UNIVERSIDAD DON BOSCO DE EL SALVADOR

VICERRECTORÍA DE ESTUDIOS DE POSTGRADO

TRABAJO DE GRADUACIÓN

PARA OPTAR AL GRADO DE MAESTRO EN SEGURIDAD Y GESTIÓN DE RIESGOS INFORMATICOS

MODALIDAD PROYECTO DE INVESTIGACIÓN:

DESAFÍOS A ENFRENTAR EN LA APLICACIÓN DE LEYES SOBRE DELITOS INFORMÁTICOS EN EL SALVADOR

PRESENTADO POR:

OSCAR CARLOS ERNESTO AGUIRRE LINARES

JORGE ANTONIO SEVILLANO FLORES

Contenido

INTRODUCCIÓN

I. INTRODUCCIÓN

El presente proyecto tiene como objetivo brindar una visión global de los delitos informáticos en El Salvador, respecto a regulación, iniciativas de investigación, tecnología y formación de los especialistas que investigan dicho delitos, así como también identificar los retos y brechas que deben de ser superados para su tratamiento.

Se planteará un marco conceptual de los delitos y la criminalidad informática, así como también las leyes relacionadas que se encuentran establecidas en nuestra legislación, nos referiremos al perfil necesario para ejercer como perito, la acreditación de los mismos y las fases del proceso pericial. Además del perfil necesario para ejercer como perito, en el documento se establecen las habilidades de un perito.

Finalmente haremos una investigación de cómo se están tratando los delitos informáticos en Latinoamérica y observaremos los retos a nivel de formación, limitaciones tecnológicas, así como el marco legal de El Salvador para hacer frentes a delitos que hacen uso de tecnología.

OBJETIVOS

II. OBJETIVOS

Objetivo General

Realizar una investigación que origine un documento que sirva como guía para identificar los delitos informáticos, como tratarlos, como documentarlos, bajo que legislación deben de ser tratados, que habilidades o características debe de poseer el perito informático para llevar a buen término la investigación que corresponde a la informática forense.

Objetivos Específicos

- Elaborar un marco conceptual que permita identificar los delitos informáticos en El Salvador, así como también identificar el marco legal establecido para el tratamiento de dichos delitos.
- Proponer el perfil de un perito informático que sea capaz de realizar una investigación forense en la rama de las tecnologías de la información.
- Elaborar una propuesta que identifique la entidad que administrará los delitos informáticos, tomando como base los retos a superar en cuanto a las disposiciones establecidas en la legislación salvadoreña. Así mismo se elaborará una propuesta de un organigrama funcional que debe de tener dicha entidad. En la propuesta se incluirá el análisis y revisión de las regulaciones existente en Latinoamérica y que puedan aplicar a nuestra legislación. Además se presentarán los inconvenientes que se presentan en el proceso pericial y de investigación tecnológica.

CAPITULO 1

1. MARCO CONCEPTUAL Y LEGISLACION EN EL SALVADOR

1.1. LOS DELITOS INFORMÁTICOS

Hoy día, la informática está presente en casi todos los campos de la vida moderna, tarde o temprano cualquier rama del saber humando utiliza los progresos tecnológicos y empiezan a utilizar sistemas informáticos.

Hace un par de años atrás, teníamos la seguridad que nadie podía acceder a nuestra información privada. Hoy en día, dado que la información personal es un bien cotizado, existen sistemas que pueden guardar grandes cantidades de información y a su vez transmitirla en corto tiempo, esto sin que ninguna legislación pueda regularlo satisfactoriamente.

Investigar cualquier tipo de delito es una tarea compleja y con el paso del tiempo, la globalización no solo ha tenido beneficios, sino que ha contribuido a la masificación de algunos delitos y a su tecnificación, a partir de esto surgen los que ahora conocemos como delitos informáticos. Dichos delitos son catalogados por algunos expertos en la materia, como parte del crimen organizado (ver artículo del Dr. Santiago Acurio del Pino http://www.alfa-redi.org/sites/default/files/articles/files/acurio_0.pdf). Dentro del crimen organizado y al individualizar los delitos, surgen los personajes conocidos como CRACKERS, los verdaderos piratas informáticos, que a través del cometimiento de infracciones informáticas, han causado la perdida de varios millones de dólares, a empresas, personas y también a algunos estados.

¿Por qué los crackers son clasificados como crimen organizado?

Como escribe Albanese, citado por Carlos Resa[1], *"el crimen organizado no existe como tipo ideal, sino como un "grado" de actividad criminal o como un punto del 'espectro de legitimidad"*. En este contexto es el crimen organizado que a través de los años ha ido transnacionalizando su actividad y por ello se habla de Delincuencia Transnacional.

Su repertorio de actividades incluye el delito de cuello blanco y el económico (en donde se encontrarían los Delitos Informáticos), pero supera a éste último en organización y control, aunque los nexos de unión entre ambos modelos de delincuencia tienden a fusionarse.

Por lo tanto, abordar el estudio de las implicaciones de la informática en la delincuencia, resulta apasionante tanto para los especialistas de la seguridad de la información así como también para los especialistas en legislaciones y sistemas judiciales, ya que cada vez surgen nuevos escenarios y problemas por el uso de la tecnología.

Paralelamente al avance de la tecnología, también los comportamientos de los delincuentes cambian, y al utilizar las tecnologías resulta difícil la tipificación de los delitos en normas penales tradicionales.

Nuestro país, sin lugar a duda parte de la globalización, se ve afectado por los elementos antes mencionados, y resulta un hecho preocupante que nuestro código penal entró en vigencia en 1974, ya hace 40 años, por lo que es claro que los delitos resultantes de actos informáticos no

1 RESA NESTARES CARLOS: Crimen Organizado Transnacional: Definición, Causas Y Consecuencias, Editorial Astrea, 2005.

están incluidos en nuestra legislación. Por lo que hay que empezar a tomar medidas ante una situación que ya es una realidad, es por ello que el presente trabajo pretende dar un aporte de referencia documental acerca de los delitos informáticos en El Salvador.

Al profundizar sobre las fuentes, encontramos que el Convenio de Cyber-delincuencia del Consejo de Europa, 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*".

Es importante recalcar, que el convenio europeo resalta, los tres elementos que integran el concepto de seguridad: 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

La criminología trata de investigar el por qué y que fue lo que llevo al individuo a cometer el delito, mientras que la criminalística se define 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.

A continuación presentamos algunos datos recabados por REDIRIS, que muestra la evolución histórica de los incidentes:

Según REDIRIS la razón principal que explica el descenso de incidentes atendidos durante el año 2013 es que, no ha sido posible atender algunas quejas procedentes de sistemas automáticos externos que requieren mucha dedicación de recursos, puesto que desde Agosto de 2012 el CERT no dispone del recurso que proporcionaba el primer nivel de atención de incidentes.

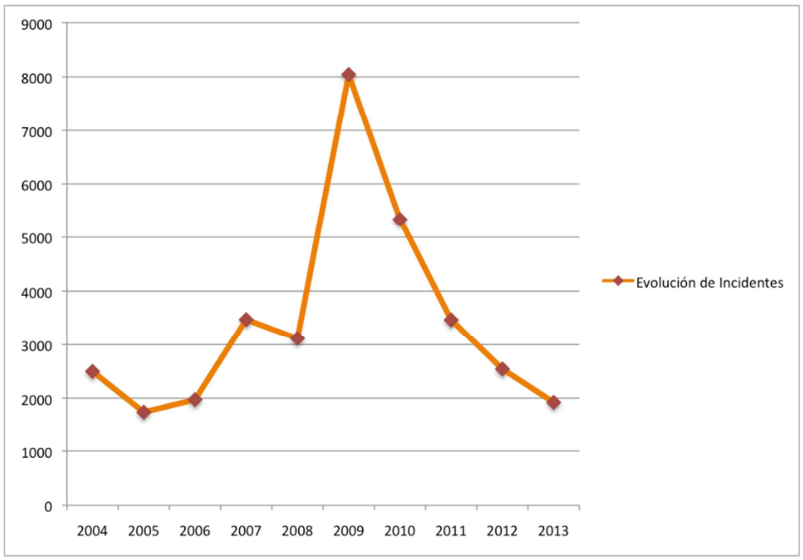

Ilustración 1- Evolución histórica de incidentes 2013

Otro organismo que realiza investigaciones de este nivel es el CERT-UNAM que publica una gran variedad de estadísticas relacionadas con vulnerabilidades e incidentes:

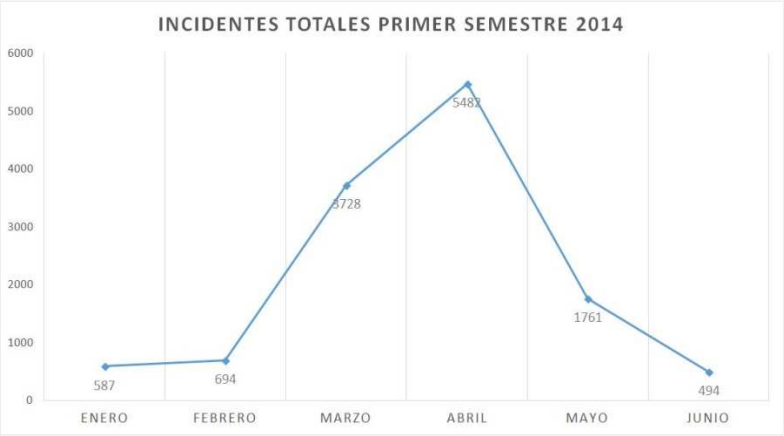

Ilustración 2-Incidentes CERT - UNAM 2014

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.

TIPOS DE DELITOS INFORMÁTICOS.

Podemos definir que con respecto al delito del hurto, el bien jurídico protegido 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. A partir de esto resulta la tabla 1, tipificación de los delitos informáticos.

<table>
<tr><th>Reconocidos por la Naciones Unidas
Fuente: Organización de Naciones Unidas</th><th>Abogados especializados en delitos informáticos
Fuente: http://informática-jurídica.com</th></tr>
<tr><td>Fraudes mediante la manipulación de computadoras (programas, datos de entrada y salida, repetición automática de procesos</td><td rowspan="2">Fraudes mediante la manipulación de computadoras:
1. Delitos contra elementos físicos – Hardware (robo, estafa)
2. Delitos contra elementos lógicos (daños, accesos ilícitos a sistemas, acceso ilícito a datos, protección de programas.</td></tr>
<tr><td>Falsificaciones informáticas (alteración de documentos, falsificación de documentos</td></tr>
<tr><td>Daños o modificaciones de programas o datos computarizados (sabotaje, virus, bombas lógicas)</td><td rowspan="2">Delitos cometidos a través de sistemas informáticos:
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</td></tr>
<tr><td>Accesos no autorizados a servicios y sistemas informáticos (piratas, reproducción no autorizada</td></tr>
</table>

Tabla 1- Tipificación de los delitos informáticos

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

- 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.).
- 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.).
- Espionaje informático: Divulgación no autorizada de datos reservados
- Pornografía Infantil: Inducción, promoción, producción, venta, distribución facilitamiento de prostitución, cuando se utilizan menores con fines de exhibicionistas o pornográficos.
- Infracciones de Propiedad Intelectual: Copia o reproducción no autorizada de programas informáticos de protección legal.

1.1.2. 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.

1.1.2.1. 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.

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, realizando todas las medidas de precaución necesarias para no contaminarla y que sea objeto de desestimación ante un proceso litigioso.

1.1.2.2. LA INFORMÁTICA FORENSE.

El FBI define la informática forense como "*la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y almacenados en un medio computacional*".

Esta ciencia se aplica tanto para las investigaciones de delitos tradicionales tales como: fraudes financieros, narcotráfico, terrorismo, etc.; como para aquellos que están estrechamente relacionados con las tecnologías de la información y las comunicaciones, entre los que se 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.

1.1.2.2.1. 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.

1.1.2.2.2. 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:

1) Levantar la operación del sistema. 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) Investigación forense detallada. Al seleccionar esta alternativa el profesional 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 uno de los pasos realizados y características o información de los hallazgos encontrados, es recomendable que durante el desarrollo de este proceso, lo asista u acompañe una persona, preferentemente imparcial.

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

(tabla 2) 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 2. Guías de mejores prácticas de computación forense.

1.1.2.3. 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. 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.

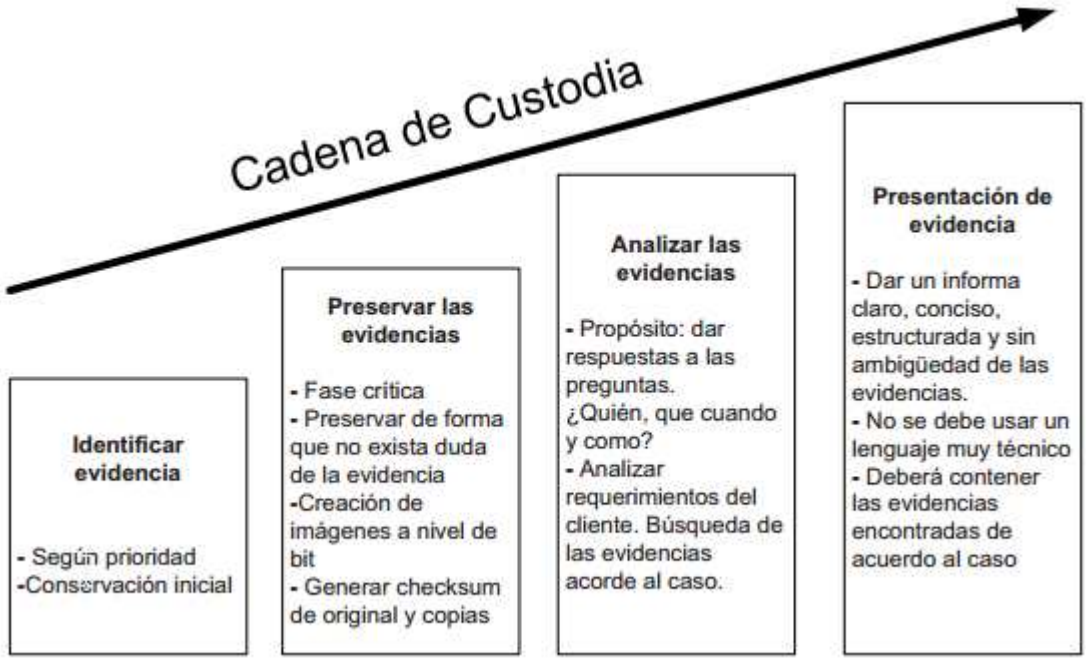

Ilustración 3 - Metodología del análisis forense. Blog Informática Forense Marta Cardenas

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.

1.1.2.3.1. 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?
- ¿Quiénes lo llevaron a cabo?
- ¿Bajo qué circunstancia se produjo y cuál era su objetivo?
- ¿Cuáles fueron los daños que se causaron?

1.1.2.4. 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.

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.

Dicho artículo también contempla que en el caso de que hubiesen desaparecido los vestigios de la infracción, los peritos opinarán, en forma debidamente motivada sobre si tal desaparición ha ocurrido por causas naturales o 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	Windows	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 3 - Solución de software forense

1.1.2.5. LA AUDITORÍA 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 sin número 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.

