ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL.

Facultad de Ingeniería en Electricidad y Computación

Maestría en Sistemas de Información Gerencial (MSIG)

"RETOS A SUPERAR EN LA ADMINISTRACIÓN DE JUSTICIA ANTE LOS DELITOS INFORMÁTICOS EN EL ECUADOR"

TESIS DE GRADO

Previa a la obtención del Título de:

MAGISTER EN SISTEMA DE INFORMACIÓN GERENCIAL

Presentado por:

Lcda. Laura Alexandra Ureta Arreaga

Guayaquil - Ecuador

2009

Agradecimiento

Principalmente a Dios por otorgarme la sabiduría y la salud para la culminación de este trabajo y sobre todo por haber tenido la oportunidad de intercambiar ideas con mis amigos y compañeros de la maestría.

Gracias a mi familia y amigos por impulsarme y su especial colaboración durante el desarrollo de este trabajo.

Dedicatoria

Dedico este trabajo con todo mi cariño y amor a León B. Noboa Neira por su apoyo incondicional y constante al permitirme ampliar mis conocimientos y estar más cerca de mis metas profesionales.

Laura Alexandra Ureta Arreaga

Tribunal

_____

Ing. Lenin Freire

Presidente del Tribunal

_____

Ing. Fabricio Echeverria

Director de Tesis

_____ _____

Abg. Rosa Elena Jimenez Ing. Karina Astudillo

Miembro Principal Miembro Principal

Declaración Expresa

La responsabilidad por los hechos, ideas y doctrinas expuesto en este proyecto, nos corresponden exclusivamente; y, el Patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral.

(Reglamento de Exámenes y Títulos Profesionales de la ESPOL).-

_____

Laura Ureta Arreaga

RESUMEN

El presente proyecto tiene como objetivo 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 dicho delitos, así como también identificar los retos y brechas que debe ser superada por el Ecuador para el tratamiento de los mismos.

En el Capitulo 1 se abordará el marco conceptual de los delitos y la criminalidad informática, así como también las leyes relacionadas que se encuentran establecidas en la legislación ecuatoriana.

En el Capitulo 2 se referirá a los peritos, el perfil requerido, los organismos de acreditación, los requisitos solicitados para poder acreditarse, además se abordaran las implicaciones legales y causales para la pérdida de credenciales, e igualmente se abordará las fases del proceso pericial.

En el Capitulo 3, se explican las iniciativas que convergen como propuestas iniciales y recomendaciones externas para el tratamiento de los delitos informáticos, Igualmente se dará una vista de cómo están actuando países de Latinoamérica en tanto a sus regulaciones establecidas para el manejo de dichos actos ilícitos relacionados con la informática.

Por último en el Capítulo 4, se observará los retos a nivel de formación, limitaciones tecnológicas, el marco legal que el Ecuador debe superar para hacer frente a estas conductas delictivas que hacen uso de las nuevas tecnologías.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Esta propuesta de tesis servirá 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 evidencia digital por parte del Perito Informático en el Ecuador.

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 los delitos informáticos en nuestro medio, habilitando y definiendo aspectos legales que permitan la regulación y la tipificación de los delitos informáticos. También es importante identificar de forma general cuáles son los aspectos contemplados en las leyes de los países a nivel latinoamericano que cuentan en su legislación con las leyes que regulan los delitos informáticos.

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 un claro entendimiento de que se requiere en la petición de la pericia, alcance de la pericia, 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.

CAPÍTULO 1

MARCO CONCEPTUAL Y LEGISLACION EN EL ECUADOR.

1.1. Los delitos informáticos.

El progreso tecnológico que ha experimentado la sociedad, supone una evolución en las formas de infringir la ley, dando lugar, tanto a las diversificaciones de los delitos tradicionales como la aparición de nuevos actos ilícitos. Esta situación ha motivado un debate en torno a la necesidad de diferenciar o no los delitos informáticos del resto y de definir su tratamiento dentro del marco legal.

María de la Luz Lima [(1)] indica que el delito electrónico en un sentido amplio es "cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin", y que en un sentido estricto, el delito informático, es "cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin".

Julio Téllez Valdés [2] conceptualiza al delito informático en forma típica y atípica, entendiendo que en la forma típica son "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y la forma atípica "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin".

El Convenio de Cyber-delincuencia del Consejo de Europa [3], define a los delitos informáticos como "los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas redes y datos"

Conviene destacar entonces, que diferentes autores y organismos han manifestado diferentes apreciaciones para señalar las conductas ilícitas en las que se utiliza la computadora, esto es "delitos informáticos", "delitos electrónicos", "delitos relacionados con la computadora", "crímenes por computadora", "delincuencia relacionada con el computador". Tal como podemos notar en las definiciones establecidas por autores anteriores, no existe una definición de carácter universal propia de delito informático, sin embargo, debemos resaltar que han sido los esfuerzos de especialistas que se han ocupado del tema y han expuesto conceptos prácticos y modernos atendiendo entornos nacionales concretos, pudiendo encasillar parte de los temas en esta área de la criminalística. Es preciso señalar que la última definición brindada por el Convenio de Cyber-delincuencia del Consejo de Europa

anota especial cuidado en los pilares de la seguridad de la información: la confidencialidad, integridad y disponibilidad.

El delito informático involucra acciones criminales que en primera instancia los países han tratado de poner 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 imperante de establecer regulaciones por parte de la legislación.

1.1.1. Delincuencia y criminalidad informática

Carlos Sarzana [(4)], describe en su obra "Criminalitá e Tecnología", que los crimines 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, están sujetos 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 que fue lo que llevo al individuo a cometer el delito, mientras que la criminalística según Montiel Sosa [(5)], 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 repunte a los 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[(6)], 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, religiosos, político o de ansias de poder. (Ver Fig. 1.1)

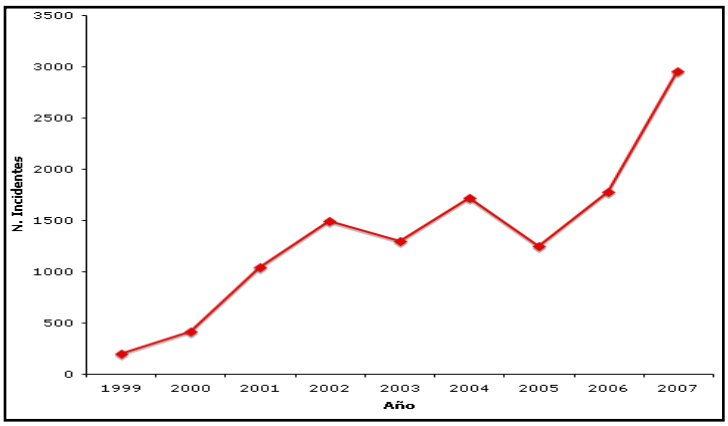

Figura. 1.1. Evolución de incidentes de seguridad
Fuente: REDIRIS – Informe de Evolución de Incidentes de Seguridad 2007.

Otro organismo que realiza investigaciones de este nivel es el CERT [(7)], 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 su 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 (Ver Fig. 1.2)

Figura. 1.2. Estadísticas de Vulnerabilidades
Fuente: CERT – Informe de vulnerabilidades reportadas 2007

Por último Computer Security Institute (CSI) en conjunto con la Oficina Federal de Investigaciones (FBI) [8], 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 (Chief Information Officer), CEOs (Chief Executive Officer), CISOs (Chief Information Security Officer), Oficiales de Seguridad y Administradores de Sistemas.

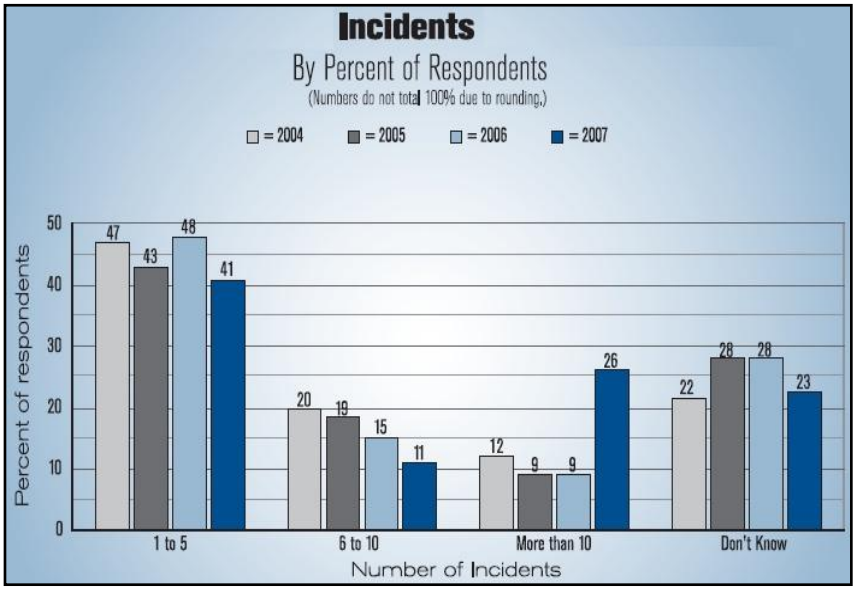

Figura. 1.3. Incidentes ocurridos en el 2007
Fuente: CSI 2007 – Computer Crime and Security Survey

En la Figura 1.3 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 Mas de 10 ataques.

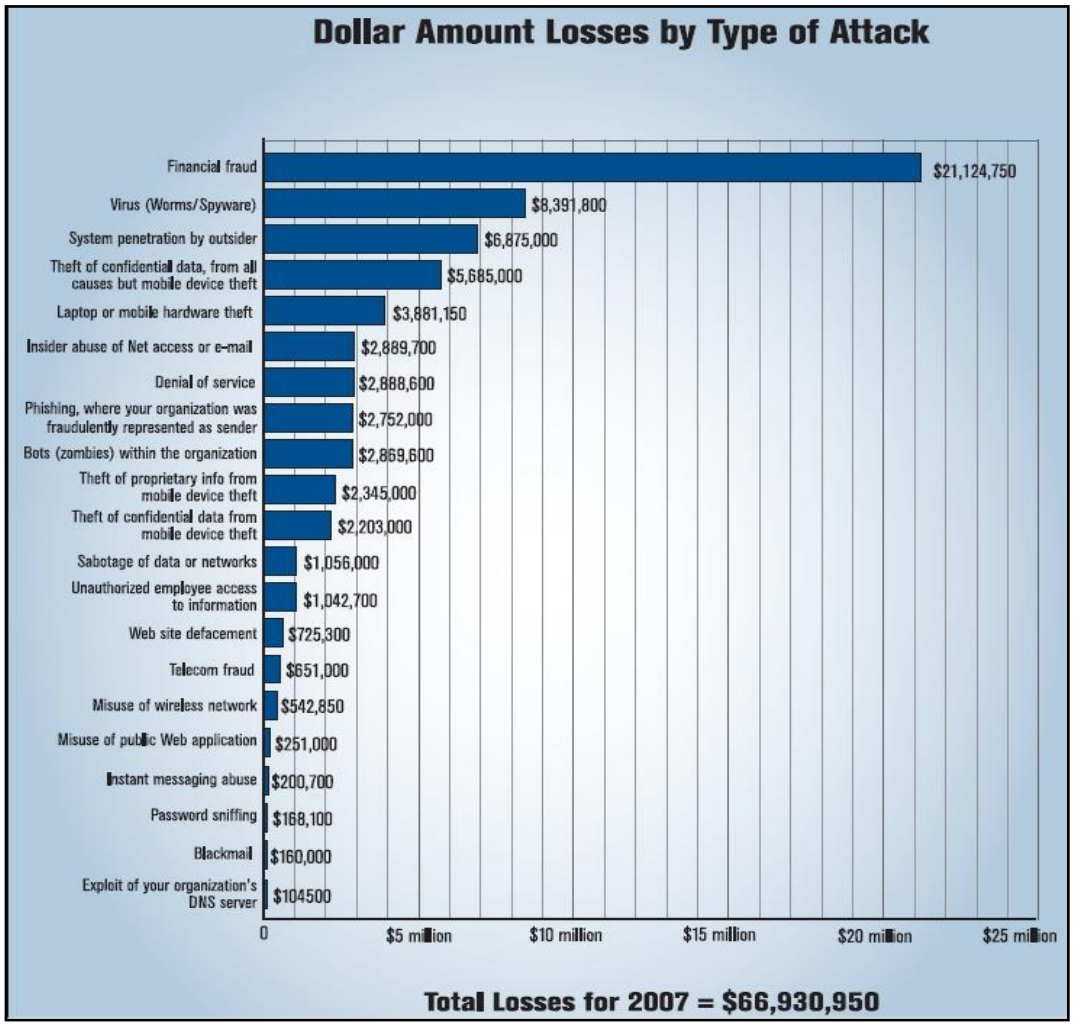

Figura. 1.4. Costos de incidentes por tipo de ataque
Fuente: CSI 2007 – Computer Crime and Security Survey

El total de 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 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.

1.1.2. Tipos de delitos informáticos

La tipificación o clasificación de los delitos procura, salvaguardar los bienes jurídicos. Los bienes jurídicos son intereses relevantes de las personas en tantos sujetos sociales, considerados especialmente valiosos, dignos de protección penal frente a conductas que los dañen o ponen en peligro, entonces por ejemplo: con respecto al delito del hurto, el bien jurídico es la propiedad; en caso del delito de homicidio el bien jurídico protegido es la vida; y, en el caso de las nuevas tecnologías el bien jurídico protegido es la información.

