la seguridad será reprimido con prisión de 6 meses a 1 año y multa de 500 a 1000 dólares de los estados unidos de Norteamérica"	***ARTICULO 202.1 DELITOS CONTRA LA INFORMACION PROTEGIDA.-***"El que empleando cualquier medio electrónico, informático o a fin, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto confidencialidad y reserva o simplemente vulnerar la seguridad será reprimido con prisión de 1 a 5 años, dependiendo de la gravedad de la información y multa de 1000 a 10000 dólares de los estados

	unidos de Norteamérica, dejando a salvo al agraviado de iniciar la acción de daños y perjuicios, por el monto de la pérdida económica si la hubiere.
“Si la información obtenida se refiere a seguridad nacional o a secretos comerciales o industriales, la pena será de 1 a 3 años de prisión y multa de 1000 a 1500 dólares de los estados unidos de Norteamérica”	Si la información obtenida se refiere a seguridad nacional que afecte los intereses del estado ecuatoriano, la pena será de 25 años de reclusión extraordinaria.
CAPÍTULO V **DE LOS DELITOS CONTRA LA INVIOLABILIDAD DEL SECRETO (CÓDIGO PENAL)** **Art. 197.-** Serán reprimidos con prisión de dos meses a un año y multa de cuarenta a cien sucres, los empleados o agentes del Gobierno y los del servicio de estafetas y telégrafos que hubieren abierto o suprimido cartas confiadas al correo, o partes telegráficos, o que hubieren facilitado su apertura o supresión.	Se debe reformar urgente Código Penal y más tomando en cuenta la época en que fue redactado no se encuentra modernizado en ese sentido y es imperiosa la necesidad de igualar al correo común el correo electrónico. Realizando las siguientes reformas: Sustituir la pena de 1 a 3 años y La multa mínima de 4 salarios unificados. Se debe establecer tipos penales que definan delitos informáticos y mantener los tipos penales ya existentes y agregar paralelamente otros en que el uso o la afectación de una computadora constituyan un

	agravante del delito.

Agregar al Código Penal

A los delitos mencionados en el Código Penal se debe agregar otros como:

““CONDUCTA TIPICA, ANTIJURIDICA Y CULPABLE QUE ATENTE CONTRA EL SOPORTE LOGICO DE UN SISTEMA DE PROCESAMIENTO DE INFORMACION, SEA PROGRAMAS O DATOS RELEVANTES A TRAVES DEL USO NATURAL DE LAS TECNOLOGIAS DE LA INFORMACION.” Que consiste Consiste en el hurto del 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 supe carretera 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.

Tipificar estas infracciones informáticas con el cumplimiento de una pena y una sanción pecuniaria de ser el caso:

1. ***APROPIACIÓN DE INFORMACIONES RESIDUALES.-*** 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.
2. ***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 o empresa determinada.

3. ***LAS PUERTAS FALSAS (TRAP DOORS).-C***onsiste 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.
4. ***LA LLAVE MAESTRA (SUPERZAPPING).-E***s 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

5. ***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.

Los cambios que se deben hacer en la normativa legal de este tipo de delitos es importante saber que existen algunos inconvenientes para el manejo de los delitos informáticos como por ejemplo Falta de la infraestructura y tecnologías adecuada en los entes u organismos de investigación como: el Ministerio Público y la Policía Judicial.

5.2. Proyecto de Ley Reformatoria en Materia Penal

PROYECTO DE LEY REFORMATORIA EN MATERIA PENAL

LA ASAMBLEA NACIONAL

CONSIDERANDO

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

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

Que el numeral 6 del artículo 76 de la Constitución de la República establece, como garantía básica del debido proceso, que la Ley establecerá la debida proporcionalidad entre las infracciones y las sanciones penales,

Que el artículo 82 de la Constitución de la República señala, en forma expresa, que el derecho a la seguridad jurídica se fundamenta en el respeto a la Constitución y en la existencia de normas jurídicas previas ,claras, públicas y aplicadas por las autoridades competentes,

Que el artículo 19 del código Orgánico de la Función Judicial, en su inciso tercero, establece que se propenderá a reunir la actividad procesal en la menor cantidad posible de actos, para lograr la concentración que contribuya a la celeridad del proceso,

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

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

Que es necesario introducir reformas al Código Penal, con la finalidad de asegurar los derechos al debido proceso y a la seguridad jurídica, de conformidad con lo previsto en los artículos 76 y 82 de la Constitución de la República.