1.2. CONDICIONES ESTABLECIDAS EN LA LEGISLACIÓN SALVADOREÑA

Si bien es cierto El Salvador carece de leyes para castigar los delitos informáticos que se cometen, existe legislación o normas jurídicas que se relacionan indirectamente con las tecnologías de información las cuales se detallan a continuación a través de los elementos que conforman la pirámide de Kelsen en nuestro Sistema Jurídico Salvadoreño:

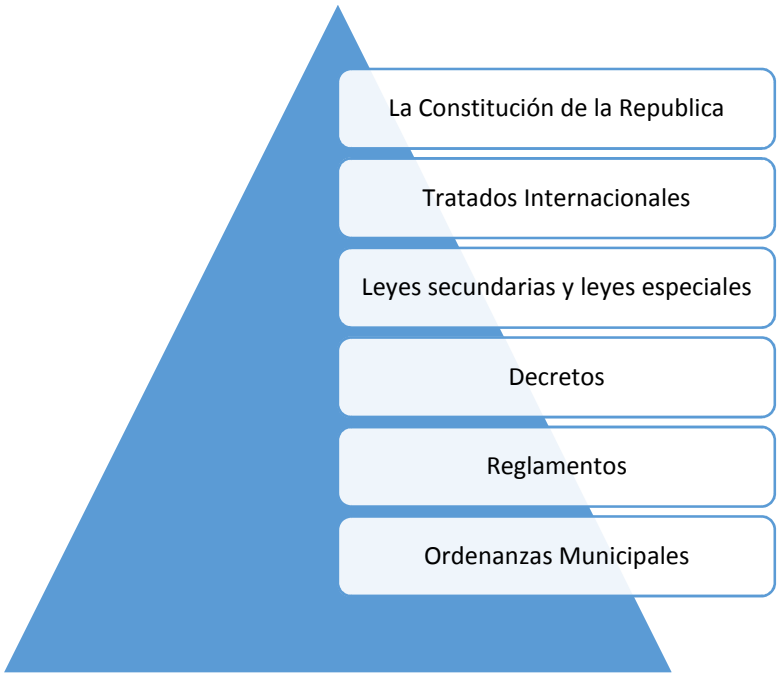

Ilustración 4 - Pirámide de Kelsen Sistema Jurídico Salvadoreño

Considerando lo anterior en la legislación de El Salvador se mantienen leyes que establecen apartados y especificaciones acorde con la importancia de las tecnologías, tales como:

Tipo de Legislación	Objeto de Ley	Ref. de Publicación	Fecha de Publicación
Ley de Acceso a la Información Pública	Garantizar el derecho de acceso de toda persona a la información pública, a fin de contribuir con la transparencia de las actuaciones de las instituciones del estado.	Diario Oficial No. 70 Decreto 534	02/12/2010
Ley de Propiedad Intelectual	Establecer las disposiciones que aseguran una protección suficiente y efectiva de la propiedad literaria, artística o científica e industrial.	Diario Oficial No. 150 Decreto 604	15/07/1993
Ley de Telecomunicaciones	Regula las actividades del sector telecomunicaciones, servicio público de telefonía, recursos esenciales y plan de numeración; lo anterior de conformidad con el articulo No.110 de la Constitución, es deber del estado regular y vigilar los servicios públicos, así como aprobar sus tarifas.	Diario Oficial No. 218 Decreto 142	06/11/1997
Ley Especial Para la Intervención de las Telecomunicaciones	Garantiza el secreto de las telecomunicaciones y el derecho a la intimidad, de manera excepcional podrá autorizarse judicialmente, por escrito y motivada la intervención temporal de las telecomunicaciones	Diario Oficial No. 51 Decreto 285	18/02/2010
Ley del Desarrollo Científico y	Establece las directrices para el desarrollo de la ciencia y de la tecnología, propiciando instrumentos y mecanismos institucionales y operativos	Diario Oficial No. 34 Decreto 234	14/12/2012

Tecnológico	para implementar una política nacional de innovación, ciencia y tecnología.		
Ley de Protección al Consumidor	Establece las disposiciones que protegen los derechos de los consumidores, crea el sistema nacional y la defensoría del consumidor.	Diario Oficial No. 166 Decreto 776	18/08/2005
Ley Especial Contra Actos de Terrorismo	Prevenir, investigar, sancionar, erradicar los delitos contra la paz pública.	Diario Oficial No. 193 Decreto 108	21/09/2006
Ley Orgánica de la Policía Nacional Civil de El Salvador	Protege y garantizar el libre ejercicio de los derechos y libertades de las personas; prevenir y combatir toda clase de delitos, así como la colaboración en el procedimiento para la investigación de delitos	Diario Oficial No. 240 Decreto 653	06/12/2001
Código Penal	Enuncia los delitos o faltas que cometen las personas y las penas que tendrán que cumplir	Diario Oficial No. 105 Decreto 1030	26/04/1997

Tabla 4 - Tabla resumen legislación Salvadoreña aplicable a delitos informáticos

1.2.1.LEY DE ACCESO A LA INFORMACIÓN PÚBLICA

La Ley de Acceso a la Información publicada en el Diario Oficial No. 70 Decreto 534 emitida el 02 de diciembre de 2010 tiene por objeto garantizar el derecho de acceso de toda persona a la información pública, a fin de contribuir con la transparencia de las actuaciones de las instituciones del estado; lo anterior tomando de base lo establecido en la Constitución de la Republica y tratados internacionales sobre Derechos Humanos en cuanto a que toda persona tiene derecho a la libertad de expresión, la cual comprende la libertad de buscar y difundir informaciones de toda

índole sin consideración de fronteras, ya sea escrita, verbal, electrónica o por cualquier otra forma.

La Corte Suprema de Justicia reconoció el año 2004 el derecho fundamental de todos los salvadoreños para la protección de datos o la autodeterminación informativa, considerando que toda persona tiene el derecho a acceder a la información sobre sí misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en el caso de que fuere necesario, actualizarla, rectificarla y/o enmendarla; lo anterior de conformidad a lo establecido en el Articulo No.3 Declaración de Principios de Libertad de Expresión, OEA, por lo anterior se considera importante la existencia del Habeas Data en la legislación salvadoreña:

- *"El Habeas data es una acción legal que permite a toda persona acceder al registro de la información que sobre ella existe en un banco de datos, y le permite solicitar la corrección de esos datos si le causa algún perjuicio".*

- *"Países como México, han desarrollado normas de protección de datos personales por parte de empresas e instituciones públicas. Uruguay, Argentina, Bolivia, Brasil, Colombia, España, Venezuela, Perú y Panamá son los que han adoptado tal disposición en sus Cartas Magnas".*

- *"El año 2000, España mediante una resolución del Tribunal Constitucional reconoció el derecho a la protección de datos como un derecho autónomo del derecho a la intimidad".*

- *"En El Salvador no existe tal nivel de desarrollo, al igual que en el resto de Centroamérica. El asunto sólo puede ser analizado por la Corte Suprema de Justicia al no existir una ley especial que regule la protección de datos".*

Según el segundo monitoreo al cumplimiento de la Ley de acceso a la información pública realizado en mayo de 2013 existe una tendencia orientada al debido cumplimiento por parte de las instituciones del sector público; así como también se muestra una tendencia de avance en el cumplimiento de las instituciones en la divulgación de información oficiosa desde sus portales

web de transparencia, el 73% de los entes obligados reflejaron avances, el 20% de las instituciones retrocedió y un 7% de instituciones se mostró invariable respecto al ranking anterior.

1.2.2 LEY DE PROPIEDAD INTELECTUAL

La Ley de Propiedad Intelectual publicada en el Diario Oficial No. 150 Decreto 604 emitida el 15 de julio de 1993 tiene por objeto establecer las disposiciones que aseguran una protección suficiente y efectiva de la propiedad literaria, artística o científica e industrial; lo anterior considerando:

1) *"Que según lo establecido en el inciso segundo del Artículo 103 de la constitución el cual reconoce la propiedad intelectual y artística, por el tiempo y en la forma determinados por la Ley".*

2) *"Que el inciso tercero del Articulo 110 de la constitución, establece que se podrá otorgar privilegios por tiempo limitado a los descubridores e inventores y perfeccionadores de los procesos productivos".*

3) *"Que en vista del desarrollo alcanzado por tales materias, es necesario dictar nuevas disposiciones legales que protejan y regulen aspectos de suma importancia como lo son entre otros, la gestión colectiva, la protección de los modelos de utilidad, diseños industriales, secretos industriales y comerciales, que la legislación vigente no comprende".*

4) *"Que tanto la propiedad literaria, artística o científica, como la propiedad industrial, son las dos ramas que forman la propiedad intelectual, por lo que todas las disposiciones que regulen tales materias pueden reunirse en un solo cuerpo legal".*

La entidad encargada de supervisar las actividades relativas al derecho de autor y la propiedad intelectual en El Salvador es el Centro Nacional de Registros (CNR) quien según su misión institucional es la encargada de "*Contribuir a garantizar la seguridad jurídica y equidad en la prestación de servicios de registro de comercio, inmobiliario y propiedad intelectual; así como proveer información geográfica, cartográfica y catastral de El Salvador, en forma oportuna,*

confiable y de calidad; mediante una gestión transparente, solidaria y comprometida con el desarrollo económico y social del país".

Dar a conocer la importancia que tiene la Propiedad Intelectual en El Salvador 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.

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; además 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 de Propiedad Intelectual en su Artículo No. 14 incluye la protección de bases de datos que se encuentren en forma legible por maquina o en otra forma, así como también los programas de ordenador (software) los cuales son considerados como obras literarias, tal como lo establece los Artículos No. 12 y 13 de la referida Ley.

El estudio de piratería mundial de software, que corresponde al año 2011, realizado por la International Data Corporation (IDC), publicado por la Business Software Alliance (principal impulsor de la industria del software mundial ante lo gobiernos y el mercado internacional), establece que El Salvador mantiene una tasa de piratería de un 80%, que constituyen pérdidas por

aproximadamente 58 millones de dólares y representan un incremento aproximadamente del 48% con respecto a la medición del 2007 (30 millones de dólares).

Las iniciativas dadas para la protección y respeto de las especificaciones de la Ley de Propiedad Intelectual en nuestro país han sido promovidas por el CNR a través de concursos que pretenden incentivar a inventores salvadoreños para que presenten sus creaciones y conozcan sobre la protección de los derechos intelectuales; así como campañas que impulsa Business Software Alliance (BSA) tales como “Defiende los derechos de la propiedad intelectual”, “Detiene el robo de software”, “Educa la Publico”, “predicar con el Ejemplo”, este último está orientado a los gobiernos quienes son los mayores usuarios de software en el mundo, ellos deben demostrar liderazgo asegurándose de que están usando solo software completamente licenciado en sus propias operaciones.

1.2.3 LEY DE TELECOMUNICACIONES

La Ley de Telecomunicaciones publicada en el Diario Oficial No. 218 Decreto 142 emitida el 06 de noviembre de 1997 tiene por objeto regular las actividades del sector telecomunicaciones, servicio público de telefonía, recursos esenciales y plan de numeración; lo anterior de conformidad con el articulo No.110 de la Constitución, es deber del estado regular y vigilar los servicios públicos, así como aprobar sus tarifas.

La entidad responsable de aplicar y velar por el cumplimiento de las normas y regulaciones establecidas en esta Ley y su reglamento es la Superintendencia General de Electricidad y Telecomunicaciones.

1.2.4 LEY ESPECIAL PARA LA INTERVENCIÓN DE LAS TELECOMUNICACIONES

La ley especial para la intervención de las telecomunicaciones, publicada en el Diario Oficial No. 51 Decreto 285 emitida el 18 de febrero de 2010 tiene por objeto garantizar el secreto de las

telecomunicaciones y el derecho a la intimidad, de manera excepcional podrá autorizarse judicialmente, por escrito y motivada la intervención temporal de las telecomunicaciones; lo anterior de acuerdo a:

1) *"Los artículos No. 2 de la constitución, 17 del Pacto Internacional de Derechos Civiles y Políticos y 11 de la Convención Americana sobre Derechos Humanos nadie puede ser objeto de injerencias ilegales, arbitrarias o abusivas en su vida privada y la de su familia, y toda persona tiene derecho a la protección contra esas injerencias o ataques".*

2) *"Que entre los instrumentos o herramientas de persecución penal que se consideran más eficaces en la lucha contra la delincuencia grave, organizada y transnacional se encuentra la posibilidad de intervenir la telecomunicaciones como limitación legitima, necesaria, proporcionada y razonable del derecho constitucional al secreto de las comunicaciones, en el ámbito del derecho fundamental a la intimidad".*

3) *"Que mediante el acuerdo de reforma constitucional No.5, de fecha 29 de abril, publicado en el Diario Oficial No.88, Tomo No. 383, de fecha 15 de mayo, ratificado por Decreto Legislativo No. 36, del 27 de mayo, publicado en el Diario Oficial No.102, Tomo No.383, del 4 de junio, todas las fechas de 2009, se reformo el artículo 24 de la Constitución a fin de permitir excepcionalmente la intervención temporal de las telecomunicaciones, previa autorización judicial motivada, para la investigación de los delitos que una Ley Especial determine".*

4) *"Que la intervención de las telecomunicaciones constituye un instrumento útil en la persecución del delito, en particular la criminalidad organizada, pero su utilización debe estar resguardada por garantías que eviten abusos contra la intimidad de las personas".*

1.2.5 LEY DEL DESARROLLO CIENTÍFICO Y TECNOLÓGICO

La Ley del Desarrollo Científico y Tecnológico, publicada en el Diario Oficial No. 34 Decreto 234 emitida el 14 de diciembre de 2012, tiene por objeto establecer las directrices para el desarrollo de la ciencia y de la tecnología, propiciando instrumentos y mecanismos institucionales y

operativos para implementar una política nacional de innovación, ciencia y tecnología; lo anterior considerando:

1) *"Que de conformidad con el artículo No. 53 de la Constitución, es obligación del Estado propiciar la investigación y el quehacer científico, con la finalidad de contribuir, de forma sostenible, al desarrollo social, económico y ambiental del país".*

2) *"Que es de suma importancia dotar al país de mecanismos institucionales y legales para propiciar la investigación, al igual que el quehacer científico y tecnológico y promover la innovación".*

3) *"Que se requiere crear las condiciones adecuadas para que la ciencia y la tecnología, se constituyan en factores relevantes de la eficiencia de aquellos sectores en los cuales el progreso científico y tecnológico tengan incidencia en su desarrollo, y en consecuencia, contribuya al enriquecimiento de la cultura y la elevación del nivel de vida de la población salvadoreña".*

1.2.6 LEY DE PROTECCIÓN AL CONSUMIDOR

La Ley de Protección al Consumidor, publicada en el Diario Oficial No. 166 Decreto 776 emitida el 18 de agosto de 2005, tiene por objeto establecer las disposiciones que protegen los derechos de los consumidores, crea el sistema nacional y la defensoría del consumidor; lo anterior considerando:

1) *"Que el articulo No.101 de la constitución dispone que el orden económico debe responder esencialmente a principios de justicia social, con el fin de asegurar a todos los habitantes del país una existencia digna del ser humano, correspondiéndole al Estado la promoción, la productividad y la racional utilización de los recursos; así como el fomento de los diversos sectores de la producción y defender el interés de los consumidores".*

2) *"Que según lo establecen las Directrices de Naciones Unidad para la Protección del Consumidor, corresponde a los gobiernos formular y mantener una política de protección al consumidor, tomando en cuenta el derecho de los consumidores de tener acceso a productos*

seguros, así como la importancia de promover un desarrollo económico y social justo, equitativo y la protección del medio ambiente".