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

Reconocidos por la Naciones Unidas **Fuente: Organización de Naciones Unidas**	**Abogados especializados en delitos informáticos** **Fuente: http://informática-jurídica.com**
Fraudes mediante la manipulación de computadoras (programas, datos de entrada y salida, repetición automática de procesos	Fraudes mediante la manipulación de computadoras: 1. Delitos contra elementos físicos – Hardware (robo, estafa) 2. Delitos contra elementos lógicos (daños, accesos ilícitos a sistemas, acceso ilícito a datos, protección de programas.
Falsificaciones informáticas (alteración de documentos, falsificación de documentos	
Daños o modificaciones de programas o datos computarizados (sabotaje, virus, bombas lógicas)	Delitos cometidos a través de sistemas informáticos: 1. Estafas 2. Apoderamiento de dinero por tarjetas de cajero 3. Uso de correo electrónico con finalidad criminal 4. Utilización de internet como medio criminal
Accesos no autorizados a servicios y sistemas informáticos (piratas, reproducción no autorizada	

Tabla 1.1. Tipificación de delitos informáticos.

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

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.

1.1.3. 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 desvirtuación 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 de delito informático.

1.1.3.1 La evidencia digital

Así como se han establecido diferentes definiciones para los delitos informáticos, se han establecido diferentes y especiales consideraciones para su principal y especial insumo que es la evidencia digital.

De acuerdo a la conceptualización de Eoghan Casey [(9)], "la evidencia digital es un tipo de evidencia física. Esta construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales".

Miguel López Delgado [10], define la evidencia digital como el conjunto de datos en formato binario, esto es, comprende los ficheros, su contenido o referencia a estos (metadatos) que se encuentran en los soportes físicos o lógicos del sistema vulnerado o atacado.

Según Jeimy J. Cano M. [11], la evidencia digital es la materia prima para los investigadores, donde la tecnología informática es parte fundamental del proceso. La evidencia digital posee, entre otros, los siguientes elementos que la hacen un constante desafío para aquellos que la identifican y analizan en la búsqueda de la verdad: Es volátil, es anónima, es duplicable, es alterable y modificable, es eliminable. Estas características advierten sobre la exigente labor que se requiere por parte de los especialistas en temas de informática forense, tanto en procedimientos, como en técnicas y herramientas tecnológicas para obtener, custodiar, revisar, analizar y presentar la evidencia presente en una escena del delito. Además, revela con respecto al tratamiento de la evidencia digital, que se debe guardar especial cuidado a: su debido registro, admisibilidad, valor probatorio, preservación transformación y recuperación.

Con estos argumentos, la evidencia digital, es un insumo de especial cuidado, para el proceso de investigación de delitos informáticos, que debe ser tratada por parte de los especialistas, tratando de conservar todas las medidas de precaución necesarias para no contaminarla y que sea objeto de desestimación ante un proceso litigioso.

1.1.3.2 La informática forense

El FBI [(12)], 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.

Gerberth Adín Ramírez [(13)], identifica los objetivos de la informática forense con el fin de: perseguir y procesar judicialmente a los criminales; crear y aplicar políticas para prevenir posibles ataques y de existir antecedentes evitar casos similares; compensar daños causados por los criminales o intrusos.

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 relacionas con las tecnologías de la información y las comunicaciones, entre los que se tienen la piratería de software, distribución pornográfica infantil, tráfico de bases de datos, etc.

Adicionalmente, el desarrollo de la ciencia de la informática forense, es una técnica utilizada por los especialistas durante el proceso de investigación de los llamados delitos informáticos.

El análisis forense digital, según Miguel López Delgado [14], 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 determinado caso pueden ser aceptadas legalmente en un proceso judicial". Para esta ciencia se han identificado las fases que se consideran de relativa importancia ante un proceso de análisis forense:

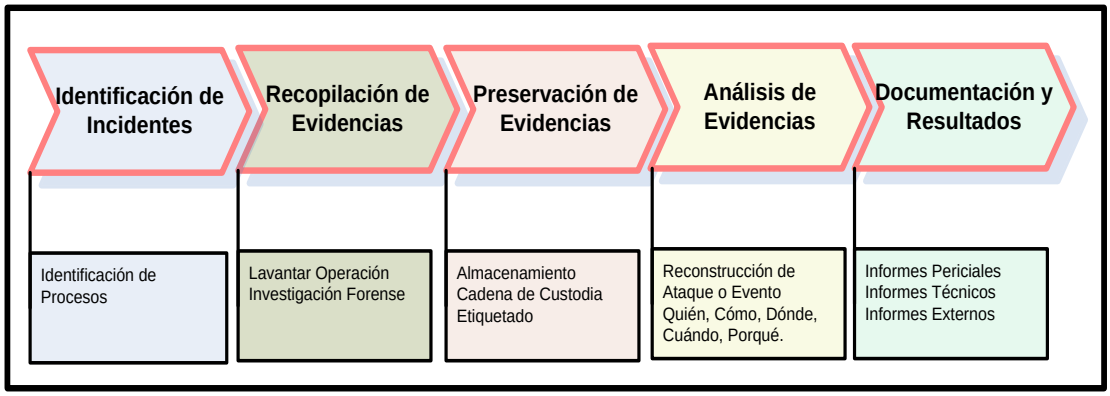

Figura. 1.5. Fases del Análisis Forense Digital

Fuente: Miguel López Delgado - Análisis Forense Digital

1.1.3.2.1 Identificación de incidentes

En ésta primera fase se debe asegurar la integridad de la evidencia original, es decir, que no se deben realizar modificaciones ni alteraciones sobre dicha evidencia, en este aspecto tratar 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. Por ejemplo, entre las principales actividades durante esta fase se deben consultar los registros del sistema, en busca de avisos de fallos, accesos no autorizados, conexiones fallidas, cambios en archivos específicos del sistema.

1.1.3.2.2 Recopilación de evidencias digitales

Si mediante los hallazgos del proceso de identificación de incidencias 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 esta actitud 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.

Hay que asegurarse de llevar un registro de cada unos de los pasos realizados y características o información de los hallazgos encontrados, es imprescindible tratar de obtener la mayor cantidad de información posible, así como también, es recomendable que durante el desarrollo de este proceso, lo asista u acompañe una persona, preferentemente imparcial, la misma que actuaría como testigo de dichas acciones y procedimientos realizados.

Durante esta fase, es recomendable utilizar una técnica o metodología de recolección de evidencias, para ello, el profesional debe hacer uso de prácticas o metodologías que sean reconocidas y que sobretodo puedan ser reproducidas o replicadas, bajo el mismo contexto del escenario presente.

Para la recolección de evidencias se dispone de marcos de trabajo de distribución libre que han sido desarrollados tomando en cuenta las mejores prácticas. A continuación la siguiente tabla lista algunas de las guías de reconocimiento mundial, para la recolección de evidencias en computación forense:

GUIA	PATROCINADOR	DISTRIBUCION
RFC 3227 - Guía para recolectar y archivar evidencia	Network Working Group http://www.ietf.org	Libre
Guía IOCE - Guía de mejores prácticas en el examen forense de tecnología digital	International Organization on Computer Evidence http://www.ioce.org	Libre
Guía DoJ1 - Investigación en la escena del crimen electrónico	U.S. Department of Justice http://www.usdoj.gov	Libre
Guía DoJ2 - Examen forense de evidencia digital	U.S. Department of Justice http://www.usdoj.gov	Libre
Guía Hong Kong Computación forense – Parte 2 – Mejores Practicas	SWGDE - Scientific Working Group on Digital Evidence http://www.swgde.org/	Libre
Guía Reino Unido - Guía de Buenas prácticas para evidencia basada en computadoras	ACPO - Association of Chief Police Officers http://www.acpo.police.uk/	Libre
Guía Australia - Guía para el manejo de evidencia en IT	Estándar Australiano http://unpan1.un.org	No libre

Tabla 1.2. Guías de mejores prácticas de computación forense.

1.1.3.2.3 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 manipulen la evidencia digital, Se requiere preparar un documento en el que se lleve el registro (nombres, fechas, custodios, lugar de almacenaje, transporte, entre otros.), y los datos personales de todos los implicados en el proceso de manipulación de copias, desde su proceso de obtención hasta su proceso de almacenamiento (Ver ANEXO 1 – Formulario de Cadena de Custodia de Evidencia Digital).

1.1.3.2.4 Análisis de la evidencia

Luego de que ya se ha 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.

Dicho análisis debe resultar respondiendo las interrogantes de cómo se produjo el ataque, quienes lo llevaron a cabo, bajo que circunstancia se produjo y cuál era su objetivo, igualmente se deben identificar cuáles fueron los daños que se causaron.

1.1.3.2.5 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 deban 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 (CPP) del Ecuador El informe pericial contendrá 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 de que en el caso de que hubiesen desaparecido los vestigios de la infracción, los peritos (Ver el Capítulo 2 – El perito y el peritaje informático) opinaran, en forma debidamente motivada sobre si tal desaparición ha ocurrido por causas naturales o ratifícales.

Es imprescindible destacar que existen en el mercado soluciones de software que permiten realizar el análisis forense de evidencias digitales entre los cuales de destacan los siguientes:

SOFTWARE	SISTEMA OPERTIVO	FUNCIONES/HERRAMIENTAS
WINHEX	Window	Informática forense, recuperación de archivos, peritaje informático, procesamiento de datos de bajo nivel y seguridad informática
HELIX Live Forensics	Linux	Respuesta a Incidentes y herramientas forenses.
ENCASE	Windows, Linux, AIX, Solaris, OS X	Manejo de evidencias y herramientas forenses

Tabla 1.3. Soluciones de Software Forense.

1.1.3.4 La auditoria informática

Otro procedimiento del cual hacen uso los especialistas informáticos, durante el proceso de investigación es la auditoria informática, técnica sobre la cual se han desarrollado un sinnúmero de marcos de referencia y mejores prácticas para su correcta aplicación que es utilizada generalmente para la prevención y detección de fraudes de una manera especializada.

Esta rama también ha desarrollado la auditoria forense, la cual es conceptualizada por Pedro Miguel Lollet [(15)], como “el uso de técnicas de investigación criminalística, integradas con la contabilidad, conocimientos jurídicos procesales, y con habilidades en finanza y de negocio, para manifestar información y opiniones como pruebas en los tribunales”. Este es un proceso estructurado donde intervienen contadores, auditores, abogados, investigadores, informáticos entre otros.

1.2. 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 mostrará cual es la estructura general de dichas regulaciones, para ello, se toma como referencia la Pirámide Kelseniana [(16)]. El cual es un recurso que permite ilustrar, la jerarquía de las normas jurídicas:

Figura. 1.6. Jerarquía de Leyes – Pirámide de Kelsen.

Desde los años ochenta, las Naciones Unidas han venido promoviendo por medio de la Uncitral (CNUDMI – Comisión de las Naciones Unidas para el Derecho Mercantil Internacional) una adecuación de las diferentes legislaciones mundiales a sus leyes modelos, entre los documentos aprobados por dicha comisión están, por ejemplo: la Ley Modelo sobre Comercio Electrónico [(17)] y la Ley Modelo sobre Firmas Electrónicas [(18)].

En Sudamérica, el primer país que se preocupó por estos temas fue Colombia, ya que en 1999 publica su ley 527, la misma que regula el comercio electrónico, firmas digitales y las entidades de certificación, luego en el mes de mayo del año 2000 Perú publica la ley 27269, sobre Ley de Firmas y Certificados Digitales. Luego, le siguen en el 2001 Argentina y Venezuela en el año 2001, luego Chile y Ecuador en el año 2002.

Gerberth Adín Ramírez Rivera [(19)], expresa "para que todo lo realizado en la informática forense sea exitoso, es necesario que se tengan regulaciones jurídicas que penalicen a los atacantes y que pueda sentenciárseles por los crímenes cometidos. Cada país necesita reconocer el valor de la información de sus habitantes y poder protegerlos mediante leyes. De manera que los crímenes informáticos no queden impunes".

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, tales como:

1) Ley Orgánica de Transparencia y Acceso a la Información Pública.
2) Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
3) Ley de Propiedad Intelectual.
4) Ley Especial de Telecomunicaciones.

5) Ley de Control Constitucional (Reglamento Habeas Data).

1.2.1. 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 se señala 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.

De acuerdo a un estudio realizado por el Grupo Faro [(20)], en marzo del 2007. Los Ministerios Ecuatorianos cumplen, en un promedio del 49% de lo dispuesto en la Ley Orgánica de Transparencia y Acceso a la Información.

Otro organismo que vigila, analiza, realiza controles permanentes y se encarga del cumplimiento de la Ley Orgánica de Transparencia y Acceso a la Información Pública, es la Defensoría del Pueblo, quienes a través de un informe, publicado en el Diario El Telégrafo [21], del 27 de octubre del 2008, revelaron los siguientes datos con respecto del monitoreo de la ley:

1. De 380 instituciones públicas, 291 cumplen publicando su información de acuerdo a lo dispuesto en la Ley.
2. A 89 instituciones se les notificó para que cumplan con la Ley.
3. 72 instituciones solicitaron una prórroga para completar y cumplir con las disposiciones de la Ley.
4. 70 instituciones cumplieron luego de haber recibido la notificación.
5. 17 instituciones no remitieron ninguna respuesta acerca de la notificación.
6. 12 instituciones respondieron la notificación indicando que las páginas se encuentran en fase de construcción.
7. Por último 7 instituciones no cumplen con las disposiciones de la Ley.

El mismo informe revela que en el caso de la Provincia del Guayas la Defensoría del Pueblo suscribió un convenio con Participación Ciudadana que promueve el cumplimiento de la Ley, el cual inicio el mes de junio del 2008.