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

EXPOSICIÓN DE MOTIVOS

Que en la actualidad las computadoras se usan no solo como herramientas de apoyo a diferentes actividades humanas, sino como medio para conseguir información, es decir, se trata de un nuevo método de comunicación y condiciona su desarrollo de la informática, tecnología que se resume en la creación, procesamiento, almacenamiento y transmisión de datos;

Que la Informática está presente en todos los campos de la vida moderna y que el ser humano se rinde ante la tecnología y utiliza los sistemas de información para ejecutar tareas que en épocas anteriores se realizaban manualmente;

Que el progreso de los sistemas computacionales permiten poner a disposición de la sociedad una cantidad considerable de información de toda naturaleza al alcance de millones de usuarios en aspectos importantes como: científico, técnico y profesional que se puede conseguir a través del internet en minutos o segundos;

Que los progresos mundiales de la computación, el creciente aumento de las capacidad de almacenamiento y procesamiento, la miniaturización de los chips de las computadoras instaladas en productos industriales, la función del proceso de la información con nuevas tecnologías de comunicación así como la investigación en el campo de la inteligencia artificial nos llevan a la era de la información;

Que así como las computadoras han cambiado con la tecnología a la sociedad, también ha sido utilizada como instrumento para cometer actos delictivos, tales como: fraudes, estafas, sabotaje informático, defraudaciones a la propiedad intelectual, robo de servicios, espionaje informático, pinchado de líneas, entre otros ilícitos;

Que es necesario incorporar nuevos hechos delictivos de carácter informático que no se hallan tipificados y sancionados por el Código Penal Ecuatoriano.

AGREGAR ARTICULO INNUMERADO.- USO DE VIRUS (SOFTWARE MALICIOSO)

La persona o personas que produzcan, trafiquen, adquieran, distribuyan, vendan, envíen, introduzcan o extraigan del territorio nacional virus (software malicioso) u otro programa de computación de efectos dañinos será sancionado con una pena de tres a seis años de prisión y con una multa de mil a diez mil dólares americanos. Si el daño producido es a nivel de todo el país la multa será igual al daño producido.

AGREGAR ARTICULO INNUMERADO.- SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES.

Será sancionado quien, con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes. También quien modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, serán sancionados con prisión de dos a cuatro años y con multa de dos a cinco mil dólares americanos.

AGREGAR ARTICULO INNUMERADO.- APROPIACIÓN DE PROPIEDAD INTELECTUAL

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

AGREGAR ARTICULO INNUMERADO.- EXTORSIÓN

El que para procurar un lucro obligare a otro con intimidación o con amenazas graves a tomar una disposición patrimonial perjudicial para sí mismo o para un tercero, valiéndose de cualquier manipulación

informática, telemática, electrónica o tecnológica, será reprimido con prisión de cinco a diez años y con una multa de acuerdo al monto que se benefició de la víctima.

AGREGAR ARTICULO INNUMERADO.- FRAUDE INFORMÁTICO

Son responsables de fraude informático la persona o personas que con ánimo de lucro y valiéndose de cualquier método o medio, alteren, manipulen, o modifiquen el funcionamiento de un programa informático, sistema informático, telemático, o un mensaje de datos para procurarse para sí o para otros un activo patrimonial de otra persona, en perjuicio de ésta o de un tercero, serán sancionados con pena de prisión de uno a cinco años y con multa de 1.000 a 10.000 dólares o con una de estas dos penas.

La pena indicada en el inciso anterior será impuesta al máximo establecido, si la persona que cometiere el delito tipificado en el párrafo anterior, lo comete en razón de su empleo u oficio.