3) *"Que la Ley de Protección al Consumidor, aprobada por Decreto Legislativo No.666, de fecha 14 de marzo de 1996, publicado en el Diario Oficial No.58, Tomo No. 330 del 22 de ese mismo mes y ano, no obstante las innovaciones que introdujo, requiere una mejor estructura y desarrollo sistemático, así como una visión integral y preventiva que garantice la protección de los consumidores".*

4) *"Que es indispensable mantener la vigencia plena de los principios rectores del modelo de economía de mercado, fomentando el comportamiento ético de los empresarios y promoviendo la igualdad de oportunidades entre los mismos".*

1.2.7 LEY ESPECIAL CONTRA ACTOS DE TERRORISMO

La Ley Especial Contra Actos de Terrorismo, publicada en el Diario Oficial No. 193 Decreto 108 emitida el 21 de septiembre de 2006, tiene como objeto prevenir, investigar, sancionar, erradicar los delitos contra la paz pública; lo anterior considerando:

1) *"Que el Salvador reconoce a la persona humana como el origen y el fin de la actividad del Estado y es su obligación asegurar a los habitantes el goce de la libertad, la seguridad jurídica y el bien común, de conformidad con la Constitución".*

2) *"Que El Salvador es suscriptor de la Carta de la Organización de la Naciones Unidad, la cual contiene principios fundamentales para los Estados, tales como mantener la paz y la seguridad internacional, su debido cumplimiento; así como de las resoluciones dictadas por el Consejo de Seguridad de Naciones Unidad, por las cuales se deben tomar medidas eficaces para prevenir, combatir y erradicar amenazas contra la paz, considerando entre las más graves al terrorismo y todas sus manifestaciones, incluyendo su financiamiento".*

3) *"Que actualmente el terrorismo constituye una grave amenaza para la seguridad del país, la paz pública y la armonía de los Estados, afectando directa e indirectamente a sus nacionales en su integridad física y moral, así como en la propiedad, posesión y conservación de sus derechos, lo que hace necesario la creación de una ley especial para prevenir, investigar,*

sancionar y erradicar las actividades terroristas respondiendo a las circunstancias actuales y excepcionales que afectan a la comunidad internacional".

1.2.8 LA LEY ORGÁNICA DE LA POLICÍA NACIONAL CIVIL DE EL SALVADOR

La Ley Orgánica de la Policía Nacional Civil de El Salvador, publicada en el Diario Oficial No. 240 Decreto 653 emitida el 06 de diciembre de 2001, tiene por *objeto* proteger y garantizar el libre ejercicio de los derechos y libertades de las personas; prevenir y combatir toda clase de delitos, así como la colaboración en el procedimiento para la investigación de delitos; lo anterior considerando:

1) Que la Constitución, establece que *"la Policía Nacional Civil tendrá a su cargo las funciones de policía urbana y policía rural, quien garantizara el orden, la seguridad y la tranquilidad pública, así como la colaboración en el procedimiento de investigación del delito, todo ello con apego a la ley y estricto respeto a los derechos humanos".*

Además de lo anterior descrito El Salvador ha mostrado interés en implementar la tecnología de información en su legislación para lo cual durante el año 2013 se inició con el proyecto de Ley de Firma Electrónica el cual tiene como objeto, equiparar la firma electrónica simple y firma electrónica certificada con la firma autógrafa, además de regular y fiscalizar lo relativo a los proveedores de servicios de certificación electrónica; este proyecto esta es iniciativa del Ministerio de Economía y de la Asociación Nacional de la Empresa Privada (ANEP) del cual aún no existe respuesta por parte del Gobierno Salvadoreño.

1.2.9 EL CODIGO PENAL

El Código Penal, publicado en el Diario Oficial No. 105 Decreto 1030 emitida el 26 de abril de 1997, enuncia los delitos o faltas que cometen las personas y las penas que tendrán que cumplir; lo anterior tomando como antecedente:

1) *"Que el Código Penal, fue aprobado por Decreto Legislativo No. 270 de fecha 13 de febrero de 1973, publicado en el Diario Oficial No. 63, Tomo 238, de fecha 30 de marzo del mismo*

año, el cual entro en vigencia el 15 de junio de 1974, y este represento un adelanto dentro del desarrollo de la ciencia penal y la técnica legislativa y en la actualidad ya no se perfila de la misma manera porque su contenido no guarda concordancia con el texto de la Constitución de la Republica de 1983, ni con la realidad política y social que vive el país".

2) *"Que los estados Democráticos de Derecho, se han visto en la necesidad de adecuar sus normativas penales a la nueva orientación doctrinaria, que considera el Derecho Penal como último recurso para resolver los conflictos sociales y el instrumento más efectivo para lograr la paz y seguridad jurídica de los pueblos, lo cual El Salvador comparte plenamente".*

3) *"Que con el objeto de orientar nuestra normativa penal dentro de una concepción garantista, de alta efectividad para restringir la violencia social y con una amplia proyección de función punitiva no selectivista, resulta conveniente que se emita un nuevo Código Penal, que sin apartarse de nuestros patrones culturales, se constituya en un instrumento moderno, dinámico y eficaz para combatir la delincuencia".*

CAPITULO 2

2. EL PERITO Y EL PERITAJE INFORMATICO

2.1 EL PERITO

La conceptualización de un perito en general, es que son personas expertas en una determinada materia que gracias a sus conocimientos, actúa como fuente de consulta para la resolución de conflictos; 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.

Schiaffino Machado (1), estable que el rol del Perito "*como parte del todo, tanto procesal como extraprocesalmente, hace a un plexus emisor-operador-receptor. Si bien se ha avanzado, los intentos por investigar aún no han proporcionado elementos estructurados para una revisión crítica o formulaciones de singular importancia*".

2.1.1. LA PERICIA Y LA PERITACIÓN.

La pericia es un informe, un análisis, una tasación realizada para personas interesadas en su opinión.

Por otra parte la peritación se entiende como una actividad procesal por naturaleza porque tiene lugar en un proceso judicial o como medida procesal previa.

Según el autor Hernando Devis Echandia (2) la labor del perito "*Es una actividad procesal, desarrollada en virtud de encargo judicial, por personas distintas a las partes en el proceso, especialmente calificadas por sus conocimientos técnicos, artísticos o científicos, mediante la cual se suministran al juez argumentos o razones para la información de sus convencimientos respecto de ciertos hechos cuya percepción o entendimiento escapa a las aptitudes del común de las gentes*".

Emilio del Peso Navarro (3), 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.

2.1.2. Organismo Facultado Para la Acreditación de los Peritos

En El Salvador la entidad encargada[2] de registrar a los peritos evaluadores es la Superintendencia del Sistema Financiero; aunque hoy en día esta actúa sobre la base de la Ley de Bancos y las Normas NPB4-39 "Normas Para la Inscripción de Peritos Valuadores" y sus Obligaciones Profesionales en el Sistema Financiero y para los efectos de la valoración de los bienes muebles e inmuebles de los bancos, así como cuando por disposiciones legales se hace necesario valorar dichos bienes que reciban en garantía.

En la actualidad la inscripción es por un plazo de dos años, pudiéndose prorrogar siempre que el perito cumpla los requisitos legales y reglamentarios aplicables.

Deberes del Perito.

Los deberes del Perito, según Devis Echandía (2) se descomponen así: "*de asumir el cargo, cuando la designación no es hecha libremente por la parte; de comparecer ante el Juez, cuando existe esa formalidad; de posesionarse y prestar el juramento; de practicar personalmente las operaciones necesarias para su dictamen, bajo el control del Juez y en la forma como la Ley Procesal determine; de obrar y conceptuar con lealtad, imparcialidad y buena fe; de fomentar su dictamen y de rendirlo en forma clara y precisa; de guardar el secreto profesional, cuando el caso lo requiera*."

[2] Art. 226 código procesal penal establece quienes pueden ser peritos. Auditores de TI de la corte de cuentas, profesionales que dan fe pública, contadores públicos, abogados.

Tanto la defensa de sus Derechos como la exigencia de sus Deberes y Responsabilidades apuntan a un mismo objetivo: la eficacia probatoria del Dictamen en sede Judicial.

2.1.3. DERECHOS DEL PERITO.

De dos clases son los Derechos[3] que al Perito le corresponden: "*a) el Derecho Patrimonial a que se le suministre el dinero para los gastos y a recibir una remuneración por su trabajo; b) el Derecho a que se le faciliten los medios adecuados para el estudio de las cuestiones sometidas a su consideración y a gozar de absoluta libertad para su investigación*."

A diferencia del testigo que al deponer cumple un deber cívico, el perito al dictaminar cumple una simple función profesional; y de aquí que tiene derecho no sólo a una indemnización por los gastos, sino también a los honorarios

La capacidad de la persona para desempeñar la función de Peritos, puede ser:

a) **La abstracta** o general se refiere a requisitos de edad, ser la persona mayor de 21 años, por ser el cargo de perito de una gran responsabilidad, nuestra legislación procesal civil no señala como requisito que sean mayores de edad, pero consideramos que una persona mayor de edad tienen conocimientos medios o ha adquirido conocimientos técnicos conforme al desarrollo de nuestra civilización que lo pueden capacitar para comprender mejor sus decisiones. Es necesario, también, que se encuentre gozando de sanas facultades mentales, por lo cual debe de descartarse como Perito aquellas personas afectadas por una enfermedad mental o que posean deficiencias o perturbaciones mentales; así como aquellas que fueren condenadas por perjuros o falsarios, y si esto es una incapacidad para ser testigo, por razones de probidad, con mucha mayor razón para el desempeño de esta función Pericial; finalmente, los que tuvieren algún interés, ya sea económico con las partes y el juez instructor del proceso.

b) **Específica** se refiere a las aptitudes de carácter técnico o conocimientos especiales en una ciencia, arte o industria, destreza o condiciones fundamentales.

[3] Artículo 229, 240 código procesal penal.

c) La concreta se refiere al proceso de que se trate, en el cual se pueden presentar motivos en que el perito esté impedido de ejercitar su función en el caso concreto sometido a Dictamen.

Estos motivos pueden ser impedimentos o causas de incompatibilidad en relación con otra clase de función distinta a la Pericial; por causa de exclusión en relación con las personas y los hechos del proceso donde deberá dictaminar o por reexcusarse del cargo.

2.1.4. Perfil del Perito Informático

El perito informático debe poseer un perfil[4] definitivamente técnico, siendo de vital importancia que el perito esté familiarizado con las técnicas de análisis y recuperación de datos. Como elemento adicional, el perito debe contar con amplios conocimientos legales que le permitan desarrollar su tarea sin que la misma sea descalificada o impugnada durante su presentación judicial.

Las tareas a desarrollar por el perito informático no son distintas de la de otros peritos judiciales. Por lo tanto deberá recopilar la información que es puesta a su disposición, analizar la misma en busca de los datos que el juez le ha requerido y emitir un informe o dictamen en donde vuelque las conclusiones de la investigación realizada.

2.1.4.1. Deberes del Perito Informático[5]

- Aceptar el cargo que le es asignado, colaborar con el resto de los peritos o consultores técnicos y declarar ante el juez en el caso de que este lo requiera.
- Fundamentar sus conclusiones técnicas, expresando claramente los elementos analizados y las técnicas utilizadas para llegar a las mismas.
- Respetar el código de ética que le impone su profesión.

2.1.4.2. Áreas de Actuación de los Peritos Informáticos

- Propiedad industrial: Espionaje / Revelación de secretos.
- Acceso o copia de ficheros de la empresa, planos, fórmulas, etc.
- Uso de información: Competencia desleal de un empleado.

[4] Artículo 227 código procesal penal
[5] Artículo 228, 236, 239 código procesal penal

- Vulneración de la intimidad. Lectura de correo electrónico.
- Despido por causas tecnológicas.
- Valoraciones de bienes informáticos.
- Interceptación de telecomunicaciones.
- Protección de datos personales y datos reservados de personas jurídicas.
- Apoderamiento y difusión de datos reservados.
- Manipulación de datos o programas.
- Valoraciones de bienes informáticos.
- Hardware, redes y componentes (todos los sistemas).
- Instalaciones y desarrollos llave en mano.
- Vulneración de la buena fe contractual.
- Publicidad engañosa, competencia desleal.
- Delitos económicos, monetarios y societarios.
- Delitos contra el mercado o contra los consumidores.
- Delitos contra la propiedad intelectual.
- Uso de software sin licencia. Piratería.
- Copia y distribución no autorizada de programas de ordenador.
- Daños mediante la destrucción o alteración de datos. Sabotaje.
- Estafa, fraudes, conspiración para alterar el precio de las cosas, etc.
- Pornografía infantil: acceso o posesión, divulgación, edición, etc.
- Uso indebido de equipos informáticos: daños o uso abusivo.

2.1.5. Delitos Informáticos vs Peritos Informáticos

De acuerdo a diferentes estudios actuales, los delitos informáticos son los de mayor crecimiento en los últimos años. La posibilidad de su ejecución a través de Internet permite que sin mayores complicaciones, el delincuente pueda estar en determinado lugar e incluso país, usar servicios de otros, para finalmente atacar a una o más víctimas. La Evidencia digital es la madre de todas las evidencias y ayuda de manera inequívoca a esclarecer la causa de la mayoría de los litigios y no solo los tecnológicos.

Estos tipos de delitos conllevan a la necesidad de poder contar con profesionales expertos en informática y derecho que apliquen de forma práctica la pericia informática, sepan cómo realizar valoraciones, dictámenes y peritaciones informáticas con el fin de colaborar en la resolución de

litigios por medio de la extracción de la evidencia digital y presentarlas ante el Juez. Estos profesionales deben actualizar sus conocimientos para resolver problemas que surgen en su quehacer profesional y tomar decisiones tácticas y estratégicas en sus puestos.

De acuerdo a diferentes estudios actuales, los delitos informáticos son los de mayor crecimiento en los últimos años. La posibilidad de su ejecución a través de Internet permite que sin mayores complicaciones, el delincuente pueda estar en determinado lugar e incluso país, usar servicios de otros, para finalmente atacar a una o más víctimas.

El Perito Judicial Informático en países como España y su pericia en la extracción de evidencias electrónicas; está teniendo especial relevancia con un gran peso en todo tipo de procedimientos tanto judiciales como extrajudiciales tanto en temas penales, civiles, sociales, mercantiles, laborales e incluso personales; las evidencias digitales están en los elementos que usamos de manera cotidiana como el ordenador, móvil y otros dispositivos que están presentes en todo tipo de litigios.

En El Salvador existe un aproximado de 27 Universidades, sin embargo existe una tendencia de formación en 3 grandes áreas, i) Programadores, ii) analistas de Sistemas, iii) Administradores de Base de datos, quedando casi nula la formación de profesionales especialistas en auditoria, y/o informática forense.

2.1.6. Requisitos de Acreditación de Peritos

La base legal[6] para la inscripción de peritos evaluadores en El Salvador está sustentada en el Artículo 236 de La Ley de Bancos y la Norma **NPB4-42** Normas para la inscripción de peritos valuadores y sus obligaciones profesionales en el sistema financiero: importante es mencionar que la especialización de los Peritos Valuadores según el Articulo No. 5 de la citada Ley se centran en tres categorías:

- Terrenos y construcciones, que comprende la valuación de: terrenos urbanos, lotificaciones, urbanizaciones, vivienda mínima, residencias, edificios y locales comerciales;

- Inmuebles agropecuarios y bienes industriales, que comprende la valuación de: construcciones y terrenos agroindustriales, pecuarios y rústicos, maquinaria y equipo agrícola, semovientes y productos agrícolas e industriales, plantaciones, inmuebles industriales, maquinaria y equipo industrial y otros análogos;

[6] Artículo 226 código procesal penal

- Medios de transporte y otros bienes muebles, que comprende la valuación de: automotores, vehículos pesados, aeronaves, bienes náuticos y otros bienes muebles

De conformidad a la experiencia y capacidad del Perito, este puede solicitar que se le inscriba en una o varias de las categorías antes mencionadas; la legislación salvadoreña actual no contempla lo relacionado a peritaje en informática forense.