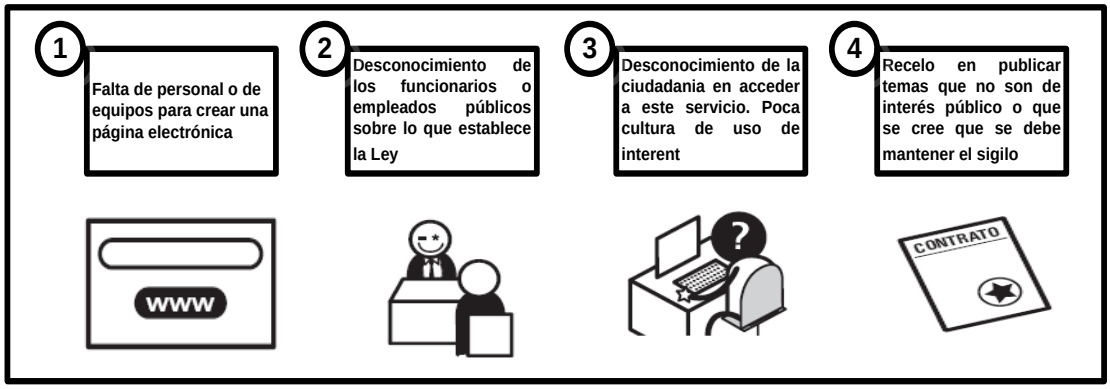

Figura. 1.7. Factores que inciden en la poca información pública
Fuente: Defensoría del Pueblo / Grafico Diario El Telégrafo

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

La Ley de Comercio Electrónico, Firmas Digitales y Mensaje de Datos (LCElec.) 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 de Comercio Electrónico, Firmas Digitales y Mensaje de Datos está conformada por cinco títulos conteniendo cada uno varios capítulos y artículos

1) Título Preliminar.
2) De las Firmas electrónicas, certificados de firmas electrónicas, entidades de certificación de información, organismos de promoción de los servicios electrónicos, y de regulación y control de las entidades de certificación acreditadas.
3) De los servicios electrónicos, la contratación electrónica y telemática, los derechos de los usuarios, e instrumentos públicos.

4) De la prueba y notificaciones electrónicas.
5) De las infracciones informáticas.

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.

Como punto esencial, se establece que la firma electrónica tendrá validez cuando conste como un requisito de legalidad documental. Además se protege las bases de datos creadas u obtenidas por transmisión electrónica de un mensaje de datos, concediendo al titular de dichos datos el poder para autorizar la disposición de su información, sea que dichos datos fueron obtenidos como usuario de un servicio o sea que fueron obtenidos en el intercambio de mensajes de datos. Se ratifica la defensa legal mediante el Derecho Constitucional de Habeas Data.

Se busca que especialmente en los negocios relacionados con el comercio electrónico las notificaciones sean por medio de correo electrónico, estableciéndose obligatoriedad de notificar por éste medio y por el tradicional para el caso de resoluciones sometidas a Tribunales de Arbitraje. El documento electrónico será considerado como medio de prueba con todos sus efectos legales. Para que existan presunciones legales sobre la veracidad de un documento, éste deberá cumplir los principios de integridad e identidad, para justificar la voluntad contractual de obligarse por dicho documento. Aquella parte que niegue la validez de un documento electrónico deberá probar que este no cumple con los requisitos técnicos mencionados anteriormente. Se establecen varios requisitos para la correcta aplicación de la prueba en estos casos, entre ellos señalamos:

1) La presentación de los soportes necesarios en papel del documento electrónico y los mecanismos para la lectura y verificación de la firma.
2) La presentación del certificado validado por un proveedor de servicios de certificación.
3) Los demás mensajes de datos deberán guardar especial atención con la integridad de su contenido. Las pruebas serán juzgadas y valoradas de acuerdo con “la seguridad y fiabilidad con la cual se la verificó, envió, archivó y recibió”. Para una mejor apreciación de la prueba el juzgador contará con el asesoramiento de un perito en la materia, es decir un perito informático.

El organismo facultado para autorizar a las entidades de certificación de información es el Consejo Nacional de Telecomunicaciones, según lo dispuesto en la Ley de Comercio Electrónico, Firmas Digitales y Mensaje de Datos y el Reglamento expedido por el Presidente de la República, mediante Decretos Ejecutivos 3496 (31 de julio del 2002) y 1356 (29 de Septiembre del 2008) en los que se establecen el modelo de Resolución para la Acreditación como Entidad de Certificación y Información y Servicios Relacionados, tal como lo establece el Art. 29 del Capítulo II de la ley (Ver ANEXO 2 – Modelo de Acreditación Entidad de Certificación de Información y Servicios Relacionados).

Las funciones y responsabilidades otorgadas por el Consejo Nacional de Telecomunicaciones, a las entidades de certificación de información y servicios relacionados, es que dichas entidades se encargan de la generación, gestión, administración, custodia y protección de las claves y los certificados de firma electrónica, así como la validación de la identidad e información de los usuarios o solicitantes de firmas electrónicas, mediante el uso de infraestructura y recurso humano capacitado para operar dicha infraestructura con absoluta pericia y confidencialidad. Uno de los organismos que obtuvo la autorización del Consejo Nacional de Telecomunicaciones como Entidad de Certificación es el Banco Central del Ecuador para emitir certificados a personas naturales, jurídicas y funcionarios públicos (Ver ANEXO 3 – Formularios de Certificados PKI – Banco Central del Ecuador)

1.2.3. Ley de Propiedad Intelectual

La Ley de Propiedad Intelectual (LPInt.), 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.

Dar a conocer la importancia que tiene la Propiedad Intelectual en el Ecuador y su debida aplicación en los sectores económico, industrial, intelectual y de investigación, debe ser tarea no sólo del profesional del derecho, sino de los industriales y empresarios, de las instituciones públicas y privadas, de los centros superiores de estudios e inclusive del propio estado ecuatoriano.

Conocer la propiedad intelectual es también conocer, que uno de los principales problemas que enfrenta esta rama del derecho moderno, es la piratería y falsificación

de las obras del intelecto humano, las cuales traen graves consecuencias económicas y sociales; a más de los perjuicios de los titulares de derechos de propiedad intelectual, pues esta pérdida no solo afecta a los fabricantes de los productos falsificados, sino a la reducción de ingresos tributarios e inclusive la pérdida de empleos, debido a los efectos negativos resultantes de la mano de obra clandestina, de las labores creativas y de investigación, perjudicando la vitalidad cultural y económica de un país.

Es importante resaltar que la ley incluye en su codificación la protección de bases de datos que se encuentren en forma impresa u otra forma, así como también los programas de ordenador (software) los cuales son considerados como obras literarias.

El estudio de piratería mundial de software [(22)], que corresponde al año 2007, realizado por la International Data Corporation (IDC), publicado por la Business Software Alliance, establece que Ecuador mantiene una tasa de piratería de un 66%, que constituyen pérdidas por aproximadamente 33 millones de dólares y representan un incremento del 10% con respecto a la última medición (30 millones de dólares). Las iniciativas dadas para la protección y respeto de las especificaciones de la Ley de Propiedad Intelectual, así como los Derechos de Autor se han desarrollado por campañas de la Business Software Alliance (BSA) tales como "Marca el Límite", "Anímate 2007", "Buenos Negocios", "Evite riesgos, use software legal" como acciones puntuales que impulsan el uso de software legal. Otro proyecto impulsado

por la BSA es la habilitación del portal "Reporte confidencial sobre piratería de software", que permite denunciar de manera confidencial la piratería del software en América Latina.

1.2.4. 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.

La Ley Especial de Telecomunicaciones tiene por objeto normar en el territorio nacional la instalación, operación, utilización y desarrollo de toda transmisión, emisión o recepción de signos, señales, imágenes, sonidos e información de cualquier naturaleza por hilo radioelectricidad, medios ópticos y otros sistemas electromagnéticos.

1.2.5. Ley Orgánica de Control Constitucional

La Ley Orgánica de Control Constitucional (LOCConst.), fue publicada en el Registro Oficial N° 99 del 2 de Julio de 1997 y fue calificada con Jerarquía y carácter

de Ley Orgánica, por resolución Legislativa, publicado en Registro Oficial 280 del 8 de Marzo del 2001.

La Ley Orgánica de Control Constitucional, en su Capítulo II del Habeas Data establece que "las personas naturales o jurídicas, nacionales o extranjeras, que desean tener acceso a documentos, bancos de datos e informes que sobre si misma o sus bienes están en poder de entidades públicas, de personas naturales o jurídicas privadas, así como conocer el uso y finalidad que se les haya dado o se les este por dar, podrán imponer el recurso de Habeas Data para requerir las respuestas y exigir el cumplimiento de las medidas tutelares prescritas en esta ley, por parte de las personas que posean tales datos o informaciones".

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.

1.2.6. Código de Procedimiento Penal y Código de Procedimiento Civil.

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 de Procedimiento Penal, se muestran a continuación en la siguiente tabla:

INFRACCIONES INFORMATICAS	REPRESION	MULTAS
Delitos contra la información protegida (CPP Art. 202) 1. Violentando claves o sistemas accede u obtiene información 2. Seguridad nacional o secretos comerciales o industriales 3. Divulgación o utilización fraudulenta 4. Divulgación o utilización fraudulenta por custodios 5. Obtención y uso no autorizados	6 meses a 1 año 1 a 3 años 3 a 6 años 6 a 9 años 2 meses a 2 años	$500 a $1000 $1.000 - $1500 $2.000 - $10.000 $2.000 - $10.000 $1.000 - $2.000
Destrucción maliciosa de documentos (CCP Art. 262)	3 a 6 años	---
Falsificación electrónica (CPP Art. 353)	3 a 6 años	---
Daños informáticos (CPP Art. 415) 1. Daño dolosamente 2. Servicio público o vinculado con la defensa nacional 3. No delito mayor	6 meses a 3 años 3 a 5 años 8 meses a 4 años	$60 – $150 $200 - $600 $200 - $600
Apropiación ilícita (CPP Art. 553) 1. Uso fraudulento 2. Uso de medios (claves, tarjetas magnéticas, otros instrumentos	6 meses a 5 años 1 a 5 años	$500 - $1000 $1.000 - $2.000
Estafa (CPP Art. 563)	5 años	$500 - 1.000
Contravenciones de tercera clase (CPP Art. 606)	2 a 4 días	$7 - $14

Tabla 1.4 Infracciones informáticas.
Fuente: Código de Procedimiento Penal del Ecuador

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 primero 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.

CAPÍTULO 2

EL PERITO Y EL PERITAJE INFORMATICO.

2.1. El Perito.

La conceptualización que brinda Juan Carlos Riofrío [23], 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.

Emilio del Peso Navarro [24], aporta una definición para el perito informático en la cual lo describe como "un 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. Así puede influir para su selección la plataforma tecnológica el lenguaje de programación usado, el sistema de base de datos, sistemas operacional, entre otros.", entonces, tomando en consideración esta descripción, al ser el perito informático un profesional que va a

emitir un criterio u opinión, la cual, debe estar fuertemente sustentada tanto en la parte técnica como científica, logre llegar a conclusiones objetivas e imparciales sobre un hecho, y no solo basarse en impresiones u opiniones.

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".

En el caso de que no se encuentren peritos habilitados en la rama a investigar el mismos CPP en su Art. 95 establece que "si en el lugar donde se deba realizar la diligencia no hubiera peritos habilitados, el Fiscal nombrará a personas mayores de edad, de reconocida honradez y probidad, que tengan conocimientos en la materia sobre la que deban informar", conviene entonces que las personas designadas en calidad de perito, para estos casos, deban acreditar el conocimiento suficiente y verificable en la materia, sobre la cual van a emitir un criterio u opinión.

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.

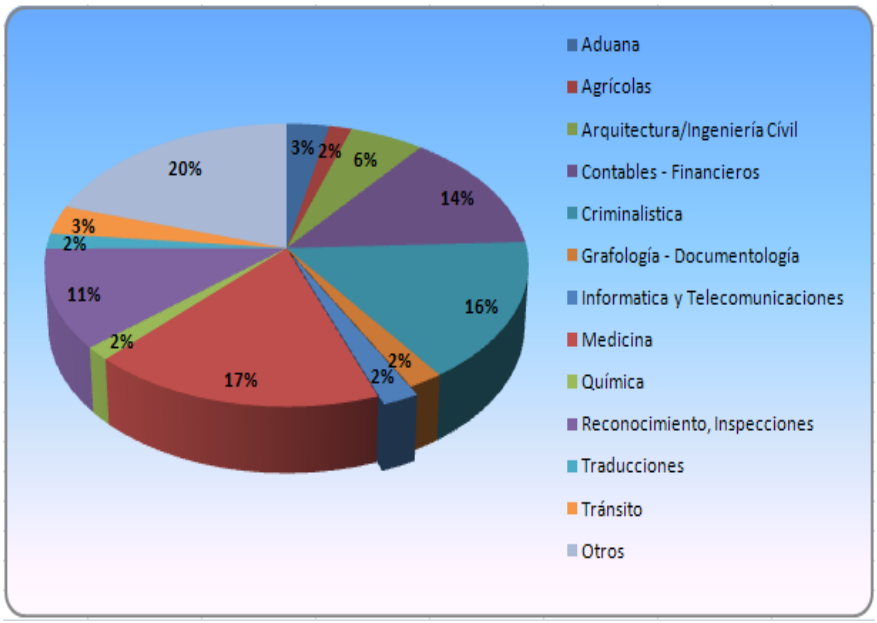

Figura. 2.1. Peritos profesionales por rama en Ecuador.
Fuente: Nómina de Peritos del Ministerio Público de Ecuador – Agosto 2008

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:

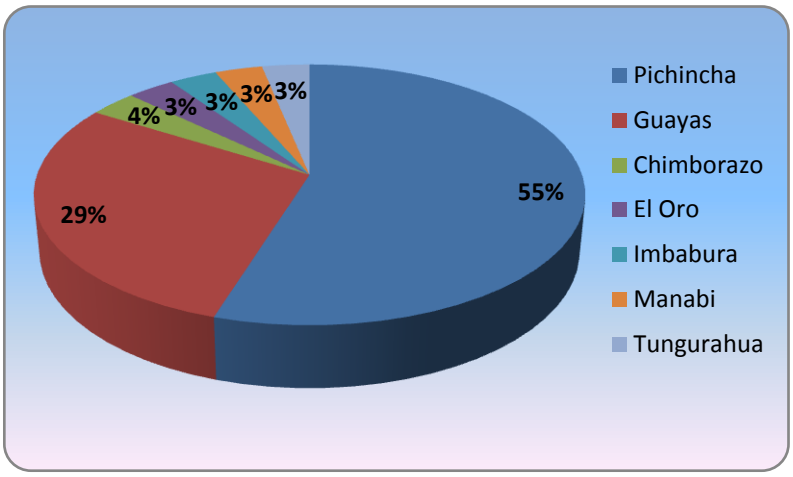

Figura. 2.2. Distribución geográfica de peritos informáticos por provincia.
Fuente: Nómina de Peritos del Ministerio Público de Ecuador – Agosto 2008

2.1.1. Perfil del perito informático

De acuerdo a Jeimy Cano [25], 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, conocimientos teóricos y prácticos, habilidades en la aplicación de procedimientos y metodologías, y que sus informes sean metódicos y estructurales, entre otros. 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.

