CAPÍTULO IV

"La ciencia se compone de errores, que a su vez,
son los pasos hacia la verdad."

Julio Verne

INFORMÁTICA FORENSE, INSERCIÓN JURÍDICA

4.1. Informática forense y su realidad procesal en el Ecuador.

4.2. Informática forense, leyes internacionales

4.3. Leyes ecuatorianas e internacionales

4.4. Otras consideraciones

4.1. INFORMÁTICA FORENSE Y SU REALIDAD PROCESAL EN EL ECUADOR

El delito informático se puso de moda en Ecuador desde que en 1999 se puso en el tapete la discusión del proyecto de Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, en el país se empezaron a realizar cursos, seminarios, encuentros, se conformaron comisiones para la discusión de la Ley y para que se formulen observaciones, aquí intervinieron organismos que se encontraban directamente interesados como el CONATEL, la Superintendencia de Bancos, las Cámaras de Comercio y otros, entidades que veían en el comercio electrónico una buena oportunidad de hacer negocios y de paso hacer que el país entre en este nuevo auge y no se quede retrasado.

Como es lógico cuando la ley se presentó en un inicio, tenía una serie de falencias, que hasta el momento se han ido puliendo, sobre todo basadas en la realidad Ecuatoriana, una de las partes que más ha tenido cambios es la parte penal, en un inicio los llamados delitos informáticos se sancionaban de acuerdo al Código Penal, para ese entonces el Código Penal no contaba con los tipos penales necesarios para abarcar los nuevos adelantos informáticos, por lo tanto eran inútiles para dar seguridad al Comercio Electrónico ante el posible asedio del crimen informático.

Basados en las variadas observaciones y de largas discusiones el Congreso Nacional y sus honorables diputados por fin aprobaron el texto definitivo de la Ley de Comercio Electrónico, Mensajes de Datos y Firmas electrónicas, y en consecuencia también se realizaron varias reformas al Código Penal que daban cabida a los llamados Delitos Informáticos.

Aun así se puede advertir que siguen existiendo algunas cosas por definir, según la misma ley "*el ejercicio de la acción pública corresponde exclusivamente al fiscal*" (Constitución política del Ecuador, titulo X,

Capítulo 3ro, Art. 219, inciso primero). Con esto se puede concluir que el dueño de la acción penal y de la investigación tanto procesal como pre-procesal es el Fiscal, quien contará con la ayuda de la Policía Judicial para que se haga la investigación de los delitos.

Ahora que ya se sabe quiénes son los encargados de realizar las investigaciones, surge la duda acerca de si éstos tienen la capacidad técnica y académica para poder investigar este tipo de delitos informáticos, es decir se hace necesario la formación tanto de los Fiscales que dirigirán la investigación como del cuerpo policial que los auxiliaran en dicha tarea.

En la actualidad en Ecuador no existe una Unidad Especializada, como existe en otros países, tal es el caso de Estados Unidos donde el FBI cuenta con el COMPUTER CRIME UNIT, o en España la Guardia Civil cuenta con un departamento especializado en esta clase de delitos, eso solo por mencionar algunos. Pero también por el lado de la Función Judicial falta la suficiente preparación por parte de Jueces y Magistrados, en este sentido puede darse el caso que los llamados a impartir justicia se encuentran confundidos con la particularidad de estos delitos y tienden a confundirlos con los delitos tradicionales que por su estructura típica son incapaces de subsumir a estas nuevas conductas delictivas que tiene a la informática como su medio o fin.

Con esto lo que se evidencia es que se hace necesario que se formen unidades investigativas tanto policiales como del Ministerio Público especializadas en abordar cuestiones de la delincuencia informática e informática forense. Estas unidades también pueden servir de base para una cooperación internacional formal o una cooperación informal basada en redes transnacionales de confianza entre los agentes de aplicación de la ley.

Una solución o fase inicial es la de apelar a la cooperación internacional, de países amigos que ya cuentan con la infraestructura y recurso humano capacitado en este tipo de tareas, siempre tomando conciencia de que con la tecnología digital en los últimos años, ha surgido una nueva generación de delincuentes que expone a los gobiernos, empresas e individuos a estos peligros.