2.2. ACREDITACIÓN DE PERITOS INFORMÁTICOS.

Actualmente para la acreditación de peritos a nivel internacional existen dos asociaciones que han desarrollado programas de certificación forense en informática:

- La Asociación Internacional de Especialistas en Investigaciones Computacionales **IACIS**[7].
- La Red Del Crimen De la Alta Tecnología **HTCN**[8],

Ambas detallan las habilidades requeridas y las capacidades deseables en los investigadores informáticos. A continuación se presenta ejemplos de las certificaciones expedidas por cada una de las asociaciones antes mencionadas y una breve explicación de éstas:

- Certificación Externa de Computación Forense **CFEC**[9] , la cual se encuentra diseñada para personas que pertenecen al área informática y tiene pocos conocimientos del ámbito legal o del policial. (**IACIS**).
- Certificación de Investigador Certificado en Delito Informático **CCCI10** nivel básico y avanzado. El propósito de la certificación es desarrollar un alto nivel de profesionalismo y entrenamiento continuo que soporte investigaciones de crímenes de alta tecnología en la industria y las organizaciones. Esta certificación es avalada y reconocida en diferentes tribunales y cortes del mundo, dada la seriedad y rigurosidad de proceso de certificación.
- Certificación de técnico en informática forense **CCFT** nivel básico y avanzado. Certificación que provee expertos con herramientas para acceder y evaluar información crítica en el curso de una investigación.

[7] International Association of Computer Investigative Specialist
[8] High Technology Crime Network
[9] Computer Forensic External Certification
[10] Certified Computer Crime Investigator

En nuestro país actualmente no se cuenta con una entidad certificadora. Para evitar e investigar los delitos informáticos las instituciones que intervienen son las mismas que se encargan de velar por los derechos de las personas y hacer justica en toda situación legal.

Para este propósito, La Fiscalía General de la República es la encargada de la parte acusatoria y de la búsqueda de pruebas incriminatorias. La policía nacional civil forma parte de los procesos judiciales como ente encargado de guardar la cadena de custodia. La corte suprema de justicia se encarga de verificar el cumplimiento de las leyes y dar el veredicto final en la resolución de un caso por medio del juez.

2.3. REQUISITOS DE ACREDITACIÓN DE PERITOS.

Para ser acreditado por parte de **IACIS** con la certificación **CFCE**, se debe de cumplir con dos etapas:

- Revisión por parte de un miembro certificado. En esta etapa se incluyen los siguientes requerimientos:
    - Cuatro problemas prácticos.
    - 30 días para completar cada problema.
    - Se asigna un 'coach' que le guiará a través de los problemas prácticos.
    - Se debe de aprobar los cuatro problemas prácticos para ser elegible a la etapa de certificación.
- Fase de certificación. Esta fase consta de los siguientes elementos:
    - Problemas prácticos de disco duro.
    - Prueba objetiva basada en conocimiento.

Para obtener la certificación **CCCI**, se debe tomar en cuenta que esta consta de dos tipos, básico y avanzado, a continuación los requisitos para cada una de ellas:

- Certified Computer Crime Investigator (**CCCI**) Basic:
    - Tres años de experiencia en la investigación de incidentes técnicos o crímenes técnicos.
    - Completar curso de 40 horas impartido por agencia aprobada, ya sea una organización o empresas de entrenamiento.
    - Proveer un reporte narrativo con el detalle de la experiencia obtenida de la investigación de al menos 10 casos relacionado con crímenes por computadora.

- Certified Computer Crime Investigator (**CCCI**) Advanced:
    - Cinco años de experiencia en la investigación de incidentes técnicos o crímenes técnicos.
    - Completar curso de 80 horas impartido por agencia aprobada, ya sea una organización o empresas de entrenamiento.
    - Ser investigador líder en al menos 20 casos y haber participado en otros 40 casos como líder, supervisor o soporte. El total mínimo de casos en el que se ha participado debe de ser 60.
    - Proveer un reporte narrativo con el detalle de la experiencia obtenida de la investigación de al menos 15 casos relacionado con crímenes por computadora.

Por su parte para obtener la certificación **CCFT** es necesario cumplir con lo siguiente:

- Certified Computer Forensic Technician (**CCFT**) Basic:
    - Tres años de experiencia en la investigación de incidentes técnicos o crímenes técnicos.
    - Completar curso de 40 horas impartido por agencia aprobada, ya sea una organización o empresas de entrenamiento.
    - Proveer un reporte narrativo con el detalle de la experiencia obtenida de la investigación de al menos 10 casos relacionado con crímenes por computadora.
- Certified Computer Forensic Technician (CCFT) Advanced:
    - Cinco años de experiencia en la investigación de incidentes técnicos o crímenes técnicos.
    - Completar curso de 80 horas impartido por agencia aprobada, ya sea una organización o empresas de entrenamiento.
    - Ser investigador líder en al menos 20 casos y haber participado en otros 40 casos como líder, supervisor o soporte. El total mínimo de casos en el que se ha participado debe de ser 60.

Tabla 5 - RESUMEN EL PERITO		
Deberes	**Derechos**	**Áreas de actuación**
Asumir el caso cuando la designación no es hecha	Derecho patrimonial, que se suministre dinero para	Propiedad industrial: Espionaje / Revelación de

libremente.	gastos y recibir su remuneración	secretos.
Comparecer ante el juez.	Derecho a que se faciliten los medios adecuados para estudios de cuestiones sometidas a su consideración.	Uso de información: Competencia desleal de un empleado.
Posesionarse y prestar juramento.		Vulneración de la intimidad. Lectura de correo electrónico.
Practicar operaciones necesarias para dictamen.		Interceptación de telecomunicaciones. Protección de datos personales y datos reservados de personas jurídicas.
Obrar con lealtad, imparcialidad y buena fe.		
Fomentar dictamen y rendirlo de forma clara y precisa.		Publicidad engañosa, competencia desleal. Delitos económicos, monetarios y societarios. Delitos contra el mercado o contra los consumidores. Delitos contra la propiedad intelectual.

Guardar el secreto profesional.		Uso de software sin licencia. Piratería. Copia y distribución no autorizada de programas de ordenador. Daños mediante la destrucción o alteración de datos. Sabotaje. Estafa, fraudes, conspiración para alterar el precio de las cosas, etc. Pornografía infantil: acceso o posesión, divulgación, edición, etc.

Tabla 5 - RESUMEN EL PERITO

2.4. 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.

El peritaje informático se define como: *"El objeto de la pericia es el estudio, examen y aplicación de un hecho, un comportamiento, una circunstancia o fenómeno. Además de la prueba pericial establecer la causa de los hechos y los efectos del mismo, la forma y circunstancia como se cometió el hecho delictivo".*

Es vital que ante una pericia o experticia práctica se tengan claro los siguientes aspectos: la ductibilidad y la interpretación (Ilustración 5):

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, 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.

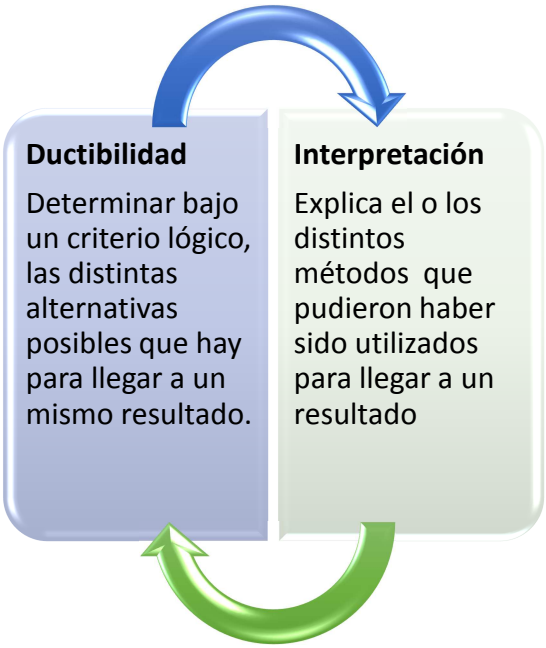

Ilustración 5 -Aspectos de la pericia o experticia práctica

2.5. 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.

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 ver ilustración 6:

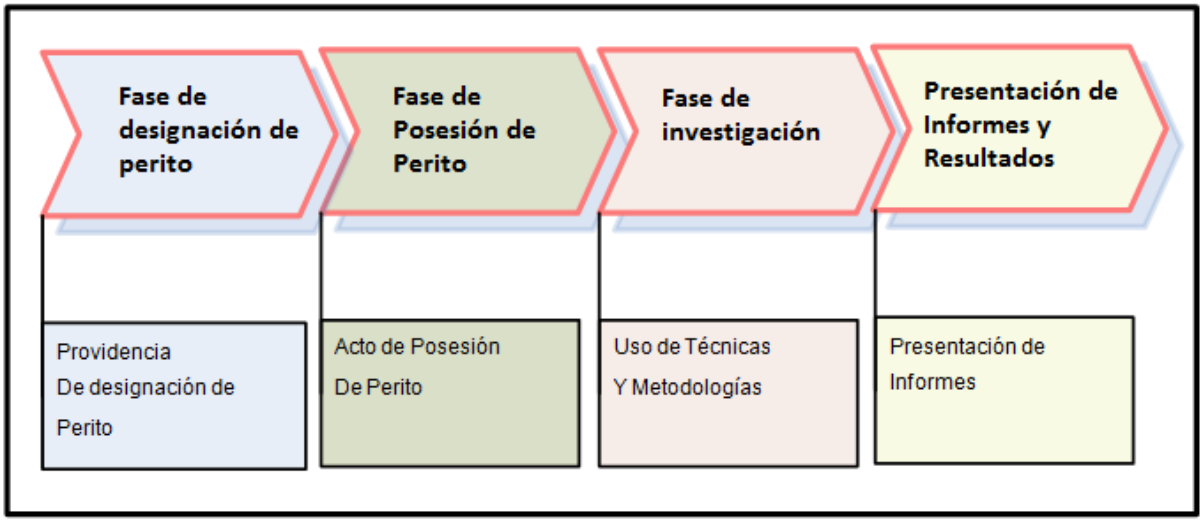

Ilustración 6 - El Proceso Pericial.
Fuente: Código de Procedimiento Penal del Ecuador

2.5.1. Fase de designación de perito

La fase de designación del perito, se establece a través del fiscal o juez de la causa, para lo cual, se procede a requerir en las entidades de acreditación el listado de peritos habilitados en la rama a investigar, luego que se localiza el o los peritos habilitados que serán los encargados de realizar la investigación.

Para realizar una designación, se debe de tomar en cuenta lo siguiente: identificar 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.

2.5.2. Fase de Posesión 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, 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.

2.5.3. 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 2 del Capítulo 1.

2.5.4. Presentación de Informes y Resultados

En este proceso el perito debe remitir dentro del plazo o término estipulado los hallazgos encontrados durante su investigación, con sus respectivas conclusiones. El perito luego de realizar la entrega de su informe[11] 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.

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.

2.6. Elaboración del dictamen pericial

Existen tres fases bien diferenciadas en la elaboración del dictamen pericial: fase de adquisición de las pruebas, fase de investigación y elaboración del informe pericial (ver figura 3.3) . Cada una de

[11] Artículo 235 código procesal penal. Siempre que sea posible y conveniente, los peritos practicarán conjuntamente el examen y deliberarán en sesión conjunta.

estas fases requiere un especial cuidado, ya que el más mínimo defecto puede dar lugar a la desestimación del informe del experto.

2.6.1. Fase de adquisición de las pruebas

La fase de adquisición de las pruebas consiste, tal y como su nombre indica, en la adquisición por parte del perito de todos los elementos que van a intervenir en la investigación. Es importante que el proceso de intervención de las computadoras, se lleve a cabo con todas las garantías para las partes involucradas en el litigio.

2.6.2. Fase de investigación

Durante la fase de investigación, los elementos que deben regir el desarrollo del trabajo del perito son la no alteración de la prueba y el principio de imparcialidad. La mejor manera que tiene un perito para garantizar la no alteración de una prueba es la elaboración de una imagen de todos los dispositivos de almacenamiento, es decir una copia exacta. El perito informático dispone de una ventaja de la que lamentablemente carecen los peritos del resto de disciplinas: la posibilidad de crear un número ilimitado de clones de la prueba principal, eliminando de este modo las posibilidades de contaminación involuntaria de la evidencia y reduciendo al mínimo las posibles fallas en las unidades analizadas.

2.6.3. Fase de elaboración del dictamen pericial.

En la fase de la elaboración del dictamen pericial[12], si se cumple con todos estos preceptos anteriormente expuestos, es muy difícil que durante la fase de exposición el testimonio del perito pueda ser rechazado.

Todo dictamen pericial debe contener:

a) La descripción de la persona, objeto o materia de examen o estudio, así como, el estado y forma en que se encontraba.
b) La relación detallada de todas las operaciones practicadas en la pericia y su resultado.
c) Los medios científicos o técnicos de los cuales se auxiliaron para emitir su dictamen.
d) Las conclusiones a las que llegan los peritos.

[12] Artículo 236 código procesal penal. Dictamen.

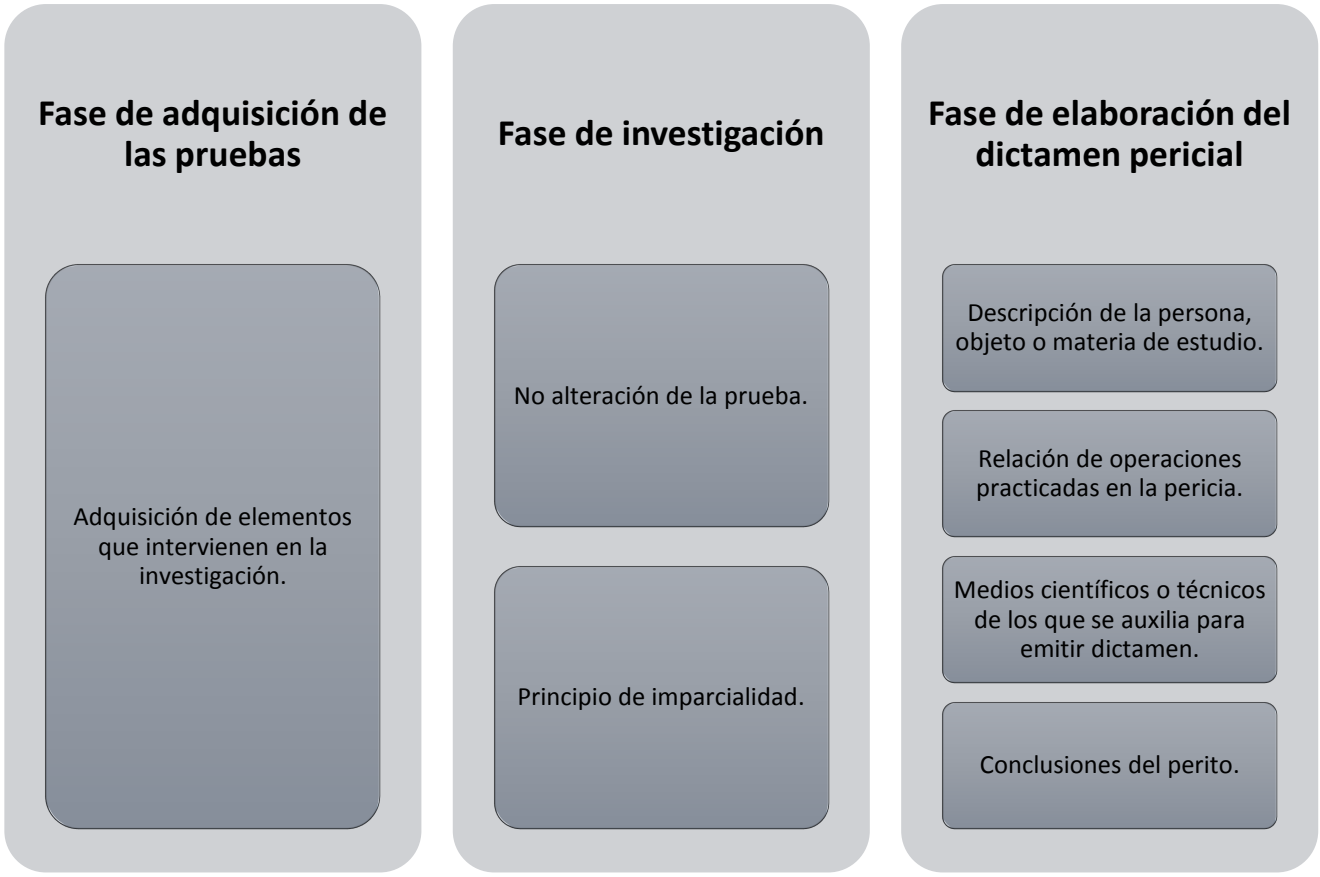

Ilustración 7 - Elaboración del dictamen pericial

2.6.4. HERRAMIENTAS UTILIZADAS EN INFORMÁTICA FORENSE

En lo referente a las *herramientas para la informática forense*[13], existe una gran variedad y dependen del objetivo para la cual van a ser utilizadas. Existen para la recolección de evidencia, para el monitoreo o control de computadoras, para el marcado de documentos y de hardware (dispositivos físicos para la recolección de evidencia).