A fin de desarrollar el perfil forense o de seguridad requerido en las ramas de informática, existen instituciones internacionales tales como IACIS (International Association of Computer Investigative Specialist), HTCN (High Technology Crime Network), ACFE (Association of Certified Fraud Examiners), EC – Council, que en este sentido han desarrollado programas de certificación aplicables a la informática, que permiten luego de seguir un programa de especialización desarrollar habilidades y capacidades deseables en los especialistas informáticos ante la investigación de un hecho, la siguiente tabla muestra por ejemplo algunas certificaciones de este nivel:

TIPO	CERTIFICACION	INSTITUCION
Forense	CFEC –Computer Forensic External Certification	IACIS
	CCCI – Certified Computer Crime Investigator	HTCN
	CCE – Certified Computer Examiner	ACFE
	CFE – Certified Fraud Examiners	ACFE
Seguridad Informática	CFA – Computer Forensic Analysis	WISE
	CCI – Computer Crime Investigator	EC-Council
	CEH – Certified Ethical Hacker	EC-Council
	CHFI – Computer Hacking Forensic Investigator	EC-Council

Tabla 2.1. Certificaciones forenses y de seguridad informática.

Es menester recalcar, que el perito debe contar, además de sus vastos conocimientos, con altos valores éticos morales y profesional (teoría del deber y/o deontológica), 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.

Después de que se ha realizado el proceso de investigación por parte del perito, y luego de haber entregado su informe, él podría ser llamado por la autoridad competente, para aclarar u ampliar su informe, ya sea de manera escrita u oralmente mediante declaraciones durante un proceso de indagación acusación, penal, por ello, debe tener la capacidad de comunicar lo que ha realizado y estudiado dentro de su análisis pericial, debe justificar al juez, fiscal, o tribunal, porque se le debe creer en lo que respecta a sus conclusiones, las herramientas o técnicas que ha utilizado durante el proceso de análisis e incluso, podría indagarse sobre los procedimientos realizados y las técnicas utilizadas durante su investigación.

2.1.2. 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.

Según lo establecido en el Art 97 del Código de Procedimiento Penal sobre la prohibición de recusación "los peritos no podrán ser recusados, sin embargo, el informe no tendrá valor alguno, si el perito que lo presento tuviera motivo de inhabilidad o excusa.", es decir, que los peritos no podrán ser recusados por ninguna de las partes litigantes, a menos que se compruebe que tuviera motivo de inhabilidad o excusa, en cuyo caso, su informe presentado no tendrá ninguna validez dentro del proceso.

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 (Ver ANEXO 4 – Reglamento de 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.

2.2. 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 preprocesales 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.

En el Reglamento para el Sistema de Acreditación de Peritos, se establecen las competencias, las especialidades, las obligaciones y sanciones a los que están sujetos los especialistas acreditados.

2.2.1. 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.

Otro de los organismos que establecen requisitos para la acreditación de peritos especializados o normas para la calificación y registros de peritos evaluadores son los Centros de Conciliación y Arbitraje establecidos a nivel nacional, así como también la Superintendencia de Bancos y Seguros del Ecuador.

2.2.2. Requisitos de acreditación de peritos.

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 Titulo legalizado y registrado en el CONESUP, que acredite la formación académica en las ciencias de la especialidad cuya acreditación se solicita.
6) Copia notarizada del certificado del CONESUP.
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.
    a. Comprobante de depósito.
    b. Originales de la cedula de ciudadanía y certificado de votación.
12) 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.

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 CONESUP.
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.

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

1) Hoja de Vida.
2) Copia de la Cédula de Identidad.
3) Copia del certificado de votación.
4) Record policial original y copia certificada.

5) Mínimo tres certificados de honorabilidad.
6) Copia notariada del Título Profesional.
7) Certificado del CONESUP, original o copia notariada.
8) Mínimo tres certificados de trabajos originales o copias notariadas.
9) Copia de Deposito de tasas Judiciales.

    a. Por inscripción.
    b. Cuota Anual.

La 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.

En el Reglamento de Funcionamiento a su vez se establecen, especificaciones para los informes periciales (Ver ANEXO 5 – Reglamento de Funcionamiento del Centro

de Arbitraje y Mediación de la Cámara de Comercio Ecuatoriano Americana-Sección VIII).

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.

Durante el proceso de acreditación, no hay diferencia en lo que respecta a los requisitos que deben ser cumplidos por los profesionales en la rama que se desean acreditar, es decir, todos deben cumplir los mismos requisitos solicitados por el organismo competente.

2.2.3. 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 está 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. De igual manera los peritos pueden apelar la sanción e incluso establecer un recurso de amparo en el caso, de que se compruebe, que hayan sido violentados sus derechos.

Los actuantes de un proceso deben principalmente referirse hacia el contenido del informe y no en forma personal hacia el perito, aún en el caso de que el profesional haya actuado a petición del acusado, lo cual es legal de acuerdo a lo establecido en el Código de Procedimiento Penal en su Art. 95 “el imputado o acusado podrá designar al perito, mediante petición al Fiscal”, sin que esto implique que el informe resultante le favorezca en sus conclusiones.

El retiro de la acreditación inhabilita al perito por un periodo de 5 años consecutivos, luego de lo cual puede volver a pasar por el proceso de acreditación.

2.3. El peritaje.

El peritaje, es una ciencia auxiliar, que permite brindar al juez, un apoyo para iluminar sobre aspectos técnicos que por su especialidad no puede interpretar, pues al igual que la medicina legal o una pericia contable, no puede comprender en su total magnitud.

Es vital que ante una pericia o experticia práctica se tengan claro los siguientes aspectos: la ductibilidad y la interpretación.

1) La ductibilidad:- El perito de cualquier especialidad se apoya en la ductibilidad, a efectos de determinar bajo un criterio lógico, las distintas alternativas posibles que hay para llegar a un mismo resultado, es importante mencionar que la ductibilidad no es sinónimo de sentido común o criterio, permite tener una visión global y detallada de los distintos problemas a resolver para llegar a un resultado, a diferencia del criterio común para que haya ductibilidad el perito debe contar con profundos conocimientos en la materia a ser estudiada.
2) La interpretación:- El perito se apoya en la interpretación para explicar el o los distintos métodos que pudieron haber sido utilizados para llegar a un resultado, vale decir que en medida de la profundidad de conocimiento del perito se descartan los distintos métodos posibles.

El peritaje informático según la definición de Jeimy Cano [(26)], es "una disciplina que convierte la información contenida en medios informáticos, aunada al conocimiento que posee una persona sobre tecnologías de la información, en herramientas valiosas para ofrecer certeza o convencimiento al juez sobre unos hechos determinados".

La computación avanzada no forma parte de los conocimientos del juez o fiscal para poder valorarlos adecuadamente, por ello requiere de la prueba pericial, siendo ésta una prueba idónea cuando de un hecho jurídico informático se trate. Cabe recalcar que una pericia informática puede recaer en diversas ramas de la informática o sobre cualquier tipo de programa, aplicación, coreos electrónicos, bases de datos, en la cual se pide a los expertos se pronuncien sobre aspectos que puedan estar relacionados con el origen o procedencia de un evento o suceso realizado.

De acuerdo a lo contemplado en el Art. 95 del Código de Procedimiento Penal, sobre la designación de peritos, se indica que "durante la indagación previa, o en la etapa de instrucción, el fiscal ordenará que se realicen por peritos las experticias correspondientes. Para el efecto, el Fiscal designará el número de peritos que crea necesario. El imputado o acusado podrá designar un perito, mediante petición al Fiscal, sin que por tal motivo se retarde la práctica del reconocimiento. Si en el lugar donde se deba realizar la diligencia no hubiera peritos habilitados, el Fiscal nombrará a personas mayores de edad, de reconocida honradez y probidad, que tengan conocimientos en la materia sobre la que deban informar. Los peritos están obligados

a comparecer a posesionarse y a informar, en los plazos señalados por el Fiscal", en este artículo se mencionan temas como la designación, posesión de los peritos que serán tratados en las fases del proceso pericial en este mismo capítulo.

Analizando las especificaciones del Art. 95 del CPP, la autoridad competente tiene la facultad de designar el número de peritos que considere necesario, en cualquier etapa del proceso, ante lo cual, es preciso que se consideren los conocimientos y especializaciones de los peritos designados, más aún en lo que respecta a temas de informática, el profesional de esta rama puede ser especialista en programas de computación, bases de datos, sistemas de información específicos, entre otras, el que este aspecto pase desapercibido podría generar que los informes periciales guarden una divergencia con respecto a los análisis realizados, además de que se requeriría de un proceso adicional en el cual se nombrarían nuevos peritos para dilucidar los resultados de los informes periciales resultantes previos.

El Código de Procedimiento Civil del Ecuador (CPC), también establece especificaciones con respecto a los peritos, sus actuaciones y procedimientos durante el proceso de investigación (Ver ANEXO 6 – Código de Procedimiento Civil del Ecuador – de los Peritos).

Las definiciones detalladas en el CPC establecen según el Art. 247 "Ordenada la inspección, el juez señalará, en la misma providencia, la fecha y hora de la diligencia,

y designará perito tan solo si lo considerare conveniente", continuando con el Art. 248 "En el día y hora señalados, concurrirá el juez al lugar de la inspección; oirá la exposición verbal de los interesados, y reconocerá con el perito o peritos la cosa que deba examinarse.".

Observando estas especificaciones, la diferencia se da entre el CPP y el CPC, ya que el juez reconoce con la ayuda del perito el elemento que debe examinarse, en cuyo caso, es realizada una revisión general y se establece el alcance de la investigación que deberá ejecutar el perito sobre el elemento reconocido, esto conviene en el proceso ya que ayuda a tener una visión más amplia por parte del profesional con respecto a los procedimientos y tiempo que requerirá para su investigación, los cuales quedan establecidos en el documento resultante de dicha inspección realizada en conjunto con la autoridad.

El Código de Procedimiento Civil aclara en el Art. 253 "Puede el juez no apreciar el dictamen del perito o peritos, contrario a lo que el mismo percibió por sus sentidos en el reconocimiento, y ordenar que se practique nueva inspección con otro u otros peritos"

2.3.1. Fases del proceso pericial.

El perito debe estar al tanto, sobre cuál es su ámbito de acción, y para ello debe conocer las fases de un proceso pericial.

Para establecer cuáles son las fases por las cuales pasa un proceso pericial, se han revisado las estipulaciones que constan dentro del Código de Procedimiento Penal, de la misma manera, se enunciaran los documentos habilitantes en cada una de dichas fases que proporcionan validez legal al mismo dentro de un proceso judicial.

La autoridad competente ordenará que se realicen las experticias que correspondan dentro de un proceso, el mismo que puede haber sido solicitado por una de las partes intervinientes, para la investigación de un determinado delito, especificando la necesidad de la experticia, para ello se contemplan los siguientes procesos:

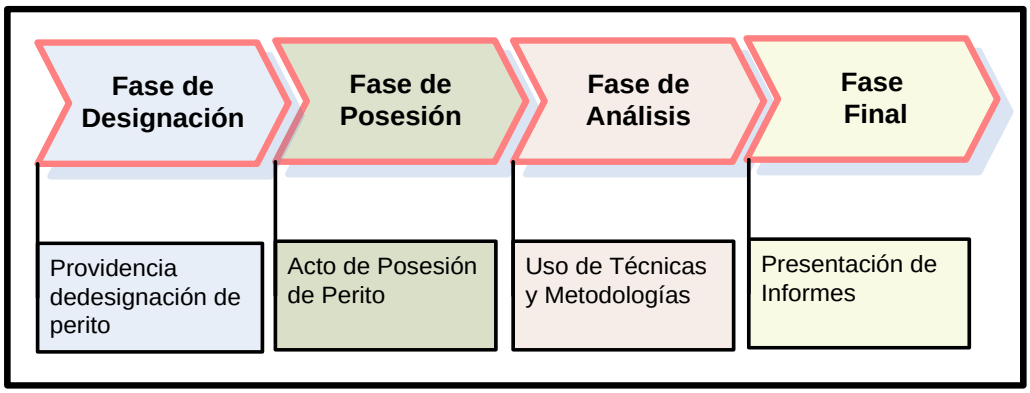

Figura. 2.2 El Proceso Pericial.
Fuente: Código de Procedimiento Penal del Ecuador

2.3.1.1 Fase de designación de perito

La fase de designación de perito, se establece mediante providencia del fiscal o juez de la causa, para lo cual, se proceden a requerir en las entidades de acreditación el listado de peritos habilitados en la rama a investigar, luego que se localiza el o los perito habilitado se realiza por parte del Fiscal o Juez, dicha providencia

La providencia de designación (Ver ANEXO 7 – Formato de providencia de designación de perito), contendrá los siguientes datos: se identifica el proceso, se determina la fecha y hora de designación, se hará constar el nombre del perito con la numeración de su credencial, se especificará el requerimiento a investigar, y se dispondrá la fecha en que debe realizarse la diligencia, también se hará constar el tiempo con él que el perito dispone para proceder con la entrega del informe de su investigación.