4.1.1. Unidad de Delitos Informáticos del Ministerio Público (UDIMP)

En el caso de Ecuador en un inicio se creó la una unidad de Delitos Informáticos del Ministerio Público, esta se denominó UDIMP y estaba estructurada de la siguiente forma:

1. **COORDINACIÓN NACIONAL,** es la encargada de dar las políticas y directrices generales de la investigación de los Delitos Informáticos a nivel nacional, es quien mantendrá la coordinación entre el Ministerio Público y la Policía Judicial.

   Estará conformada por un Coordinador Nacional, los Agentes Fiscales y personal de apoyo de la Unidad con conocimientos en Delitos Informáticos.

   Para la Coordinación Nacional los nombres son:

   - **COORDINADOR NACIONAL:** Dr. Santiago Acurio Del Pino (593-2) 3985800, ext. 173082
   - **FISCAL 1:** Dr. Bormann Peñaherrera Manosalvas
   - **FISCAL 2:** Dr. Marco Esquetini Proaño
   - **SECRETARIO DE LA UNIDAD:** Sr. Gonzalo Núñez Velasco
   - **AMANUENSE:** Sr. Santiago Moreira
   - **AMANUENSE:** Sr. Xavier Torres
   - **JEFE DE SECCIÓN TÉCNICA FORENSE:** Sr. Fabián Moreano.

2. **SECCIÓN DE INTELIGENCIA,** es la encargada de recoger la información, datos y otros indicios que tengan relación con el

cometimiento de uno o más delitos informáticos, estará conformada por miembros de la Policía Judicial altamente especializados en el área de Inteligencia y con especiales conocimientos de informática.

3. **SECCIÓN OPERATIVA,** encargada de realizar las investigaciones de todo lo relacionado con la llamada criminalidad informática. Estará divida en Grupos de Investigaciones de acuerdo a las infracciones Informáticas.

   - **GRUPO 1: FRAUDES INFORMÁTICOS Y TELECOMUNICACIONES:** Es el encargado de la investigación de todo lo relacionado con el cometimiento de los llamados fraudes informáticos y sus diferentes modalidades, inclusive el uso fraudulento de tarjetas magnéticas y el By Pass.
   - **GRUPO 2: PORNOGRAFÍA INFANTIL:** Es el encargado de perseguir e investigar activamente a los depredadores pedófilos que utilizan la Internet para desarrollar relaciones personales con menores de edad con el propósito de atraerlos a una cita en persona y realizar las investigaciones pertinentes a fin de encontrar y terminar con el tráfico de material pornográfico de niños, niñas y adolescentes que está siendo difundido y transmitido a través de la Internet.
   - **GRUPO 3: SEGURIDAD LÓGICA Y TERRORISMO INFORMÁTICO (CIBERTERRORISMO[1]):** Es el encargado de perseguir e investigar activamente, las infracciones informáticas que amenacen a la seguridad lógica de los Sistemas de Información, al tráfico y fiabilidad de la información, así como las amenazas a la seguridad interna y externa sobre posibles ataques de terrorismo informático.

[1] Según el FBI el Ciberterrorismo es el uso ilegal de la fuerza y de la violencia contra personas o la intimidación para forzar un gobierno, población civil, o cualquier segmento con a cambios políticos o sociales, usando para ellos las redes telemáticas, ya sea produciendo ataques de denegación de servicio, colapsando las redes de información local (LAN), mediante él envió de virus informáticos o instalando bombas lógicas, en definitiva provocando cualquier clase de daño informático que comprometa de forma grave a las instituciones de un estado a sus ciudadanos.

Los miembros de la Sección Operativa, podrán ser personal calificado del Ministerio Público y miembros de la Policía Judicial con conocimientos en la realización de investigaciones, de informática, electrónica, programación y auditoría de sistemas.