En los últimos años se ha aumentado el número de herramientas de informática forense, es posible encontrar desde las más sencillas y económicas cuyas prestaciones habitualmente son muy limitadas, hasta herramientas muy sofisticadas que incluyen tanto software como dispositivos de hardware.

Las siguientes características son una guía a seguir para la selección de una herramienta:

- Asegurar un copiado sin pérdida de datos y que corresponde a una copia fiel.

[13] Ver tabla 2 Herramientas de la Información Forense

- Copia comprimida de discos origen para facilitar el manejo y conservación de grandes volúmenes de información.
- Búsqueda y análisis de múltiples partes de la evidencia en forma paralela en diferentes medios como discos duros, discos extraíbles, discos “Zip” CD’s y otros.
- Capacidad de almacenar la información recabada en diferentes medios, como discos duros IDE o SCSI, drives ZIP, y Jazz. Uno de los medios ideales son los CD-ROM pues contribuyen a mantener intacta la integridad forense de los archivos.
- Ordenamiento y búsqueda de los archivos de la evidencia de acuerdo con diferentes campos, incluyendo campos como las tres estampillas de tiempo (cuando se creó, último acceso, última escritura), nombres de los archivos, firma de los archivos, extensiones y propiedades.
- Soporte de múltiples sistemas de archivos tales como: DOS, Windows (todas las versiones), Macintosh (MFS, HFS, HFS+), Linux, UNIX (Sun, Open BSD), CD-ROM, y los sistemas de archivos DVDR. Esta es la limitación de algunas herramientas, pues está diseñadas para un número limitado de sistemas de archivos o es necesario adquirir módulos aparte.
- Recuperación de contraseñas: en muchas ocasiones la información recuperada puede estar protegida con contraseñas por lo que será necesario descifrarlos. Generalmente esta facilidad no viene incluida en estas herramientas, se deben comprar a parte.
- Las herramientas debería incluir facilidades de gestión para el manejo mismo de los Expedientes y reportes de las investigaciones.

A continuación en la ***tabla 6*** se presenta una breve descripción sobre las herramientas de investigación forense más conocidas y utilizadas.

NOMBRE	DESCRIPCIÓN
F.I.R.E. *	Para realizar análisis, respuesta del incidente, la recuperación de los datos, la exploración de virus y vulnerabilidad del equipo. También proporciona las herramientas necesarias para el análisis forense inmediato.
Encase *	Herramienta para la prevención, detección e investigación de fraudes en entornos virtuales. Dispositivo útil a los peritos forenses en diferentes casos.

ByteBack - Tech Assist, Inc *	Copia de discos duros de cualquier formato, transferencia a otros medios internos o externos, sistema de análisis binario para recuperación no destructiva de particiones y sectores de arranque tipo FAT y NTFS (NT) búsqueda binaria, md5, hash[14] integrado, solución multi-ambiente, acceso directo, diagnóstico de superficie, control de bajo nivel de hardware.
Maresware - Mares and Company Computer Forensics *	consiste en un conjunto de programas para investigación de registros de computador, Incluye herramientas para respuesta a incidentes y ataques, descubrimiento de secretos y evidencia computacional, documentación de los procedimientos, preparación de reportes de hallazgos y de documentos para uso legal
Paraben Forensic Toll - Paraben Computer Forensic Software *	Herramienta de computación forense diseñada para PDAs y PC Pockets.
SafeBack - New Technologies Inc *	Permite hacer copias espejo de archivos de backups o de discos duros completos, para creación de evidencia en sistemas de cómputo basados en Intel, transferencia de información a otros medios y preservación de evidencia.
WinHex *	Software para informática forense y recuperación de archivos, Editor Hexadecimal de Archivos, Discos y RAM.
E E-ROL **	Es una aplicación on-line que permite a los usuarios recuperar los archivos que hayan sido borrados de unidades de disco duro, unidades ZIP y disquetes, en todos los sistemas operativos de la familia Microsoft Windows.
EasyRecovery **	Es para recuperar datos, reparar archivos y correo electrónico y realizar diagnósticos de discos.
Snort **	Sistema de prevención y detección de intrusos en la red, métodos basados anomalía de la inspección.
NMap **	Potente localizador de vulnerabilidades.
Nessus **	Escanear vulnerabilidades.
Ethereal **	Potente sniffer para el rastreo de los paquetes por la red.
Fport **	Identifica puertos abiertos y aplicaciones asociadas a ellos.
NOMBRE	**DESCRIPCIÓN**
Putty **	Cliente que utiliza el protocolo de seguridad SSH.

[14] Ver *Glosario de término* para una mayor comprensión.

AirSnort **	Herramienta Wireless para recuperar claves cifradas.
Aircrack **	sniffer y WEP craqueador de Wireless.
NetStumble **	Localizador de los puntos de acceso Wireless.
The Autopsy **	Browser para la informática forense.

** Herramientas que ofrecen garantía y la transparencia permitiendo su confiabilidad durante un proceso judicial.*

*** Productos tradicionales cuyo objetivo primordial no es la computación forense, pero por incluir herramientas para la recuperación de archivos, en ocasiones pueden ser útiles, aunque la integridad de la evidencia recabada a través de estas herramientas podría estar más expuesta y su valor probatorio podría ser menor que el de evidencias obtenidas a través de herramientas altamente especializadas que garantizan la veracidad de la evidencia.*

Los productos mencionados en este cuadro es una muestra representativa de las distintas herramientas que se pueden encontrar en el mercado para apoyar a un informático forense.

Tabla 6: Herramientas de software como apoyo a la Información Forense

CAPITULO 3

3. INICIATIVAS PARA EL MANEJO DE DELITOS INFORMATICOS EN EL SALVADOR

3.1 PROPUESTAS INTERNAS

Hoy en día no existe ninguna actividad delictiva que no tenga algún soporte o vinculación con las tecnologías de la información y la comunicación (TIC); es por tal razón que en muchos países del mundo y El Salvador no es la excepción la tecnología va más rápida que las leyes y el delito va mucho más rápido que las regulaciones.

La explosión de las redes sociales y el uso de internet en el país, ha abierto la puerta a numerosos delitos que van desde pornografía infantil hasta extorsiones, robos de información confidencial e identidad y muestras de violencia extrema. Delitos que prosperan en un marco jurídico y una investigación policial con grandes debilidades.

De acuerdo al procedimiento actual que la PNC ejecuta ante un incidente de delito informático es iniciar la investigación cuando la persona pone una denuncia a la Fiscalía General de la República (FGR) sobre una página, perfil o muro de una red social o página web que presenten mensajes textuales o visuales de violencia o que podrían tipificarse como delito.

Luego la fiscalía tiene que direccionar a la PNC para que ésta comience a indagar quien le brinda servicio de internet a la persona que puso la denuncia; A partir de eso la PNC debe indagar con el proveedor cuál es el IP del equipo de donde se subieron esos archivos (pornografía, violencia, amenaza, acoso, etc.), pero para llegar a donde deliberadamente subieron esos archivos o enviaron esos mensajes, que puede ser en cualquier parte del mundo, antes hay que llegar al proveedor de servicio.

En el escenario más fácil usted debe pedirle al proveedor algunos datos de la IP, luego pedirle a Facebook a quién está asignada determinada cuenta, qué IP se pegó o respaldó la conexión a esa cuenta en el día, hora, minutos y segundos exactos.

Luego la PNC esperará la respuesta de la red social que también debe hacer una indagación para darle a las autoridades la IP que respaldó la conexión, y si es en el país (en este caso El Salvador)

se podría proceder a un allanamiento y hasta confiscar el equipo y realizarle un análisis informático forense.

Sin embargo una de las mayores limitaciones que tiene la policía para actuar son los vacíos de Ley, ya que ni el Código Procesal Penal, ni el Código Penal contemplan específicamente este tipo de delitos por medios electrónicos: "*La parte más delicada es la jurídica porque El Salvador pese a los esfuerzos que la Policía ha hecho en querer incorporar desde el 2000 a nuestra legislación algunos artículos y especificaciones y aclaraciones que a nuestro juicio ayudarían para una mejor investigación y abordaje del delito, no hay una buena base jurídica*", sostiene el representante de la unidad de delitos especializados de la PNC; hoy en día las leyes no obligan a las empresas servidoras de Internet a guardar un respaldo del registro de IP de todos los que se van conectando en el servicio web a los servidores de ellos.

Otra limitante es que la FGR no tiene una unidad específica para investigar delitos informáticos, por lo que sólo son procesados como delitos los ya tipificados, pero no tienen que ver específicamente con medios informáticos.

El gobierno de El Salvador a través del Ministro de Seguridad, David Munguía Payés, reveló que se ha presentado una propuesta de ley contra el delito cibernético para su análisis y posterior envío a la Asamblea Legislativa. La normativa permitiría castigar penalmente a quienes desde el anonimato, acosen, calumnien y cometan otro tipo de crímenes cibernéticos.

"*Hay mucha gente que se aprovecha del anonimato. Esos delitos provocativos decantan en violaciones, agresiones o acosos; también desprestigian a personas con calumnias, desde el anonimato hacen fraudes a bancos, instituciones financieras, etc*.", David Munguía Payés.

La ley contra delitos cibernéticos o informáticos daría herramientas legales para procesar a quienes sin escrúpulos usan internet y las redes sociales para dañar a terceros. De momento, dichos delitos en la mayoría de los casos quedan impunes por la falta de una legislación especial.

"*Es de mucha importancia que el país cuente con una ley para castigar delitos informáticos, ya que estos son muy comunes, porque estos ciber-delincuentes están enterados que no hay nada y nadie los castigue ni les prohíba sus acciones*", opina Erika Candray.

Esaú Jiménez opina que, de aprobarse la ley, "*deben existir personas especializadas para investigar, castigar y acusar. La falta de conocimiento en el área informática en la Asamblea Legislativa contribuye a que no se creen leyes aplicables a esta materia y obstaculiza el combate a los delitos informáticos*".

Países de Latinoamérica como México, Brasil, Venezuela, Colombia y más recientemente Costa Rica cuentan con una ley contra delitos cibernéticos que castiga hasta con seis años de prisión a quienes calumnien, difamen a través de correos electrónicos o usen sistemas informáticos para fraudes, robos de contraseñas o distribución de virus.

3.1.1 Estructura de la Policía Nacional Civil en El Salvador.

La estructura organizativa de la Institución es de naturaleza jerárquica, su mando ordinario lo ejercerá el Director General, quien podrá recomendar al Presidente de la República la creación o supresión de las dependencias que considere necesarias; dicha estructura se describe a continuación:

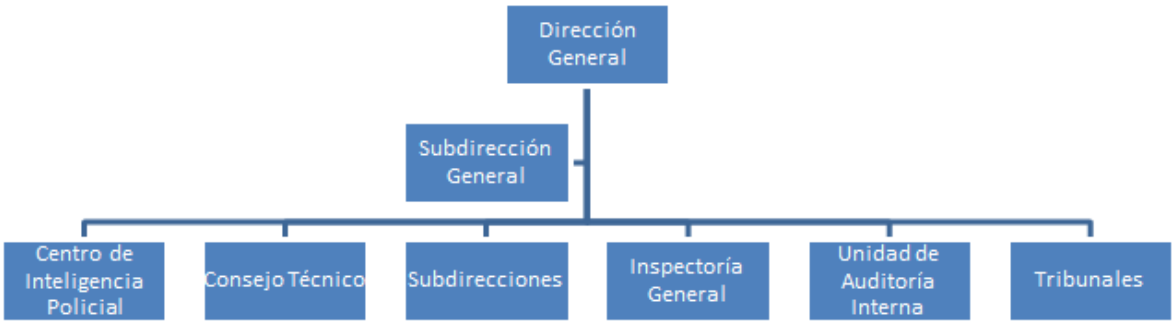

Ilustración 8- Estructura PNC

La subdirección General apoya a la Dirección General en la supervisión y coordinación de actividades y en la transmisión de órdenes a las Subdirecciones; asume también las funciones de la Dirección General en ausencia temporal del titular y lo representa cuando éste así lo requiera.

La Subdirección General coordina las Subdirecciones siguientes: Seguridad Pública, Investigaciones, Áreas Especializadas Operativas, Tránsito Terrestre, Policía Rural y de Administración y Finanzas.

Como se podrá evidenciar en la estructura antes descrita dentro de la estructura organizativa de la Policía Nacional Civil en El Salvador no existe una entidad técnica que vele por la investigación de los delitos informáticos.

3.1.2 Proyecto de Ley Especial de Protección Contra los Delitos Informáticos y de Datos.

La Comisión de Seguridad Pública y Combate a la Narcoactividad, han recibido de parte del consultor internacional, Emilio Viana, el proyecto de Ley Especial de Protección Contra los Delitos Informáticos y de Datos, que buscará proteger los bienes jurídicos y sancionar ciberdelitos que son conductas criminales cometidas por medio del uso de las tecnologías de la información y comunicación (TIC).

Viana quien trabajó cuatro meses en la elaboración del proyecto, manifestó ante los parlamentarios que "están poniendo a El Salvador entre los pocos países, particularmente de América Central y Latina que tienen una Ley Especial, hay países como Argentina que reformaron unos artículos de su código penal, pero hay muy pocos que tienen una Ley Especial sobre esto, así que su país también se va a distinguir en ese sentido".

El diputado presidente de la Comisión, Antonio Almendáriz, explicó que se conformó un equipo interinstitucional, conformado por representantes del Ministerio de Justicia y Seguridad Pública, Fiscalía General de la República, Superintendencia General de Electricidad y Comunicaciones, Consejo Nacional de la Niñez y Adolescencia y diferentes operadoras telefónicas, quienes brindaron insumos y que revisarán el documento final, para que posteriormente pase al estudio de la Comisión.

En tanto, el parlamentario Misael Mejía, indicó que después de desarrollarse varias reuniones con el consultor y presentar borradores previos, próximamente la Comisión iniciará el análisis de la propuesta de Ley: "En la actualidad solo tres países de América Latina, tienen Leyes similares y nosotros estaríamos poniendo a la cabeza en Centroamérica", afirmó Mejía.

Los legisladores coinciden en que dicha Ley es necesaria para la prevención de los actos contra de la confidencialidad, integridad y disponibilidad de los sistemas informáticos, de las redes y de los datos, así como el uso fraudulento de tales sistemas.

La legislación, de aprobarse, se aplicará en el territorio nacional e incluso tendría aplicación si una persona fuera de El Salvador comete el delito, pero su acción causa un efecto en el país.