En caso de que el perito designado no se presente al proceso de posesión, su nombramiento queda automáticamente caducado, luego de lo cual por parte del fiscal o juez emitirá una nueva providencia con el nombramiento de otro u otros peritos.

2.3.1.2 Fase de Posesión de Perito

La fase de posesión de perito, se establece mediante el Acta de Posesión de Perito (Ver ANEXO 8 – Formato de providencia de posesión de perito), que debe estar suscrito por el fiscal o juez de la causa, el secretario y el perito designado, previamente se designaran los derechos que le corresponden al perito por sus servicios prestados, esto puede estar preestablecido mediante providencia emitida por el juez. En el Acta de Posesión se deben especificar y ratificar los datos enunciados en la providencia de designación de perito.

En esta etapa es primordial que el perito no tenga ningún motivo de inhabilidad o excusa, en lo que se refiere al proceso como lo establece el Código de Procedimiento Penal, otro aspecto valioso a considerar, es que el perito designado, debe conocer y saber diferenciar en la diligencia cuando se establecen periodos de tiempo para la entrega de su informe pericial, es decir la contabilizan o no de los días no laborables.

2.3.1.3 Fase de investigación.

En esta fase el Perito debe realizar su estudio, aplicando las técnicas y herramientas necesarias, para determinar lo solicitado por el fiscal o juez de la causa, en la providencia de designación, en cuyo caso, generalmente se aplican técnicas de informática forense, o auditoria informática, entro otras, que el perito considere necesarias.

Durante esta fase se recomienda que las técnicas utilizadas deban ser sustentadas de manera técnica y científica, además de la aplicación de guías o metodologías, por parte del profesional designado, como por ejemplo las guías de mejores prácticas establecidas en la Tabla 1.2 del Capítulo 1.

2.3.1.4 Presentación de Informes y Resultados

En este proceso el perito debe remitir dentro del plazo o término estipulado en el Proceso de Posesión los hallazgos encontrados durante su investigación, con sus respectivas conclusiones. El perito luego de realizar la entrega de su informe puede

ser convocado mediante citación por la autoridad competente a pedido de por cualquiera de las partes para que emita un pronunciamiento de ampliación o declaraciones de los procedimientos técnicas u hallazgos encontrados durante su investigación.

En este capítulo se ha reconocido como los medios informáticos pueden ser objeto o medios de prueba que pueden pasar por un proceso de pericia o inspección judicial, que posibilitan a la autoridad competente acceder a la evidencia que naturalmente arrojan estos medios informáticos, sin embargo, para estos casos la garantía de integridad de dichos elementos suele ser más significativo que la de su originalidad.

Además se ha analizado el entorno de aplicación en la investigación del delito, utilizando la herramienta de la pericia por medio de un especialista, en concordancia con las especificaciones establecidas en el Código de Procedimiento Penal y el Código de Procedimiento Civil, que aplica su conocimiento en cierta ciencia, como mecanismo convocado por la autoridad competente, con lo cual, se permite responder las preguntas: cómo, cuándo, por qué, dónde y quién cometió el acto ilícito investigado.

El peritaje es un proceso que debe ser llevado con responsabilidad por los peritos acreditados, en el que se deben tomar todas las medidas de precaución para no cometer errores, que no solo pueden desembocar en implicaciones legales para el

profesional, sino también que puedes acarrear graves consecuencias para alguna de las partes litigantes, por ello, el perito debe asegurarse de poner especial cuidado en la aplicación de los procedimiento que permitirán el esclarecimiento de la verdad sobre el acto ilícito investigado.

Las autoridades competentes mantienen el registro de profesionales en distintas instituciones que se han acreditado como especialistas en diferentes ramas y que pueden ser llamados como apoyo ante la investigación de una causa. Además, se ha visto la importancia de que el profesional acreditado como perito, más allá de los conocimientos en su rama de especialización tenga conocimientos básicos en el manejo de términos legales, criminalística entre otros.

CAPÍTULO 3

INICIATIVAS PARA EL MANEJO DE DELITOS INFORMATICOS EN EL ECUADOR.

3.1. Propuestas Internas.

Conforme a las disposiciones establecidas en la Constitución Política del Ecuador vigente, en su Capítulo IV, Sección Décima sobre la Fiscalía General del Estado, en el Art. 195 señala: "La Fiscalía dirigirá de oficio o a petición de parte, la investigación preprocesal y procesal penal", esto en concordancia con el Art. 33 del Código de Procedimiento Penal que señala que "el ejercicio de la acción pública corresponde exclusivamente al fiscal". Además contará como señala el Art. 208 del Código de Procedimiento Penal con su órgano auxiliar la Policía Judicial que realizaran la investigación de los delitos de acción pública y de instancia particular bajo la dirección y control del Ministerio Público.

Phil Williams [(27)] manifiesta que "es necesario contar no solo con las leyes e instrumentos eficaces y compatibles que permitan una cooperación idónea entre los estados para luchar contra la delincuencia informática, sino también con la

infraestructura tanto técnica como con el recurso humano calificado para hacerle frente a ese nuevo tipo de delitos".

Estas aserciones promueven que a más de las regulaciones, los especialistas necesitan contar con la infraestructura necesaria para la investigación de hechos que involucran el uso de las tecnologías.

3.1.1. Departamento de Criminalística de la Policía Judicial

La Ley Orgánica del Ministerio Público, según el Art. 2 inciso tercero, dispone que la Policía Judicial estará a órdenes del Ministerio Público para el cumplimiento de sus funciones, siendo entonces, este organismos quién colabore con las investigaciones de orden técnico científico del delito. El Reglamento de la Policía Judicial, fue publicado en el Registro Oficial # 368 de 13 de Julio de 2001, en donde se establecen sus atribuciones, departamentos, atribuciones, y sus campos de acción.

El Reglamento de la Policía Judicial, Art. 4 de la Naturaleza y Atribuciones especifica que: "La Policía Judicial es un cuerpo auxiliar del Ministerio Público, integrado por personal especializado de la Policía Nacional. Su funcionamiento se sujetará a las disposiciones contempladas en la Constitución Política de la República; en la Ley Orgánica del Ministerio Público; en la Ley Orgánica de la Policía Nacional; en el Código de Procedimiento Penal; y en el Reglamento de la Policía Judicial".

La enumeración que se constituyen en el Reglamento para el Departamento de Criminalística, establece que: “Bajo la dirección de los fiscales, corresponde a los departamentos de criminalística, acudir al lugar de los hechos para proteger la escena del delito; buscar, fijar, levantar, etiquetas las muestras dando inicio a la cadena de custodia, y analizar todos los indicios, señales o evidencias sobre un presunto hecho delictivo, de conformidad con lo establecido en Código de Procedimiento Penal”.

La Policía Judicial, mantiene Departamentos de Criminalística en las provincias de: Pichincha, Guayas, Manabí, Chimborazo, Azuay, Tungurahua e Imbabura Loja, Cotopaxi y Los Ríos. Los departamentos de criminalística cuentan con las siguientes secciones:

Secciones del Departamento de Criminalística			
Inspección ocular técnica	Audio, video y afines	Fotografía pericial	Dibujo y planimetría
Identidad física humana	Registro de Detenidos	Balística	Biología
Identificación de grabados y marcas seriales	Incendios y explosivos	Análisis Informático y Telecomunicaciones	Centro de Acopio y conservación de evidencias
Química analítica	Toxicología Analítica	Física	Documentología

Tabla 3.1. Secciones del Departamento de Criminalística.
Fuente: Reglamento de la Policía Judicial

Como podemos ver en la Tabla 3.1, el Departamento de Criminalística, de la Policía Judicial, cuenta con una sección especializada en Análisis Informático y Telecomunicaciones.

En el listado de peritos profesionales que mantiene el Ministerio Público, la concentración de peritos acreditados que corresponden a la rama de Criminalística es del 16% del total de peritos a nivel nacional (Ver Figura 3.2), entre ellos se encuentran peritos de criminalística de las ramas de: levantamiento de evidencias, inspección ocular, documentología, traducciones, tránsito, contables, agrícolas, balística, entre otras especialidades.

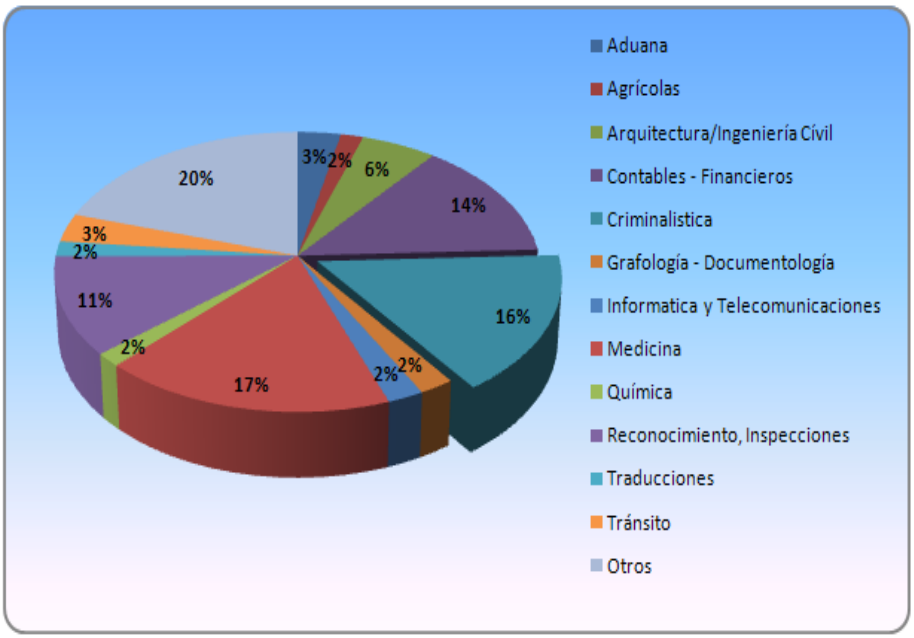

Figura. 3.2. Peritos rama de criminalística.
Fuente: Nómina de Peritos del Ministerio Público de Ecuador - Agosto 2008

Del 16 % de peritos profesionales acreditados en el Ministerio Públicos y que se identifican en las ramas de criminalística, la mayor concentración de ellos se encuentran en las Provincias de Pichincha y Guayas, el siguiente gráfico muestra a detalle el porcentaje que corresponde a las demás provincias:

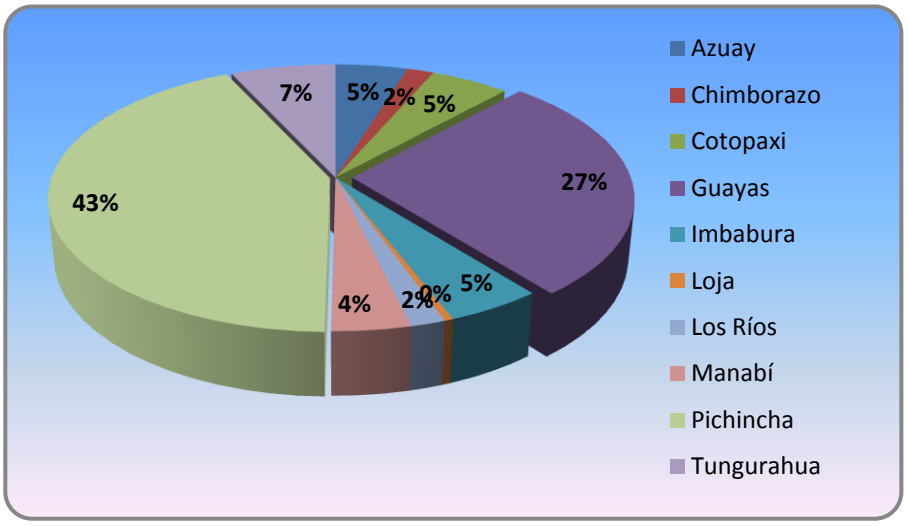

Figura. 3.2. Peritos de criminalística a nivel geográfico.
Fuente: Nómina de Peritos del Ministerio Público de Ecuador – Agosto 2008

En lo que corresponde a peritos acreditados en la rama de criminalística a nivel nacional de especialización en informática se encuentra únicamente un profesional acreditado.

Según el Reglamento de la Policía Judicial en el Art. 81, se especifica que, a la Sección de Análisis Informático y Telecomunicaciones le corresponde:

1) Identificar los procesos y autores de fraude, falsificación, invasión y atentado de los sistemas informáticos y de telecomunicaciones.
2) Recopilar y mantener actualizada la información referente a medidas de seguridad informática y en Telecomunicaciones.
3) Mantener la cadena de custodia; y

4) Demás funciones que se le asignen, creen y/o dispusiere la autoridad legal tendiente al esclarecimiento de un hecho punible.