4. **SECCIÓN TÉCNICA Y FORENSE,** Es la encargada de brindar el apoyo técnico y realizar el análisis forense de las evidencias encontradas en la escena del delito, estará compuesto por dos grupos:
   - **GRUPO DE APOYO TÉCNICO**
     Personas especializadas en recolección de evidencias.
   - **GRUPO DE ANÁLISIS FORENSE**
     Personas altamente capacitadas en las herramientas tanto de hardware como de software que permiten hacer el análisis forense.

   Los miembros de esta sección podrán ser parte del Ministerio Público y la Policía Judicial, además deberán ser Ingenieros en Sistemas con amplios conocimientos en informática forense, auditoría de sistemas informáticos y seguridad informática. De igual forma tendrán que ser especialistas en el uso de hardware y software especializado para este tipo de investigaciones.
5. **SECCIÓN DE CAPACITACIÓN Y ENTRENAMIENTO**
   Esta sección se encargará de la formación continua del personal de la Unidad mediante talleres de capacitación, seminarios, charlas, prácticas. Los mismos que serán dictados por expertos nacionales e internacionales, así como mantendrá la coordinación con las Agencias Gubernamentales Internacionales dedicadas a este tema para así obtener capacitación y entrenamiento en el descubrimiento y prevención de los Delitos Informáticos. También será la encargada de acreditar a los Peritos Informáticos a nivel nacional, esta sección estará bajo la supervisión de la Escuela de Fiscales.

Por motivos logísticos la Unidad deberá establecerse en un solo lugar o espacio físico en donde funcionarán los laboratorios técnicos y forenses, además deberá existir un área administrativa donde funcione la Coordinación General y las Secciones Operativas y de Inteligencia, de igual forma deberá existir un área de capacitación y entrenamiento. Todas estas áreas deberán estar equipadas con conexiones de red, y los más modernos equipos ofimáticos. Se deberá contar igualmente con un área para el servidor y demás equipos de red, así como una bodega de evidencias, en la cual se almacenarán los elementos de convicción y demás pruebas necesarias dentro de los diferentes casos que lleve la Unidad.

Con el tiempo y la disponibilidad de recursos, se deberán ir formando equipos logísticos y técnicos en cada ciudad principal del país a fin de formar una red de Equipos de Respuesta de Incidentes, los cuales formarán parte de la Unidad De Delitos Informáticos del Ministerio Público UDIMP. Los Incidentes de seguridad, son como cualquier evento no programado (anomalía), hechos que pudieran afectar a la seguridad de la información, entendiendo “afectar a la seguridad” como una pérdida de disponibilidad, integridad o confidencialidad de la misma o de un sistema de información, y que se encuentran relacionados con el cometimiento de una o varias infracciones informáticas.