Los hechos punibles y con responsabilidad fiscal que sugiere el consultor a los diputados son: acceso ilícito, interceptación ilícita, interferencia de datos, interferencia en el sistema y abuso de los dispositivos. También, hay un apartado para sancionar la falsificación y fraude informático, y el robo de identidad. El borrador considera que el robo de identidad es "*utilizado con el fin de perjudicar a una persona, es decir, difamarlo o manchar su nombre con diversos fines que el criminal busque*".

Ernesto Angulo, diputado de ARENA, celebró que se proponga castigar la difamación vía internet. El diputado Angulo aseguró que esa regulación no afectará la libertad de expresión.

Por su parte, Antonio Echeverría Veliz, del FMLN, explicó que la ley abarcaría los delitos de pornografía infantil por medio de internet.

Douglas Avilés, diputado de Cambio Democrático (CD), aclaró que la ley no pretende proteger a funcionarios, sino cuidar datos que puedan tener guardados personas jurídicas o naturales.

Dentro de las regulaciones propuestas están:

- El artículo 9 dice que el acceso a datos con la intención de cometer un delito como defraudación, violación de derechos de autor, hurto, hurto agravado, delitos contra el patrimonio entre otros, será sancionado con prisión de seis meses a dos años.
- El artículo 10 del borrador de la legislación que entregó el consultor Emilio Viano dice que será culpable del delito de interferencia agravada con datos informáticos y podrá ser sancionado con una multa de 60 a 180 días o con prisión de uno a tres años.
- El artículo 11 de la ley se refiere a la interferencia del sistema informático. Ese delito podrá ser sancionado con una multa de 30 a 90 días multa o prisión de seis meses a un año. Los diputados están abiertos a discutir y aprobar la sanción a esa acción.

3.2 PROPUESTAS EXTERNAS.

Dado el crecimiento de la tecnologías informáticas en los últimos años, han surgido generaciones de delincuentes que representan amenazas para los gobiernos, empresas e individuos, dichas amenazas incluyen la difusión de pornografía infantil, el incremento de incidentes de seguridad e incluso actividades terroristas, los cuales resultan 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 DELITOS INFORMÁTICOS Y LA ORGANIZACIÓN DE ESTADOS AMERICANOS (OEA)

Dada la dificultad que pueden encontrarse a la hora de resolver delitos informáticos, es necesario para los países ponerse de acuerdo con el objetivo de combatir los delitos informáticos de forma efectiva. Para ello es necesario trabajar y definir las respectivas tipificaciones de delitos.
Por esta razón la Organización de Estados Americanos (OEA), que está conformada por 35 países independientes de las Américas, de Norte, Sur y Centroamérica y el Caribe y que han ratificado la carta de la OEA y pertenecen a la Organización, han realizado un esfuerzo para poder buscar la estrategia adecuada para atacar la situación, por esto es que trabajaron en la creación de *"La convención de delitos informáticos de la OEA"*.

En este contexto todos los Ministros de Justicia de las Américas que pertenecen a la OEA, encomendaron establecer un Grupo de Expertos Intergubernamentales en Materia de Delitos Cibernéticos, que les permita:

- Realizar un diagnóstico de la actividad delictiva vinculada a las computadoras y la información de los Estados miembros.
- Realizar un Diagnóstico de la legislación, las políticas y las prácticas nacionales con respecto a dicha actividad.
- Identificar las entidades nacionales e internacionales que tienen experiencia en la materia.
- 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 Jueves 27 y viernes 28 de febrero de 2001 en Washington DC, de los Estados Unidos, se efectuó un cuestionario a los países miembros de la OEA (Ver ANEXO 1 – 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 2 – 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.

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. Dichas regulaciones implementadas en los países latinoamericanos se listan a continuación:

- Ley de Propiedad Intelectual.
- Ley de Comercio Electrónico.
- Ley de Habeas Data.
- Ley de Firmas Digitales.

A continuación, se presenta la tabla 7 la cual presenta un resumen de manera general con 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.

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 7 Leyes en Países Latinoamericanos.

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 8. Legislación en Chile – Informática e Información.

La Ley 19223 (Ver ANEXO 3 – 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 de Investigadores del Ciber Crimen, que pertenece como Unidad departamental a la Policía de Investigaciones de Chile, cuya creación fue en el año 2000, a pesar de contar con la Ley desde 1993, que se especializa en los delitos cometidos vía Internet, tales como amenazas, estafas, falsificación, pornografía infantil en Internet, entre otros. La brigada estructuralmente está formada de la siguiente manera:

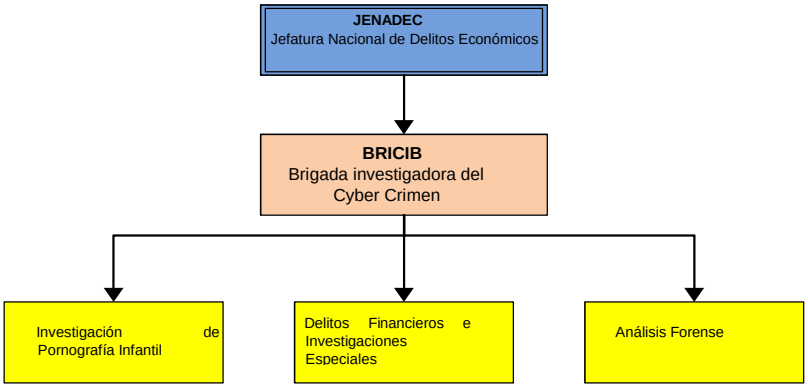

Ilustración 9 - Estructura Orgánica de la Brigada Investigadora del Cyber Crimen.

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 débito, traspasos no autorizados vía web. Además de todas las investigaciones de carácter especial, tales como, amenazas vía internet, Infracción a la Ley 19.223, Infracción a la Ley de propiedad Intelectual e industrial.
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, 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.

Cabe 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.

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 9 -. Legislación en Argentina – Informática e información.

La Ley 26388 (Ver Anexo 4 – 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.

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 10 - 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 5 – 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 11 -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, 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), 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 tráfico 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 se cuenta en El Salvador 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 creación de una unidad especializada en nuestro país.

Cabe destacar que además de 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.

CAPITULO 4

4. RETOS A SUPERAS EN EL MANEJO DE DELITOS INFORMATICOS EN EL SALVADOR

4.1 INCONVENIENTES EN EL PROCESO PERICIAL Y LA INVESTIGACION TECNOLOGICA ANTE EL DELITO INFORMATICO.

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.

En nuestro país como en cualquier parte del mundo los 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 El Salvador 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 de Justicia y Seguridad Publica, la Policía Nacional Civil, la Corte Suprema de Justicia, investigadores, y hasta la misma sociedad.

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

4.1.1 MARCO LEGAL

Debemos considerar la problemática Jurídica, ya que si bien es cierto El Salvador ha tenido indicios de dar sus primeros pasos en la generación de Leyes y Decretos que contemplan aspectos significativos de las nuevas tecnologías, 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 de Justicia y Seguridad Publica, la Policía Nacional Civil. 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 las distintas unidades del Ministerio de Justicia y Seguridad Publica 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.
- 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 una pericia; lo anterior con la finalidad que existan requerimientos solidos sobre lo que se va a investigar.
- Falta de un procedimiento adecuado para la calificación de peritos informáticos por parte de la Superintendencia del Sistema Financiero y el Ministerio de Justicia y Seguridad Publica.
- 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 de Justicia y Seguridad Publica, la Policía Nacional Civil, 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 estén relacionados con los delitos informáticos.
- Falta de cultura informática, aquellas personas que no tienen conocimientos informáticos básicos (Internet, correo electrónico), son más vulnerables y tienen mayores probabilidades de ser víctimas de un delito.

4.1.3 LIMITACIONES TECNOLÓGICAS

Alrededor del mundo existe una amplia diferencia en la distribución de las tecnologías de la información y las comunicaciones, lo que lleva a que existan grandes brechas en los tipos y números de adelantos tecnológicos entre los países. De esta situación surge lo que hoy día se conoce como brecha digital, la cual fue reconocida desde la declaración del milenio hecha por las Naciones Unidas en el año 2000.

La brecha digital hace referencia a las desigualdades en el acceso a internet, nuevas tecnologías (TIC), como el computador personal, telefonía móvil, banda ancha y otros dispositivos.

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.

Tomando en cuenta las brechas que nuestro país tiene en tecnologías de la información, no resulta fuera de la realidad que no se cuente en nuestro país con peritos especializados en la rama de la informática, razón por la cual la investigación de los delitos informáticos recae

sobre profesionales del peritaje que no están capacitados en las ramas de las tecnologías de la información.

En nuestro país el gobierno ha contado con el apoyo técnico y logístico de los Estados Unidos, para poder implementar el monitoreo de llamadas, correos electrónicos, y todo lo que está inmerso dentro del espectro electromagnético de comunicaciones, con la creación del centro de intervención a las telecomunicaciones.

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 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.

CONCLUSIONES Y RECOMENDACIONES

5. CONCLUSIONES Y RECOMENDACIONES

El Salvador está intentando dar sus primeros pasos en el desarrollo de iniciativas que permitan 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.

A continuación se presentan a manera de conclusiones las habilidades necesarias de un perito así como también las estrategias investigadas para tratar y documentar delitos informáticos.

Habilidades básicas necesarias de un perito:

HABILIDADES
Habilidad de emitir criterio y opiniones fuertemente sustentadas tanto en la parte técnica como científica y que logre llegar a conclusiones objetivas e imparciales.
Certificaciones de La Asociación Internacional de Especialistas en Investigaciones Computacionales IACIS o La Red Del Crimen De la Alta Tecnología HTCN.
Alto nivel de profesionalismo.
Entrenamiento continuo que soporte investigaciones de crímenes de alta tecnología en la industria y las organizaciones.
Conocimiento y uso de con herramientas para acceder y evaluar información crítica en el curso de una investigación.
Secreto profesional.

Tabla 12 - Habilidades perito informático

Estrategias investigadas para tratar y documentar delitos informáticos:

ESTRATEGIAS
Realizar un diagnóstico de la actividad delictiva vinculada a las computadoras.
Establecer unidades para que efectúen la investigación y persecución del delito cibernético.

Mantener información del punto nacional de contacto para la cooperación internacional en materia de delito cibernético.
Adoptar legislación en materia de delito cibernético.
Adoptar legislación y procedimientos para la utilización de la prueba electrónica en los procesos penales.
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.
Considerar la aplicación de los principios de la Convención del Consejo de Europa sobre la Delincuencia Cibernética.
Asegurarse de llevar un registro de cada uno de los pasos realizados y características o información de los hallazgos encontrados, es recomendable que durante el desarrollo de este proceso, lo asista u acompañe una persona, preferentemente imparcial.
Utilizar una técnica o metodología de recolección de evidencias, para ello, el profesional debe hacer uso de prácticas o metodologías que sean reconocidas.
Si el sistema está comprometido, se tienen los siguientes dos caminos: • Levantar la operación del sistema. 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. • Investigación forense detallada. Al seleccionar esta alternativa el profesional 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.

Tabla 13 - Estrategias para tratar delitos informáticos.

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

SECCIÓN	RECOMENDACIÓN
	1. Establecer y alinear una política de lucha en contra de la delincuencia

Gubernamental	informática. 2. Incentivar mecanismos de cooperación con otros países con el objetivo de prevenir y sancionar el delito informático que traspasa las fronteras de las naciones.
Marco Legal	1. Proyecto de Ley de Delitos Informáticos. 2. Proyecto de Ley de Comercio Electrónico, Mensajes de Datos y Firma Digital. 3. Reformas al Código procesal penal 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 y promover que se oficialicen 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 judicial (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 el razonamiento del peritaje informático, legislación existente que corresponda a la informática, criminalística. 4. Desarrollo de programas de especialización que 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 14 - Recomendaciones por sector – Delitos Informáticos.

BIBLIOGRAFÍA

Bibliografía

- Dr. Santiago Acurio del Pino, Delitos Informáticos Generalidades.
- Roberto Lemaitre Picado, Manual sobre delitos informáticos.
- Sitio web que aporta información a los investigadores relacionados con el derecho informático
  http://www.informatica-juridica.com/
- RedIRIS es la red española para Interconexión de los Recursos Informático de las universidades y centros de investigación.
  http://www.rediris.es/
- Sitio Web de la Coordinación de Seguridad de la Información (CSI) /UNAM-CERT de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación , UNAM.
  http://www.cert.org.mx/estadisticas.dsc
- Noticia "Sin leyes para castigar el delito informático", del periódico El Diario de Hoy, El Salvador.http://www.elsalvador.com/mwedh/nota/nota_completa.asp?idCat=47859&idArt=7339417
- Noticia "Proyecto de ley de firma electrónica", publicada en el sitio web de la asamblea legislativa de El Salvador.
  http://www.asamblea.gob.sv/noticias/archivo-de-noticias/comision-de-economia-sometera-a-consulta-proyecto-de-ley-de-firma-electronica/?searchterm=firma%20electronica
- Blog del periodista salvadoreño Carlos Domínguez, mediante el cual público el artículo "Habeas Data en El Salvador"
  http://cardominguez.wordpress.com/2010/01/10/el-habeas-data-en-el-salvador/
- Estudio de la piratería mundial del software BSA 2011
  http://globalstudy.bsa.org/2011/downloads/translatedstudy/2011GlobalPiracyStudy_es.pdf
- Sitio Web de consulta de la legislación salvadoreña
  http://www.asamblea.gob.sv/eparlamento/indice-legislativo/buscador-de-documentos-legislativos/
- Segundo monitoreo al cumplimiento de Ley de Acceso a la Información Pública, El Salvador 2013.
  http://isd.org.sv/wp/wp-content/uploads/2013/05/SEGUNDO-MONITOREO-AL-CUMPLIMIENTO-DE-LA-LEY-ACCESO-INFORMACI%C3%93N-P%C3%9ABLICA-FINAL-2.pdf
- Noticia relacionada con la protección de los derechos de autor, publicada por el Diario de Hoy, El Salvador.
  http://www.elsalvador.com/noticias/EDICIONESANTERIORES/septiembre8/ESPECTACULOS/espec6.html
- Noticia relacionada con la promoción del CNR del registro de la propiedad intelectual.

http://www.contrapunto.com.sv/sociedad/derechos-humanos/cnr-promueve-el-registro-la-propiedad-intelectual

- Blog Informática Forense Marta Cardenas, especialista en informática forense. http://informaticaforense2014.blogspot.com/2014/06/cadena-de-custodia.html
- Definición perito http://definicion.de/perito/
- Peritos y evaluadores http://www.ssf.gob.sv/index.php/temas/registropublico/104-informacion-financiera/registros/199-peritos-evaluadores
- Jeimy J. Cano (2006) Estado del arte del Peritaje Informático en Latinoamérica
- ECHANDÍA, Hernando Devis; Teoría General de la Prueba Judicial. Op. Cit. Pág. 368
- Emilio del Peso Navarro, Peritajes Informáticos, Página 10, 2da Edición, Editorial Díaz de Santos S.A, 2001
- Listasal: Artículo: Universidades de El Salvador
- Ley de Bancos de la Republica de El Salvador
- Norma NPB4-42Normas para la inscripción de peritos valuadores y sus obligaciones profesionales en el sistema financiero
- Tesis Universidad de El Salvador: Estudio y análisis sobre la informática forense en El Salvador.
- High Tech Crime Network http://www.htcn.org/
- International association of computer investigative specialists. http://www.iacis.com/
- Secretaría de asuntos jurídicos OEA http://www.oas.org/juridico/spanish/cybersp_links.htm
- Policía de investigaciones de Chile http://www.policia.cl/cuentapublica2012/paginas/estructura_organica.htm
- Transparencia activa http://www.transparenciaactiva.gob.sv/analizan-propuesta-de-ley-contra-delitos-ciberneticos/
- Periódicos El Salvador http://www.elsalvador.com/mwedh/nota/nota_completa.asp?idCat=47859&idArt=7339417 http://elmundo.com.sv/asamblea-por-legislar-los-delitos-informáticos

http://www.elsalvador.com/mwedh/nota/nota_completa.asp?idCat=47859&idArt=6840520

http://www.lapagina.com.sv/docs/HJTV_LEY_ESPECIAL_PARA_INTERVENCION_DE_TELECOMUNICACIONES.pdf

- Brecha digital Wikipedia

  http://en.wikipedia.org/wiki/Digital_divide

ANEXOS

Anexos

ANEXO 1

CONSEJO PERMANENTE DE LA OEA/Ser.G

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS GE/REMJA/doc.71/01

22 octubre 2001

Grupo Especial encargado de dar cumplimiento a las Recomendaciones de las Reuniones de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas

Original: español

CUARTA REUNION DE MINISTROS DE JUSTICIA O DE MINISTROS O PROCURADORES GENERALES DE LAS AMERICAS

Proyecto de Cuestionario para el seguimiento de las Recomendaciones adoptadas en la Tercera Reunión de Ministros de Justicia

CUARTA REUNION DE MINISTROS DE JUSTICIA O DE MINISTROS O PROCURADORES GENERALES DE LAS AMERICAS

Proyecto de Cuestionario para el seguimiento de las Recomendaciones adoptadas en la Tercera Reunión de Ministros de Justicia

_____

Introducción

La siguiente propuesta de cuestionario tiene como propósito dar seguimiento al cumplimiento de las Recomendaciones del Grupo de Expertos Gubernamentales adoptadas en la Tercera Reunión de Ministros de Justicia en el marco de la OEA.