El Gobierno Nacional del Ecuador, de acuerdo con el proyecto del Plan de Seguridad Ciudadana y Modernización de la Policía (2008-2009) [(28)], ha presupuestado invertir progresivamente 320 millones de dólares en equipamiento, capacitación, servicios, y remodelación de la Policía.

Con dicho proyecto, en las ciudades de Quito y Guayaquil se prevé implementar los Centros de Ciencias Forenses, los cuales estarán equipados con infraestructura y tecnología moderna, lo que permitirá, mejorar la investigación del delito. Además se contempla habilitar en cada provincia del país 15 Unidades de Apoyo Criminalístico, que contarán con herramientas básicas de investigación, así como también unidades de criminalística móviles que operarían a nivel nacional.

El proyecto también contempla adquirir herramientas como ADN Forense, microscopio electrónico que permite confirmar residuos de pólvora, elementos que actualmente no existen en el país, así como también dotar de nuevos terminales y servidores para el Sistema IBIS (Sistema Integrado de Identificación Balística), IAFIS (Sistema Integrado Automático de Identificación de Huellas Dactilares) que se conservan en el Departamento de Criminalística.

El proyecto además contempla, iniciativas que involucran convenios con los siguientes organismos:

1) Policía Nacional del Perú.
2) Secretaria Nacional Anticorrupción.
3) Cámara de Comercio de Quito.
4) Universidad Central del Ecuador y la Universidad Católica.
5) Organismo nacional de trasplante de órganos y tejidos.

3.1.2. Unidad de Delitos Informáticos del Ministerio Público

En correlación con el avance de las tecnologías y ante el incremento de los delitos de esta índole, el Dr. Santiago Acurio del Pino, Director Nacional de Informática del Ministerio Público del Ecuador, propone, el Plan Operativo de creación de la Unidad de Delitos Informáticos del Ministerio Público (UDIMP) [(29)].

La Unidad de Delitos Informáticos del Ministerio Público, tendrá la misión de investigar, perseguir y prevenir todo lo relacionado con la criminalidad informática en todos sus aspectos y ámbitos tales como: amenazas, injurias, pornografía infantil, fraudes, terrorismo informático y hacking.

Entre los objetivos establecidos para dicha unidad se establecen los siguientes:

1) Investigar y perseguir a nivel pre-procesal y procesal penal toda infracción que utilice a la informática como medio o fin para la comisión de un delito.
2) Capacitar a los miembros de la unidad a nivel técnico para combatir esta clase de infracciones.
3) Contribuir y colaborar con la formación continua de los investigadores.
4) Formar y mantener alianzas con unidades Especiales de investigación a nivel internacional.
5) Desarrollar una política de Seguridad Informática General.
6) Implementar a nivel nacional el Sistema de Información de Delitos Informáticos
7) Promover canales de comunicación y trabajo con las distintas estructuras y organizaciones gubernamentales implicadas con la lucha contra el fenómeno de la delincuencia informática.

La unidad se conformaría por una coordinación nacional y otra coordinación internacional.

En lo que corresponde a la coordinación nacional la estructura estaría compuesta de la siguiente manera:

1) **Coordinación Nacional:-** Establecerá las políticas y directrices generales de la investigación de los Delitos Informáticos.

2) **Sección de Inteligencia:-** Se encargará de la recolección de las evidencias e indicios relacionados con el cometimiento de los delitos informáticos.
3) **Sección Operativa:-** Realizará las investigaciones de lo relacionado con la criminalidad informática.
4) **Sección Técnica y Forense:-** Brindará apoyo técnico y realizara el análisis forense de las evidencias.
5) **Sección de Capacitación y Entrenamiento:-** Formación del personal de la Unidad, de la acreditación de los Peritos Informáticos a nivel nacional.

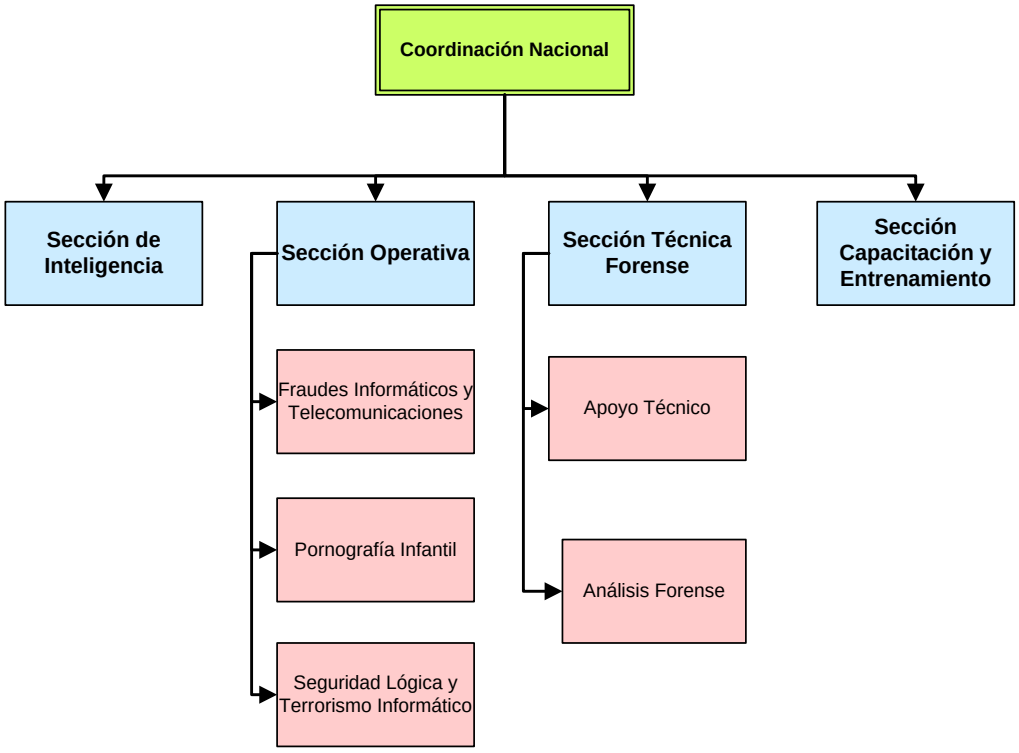

Figura. 3.1 Estructura de la Unidad Delitos Informáticos Ministerio Público.

Fuente: Plan operativo de creación de la Unidad de Delitos Informáticos del Ministerio Público – Dr. Santiago Acurio del Pino

En lo que corresponde a la coordinación internacional del Plan Operativo de creación de la Unidad de Delitos Informáticos del Ministerio Público, establece que es primordial instaurar mecanismos de cooperación con organizaciones internacionales, tales como: la INTERPOL, Unión Internacional de Telecomunicaciones(UIT), etc. , en el tema de la cyber delincuencia, para ello se contará con los servicios de la Unidad de Asuntos Internacionales del Ministerio Público del Ecuador, quienes trabajarán estrechamente y en combinación con el Coordinador Nacional, y el Ministro Fiscal General de la Nación, a su vez ellos tendrán la responsabilidad de establecer las políticas de cooperación internacional en materia de delitos informáticos.

La UDIM, requiere además contar con la logística (Física y Lógica) necesaria para el funcionamiento de la unidad.

Como podemos advertir, la iniciativa del Dr. Acurio, fomenta la creación de un organismo institucional dentro del Ministerio Público, sin embargo, se deben considerar otros factores externos como la sociedad, las funciones del Departamento de Criminalística de la Policía Judicial, y como actuaría dicha unidad ante los casos que son manejados de oficio por el Ministerio Público.

3.1.3. Colegio de Peritos Profesionales del Ecuador

El gremio del Colegio de Peritos Profesionales del Ecuador, quienes mantienen una estructura a nivel de diferentes provincias tales como: Pichincha (COPROPI), Guayas, Tungurahua, Los Ríos, El Oro, Manabí.

El Dr. Jaime Ayala Mazón, Presidente de la Prefederación de Peritos Profesionales y Presidente del Colegio de Peritos Profesionales del Pichincha, coincide con el Dr. Santiago Acurio del Pino en la necesidad de crear una Unidad de Delitos Informáticos, sin embargo, indica que deben establecerse condicionantes cuando el Ministerio Fiscal actúe de oficio, en cuyo caso, el Ministerio Fiscal forma parte del proceso. Además indica que no se deben dejar de lado las unidades que están establecidas por el Departamento de Criminalística de la Policía Judicial.

Otra de las iniciativas de este gremio es el patrocinio de la Ley de Defensa del Perito Ecuatoriano, ya que Ecuador no mantienen una política que establezca lineamientos que permita establecer condiciones para el ejercicio profesional de este nivel.

3.2. Propuestas Externas.

Con el avance de la tecnología digital de los últimos años, surgen nuevas generaciones de delincuentes que exponen los gobiernos, las empresas y los individuos a este tipo de peligros, la difusión de pornografía infantil, el incremento de incidentes de seguridad e incluso actividades terroristas son algunos ejemplos de los

nuevos delitos informáticos que presentan una realidad difícil de controlar, y que traspasa las fronteras de los países, por ello, es primordial la cooperación entre organismos estatales internacionales para hacer frente a estos nuevos delincuentes.

3.2.1. 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 [(30)], que les permita:

1) Realizar un diagnostico de la actividad delictiva vinculada a las computadoras y la información de los Estados miembros.
2) Realizar un Diagnostico de la legislación, las políticas y las practicas nacionales con respecto a dicha actividad.
3) Identificar las entidades nacionales e internacionales que tienen experiencia en la materia; y
4) Identificar mecanismos de cooperación dentro del sistema interamericano para combatir el delito cibernético.

El Grupo de Expertos Intergubernamentales en Materia de Delitos Cibernéticos conformado y creado por recomendación de los Ministros de Justicia, ha mantenido reuniones y talleres importantes a lo largo de los últimos nueve años, en las que se ha permitido conocer las realidades de los países miembros con respecto a los delitos informáticos.

Durante la cuarta reunión del Grupo de Expertos Gubernamentales en Materia de Delitos cibernéticos efectuada el 27 y 28 de Febrero del 2006 en Washington DC, de los Estados Unidos, se efectuó un cuestionario a los países miembros de la OEA (Ver ANEXO 9 – Cuestionario Delitos Cibernéticos - Grupo de Expertos Gubernamentales), sobre delito cibernético en donde se obtuvieron los siguientes resultados.

1) 50% de los países posee legislación en delito informático.
2) 40% de los países posee legislación procesal que permite la persecución del delito cibernético.
3) 53 % de los países posee investigadores especializados.
4) 40% de los países posee fiscales especializados.

Entre tanto las recomendaciones de la quinta reunión del Grupo de Expertos (Ver ANEXO 10 – Recomendaciones ante Delitos Cibernéticos - Grupo de Expertos Gubernamentales), efectuada el 19 y 20 de Noviembre del 2007, en Washington DC, de los Estados Unidos, fueron las siguientes:

1) Establecer unidades para que efectúen la investigación y persecución del delito cibernético.
2) Mantener información del punto nacional de contacto para la cooperación internacional en materia de delito cibernético.
3) Adoptar legislación en materia de delito cibernético.
4) Adoptar legislación y procedimientos para la utilización de la prueba electrónica en los procesos penales.
5) Vincularse a la "Red de Emergencia de Contactos sobre Delitos de Alta Tecnología las 24 horas los siete días de la semana" del G-8.
6) Consolidar el Portal Interamericano de Cooperación contra el Delito Cibernético.
7) Compilar las legislaciones en materia de delito cibernético y sobre la prueba electrónica.
8) Considerar la aplicación de los principios de la Convención del Consejo de Europa sobre la Delincuencia Cibernética a la adhesión a la misma.
9) Fortalecer la cooperación con otras organizaciones internacionales.
10) Desarrollar las relaciones con el sector privado para prevenir y combatir el delito cibernético.
11) Expresar su satisfacción con los resultados de los talleres auspiciados por Estados Unidos en el 2006 con la cooperación de Brasil, Costa Rica y Barbados.

12) Aceptar el ofrecimiento de los Estados unidos sobre la realización de talleres adicionales.
13) Que el grupo de Expertos se reúna por lo menos una vez entre una y otra REMJA (Reunión de Ministros de Justicia de las Américas).

Con estas iniciativas proporcionadas y puestas a consideración de los países miembros de la OEA, se impulsa la cooperación internacional para el seguimiento e investigación de los delitos que afectan las modernas tecnologías así como la habilitación de leyes y organismos que cuenten con tecnología para la persecución de la delincuencia informática.

3.3. 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 3.2. Leyes en Países Latinoamericanos.

La tabla 3.2 resumen de manera general las leyes con las que cuentan países latinoamericanos, en donde se establecen mecanismos que permiten la persecución de delitos en los que se utilizan las tecnologías.

3.3.1 Delitos informáticos: Aplicación 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.

AÑO	LEY / DECRETO/ACUERDO	ORDENANZA
1970	Ley 17336 (Inicial)	Ley de Propiedad Intelectual (incluye programas de computadora, a través de la Ley 18957 - 1990)
1993	Ley 19223	Ley de Delitos Informáticos. Figuras penales relativas a la informática
1999	Decreto 81/99	Uso de la Firma Digital y Documentos Electrónicos en la Administración del Estado
1999 2002	Ley 19628 Ley 19812	Protección de la vida privada. Protección de datos de carácter personal.
2002	Ley 19799	Ley de Firma Electrónica. Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de Firma Digital
2003	NCH 2777	Código de práctica para la Gestión de la Seguridad de la Información
2004	Ley 19927	Pornografía Infantil

Tabla 3.4. Legislación en Chile – Informática e Información.