AGREGAR ARTICULO INNUMERADO.- DAÑOS INFORMÁTICOS

Son responsables del delito de daños informáticos, la persona o personas que utilizando cualquier método o medio destruyan, alteren, deteriore, inutilicen, supriman o dañen: datos, bases de datos, programas informáticos, documentos electrónicos o cualquier mensaje de datos contenido en cualquier soporte lógico, sistema informático, o telemático; y serán reprimidas con reclusión menor de tres a seis años y con multa de 3.000 a 15.000 dólares o con una de estas dos penas.

La pena indicada en el inciso anterior será impuesta al máximo establecido, si la persona que cometiere el delito tipificado en el párrafo anterior, lo comete en razón de su empleo u oficio.

AGREGAR ARTICULO INNUMERADO.- DE LA FALSIFICACIÓN INFORMÁTICA

Son responsables de falsificación informática la persona o personas que con ánimo de lucro, o bien para causar un perjuicio a un tercero, utilizando cualquier medio alteren o modifiquen documentos electrónicos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema informático o telemático, ya sea:

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

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

3.- Suponiendo en un acto, la intervención de personas que no la han tenido, o atribuyendo a las personas que han intervenido en él declaraciones o manifestaciones diferentes de las que hubieren hecho.

4.- Faltando a la verdad en la narración de los hechos.

Cualquier alteración, falsificación, simulación, falsa suposición o imputación de un mensaje de datos. Será reprimido con reclusión menor ordinaria de seis a nueve años y multa de 15.000 a 25.000 dólares o con una de estas dos penas.

Si la infracción de falsificación informática es cometida por un funcionario público, la pena será de reclusión menor extraordinaria de 9 a 12 años y multa de 25.000 a 50.000 o con una de estas dos penas y además traerá consigo la inhabilidad permanente de ocupar un cargo público.

AGREGAR ARTICULO INNUMERADO.- DE LA INTRUSIÓN INDEBIDA A LOS SISTEMAS INFORMÁTICOS, DE INFORMACIÓN O TELEMÁTICOS

Son responsables de intrusión indebida a los sistemas informáticos o telemáticos la persona o personas que por cualquier medio o fin y con el

ánimo de apoderarse de la información contenida en dichos sistemas, o para descubrir los secretos comerciales o industriales o bien para vulnerar la intimidad, de una persona natural o jurídica, sin su consentimiento o autorización, interfieran, interrumpan, intercepten o se apoderen de cualquier mensaje de datos.

Serán reprimidos con prisión de uno a cinco años y multa de 1.000 a 10.000 dólares o con una de estas dos penas.

Si la divulgación o la utilización fraudulenta de la información reservada, los secretos comerciales o industriales, han sido obtenidas por alguna de las formas indicadas en el párrafo anterior será sancionada con pena de reclusión menor de tres a seis años y multa de 3.000 a 15.000 dólares o con una de estas dos penas.

Si la divulgación o la utilización fraudulenta de la información reservada, los secretos comerciales o industriales, se realiza por la persona o personas a las cuales se les encomendó su custodia o utilización serán sancionadas con una pena de reclusión menor extraordinaria de nueve a doce años y con multa 25.000 a 50.000 o con una de estas dos penas y además traerá consigo la inhabilidad permanente de ocupar un cargo público o el cargo al cual pertenecía.

AGREGAR ARTICULO INNUMERADO.- RECOPILACIÓN DE INFORMACIÓN NO AUTORIZADA

En caso de que una persona o personas recopilaren por medios fraudulentos datos o información nominativa personal, para después cederla, utilizarla o transferirla a cualquier título sin la autorización de su titular o titulares, serán sancionados con pena de prisión de dos meses a dos años y multa de 200 a 2.000 dólares, o con una de estas dos penas.

CONCLUSIONES

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

2. Debido a la naturaleza 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.

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

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

5. Uno de los problemas de los delitos informáticos, tiene que ver con las diferentes legislaciones en el mundo, y como ya lo hemos visto, un problema global no debe ni puede resolverse con respuestas parciales. Los legisladores deben definir de manera clara e

inmediata los tipos penales necesarios para que estos nuevos Ciberdelincuentes” nacidos bajo la sombra de la falta de legislación sobre el tema y conscientes de su actuar perjudicial y antijurídico, contengan su accionar cumpliéndose de esta manera la principal finalidad del Derecho Penal que es el prevenir los actos delictivos.