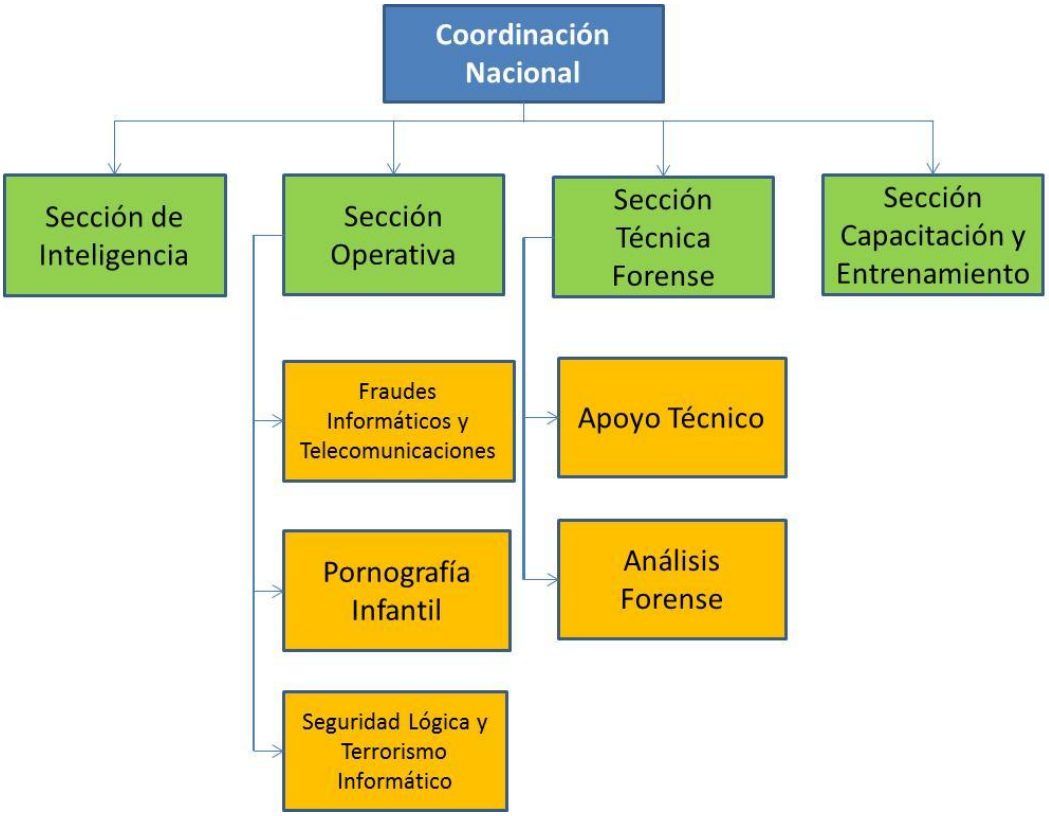

Figura. 4.1 Estructura de la Unidad Delitos Informáticos Ministerio Público.

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

Es importante mencionar que Ecuador junto con la colaboración del gobierno Español ha podido enviar personal para que se capacite en delitos informáticos[20], lo cual indica que el gobierno Ecuatoriano y el cuerpo policial se encuentran preocupados y atentos a este tema.

4.1.2. Departamento de Investigación y Análisis Forense

En la actualidad la UDIMP ahora es, el Departamento de Investigación y Análisis Forense de la Fiscalía General Del Estado, a continuación una pequeña reseña de dicho departamento:

Ante la necesidad de proteger a los usuarios de la red frente a la emergente criminalidad informática, que aprovecha las vulnerabilidades de los sistemas informáticos y el desconocimiento generalizado de la mayoría de los usuarios de la cultura digital, y ante la urgente obligación

de extender especialmente tal protección a los menores, que sufren una mayor indefensión y son víctimas de delitos como el de la pornografía infantil, sobre todo en las zonas más deprimidas y menos desarrolladas del planeta.

Esto tomando en cuenta que las nuevas tecnologías aportan una indiscutible mejora en la calidad de vida de nuestra sociedad. Por ello, han de promoverse cuantas iniciativas sean posibles para el desarrollo de la sociedad de la Información y su buen uso, a la vez que garantizar la seguridad de sus usuarios, y así poder terminar con la llamada Cifra Negra, en esta clase de infracciones.

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

Es deber del Estado y en especial de la Fiscalía el de promover las dinámicas sociales, jurídicas, tecnológicas, policiales, o de cualquier otra índole para hacer frente de forma eficaz al problema de la delincuencia informática.

De igual forma el Estado debe velar porque las aplicaciones de la tecnología sean correctas en el marco de la legalidad y de la ética, partiendo de bases y principios comunes que sean aceptados por la comunidad global, única manera de tener y mantener una verdadera protección al derecho a la intimidad.

Con estos antecedentes el Fiscal General Del Estado creo mediante Acuerdo 104-FGE-2008 el Departamento de Investigación y Análisis Forense de la Fiscalía General Del Estado.

4.1.2.1.- Misión

El departamento tiene la misión fundamental de ser una ayuda en la investigación y persecución de todo lo relacionado con la llamada criminalidad informática en todos sus espectros y ámbitos, en especial:

- Amenazas, injurias, calumnias. Por correo electrónico, SMS, tablones de anuncios, foros, newsgroups[2], Web.
- Pornografía infantil. Protección al menor en el uso de las nuevas tecnologías.
- Fraudes en el uso de las comunicaciones: By Pass[3].
- Fraudes en Internet. Fraude Informático, Uso fraudulento de tarjetas de crédito, Fraudes en subastas. Comercio electrónico.
- Seguridad Lógica. Virus. Ataques de denegación de servicio. Sustracción de datos. Terrorismo Informático
- Hacking. Descubrimiento y revelación de secreto. Suplantación de personalidad, Interceptación ilegal de comunicaciones
- Sustracción de cuentas de correo electrónico.