- “Establecer una entidad o entidades públicas con la autoridad y función específica para llevar adelante la investigación y persecución del delito cibernético”

1. ¿Ha establecido su Estado una entidad o entidades públicas con autoridad y función específica para llevar adelante la investigación y persecución del delito cibernético?

SI ____ NO____

Si la respuesta es afirmativa, sírvase suministrar la siguiente información:

- Nombre de la institución:_____
- Organismo/oficina:_____
- Dirección Postal:_____
- Teléfono: _____ Fax:_____ E-mail:_____
- “Emprender las acciones necesarias para implementar legislación sobre delito cibernético, si aún no cuentan con la misma”.
- “Realizar todos los esfuerzos necesarios para armonizar sus legislaciones en materia de delito cibernético, a fin de facilitar la cooperación internacional para la prevención y combate de estas actividades ilícitas”.

2. ¿Cuenta su Estado con legislación que permita investigar y sancionar las diversas modalidades de delito cibernético?.

SI ____ NO____

a) En caso afirmativo, por favor, sírvase informar cuáles son las disposiciones respectivas y anexar copia de las mismas.

b) En caso negativo, ¿ha emprendido su Estado acciones para adoptar legislación que permita investigar y sancionar las diversas modalidades de delito cibernético?.

SI ____ NO____

Si la respuesta fuere afirmativa, por favor indicar el tipo de acciones emprendidas y el estado en que se encuentran.

 “Identificar las necesidades de capacitación en materia de delito cibernético, propiciando esquemas de cooperación bilateral, regional y multilateral en este campo”.

3. ¿Ha identificado su Estado las necesidades que tiene en materia de asistencia técnica y capacitación de funcionarios en delito cibernético?

SI ____ NO____

En caso afirmativo, por favor indicar la forma en que se ha hecho esa identificación y, de ser posible, anexar copia del documento respectivo.

_____

4. ¿A cuáles funcionarios públicos considera su Estado que se deberían orientar, de manera prioritaria, los programas de capacitación en materia de delito cibernético? :

a) A los fiscales

b) A los jueces

c) A ambos

d) A otros funcionarios * . Por favor, especificar a quienes.

 “Considerar la posibilidad de sumarse a mecanismos de cooperación o intercambio de información ya existentes, tales como el “Grupo de contacto de 24horas/7días” a fin de iniciar o recibir información”.

5. ¿Se ha sumado su Estado al “Grupo de contacto de 24 horas/7 días” u a otro mecanismo de cooperación o intercambio de información ya existentes, en materia de delito cibernético?

SI ____ NO____

En caso afirmativo, por favor indicar el mecanismo o los mecanismos de que hace parte su Estado_____

_____

 “Tomar medidas para sensibilizar al público, incluyendo a los usuarios del sistema educativo, del sistema legal y administración de justicia sobre la necesidad de prevenir y combatir el delito cibernético”.

6. ¿Ha tomado su Estado medidas para sensibilizar al público, incluyendo a los usuarios del sistema educativo, del sistema legal y de la administración de justicia sobre la necesidad de prevenir y combatir el delito cibernético?

SI ____ NO____

Si la respuesta fuere afirmativa, por favor indicar el tipo de medidas adoptadas.

_____

_____

 “Necesidad de desarrollar lineamentos para orientar los esfuerzos nacionales en materia de delito cibernético a través de por ejemplo, la elaboración de legislación modelo u otros instrumentos jurídicos pertinentes y el diseño de programas de capacitación”.

7. ¿A través de cuál o cuáles instrumentos jurídicos considera su Estado que se debería avanzar con el fin de fortalecer la cooperación hemisférica en el combate contra el delito cibernético?

a) A través de la negociación de un Tratado en la materia:

SI ____ NO____

b) A través de la elaboración de legislación modelo:

SI ____ NO____

c) A través de ambos instrumentos jurídicos (Convención y legislación modelo)

SI ____ NO____

Por favor, sírvase indicar la siguiente información sobre el funcionario que puede consultarse en relación con las respuestas al cuestionario:

- ( ) Sr. _____
- ( ) Sra. _____
- Título/cargo: _____
- Organismo/oficina:_____
- Dirección Postal: _____
- Teléfono: _____Fax: _____ E-mail:____

ANEXO 2

1. RECOMENDACIONES II REUNION DE

MINISTROS DE JUSTICIA O DE MINISTROS O

PROCURADORES GENERALES DE LAS AMERICAS

SOBRE DELITO CIBERNETICO

(Lima, Perú - 1 al 3 de Marzo de 1999)

Fortalecimiento y desarrollo de la cooperación interamericana

A. Fortalecer y desarrollar la cooperación internacional en áreas de especial preocupación tales como la lucha contra el terrorismo, el combate contra la corrupción, el lavado de dinero, el narcotráfico, el fraude documentario, el tráfico ilícito de armas, el crimen organizado y la delincuencia transnacional.

B. Delito cibernético

En vista de la importancia y la dificultad de las cuestiones que plantea el delito cibernético y la difusión y magnitud potencial de los problemas que presenta para nuestros países, recomendó el establecimiento de un grupo de expertos gubernamentales en el marco de la OEA con el siguiente mandato:

1. Hacer un diagnóstico de la actividad delictiva vinculada a las computadoras y la información, o que utiliza las computadoras como medio para cometer un delito;
2. hacer un diagnóstico de la legislación, las políticas y las prácticas nacionales con respecto a dicha actividad;
3. identificar las entidades nacionales e internacionales que tienen experiencia en la materia; e
4. identificar mecanismos de cooperación dentro del sistema interamericano para combatir el delito cibernético.

El grupo de expertos gubernamentales deberá presentar un informe a la Tercera Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas.

ANEXO 3

http://www.leychile.cl/Navegar?idNorma=30590

TIPIFICA FIGURAS PENALES RELATIVAS A LA INFORMATICA

Teniendo presente que el H. Congreso Nacional ha dado su aprobación al siguiente Proyecto de Ley:

"Artículo 1°.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.

Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

Artículo 2°.- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.

Artículo 3°.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

Artículo 4°.- El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.".

Y por cuanto he tenido a bien aprobarlo y sancionarlo; por tanto promúlguese y llévese a efecto como Ley de la República.

Santiago, 28 de Mayo de 1993.- ENRIQUE KRAUSS RUSQUE, Vicepresidente de la República.- Francisco Cumplido Cereceda, Ministro de Justicia.

Lo que transcribo a Ud. para su conocimiento.- Saluda atentamente a Ud., Martita Worner Tapia, Subsecretario de Justicia.

ANEXO 4

(ARGENTINA)
ANTEPROYECTO DE LEY DE DELITOS INFORMATICOS
SOMETIDO A CONSULTA PUBLICA POR LA SECRETARIA DE COMUNICACIONES POR RESOLUCIÓN No. 476/2001 DEL 21.11.2001

Acceso Ilegítimo Informático:
Artículo 1.-
Será reprimido con pena de multa de mil quinientos a treinta mil pesos, si no resultare un delito más severamente penado, el que ilegítimamente y a sabiendas accediere, por cualquier medio, a un sistema o dato informático de carácter privado o público de acceso restringido.
La pena será de un mes a dos años de prisión si el autor revelare, divulgare o comercializare la información accedida ilegítimamente.
En el caso de los dos párrafos anteriores, si las conductas se dirigen a sistemas o datos informáticos concernientes a la seguridad, defensa nacional, salud pública o la prestación de servicios públicos, la pena de prisión será de seis meses a seis años.

Daño Informático
Artículo 2.-
Será reprimido con prisión de un mes a tres años, siempre que el hecho no constituya un delito más severamente penado, el que ilegítimamente y a sabiendas, alterare de cualquier forma, destruyere, inutilizare, suprimiere o hiciere inaccesible, o de cualquier modo y por cualquier medio, dañare un sistema o dato informático.

Artículo 3.-
En el caso del artículo 2º, la pena será de dos a ocho años de prisión, si mediara cualquiera de las circunstancias siguientes:
1) Ejecutarse el hecho con el fin de impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones;
2) Si fuera cometido contra un sistema o dato informático de valor científico, artístico, cultural o financiero de cualquier administración pública, establecimiento público o de uso público de todo género;
3) Si fuera cometido contra un sistema o dato informático concerniente a la seguridad, defensa nacional, salud pública o la prestación de servicios públicos. Sí del hecho resultaren, además, lesiones de las descritas en los artículos 90 o 91 del Código Penal, la pena será de tres a quince años de prisión, y si resultare la muerte se elevará hasta veinte años de prisión.

Fraude Informático
Artículo 5.-
Será reprimido con prisión de un mes a seis años, el que con ánimo de lucro, para sí o para un tercero, mediante cualquier manipulación o artificio tecnológico semejante de un sistema o dato informático, procure la transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.
En el caso del párrafo anterior, si el perjuicio recae en alguna administración publica, o entidad financiera, la pena será de dos a ocho años de prisión.

Disposiciones Comunes
Artículo 6.-
1) A los fines de la presente ley se entenderá por sistema informático todo dispositivo o grupo de elementos relacionados que, conforme o no a un programa, realiza el tratamiento automatizado de datos, que implica generar, enviar, recibir, procesar o almacenar información de cualquier forma y por cualquier medio.
2) A los fines de la presente ley se entenderá por dato informático o información, toda representación de hechos, manifestaciones o conceptos en un formato que puede ser tratado por un sistema informático.
3) En todos los casos de los artículos anteriores, si el autor de la conducta se tratare del responsable de la custodia, operación, mantenimiento o seguridad de un sistema o dato informático, la pena se elevará un tercio del máximo y la mitad del mínimo, no pudiendo superar, en ninguno de los casos, los veinticinco años de prisión.

FUNDAMENTOS

La Tecno-era o Era Digital y su producto, la Sociedad de la Información, han provocado un cambio de paradigma social y cultural, impactando drásticamente en la estructura socio-económica y provocando un rediseño de la arquitectura de los negocios y la industria.

La Informática nos rodea y es un fenómeno irreversible. Se encuentra involucrada en todos los ámbitos de la interacción humana, desde los más importantes a los más triviales, generándose lo que, en la doctrina norteamericana, se denomina "computer dependency". Sin la informática las sociedades actuales colapsarían.

Es instrumento de expansión ilimitada e inimaginable del hombre y es, a la vez, una nueva de forma de energía, e inclusive, de poder intelectual.

Naturalmente que el Derecho, como orden regulador de conductas, no queda exento del impacto de las nuevas tecnologías, destacándose la imposibilidad de adaptar dócilmente los institutos jurídicos vigentes y los viejos dogmas a estos nuevos fenómenos.

De igual manera, las tecnologías de la información han abierto nuevos horizontes al delincuente, incitando su imaginación, favoreciendo su impunidad y potenciando los efectos del delito convencional. A ello contribuye la facilidad para la comisión y encubrimiento de estas conductas disvaliosas y la dificultad para su descubrimiento, prueba y persecución.

La información, en consecuencia, ha adquirido un valor altísimo desde el punto de vista económico, constituyéndose en un bien sustrato del tráfico jurídico, con relevancia jurídico-penal por ser posible objeto de conductas delictivas (acceso ilegítimo, sabotaje o daño informático, espionaje informático, etc.) y por ser instrumento de comisión, facilitación, aseguramiento y calificación de los ilícitos tradicionales.

Atendiendo a las características de esta nueva "Era" y sus implicancias ya descriptas, consideramos que el bien jurídico tutelado en los delitos informáticos es la información en todos sus aspectos (vgr.: propiedad común, intimidad, propiedad intelectual, seguridad pública, confianza en el correcto funcionamiento de los sistemas informáticos), entendiendo que su ataque supone una agresión a todo el complejo entramado de relaciones socio-económico-culturales, esto es, a las actividades que se producen en el curso de la interacción humana en todo sus ámbitos y que dependen de los sistemas informáticos (transporte, comercio, sistema financiero, gestión gubernamental, arte, ciencia, relaciones laborales, tecnologías, etc.).

En definitiva, en esta propuesta se entiende por delitos informáticos a aquellas acciones típicas, antijurídicas y culpables que recaen sobre la información, atentando contra su integridad, confidencialidad o disponibilidad, en cualquiera de las fases que tienen vinculación con su flujo o tratamiento, contenida en sistemas informáticos de cualquier índole sobre los que operan las maniobras dolosas.

Cabe adelantar que, dentro de estas modalidades de afectación del bien jurídico tutelado, se propone la creación de tres tipos de delitos básicos, con sus correspondientes agravantes, a saber:
a) El acceso ilegítimo informático o intrusismo informático no autorizado (hacking) que supone vulnerar la confidencialidad de la información en sus dos aspectos: exclusividad e intimidad;
b) El daño o sabotaje informático (cracking), conducta ésta que va dirigida esencialmente a menoscabar la integridad y disponibilidad de la información; y
c) El fraude informático, hipótesis en la cual se utiliza el medio informático como instrumento para atentar contra el patrimonio de un tercero, que se incluye en esta ley por su propia especificidad que impone no romper la sistemática de este proyecto de ley especial y por la imposibilidad de incorporarla a los delitos contra la propiedad contemplados en el Código Penal.

Ahora bien, la información, como valor a proteger, ha sido tenida en consideración por el Derecho Penal en otras ocasiones. Sin embargo, se lo ha hecho desde la óptica de la confidencialidad, pero no como un nuevo bien jurídico tutelado abarcativo de varios intereses dignos de protección penal. Piénsese sino en las normativas sobre violación de secretos profesionales o comerciales o la más reciente legislación de Habeas Data, de confidencialidad de la información y en el Derecho Publico Provincial, por las Constituciones de las Provincias del Chaco y de la Rioja, entre otras tantas normas que dentro de regímenes específicos, resguardan a la información con una especial protección.

Asimismo se busca, de alguna manera, cubrir las lagunas legales que fueron quedando luego de la incorporación de cierta protección a determinados intangibles en nuestro derecho positivo nacional.