RECOMENDACIONES

1. Luego de analizar la realidad de los delitos informáticos en el Ecuador y exponer mecanismos y herramientas existentes para su investigación, se recomienda considerar su implementación por sectores: Gubernamental, Marco Legal, formación, tecnología y sociedad.

2. En base a las recomendaciones a la ciudadanía que nos proporciona la Fiscalía General del Estado se describe algunas de éllas con respecto a las delitos informáticos:

   En cuanto a la Seguridad Informática que se le recomienda a la ciudadanía podemos mencionar las siguientes:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.10 Evite que lo “pesquen” y roben su identidad electrónica, con la cual un delincuente puede tener acceso a sus cuentas de correo, bancos, tarjetas de crédito o su propia computadora y cometer fraudes en su contra. Mediante engaños, usted ingresa a sitios falsos en internet prácticamente iguales a los auténticos, donde sus contraseñas son robadas. Conozca las formas identificadas en que operan estos individuos.

3.11 Usted recibe un correo electrónico donde se indica que su servidor de banca en línea ha sido suspendido por diversas causas y que debe seguir las instrucciones en un “archivo adjunto” para establecerlo. Al momento de ejecutarlos

haciéndole “click”, se instala en su computadora, sin que usted lo note, un programa malicioso que registrará todo lo que usted haga en su equipo, así como todo lo que escriba en el teclado y enviará de manera constante y silenciosa a un sitio donde el delincuente determine fácilmente cuáles son las contraseñas de sus cuentas.

3.12 En otra modalidad, el correo le indica que su institución financiera requiere la confirmación de sus datos y le solicita que acceda a su sitio en internet para “solicitarle” el proceso; se incluye en el mismo correo una liga que lo enviará directamente a él. Ya en el sitio, o bien se ejecuta un programa similar al que describe en el inciso anterior o simplemente al ingresar datos o contraseñas, el delincuente los obtiene de manera instantánea.

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

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

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

3.16 Al salir a la calle, procure no utilizar un maletín muy ostentoso para su computadora portátil o laptop, llévela en una mochila que no denote a todos el contenido. En aviones, guárdele debajo del asiento del frente. Para prevenir olvidos, adquiera una alarma personal para evitar pérdida por parte de niños y ponga en su maletín la contraparte; si usted se aleja comenzará a sonar una alarma. Si requiere llevar a reparar su equipo casero puede camuflarlo metiendo en una funda plástica de una colchoneta forrándolo con una sábana.

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

3.18 En los llamados “hotspots” o ambientes inalámbricos, muy populares ya en lugares públicos y donde usted se puede

conectar con su laptop o agenda electrónica a internet, incluso de manera gratuita, evite acceder a sus cuentas bancarias así como efectuar compras utilizando sus tarjetas de crédito, ya que existe la posibilidad de que la red a la cual usted se conecte, no sea la de un proveedor seguro y los datos enviados, sean interceptados por delincuentes cibernéticos.

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

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

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

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

BIBLIOGRAFÍA

Libros:

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

Revistas:

1. Manual de Autoprotección y Seguridad Ciudadana (2010)
   Dirección Nacional de Política Criminal y la Dirección Nacional de Policía Judicial del Ecuador
2. Revista de Estadísticas Criminales (2009)
   Fiscalía General del Estado del Ecuador
3. Manual de Manejo de Evidencias Digitales y Entornos Informáticos (2009)
   Fiscalía General del Estado del Ecuador

Direcciones Electrónicas:

1. Delitos Informáticos en el Código Penal Español
   http://www.delitosinformaticos.com
2. Delitos Informáticos
   http://www1.lunarpages.com/derechohoy/informatico.htm