La Ley 19223 (Ver ANEXO 11 – 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 (Ver Anexo 12 – Estructura Orgánica Policía de Investigación 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. La brigada estructuralmente está formada de la siguiente manera:

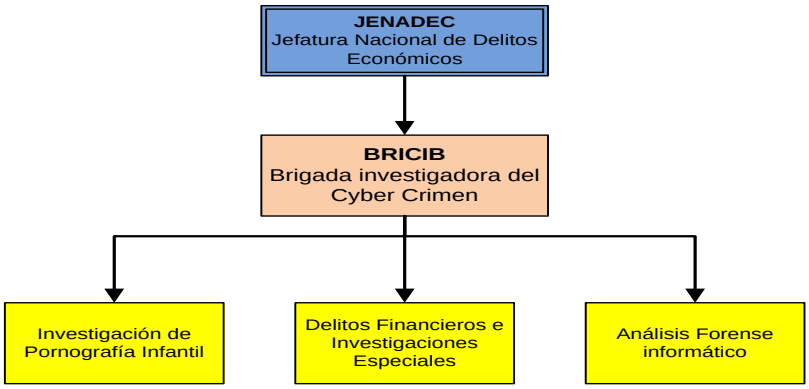

Figura. 3.2. Estructura Orgánica de la Brigada Investigadora del Cyber Crimen.
Fuente: Estructura Orgánica de la Policía de Investigaciones de Chile

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

1) 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.

2) 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 debito, 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.
3) 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.

La Policía de Investigaciones de Chile mantiene también, bajo su estructura orgánica como unidad departamental a la Jefatura Nacional de Criminalística (Ver Anexo 12 – Unidad de Investigación de Chile), el cual cuenta con laboratorios especializados por secciones de operación, las ramas de criminalística tales como: balística, huellografía y dactiloscopia, planimetría, contabilidad, fotografía, mecánica, física, química, infoingenieria entre otras.

La sección de infoingenieria utiliza métodos, técnicas y conocimientos científicos avanzados para la investigación de delitos en los que se han utilizado medios informáticos o tecnologías para la comisión de actos ilícitos, así como también de delitos informáticos, siendo ellos los encargados de efectuar los peritajes informáticos

desde las evaluaciones o levantamiento de evidencias hasta la aplicación de métodos avanzados en sus laboratorios especializados.

En lo que se refiere a estadísticas de los delitos informáticos, la policía de investigaciones de Chile expresa que los delitos más significativos, son los de destrucción de información y el robo de información, además se ha establecido que los ataques superan los 20000 diarios, pero solo se denuncian menos de 1000 anuales.

Vale destacar además que Chile, cuenta con el Código de Práctica para la Gestión de la Seguridad de la Información (NCH 2777), norma oficial chilena, que está basada en las especificaciones que brinda la Norma ISO 27001, la norma fue creada por el Instituto Nacional de Normalización (INN), el cual contribuye fomentando el uso de metodologías y normas técnicas en entidades públicas y privada, lo que conlleva a implantar conciencia de seguridad a varios niveles de las empresas chilenas.

3.3.2 Delitos informáticos: Aplicación 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:

AÑO	LEY / DECRETO/ ACUERDO	ORDENANZA
1933	Ley 11723	Régimen Legal de Propiedad Intelectual.
1996	Ley 24766	Ley de Confidencialidad.
1998	Ley 25036	Ley de Propiedad Intelectual (Modificación de la Ley 11723)
2000	Ley 25326	Habeas Data (Modificada en el 2008)
2001	Ley 25506	Firma Digital
2002	Decreto 2628/	Reglamentación de Firma Digital
2004	Ley 25891	Servicio y Comunicaciones Móviles
2005	Ley 26032	Difusión de Información
2008	Ley 26388	Delitos Informáticos.

Tabla 3.3. Legislación en Argentina – Informática e información.

La Ley 26388 (Ver Anexo 13 – Ley de delitos informáticos - Argentina), 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, en los casos en los que se encuentran computadoras u otro tipo de dispositivos informáticos

involucrados, sin embargo, también se da la figura de otro tipo de peritos entre los que se encuentran los peritos oficiales, de oficio y de parte, que pasan por un proceso de acreditación establecido de acuerdo a la jurisdicción por ser un país federal y poseer poderes judiciales descentralizados por provincias.

1) Peritos oficiales o judiciales:- Son aquellos que pertenecen a algún organismo oficial como la policía federal o gendarmería (Ministerio de Justicia, Seguridad)
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.

Es preciso destacar que a pesar de que Argentina, implantó la Ley de Delitos Informáticos recientemente, se han dado una serie de casos que han sido sancionados de acuerdo a las disposiciones del Código Penal, bajo el ámbito de haber cometido infracciones en otro tipos de delitos como la propiedad intelectual y la pornografía infantil, sin embargo al haberse aprobado recientemente la Ley de Delitos Informáticos, en Argentina, y más aún su reciente aplicación, no se cuentan con estadísticas oficiales y precisas sobre este tipo de delitos.

3.3.3 Delitos informáticos: Aplicación Colombia

Colombia ha implementado iniciativas que le permiten en diferentes espacios, establecer mecanismos que le permiten controlar los delitos relacionados con las tecnologías. En el campo jurídico, Colombia mantiene las siguientes leyes decretos y acuerdos, relacionados con la informática y la información:

AÑO	LEY / DECRETO/ ACUERDO	ORDENANZA
1985	Ley 57	Transparencia y Acceso a la Información Gubernamental
1999	Ley 527	Información en forma de mensaje de datos
2000	Decreto 1747	Entidades de Certificación, los Certificados y las Firmas Digitales
2000	Resolución 26930	Estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores.
2001	Ley 679	Explotación, la Pornografía y el Turismo Sexual con Menores de Edad
2003	Decreto 2170	Certificación y Firmas Digitales
2004	Proyecto de Ley 154	Reglamento del Derecho a la Información
2006	Acuerdo PSAA06-3334	Reglamentación de medios electrónicos e informáticos en la justicia.
2009	Ley 1273	Ley de la protección de la información y de los datos

Tabla 3.3. Legislación en Colombia – Informática e información.

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.

La Ley1273 (Ver Anexo 14 – Ley de delitos informáticos - Colombia), aprobada en enero del 2009, crea un nuevo bien jurídico tutelado, el cual se denomina "protección de la información y de los datos", en la sociedad colombiana, en la que se penalizan y sancionan los siguientes actos:

LEY 1273	
Atentados contra la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos:	
Acceso abusivo a un sistema informático	48 A 96 meses de prisión 100 a 1000 salarios mínimos legales mensuales vigentes
Obstaculización ilegítima de sistema informático o red de telecomunicaciones	48 A 96 meses de prisión 100 a 1000 salarios mínimos legales mensuales vigentes, siempre y cuando no constituya delito sancionado con una pena mayor
Interceptación de datos informáticos	36 a72 meses de prisión
Daño informático	48 A 96 meses de prisión 100 a 1000 salarios mínimos legales mensuales vigentes
Uso de software malicioso	48 A 96 meses de prisión 100 a 1000 salarios mínimos legales mensuales vigentes
Violación de datos personales	48 A 96 meses de prisión 100 a 1000 salarios mínimos legales mensuales vigentes
Suplantación de sitios web para capturar datos personales	48 A 96 meses de prisión 100 a 1000 salarios mínimos legales mensuales vigentes, siempre y cuando no constituya delito sancionado con una pena mayor
Circunstancias de agravación punitiva	Aumento de la mitad a las tres cuartas parte de las penas imponibles.
Atentados informáticos y otras infracciones: 1) Hurto por medios informáticos y semejantes 2) Transferencia no consentida de activos	

Tabla 3.4. Ley de Delitos Informáticos de Colombia – Ley 1273.

Podemos observar que las sanciones establecidas se orientas específicamente a preservar aspectos que se delinean con la seguridad de la información en la que se trata de salvaguardar la confidencialidad, integridad y disponibilidad de los datos y los sistemas informáticos.

Colombia ha sido uno de los países que ha recibido la ayuda de los Estado Unidos para la persecución de actos criminales, y la rama de investigación de naturaleza informática se originó a partir del año 1984 cuando los laboratorios del FBI y otras agencias que pertenecen a los Estados Unidos promovieron el desarrollo de programas para examinar evidencias computacionales.

Colombia mantiene el Grupo Investigativo de Delitos Informáticos (GRIDI) como parte de la Dirección de Investigación Criminal (Ver ANEXO 15- Dirección de Investigación Criminal de Colombia), que investiga las conductas delictivas que se derivan del uso de la tecnología y las telecomunicaciones, éste organismo se sustenta con el apoyo de equipos de informática forense y personal profesional capacitado que atienden incidentes informáticos presentes durante una investigación judicial.

Los grupos de investigación de delitos informáticos se encuentran equipados con laboratorios de Cómputo Forense, en las ciudades de Bogotá, Medellín, Bucaramanga, Cali y Barranquilla, los cuales permiten el análisis de la información digital.

Los organismos oficiales han declarado que los delitos relacionados con la informática en Colombia han tenido un incremento significativo en el año 2007, ya que durante el transcurso del año 2006 se encausaron 433 procesos que corresponden a los delitos informáticos, las cifras oficiales brindadas por la DIJIN (Dirección Central de Policía Judicial)[31], del mes de Enero a Septiembre del 2007, mencionan la denuncia de 630 casos, sin considerar aquellos que se llevan por la Fiscalía y el DAS (Departamento Administrativo de Seguridad), el trafico de bases de datos, fraude electrónico, falsificación o clonación de tarjetas, entre otro, han tenido un costo aproximado de 349 millones de pesos colombianos para las personas naturales y alrededor de 6.6 billones de pesos colombianos para las empresas..

Durante del desarrollo de este capítulo hemos conocido las herramientas y organismos con los que cuenta el Ecuador para la investigación de los delitos de índole tecnológicos, así como las propuestas ofrecidas por otros organismos que permitirían el desarrollo de unidades de investigación de los delitos informáticos, además se han identificado iniciativas que permiten la adecuación y mejora del Departamento de Criminalística de la Policía Judicial del Ecuador.

Vale destacar además las recomendaciones que realiza la OEA, a través del Grupo de Expertos Intergubernamentales en Materia de Delitos Cibernéticos, en pro del desarrollo de mecanismos que permitan la persecución de los delitos cibernéticos

También hemos dado una mirada, hacia las iniciativas desarrolladas en algunos países sudamericanos con el establecimiento de leyes que sancionan los delitos informáticos en primera instancia, y cómo funcionan sus unidades de investigación ante actos cometidos de naturaleza tecnológica.

CAPÍTULO 4

RETOS A SUPERAR EN EL MANEJO DE DELITO INFORMATICOS EN EL ECUADOR.

4.1. Inconvenientes en el Proceso Pericial y la investigación tecnológica ante el delito informático.

El medio electrónico se ha convertido en un blanco para cometer diferentes actos ilegales tales como: extorción, robo, fraude, suplantación de identidad, entre otros. La delincuencia informática es difícil de comprender o conceptualizar plenamente, a menudo se la considera una conducta relegada por la legislación, que implica la utilización de tecnologías para la comisión del delito.

La investigación de la delincuencia informática, no es una tarea fácil, ya que la mayoría de los datos probatorios son intangibles y transitorios. Los investigadores de delitos cibernéticos buscan vestigios digitales que de acuerdo a sus características suelen ser volátiles y de vida corta.

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 Septiembre del 2008, de la Superintendencia de Telecomunicaciones en Ecuador, hay alrededor de 1´329.713 usuarios de Internet, 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.

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 Corte de Justicia, investigadores, y hasta la misma sociedad.

A continuación se relatan algunos de los retos que Ecuador debe superar con relación al delito informático:

4.1.1. Marco Legal

Debemos considerar la problemática Jurídica, ya que si bien es ciertos Ecuador ha iniciado los primeros pasos en la generación de Leyes y Decretos que contemplan aspectos significativos de las nuevas tecnologías y también se han establecido penas y

sanciones en el Código 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 precisión de un marco legal que contemple a los delitos informáticos de una manera integral.

A continuación se detallan bajo este contexto algunos inconvenientes para el manejo de delitos informáticos:

- Falta de la infraestructura y tecnologías adecuada en los entes u organismos de investigación como: el Ministerio Público y la Policía Judicial. Las investigaciones o experticias a nivel informático en su mayoría se dan por denuncias realizadas bajo otro contexto de delitos tales como: robo, daño a la propiedad, estafas, entre otros, que son llevadas por Unidades del Ministerio Público como: la Unidad de Delitos Misceláneos, Unidad de Delitos Financieros y de Telecomunicaciones, Unidad de Daños contra la Propiedad, debido a la falta de una regulación, o unidad que opere este tipo de infracciones.
- Falta de iniciativas que permitan el desarrollo de brigadas y unidades estructuradas y especializadas, para la investigación de los delitos de índole informático, nacional y transnacional, desde su inicio con el levantamiento de evidencias hasta la aplicación de procedimientos de mayor complejidad.

- Falta de especificaciones claras y concisas en la petición de pericias informáticas, elemento importante que cabe destacar, ya que durante las peticiones de pericias informáticas solicitadas por medio de la autoridad, incurre en términos amplios sobre la "práctica de peritaje informático", en la cual no se especifican requerimientos sólidos sobre lo que se va a investigar, en cuyo caso es importante la comunicación entre los fiscales, jueces y tribunales con los investigadores o peritos de la rama de informática, previo a establecer la diligencia de la pericia.
- Falta de una comunicación efectiva entre los especialista informáticos y los judiciales; mantener un lenguaje común entre los especialistas de informática y los operadores judiciales es trascendental, principalmente, al exponer por parte del perito informático, los criterios utilizados en el desarrollo de la investigación ante una investigación judicial.
- Falta de un procedimiento adecuado para la calificación de peritos informáticos por parte del Ministerio Público y demás entidades u organismos.
- Otro aspecto, a considerar es la problemática legal, que se presenta cuando este tipo de delitos traspasa las fronteras y las jurisdicciones, lo que pone en relieve la importancia de la cooperación internacional.