Se impone aquí aclarar que, como política de legislación criminal, se ha optado por incluir estos delitos en una ley especial y no mediante la introducción de enmiendas al Código Penal, fundamentalmente para no romper el equilibrio de su sistemática y por tratarse de un bien jurídico novedoso que amerita una especial protección jurídico-penal.

Adicionalmente este esquema tiene la bondad de permitir la incorporación de nuevas figuras que hagan a la temática dentro de su mismo seno sin volver a tener que discernir nuevamente con el problema de romper el equilibrio de nuestro Código Penal, que viene siendo objeto de sucesivas modificaciones. Este es el esquema que también han seguido países como los EE.UU. en donde se tiene una alta conciencia de que la carrera tecnológica posibilita nuevas formas de cometer conductas verdaderamente disvaliosas y merecedores de un reproche penal.

Va de suyo, que este no es un anteproyecto general y omnicomprensivo de todas aquellas acciones antijurídicas, sino uno que busca dar una respuesta en un campo especifico del Derecho positivo, como lo es el Derecho Penal.

Desde el primer momento, se decidió privilegiar la claridad expositiva, el equilibrio legislativo y apego al

principio de legalidad evitando caer en una legislación errática que terminara meramente en un recogimiento de la casuística local o internacional.

Para ello se debió evitar la tentación de tomar figuras del derecho comparado sin antes desmenuzarlas y analizar estrictamente el contexto en donde se desarrollaron y finalmente ponderar cómo jugarían dentro del esquema criminal general vigente en la República Argentina.

Se buscó, asimismo, llevar nitidez estructural y conceptual a un campo en donde es muy difícil encontrarla, en donde las cuestiones técnicas ofrecen a cada paso claro-oscuros que muchas veces resultan territorios inexplorados no solo para el derecho penal, sino para el derecho en general y sus operadores.

Este anteproyecto abraza el principio de la mínima intervención en materia penal, buscando incriminar únicamente las conductas que representen un disvalor de tal entidad que ameriten movilizar el aparato represivo del Estado. Somos plenamente conscientes de que en más de una oportunidad una ilegitima conducta determinada será merecedora de un castigo extra penal, sea a través del régimen de la responsabilidad civil, del derecho administrativo o la materia contravencional.

Imbuido en este espíritu es que se ha decidido privilegiar el tratamiento de tres tipos delictivos fundamentales. El lector atento podrá notar que no una gran cantidad, sino la mayoría de las conductas que habitualmente se cometen o se buscan cometer dentro del ámbito informático son alcanzadas por alguno de los tipos tratados.

A) ACCESO ILEGITIMO INFORMÁTICO

Se ha optado por incorporar esta figura básica en la que por acceso se entiende todo ingreso no consentido, ilegítimo y a sabiendas, a un sistema o dato informático.

Decimos que es una figura base porque su aplicación se restringe a aquellos supuestos en que no media intención fraudulenta ni voluntad de dañar, limitándose la acción a acceder a un sistema o dato informático que se sabe privado o público de acceso restringido, y del cual no se posee autorización así se concluye que están excluidos de la figura aquellos accesos permitidos por el propietario u otro tenedor legítimo del sistema.

Consideramos apropiada aquí, la fijación de una pena de multa, atento que se trata de una figura básica que generalmente opera como antesala de conductas más graves, por lo que no amerita pena privativa de la libertad, la que por la naturaleza del injusto habría de ser de muy corta duración.

Este criterio resulta acorde con el de las legislaciones penales más modernas (Alemana, Austríaca, Italiana, Francesa y Española), que ven en la pena de multa el gran sustituto de las penas corporales de corta duración, puesto que no menoscaban bienes personalísimos como la libertad, ni arrancan al individuo de su entorno familiar y social o lo excluyen de su trabajo.

En cuanto a los elementos subjetivos de la figura, se añade un ánimo especial del autor para la configuración del tipo, que es la intencionalidad de acceder a un sistema de carácter restringido, es decir, sin consentimiento expreso o presunto de su titular.

Se contempla en el segundo párrafo, la pena de un mes a dos años de prisión si el autor revelare, divulgare o comercializare la información, como modalidad más gravosa de afectación del bien jurídico tutelado por la circunstancia que supone la efectiva pérdida de la exclusividad de la información, penalidad concordante con la descripción típica introducida por la ley 25.326, la que incorpora al código penal el artículo 157 bis.

Por último, se contempla en el último párrafo, como agravante de ambas modalidades de esta figura delictiva, la circunstancia que los sistemas o datos informáticos sean concernientes a la seguridad, defensa nacional, salud pública o la prestación de servicios públicos, en cuyo caso la pena prevista va desde los seis meses hasta los seis años de prisión. En esta hipótesis resulta palmario el fundamento de la agravante por la importancia que los sistemas e información comprometida involucran para el correcto funcionamiento de servicios vitales para la Nación, sin los cuales se pondría en jaque la convivencia común, en especial en los núcleos urbanos.

B) DAÑO O SABOTAJE INFORMATICO

En cuanto a la protección propiamente dicha de la integridad y disponibilidad de un sistema o dato informático, el artículo propuesto tiene por objeto llenar el vacío que presenta el tipo penal de daño (artículo 183 del Código Penal) que sólo contempla las cosas muebles.

En nuestro país la jurisprudencia sostuvo que el borrado o destrucción de un programa de computación no es una conducta aprehendida por el delito de daño (art. 183 del CP), pues el concepto de cosa es sólo aplicable al soporte y no a su contenido (CNCrimCorrec., Sala 6ta, 30/4/93, "Pinamonti, Orlando M.", JA 1995-III-236). Dicha solución es aplicable también a los datos o información almacenada en un soporte magnético.

Al incluir los sistemas y datos informáticos como objeto de delito de daño se busca penalizar todo ataque, borrado, destrucción o alteración intencional de dichos bienes intangibles. Asimismo, la incriminación tiende

también a proteger a los usuarios contra los virus informáticos, caballos de troya, gusanos, cancer routines, bombas lógicas y otras amenazas similares.

La figura proyectada constituye un delito subsidiario, ya que la acción de dañar es uno de los medios generales para la comisión de ilícitos, pero esta subsidiariedad está restringida exclusivamente a los casos en que el delito perpetrado por medio de la acción dañosa esté "más severamente penado".

Asimismo, la ley prevé figuras gravadas, previendo especialmente las consecuencias del daño como, por ejemplo, el producido en un sistema o dato informático concerniente a la seguridad, defensa nacional, salud publica o la prestación de servicios públicos.

En este sentido, conviene precisar el alcance de cada supuesto. Respecto del inciso que agrava el daño a sistemas o datos informáticos con el propósito de impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones, hemos seguido la técnica legislativa y los supuestos utilizados por el legislador al redactar el artículo 184 inciso 1° del Código Penal.

En segundo término, se protege la información de valor científico, artístico, cultural o financiero de las Universidades, colegios, museos y de toda administración publica, establecimiento público o de uso público de todo género. La especialidad de la información protegida y la condición pública o de uso público de los establecimientos ameritan agravar la pena en estas hipótesis.

En tercer lugar, la conducta se agrava cuando el daño recae sobre un sistema o dato informático concerniente a la seguridad, defensa nacional, salud pública o la prestación de servicios públicos. Aquí, la trascendencia pública, inmanentes a las obligaciones del Estado en materia de seguridad interior y exterior, salud y prestación de servicios públicos, justifican que la sanción penal se eleve por sobre el límite impuesto por la figura básica.

Por último, en función del inciso 3° se contempla como resultado, la producción de una la lesión, grave o gravísima, o la muerte de alguna persona, que pudiere ocurrir con motivo de un daño a un sistema o dato informático, elevándose la pena en función de la elevada jerarquía jurídica que reviste la integridad física de los seres humanos.

Hacemos notar que el Derecho comparado ha seguido los mismos lineamientos, pues frente a la evolución de los sistemas informáticos, las legislaciones penales debieron adaptarse a los nuevos bienes inmateriales.

Así, en la mayoría de los Códigos Penales de los Estados Unidos se ha tipificado una figura de destrucción de datos y sistemas informáticos. También la ley federal de delitos informáticos, denominada Computer Fraud and Abuse Act de 1986, contempla en la Sección (a) (5) la alteración, daño o destrucción de información como un delito autónomo.

El art. 303 a del StGB (Código Penal Alemán) establece que "1. Quien ilícitamente cancelare, ocultare, inutilizare o alterare datos de los previstos en el 202 a, par.2° será castigado con pena privativa de libertad de hasta dos años o con pena de multa".

El art. 126 a del Código Penal de Austria (östStGB) dispone que "1. Quien perjudicare a otro a través de la alteración, cancelación, inutilización u ocultación de datos protegidos automáticamente, confiados o transmitidos, sobre los que carezca en todo o en parte, de disponibilidad, será castigado con pena privativa de libertad de hasta seis meses o con pena de multa de hasta 360 días-multa".

Con la ley N°88-19 del 5 de enero de 1988 Francia incluyó en su Código Penal varios delitos informáticos. Entre ellos, destacamos la figura del art. 462-4 referida a la destrucción de datos que, establecía que "Quien, intencionalmente y con menosprecio de los derechos de los demás, introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que éste contiene o los modos de tratamiento o transmisión, será castigado con prisión de tres meses a tres años y con multa de 2.000 a 500.000 francos o con una de los dos penas". Con la reforma penal de 1992, este artículo quedó ubicado en el art. 323-1 del Nouveau Code Pénal, con la siguiente modificación: Se penaliza a quien al acceder a un ordenador de manera fraudulenta, suprima o modifique los datos allí almacenados.

El artículo 392 del Código Penal italiano incluye la alteración, modificación o destrucción total o parcial de programas de computación y el daño a la operación de un sistema telemático o informático. El artículo 420 del Código Penal, referido a atentados contra sistemas de instalaciones públicas, ha sido también modificado. Actualmente cualquiera que realice un acto con la intención de dañar o destruir sistemas informáticos o telemáticos de instalaciones públicas o sus datos, información o programas puede ser castigado con prisión de uno a cuatro años. En casos de consumación del delito (destrucción o daño a los datos) la pena se eleva de tres a ocho años.

En España, a partir de la reforma del Código penal, el nuevo artículo 264.2 reprime a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

En 1993 Chile sancionó la ley 19.223 (Diario Oficial de la República de Chile, Lunes 7 de junio de 1993) por la que se tipifican figuras penales relativas a la informática. En su art.3° dispone: "El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio".

C) FRAUDE INFORMATICO

Se ha pensado el delito de fraude informático como un tipo autónomo y no como una figura especial de las previstas en los arts. 172 y 173 del Código Penal. En este sentido, se entendió que en el fraude informático, la conducta disvaliosa del autor está signada por la conjunción de dos elementos típicos ausentes en los tipos tradicionales de fraude previstos en Código: el ánimo de lucro y el perjuicio patrimonial fruto de una transferencia patrimonial no consentida sin que medie engaño ni voluntad humana viciada. El ánimo de lucro es el elemento subjetivo del tipo que distingue el fraude informático de las figuras de acceso ilegítimo informático y daño informático en los casos en que la comisión de las conductas descriptas en estos tipos trae aparejado un perjuicio patrimonial.

El medio comisivo del delito de fraude informático consiste en la manipulación o despliegue de cualquier artificio semejante sobre un sistema o dato informático. Se ha optado por definir la conducta que caracteriza este delito como una "manipulación" o "artificio tecnológico semejante" en el entendimiento de que dichos términos comprenden tanto la acción de supresión, modificación, adulteración o ingreso de información falsa en un sistema o dato informático.

El hecho se agrava cuando el fraude informático recae en alguna Administración Pública Nacional o Provincial, o entidad financiera.

D) Disposiciones Comunes

Como artículo 6°, bajo el título de Disposiciones Comunes, se ha creído necesario, por el tipo de ley especial de que se trata, redactar un glosario que facilite la comprensión de la terminología utilizada por el Anteproyecto.

Se definen en las disposiciones comunes, los dos términos centrales, en torno a los cuales giran los tipos definidos, con el mayor rigorismo a los fines de acotar los tipos en salvaguarda del principio de legalidad, pero, a la vez, con la suficiente flexibilidad y vocabulario técnico, con el objeto de no generar anacronismos en razón de la velocidad con la que se producen los cambios tecnológicos, tratando de aprehender todos los fenómenos de las nuevas tecnologías de la información.

Se ha podido comprobar, fruto de debates que se producen en otras latitudes, que la inmensa cantidad de las conductas ilegitimas que se buscan reprimir atentan ya sea contra uno u otro de estos dos conceptos definidos. Consiguientemente se decidió -siguiendo la Convención del Consejo de Europa sobre Cyber Crime- que, demarcando con nitidez ambos conceptos y haciéndolos jugar dentro de la tipología elegida, se lograba abarcar en mayor medida las conductas reprochables, sin perder claridad ni caer en soluciones vedadas por principios centrales del derecho penal: a saber, Principio de legalidad y Principio de Prohibición de la Analogía.

Independientemente de lo manifestado, se debe tener presente que sí bien el dato informático o información, tal cual está definido en esta ley especial, es sin duda de un intangible, y que -solo o en conjunto con otros intangibles- puede revestir cierto valor económico o de otra índole, no debe, por ello, caerse en el error de -sin mas- asociarlo a lo que en los términos del Derecho de la Propiedad Intelectual se entiende por obra protegida. (vgr. :software). Si bien una obra protegida por el régimen de la Propiedad Intelectual, puede almacenarse o transmitirle a través de red o de un sistema informático y -eventualmente- ser objeto de una conducta de las descripta por esta ley, no toda información - según se define aquí- es una obra de propiedad intelectual y por ende goza del resguardo legal que otorga de dicho régimen de protección especial.

Común a las disposiciones de acceso ilegítimo, daño y fraude informáticos, se ha entendido que el delito se ve agravado cuando quien realiza las conductas delictivas es aquél que tiene a su cargo la custodia u operación del sistema en razón de las responsabilidades y deberes que le incumben, puesto que usa sus conocimientos, status laboral o situación personal para cometer cualesquiera de los delitos tipificados por la presente ley.

En cuanto a la escala penal, se le otorga al juez una amplia discrecionalidad para graduar el aumento de la pena en estos casos, pero le pone un límite, y es que la sanción no podrá superar los veinticinco años de prisión.

Por los motivos expuestos se somete a su consideración el presente anteproyecto de ley

ANEXO 5

http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia#Ref1

Ley de Delitos Informáticos en Colombia

Artículos - Invitados - Otros

Escrito por Isabella Gandini, Andrés Isaza, Alejandro Delgado

La Ley 1273 de 2009 creó nuevos tipos penales relacionado con delitos informáticos y la protección de la información y los datos con penas de prisión de hasta 120 meses y multa de hasta 1500 salarios mínimos legales mensuales vigentes[1].

El 5 de enero de 2009, el Congreso de la República de Colomb promulgó la Ley 1273 "Por medio del cual se modifica el Códig Penal, se crea un nuevo bien jurídico tutelado – denominado "D la Protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

Dicha ley tipificó como delitos una serie de conduc relacionadas con el manejo de datos personales, por lo que de gran importancia que las empresas se blinden jurídicamer para evita incurrir en alguno de estos tipos penales.

No hay que olvidar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para reci servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los caje automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo. Según la Revista Cara y Se durante el 2007 en Colombia las empresas perdieron más de 6.6 billones de pesos a raíz de delitos informáticos.

De ahí la importancia de esta ley, que adiciona al Código Penal colombiano el Título VII BIS denominado "De la Protecci de la información y de los datos" que divide en dos capítulos, a saber: "De los atentados contra la confidencialidad, integridad y la disponibilidad de los datos y de los sistemas informáticos" y "De los atentados informáticos y ot infracciones".