La seguridad pública es un derecho que debe garantizarse en cualquier entorno social, también en la Red.

4.1.2.2.- Funciones del Departamento de Análisis Forense

1. Asesorar a todas la Unidades Operativas de la Fiscalía General del Estado a Investigar y perseguir a nivel procesal y pre procesal penal toda infracción que utilice a la informática como medio o fin para la comisión de un delito en especial todo lo relacionado al fraude informático, acceso no autorizado a sistemas de información, pornografía infantil, interceptación de comunicaciones entre otros.

[2] Un tablón de anuncios o una cartelera es un lugar donde se pueden dejar mensajes públicos, por ejemplo, un aviso para comprar o vender, anunciar eventos, o proveer información.
Los grupos de noticias son un medio de comunicación en el cual los usuarios leen y envían mensajes textuales, con la posibilidad de que sean leídos y respondidos por otros usuarios.
3 El By pass evita la tarifación de la llamada internacional, y la convierte en una llamada local.

2. Desarrollar en los miembros del Departamento los conocimientos técnicos necesarios para combatir esta clase de infracciones, así como los procedimientos y técnicas de investigación forense adecuadas para el examen de las evidencias encontradas[4].

3. Contribuir a la formación continua de los investigadores; la colaboración con la Dirección Nacional de Investigaciones de la Fiscalía General del Estado y de las más importantes instituciones públicas y privadas; la participación activa en los foros internacionales de cooperación con los diferentes Ministerios Públicos, Fiscalías y las unidades policiales especializadas, además de la colaboración con la ciudadanía.

4. Formar y mantener alianzas con las Unidades Especiales de investigación de los Delitos Informáticos a nivel internacional, a fin de obtener su apoyo y soporte en esta clase de investigaciones.

5. Desarrollar una Política de Seguridad Informática General, a fin de prevenir y solucionar cualquier ataque a la integridad y fiabilidad de los sistemas informáticos de entidades públicas y privadas.

6. Implementar a nivel nacional el Sistema Información de Delitos Informáticos mediante el uso del Internet, el cual permitirá a todos los miembros de la Fiscalía obtener información sobre los Delitos Informáticos, su forma de combate y prevención.

7. Promover nuevos canales de comunicación y trabajo con las distintas estructuras y organizaciones gubernamentales implicadas en la lucha contra el fenómeno de la delincuencia informática, para

[4] La ciencia forense es sistemática y se basa en hechos premeditados para recabar pruebas para luego analizarlas. La tecnología, en caso de análisis forense en sistemas informáticos, son aplicaciones que hacen un papel de suma importancia en recaudar la información e indicios necesarios. La escena del crimen es el computador y la red a la cual éste está conectado.

buscar soluciones que permitan alcanzar los niveles de seguridad necesarios para el normal desarrollo de la Sociedad de la Información.

4.1.2.3.- Funciones del Jefe del Departamento de Análisis Forense

1. Elaborar las políticas y directrices generales de la investigación de los Delitos Informáticos a nivel nacional en conjunto con la Dirección de Actuación y Gestión Procesal y la Dirección de Investigaciones de la Fiscalía General del Estado.
2. Coordinar las acciones de la Fiscalía General del Estado y la Unidades Especializadas de la Policía Judicial en lo que se refiere a los Delitos relacionados con la tecnología.
3. Ayudar con el equipo técnico adecuado en la recopilación de los elementos de convicción (evidencia digital[5] y material):
4. Brindar apoyo técnico especializado a las unidades de la fiscalía General del Estado en el campo de la informática forense.
5. Capacitar al personal técnico del Departamento, así como ayudar al Consejo Nacional de la Judicatura con los lineamientos técnicos necesarios para acreditar a los Peritos Informáticos y formar en unión con la Policía Judicial y los Centros de Educación Superior a los investigadores especialistas en delitos informáticos.
6. Elaborar el listado actualizado de los peritos informáticos a nivel nacional.
7. Proponer al Fiscal General del Estado previa justificación o Informe Técnico la creación de Unidades especializadas en Delitos Informáticos en las diferentes Fiscalías Provinciales
8. Mantener una base de datos de todas las investigaciones realizadas en con apoyo del Departamento.
9. Las demás que le confieran otras disposiciones aplicables y órganos competentes de la Institución.