4.1.2. Formación

La formación surge como factor incluyente para cada uno de los involucrados que dirigen la investigación, pues muchas veces se encuentran confundidos ante el tratamiento de este tipo de delitos.

- Falta de preparación para los miembros de los organismos que persiguen la delincuencia en el campo informático (Ministerio Publico, Policía Judicial, jueces, etc.).
- Falta de preparación a nivel de formación en el ámbito de los procedimientos y técnicas utilizadas para la persecución de los delitos informáticos por parte de los especialistas.
- Falta de programas de capacitación que atañen a los delitos informáticos.
- Falta de cultura informática, aquellos individuos que no tienen conocimientos informáticos básicos (Internet, correo electrónico), son más vulnerables y tienen mayores probabilidades de ser víctimas de un delito.

Es importante destacar que bajo este contexto, que en Ecuador se están iniciando los primeros pasos, en donde iniciativas de las Universidades como La Pontifica Universidad Católica del Ecuador y la Escuela Politécnica Nacional, se han adicionado en sus mallas curriculares de estudio para las carreras de Ingenierías en tecnologías de la Información, la disertación de la Informática Legal (Ver Anexo 16 – Mallas Curriculares), que permiten preparar a los profesionales desde una etapa muy

temprana, sobre aspectos generales como las regulaciones existentes y que atañen a las tecnologías, así como también, el desarrollo y progreso de países vecinos en cuanto a la legislación habilitante para perseguir estos actos ilícitos no solo bajo la perspectiva local sino transnacional.

4.1.3. Limitaciones tecnológicas

La distribución de las tecnologías de la información y las comunicaciones en todo el mundo no es uniforme. Existen vastas diferencias en los tipos y números de adelantos tecnológicos en diferentes partes del mundo. La denominada brecha digital fue reconocida en la Declaración del Milenio de las Naciones Unidas del 2000.

La Declaración de Principios adoptada por la Cumbre Mundial sobre la Sociedad de la Información, establece que los beneficios de la revolución de la tecnología y la información están actualmente distribuida de manera desigual entre los países desarrollados y en desarrollo y dentro de las sociedades. Esta declaración también incluye el compromiso de transformar esta brecha digital en una oportunidad digital para todos en particular para aquellos que corren el riesgo de quedar rezagados y marginados.

Considerando este aspecto, no es inverosímil entonces, que el Departamento de Criminalística de la Policía Judicial, según consta en el listado que mantiene el Ministerio Público de los peritos, cuente solamente con un perito especializado en la

rama de informática, aspecto que contribuye a que se contraten por necesidad a los profesionales acreditados o no, y que en muchas ocasiones estos no cuenten con la experiencia, los medios u herramientas y la formación adecuada para la ejecución de la investigación del acto ilícito.

Si bien es cierto el Departamento de Criminalística, cuenta con la Sección de Análisis Informático y Telecomunicaciones y se ha determinado sus responsabilidades preliminarmente, tal como, consta en el Reglamento de la Policía Judicial, esta sección no se ha desarrollado, a favor de la sociedad ya sea por la falta de recursos o la falta de proyectos que contemplen iniciativas innovadoras que permitan el tratamiento de los delitos informáticos desde una perspectiva integral.

En este punto es prescindible destacar, que en Ecuador desde Abril del 2008 se encuentra habilitado el proyecto "Libertador", con el que se dota de una herramienta electrónica a la policía judicial y a los fiscales para la investigación criminal, que ha contado con el apoyo técnico y logístico de los Estados Unidos, la misma que permite la posibilidad del monitoreo de llamadas, correos electrónicos, y todo lo que está inmerso dentro del espectro electromagnético de comunicaciones, siendo este proyecto uno, entre los que se deberían fomentar para el desarrollo de una política en pro de la persecución de la delincuencia informática, que permita el control integral de los delitos de índole tecnológico.

La falta de infraestructura, herramientas modernas y demás implementos tecnológicos requeridos para la persecución de este tipo de delitos incrementa el riesgo de que la investigación sea realizada de una manera inadecuada por parte de los especialistas.

4.1.4. Otras consideraciones

Un factor muy relevante con la que debe contar el profesional acreditado y que cumple como perito profesional es su ética profesional, la labor que cumple como investigador es altamente sensitiva, en la que se debe tener mucho cuidado de no cometer errores, tener una adecuada madurez emocional juega un papel fundamental, para soportar la presión durante su ejercicio de investigación, y utilizar la máxima objetividad al plasmar sus conclusiones.

Por la falta de información o poco interés de las personas, muchas veces las denuncias no se las presentan, por lo cual, es importante promover el desarrollo de programas y campañas, orientadas hacia las leyes definidas y relacionadas con la información y la informática, en las que se difunda, comunique y establezca acciones de información prevención, y denuncia de actos delictivos que laceren y pongan en peligro el bien jurídico protegido en el campo informático que es la información. Por ejemplo: la iniciativa de la Defensoría del Pueblo que tiene por objetivo el cumplimiento de la Ley Orgánica de Transparencia y Acceso a la Información Pública, o en el caso de Colombia que mantiene el programa “Internet Sano” que

tiene por objetivo luchar contra de la explotación de la pornografía infantil en Internet.

4.2. Conclusiones y Recomendaciones.

Ecuador ha dado los primeros pasos en el desarrollo de iniciativas que permiten la investigación y sanción de los delitos informáticos, sin embargo, es preciso desarrollar, mejorar e implementar mecanismos que permitan que dichas investigaciones se desarrollen dentro de marcos regulados, controlados y mediante el uso de tecnología apropiada por parte los entes y profesiones dedicados a su investigación.

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

SECCION	RECOMENDACIÓN
Gubernamental	1. Establecer y alinear una política de lucha en contra de la delincuencia informática. 2. Incentivas mecanismos de cooperación con otros países con el objetivo de prevenir y sancionar el delito informático que traspasa las fronteras de las naciones.

SECCION	RECOMENDACIÓN
Marco Legal	1. Proyecto de Ley de Delitos Informáticos. 2. Revisión de la Ley de Comercio Electrónico, Mensajes de Datos y Firma Digital. 3. Reformas al Código de Procedimiento Penal del Ecuador sobre penalizaciones a las infracciones informáticas. 4. Establecer mecanismos de protección penal respecto de la delincuencia informática. 5. Implementación de mecanismos de mayor rigurosidad en los procedimientos de acreditación de peritos informáticos, en la que los profesionales acrediten además de sus conocimientos técnicos, procedimientos de manejo de evidencias, criminalística, e incluso respaldar sus conocimientos con certificaciones. 6. Convenios o suscripción de tratados internacionales. 7. Desarrollo de proyectos que permitan llevar a cabo las recomendaciones del Grupo de Expertos Gubernamentales – Delitos Cibernéticos de la OEA.
Formación	1. Desarrollo de programas de capacitación al órgano legal (Fiscales, Jueces, Abogados) sobre los delitos informáticos y la informática legal. 2. Capacitación a los profesionales de tecnología en aspectos básicos de informática legal, forense, criminalística, manejo de evidencias digitales, etc. 3. Fomentar el desarrollo de programas que involucren la disertación del peritaje informático, legislación existente que atañen a la informática, criminalística. 4. Desarrollo de programas de especialización que

SECCION	RECOMENDACIÓN
	contemplen profesionales en informática forense y/o legal que pueden darse en cooperación con organismos especializados o entre convenios universitarios.
Tecnología	1. Convenios institucionales (universidades, gremios, etc.) 2. Cooperación y transferencia de conocimiento con países vecinos, o con quienes se hayan establecido convenios internacionales, sobre la tecnología existente o el desarrollo de las mismas que permitan la persecución de los delitos informáticos. 3. Implementación de laboratorios especializados forenses informáticos.
Sociedad	1. Advertir a los usuarios sobre las posibilidades u probabilidad de ocurrencia de delitos informáticos 2. Difusión de medidas de salvaguarda tal como el cierre de brechas de seguridad, como medidas de prevención ciudadana ante delitos de índole tecnológico. 3. Concientización en las organizaciones de que las medidas de seguridad más que un gasto son una inversión que proveen mecanismo para evitar este tipo de delitos. 4. Concientización del efecto e impacto de los delitos informáticos sobre la sociedad.

Tabla 4.1. Recomendaciones por sector – delitos informáticos.

Es indudable que los países latinoamericanos están tomando iniciativas que les permite desarrollar estrategias para el seguimiento de los delitos informáticos, hemos visto como Argentina y Colombia han elaborado y aprobado las respectivas

regulaciones que protegen el bien jurídico: la información, entonces, Ecuador que cuenta ya con el entidad de certificación de las firmas electrónicas, la Ley de Comercio Electrónico, Firmas Digitales y Mensaje de Datos e iniciativas que permiten el seguimiento de ciertos aspectos tecnológicos con el proyecto "Libertador", entre otros, debe embarcarse en un proyecto de permita delinear aspectos regulatorios sobre las tecnologías de la información.

Sin duda alguna, el avance tecnológico y la necesidad de establecer mecanismos que permitan la persecución de actos ilícitos cometidos utilizando medios tecnológicos generará una nueva generación de profesionales que 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.

BIBLIOGRAFÍA

1. María de la Luz Lima, Delitos Electrónicos Pág. 100, Ediciones Porrua - México 1984.
2. Julio Téllez Valdés, Derecho Informático, 2da Edición, Mc Graw Hill – México 1996.
3. Convenio de Cyber-delincuencia del Consejo de Europa Estados miembros del Consejo de Europa y otros Estados – Budapest 2001 http://www.coe.int
4. Carlo Sarzana Criminalitá e Tecnología en Computer Crime Rasaggna Penitenziaria e Criminalitá – Roma 1979.
5. Montiel Sosa, Criminalística Tomo III Página 86, Editorial Limusa 1997.
6. Red IRIS, Informe de Evolución de Incidentes de Seguridad, 2007, http://www.rediris.es/
7. CERT, Informe de Vulnerabilidades, 2007, http://www.cert.org/
8. CSI. Computer Crime & Security Survey, 2007, http://www.gocsi.com/
9. Eoghan Casey E, Digital Evidence and Computer Crimen, Página 9, 2da Edición, Edit Elsevier Ltda, 2004
10. Miguel López Delgado, Análisis Forense Digital, Página 5, 2da Edición, 2007
11. Jeimy J. Cano M, Introducción a la Informática Forense, Revista Sistemas N° 96, Publicado por Asociación Colombiana de Ingeniero de Sistemas (ACIS), 2006, http://www.acis.org.co/
12. FBI, Computer Evidence Examinations at the FBI, 2nd International Law Enforcement Conference on Computer Evidence, 1995, http://www.fbi.gov/

13. Gerberth Adín Ramírez, Informática Forense, Página 2, Publicación Universidad San Carlos de Guatemala, 2008.
14. Miguel López Delgado, Análisis Forense Digital, Página 10-23, 2da Edición, 2007
15. Pedro Miguel Lollet R, Auditoria Forense, Publicado por ACGAF, http://auditoriaforense.net/
16. Hans Kelsen, General Theory of Law and State, Harvard University, Editorial Porruo 1945
17. Ley Modelo sobre Comercio Electrónico, CNUDMI – Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, 1996 complementada por la Comisión en 1998. http://www.uncitral.org/
18. Ley Modelo sobre Firmas Electrónicas, CNUDMI – Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, 2001, http://www.uncitral.org/
19. Gerberth Adín Ramírez, Informática Forense, Página 4, Publicación Universidad San Carlos de Guatemala, 2008.
20. Grupo Faro, Acción Colectiva para el Bienestar Público, Cumplimiento de la Ley Lotaip, 2007, http://www.grupofaro.org/
21. Diario el Telégrafo, Edición N° 45119, Transparencia en la Información Pública, Página 4 y 5, Publicación Octubre 27 del 2008.
22. Business Software Alliance BSA, 5ta Estudio Anual Global de la Pirateria de Software por BSA e IDC, 2007, http://global.bsa.org/idcglobalstudy2007/
23. Juan Carlos Riofrío – La Prueba Electrónica. Editorial TEMIS S.A. Edición 2004

24. Emilio del Peso Navarro, Peritajes Informáticos, Página 10, 2da Edición, Editorial Díaz de Santos S.A, 2001
25. Jeimy J. Cano M, Estado del arte del Peritaje Informático en Latinoamérica, 2005, http://www.alfa-redi.org/
26. Jeimy J. Cano M, Consideraciones sobre el Estado del arte del Peritaje Informático en Latinoamérica, Revista de Derecho Comunicaciones y Nuevas Tecnologías, Universidad de los Andes, 2007, http://derechoytics.uniandes.edu.co/
27. Phil Williams, Crimen Organizado y Cibernético, Centro de Enseñanza en Seguridad de la Internet de la Universidad Carnegie Mellon, http://www.pitt.edu/
28. Plan de Seguridad Ciudadana y Modernización de la Policía Judicial, http://www.policiaecuador.gov.ec/publico/img_policia/rendicion.pdf
29. Plan Operativo de creación de la Unidad de Delitos Informáticos del Ministerio Público, http://www.oas.org/juridico/spanish/cyb_ecu_plan_operativo.pdf
30. Grupo de Expertos Intergubernamentales en Materia de Delitos Cibernéticos, http://www.oas.org/juridico/spanish/cybersp.htm
31. DIJIN (Dirección Central de Policía Judicial, http://www.dijin.gov.co/