3. Problemáticas de la ley sobre Delitos Informáticos
   www.abogadosdetalca.cl
4. Reflexiones sobre los Delitos Informáticos motivadas por los desaciertos de la Ley Chilena"
   http://www.ctv.es/
5. Figuras delictivo - informáticos tipificadas en Chile
   http://www.alfa-redi.org/
6. El Fraude y Los Daños Informáticos
   http://www.delitosinfomaticos.com/
7. Delito de Estafa Informática
   http://www.delitosinfomaticos.com/
8. Los Delitos de Hacking en sus Diversas Manifestaciones
   http://www.alfa-redi.org/

Leyes:

1. Constitución Política De La República Del Ecuador
2. Ley Orgánica de Transparencia y Acceso a la Información Pública
3. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos
4. Ley de Propiedad Intelectual
5. Ley Especial de Telecomunicaciones
6. Ley Orgánica de Control Constitucional
7. Código de Procedimiento Penal y Código de Procedimiento Civil

ANEXO 1

Encuesta dirigida a los Jueces, Fiscales, Tribunales Penales, Abogados en libre ejercicio, Profesionales Informáticos de la Provincia de Imbabura.

La Universidad Técnica del Norte a través del Instituto de Postgrado, ha desarrollado su programa de Maestría en Ciencias Judiciales y ha iniciado el proceso de desarrollo de tesis, como parte de la Titulación de Maestrante y sus opiniones servirán para valorar y analizar la Investigación.

El presente cuestionario que forma parte de la investigación sobre los delitos informáticos, corresponde al trabajo de graduación de la maestría.

Puesto que sus opiniones servirán para analizar y valorar la situación, le agradeceré contestar a las preguntas, según su naturaleza. Marque la(s) opción(es) que corresponda(n) a su criterio.

DATOS PERSONALES:

Profesión:_____

Empresa / Entidad_____

Cargo / Responsabilidad: _____

1.- ¿Siente su derecho a la intimidad violado en las comunicaciones atreves de Internet?

- Si
- Tengo noticias, pero no creo que a mí me ocurra
- No

2.- ¿Considera que las compras a través de Internet son seguras?

- Si
- En determinadas circunstancias
- No

3.- ¿Cree necesaria una regulación para Internet?

- Si
- Solo en algunos casos
- No

4.- ¿Considera Usted que la seguridad a los datos personales es una cuestión alta prioridad?

- Si
- Solo en algunos casos
- No

5.- ¿Usted ha sido víctima de Violaciones a la Seguridad Informática?

- Si
- No

6.- Si la respuesta a la pregunta anterior es si, ¿Cuáles fueron los efectos de esas violaciones?

7.- Si, entre los efectos anotados en la pregunta 6 se menciona pérdidas financieras, ¿Cuál es el monto aproximado?

- $0 a $100
- $100 a $500
- $500 a $1000
- $1000 a $10000
- $10000 o más.

8.- ¿En la empresa o entidad donde trabaja, se presenta incidentes de carácter informático?

- Si
- No

9.- ¿En caso de haber respondido SI a la pregunta anterior, los incidentes han sido provocados por empleados internos de la entidad?

- Si
- No

10.- Si su respuesta a la pregunta 8, ha sido SI, ¿Cuáles incidentes se ha presentado?

Señale las más importantes y/o frecuentes.

Víctimas de ataques dirigidos

Malware o virus

Abuso de las redes informáticas

Robo de portátiles u otros dispositivos móviles

Amenazas y difamación

Abuso de confianza

Pornografía infantil

Accesos no autorizados

Otros: _____

11.- Basado en su experiencia cuáles son los ataques informáticos más comunes:

Señale las más importantes y/o frecuentes.

Penetración a su sistema del exterior.

Abuso del usuario por acceso de Internet

Virus de computadoras.

Fraude financiero

Pesca u olfateo de contraseñas

Interceptación de E-mail

Accesos no autorizados

Falsificación Informática

Cajeros automáticos

Otros: _____

12.- ¿Ha sufrido su organización o su hogar durante el último año algún delito informático?

- Si
- No sabe
- No

13.- ¿Conoce las Leyes del Ecuador que permitan sancionar las infracciones informáticas?

- Si, completamente
- He oído hablar de ella
- No del todo
- No sabe