[5] Las evidencias digitales son campos magnéticos y pulsos electrónicos que pueden ser recogidos y analizados usando técnicas y herramientas especiales.

4.1.2.4.- Sección Técnica y Forense

Es la encargada de brindar el apoyo técnico y realizar el análisis forense de las evidencias encontradas en la escena del delito, estará compuesto por:

1. Técnicos en Escenas del Crimen Informáticas, también llamados first respondenders, son los primeros en llegar a la escena del crimen, son los encargados de recolectar las evidencias que ahí se encuentran. Tiene una formación básica en el manejo de evidencia y documentación, al igual que en reconstrucción del delito, y la localización de elementos de convicción dentro de la red.

2. Examinadores de Evidencia Digital o Informática, que son los responsables de procesar toda la evidencia digital o informática obtenida por los Técnicos en Escenas del Crimen Informáticos. Para esto dichas personas requieren tener un alto grado de especialización en el área de sistemas e informática[6].

3. Investigadores de Delitos Informáticos y Cibercrimen, que son los responsables de realizar la investigación y la reconstrucción de los hechos de los Delitos Informáticos de manera general, son personas que tiene un entrenamiento general en cuestiones de informática forense, son profesionales en Seguridad Informática, Abogados, Policías, y examinadores forenses.

Las personas a cargo de este nuevo departamento son:

- **Jefe del Departamento**
  Dr. Santiago Acurio Del Pino

[6] Los miembros de esta sección podrán ser parte de la Fiscalía y la Policía Judicial además deberán ser Ingenieros en Sistemas con amplios conocimientos en informática forense, auditoria de sistemas informáticos y seguridad informática. De igual forma tendrán que ser especialistas en el uso de hardware y software especializado para este tipo de investigaciones.

acurios@minpec.gov.ec

(593-2) 3985800, ext. 173082

- **Encargados del Área Técnica**

  Ing. Fabián Moreano.

  Ing. Carolina Salas.

4.2. INFORMÁTICA FORENSE, LEYES INTERNACIONALES

Entre los países que más se destacan actualmente tanto por sus leyes como su infraestructura para tratar este tipo de delitos están España, Estados Unidos, Bolivia, Argentina, Chile, Brasil, Colombia, Francia, Holanda, Gran Bretaña, Venezuela; a continuación se describe parcialmente algunas de las leyes existentes en estos países para tratar este nuevo tipo de delitos.

A nivel de Latinoamérica algunos países como Chile, Argentina, Venezuela, Perú, cuentan con regulación, a nivel legislativo que tipifica los delitos informáticos, mientras que en otros países se ha procedido a la reforma de los Códigos de Procedimiento Penal para la aplicación de las sanciones, ante las infracciones informáticas cometidas. Además de las reformas concernientes al Código de Procedimiento Penal se mantienen leyes como: Ley de Propiedad Intelectual, Ley de Comercio Electrónico, Ley de Habeas Data[7], Ley de Firmas Digitales, entre otras, que establecen especificaciones que conciernen a la información e informática.

[7] Habeas data es una acción constitucional que tiene cualquier persona de acceder a un registro para conocer qué información existe sobre su persona, y de solicitar la corrección de esa información si le causara algún perjuicio.

Legislación de Países Latinoamericanos	Ley de Propiedad Intelectual	Ley de Habeas Data	Ley de comercio Electrónico, Mensajes de Datos	Ley de Delitos Informáticos	Ley de Transparencia y Acceso a la Informática	Ley de Pornografía Infantil	Ley de Uso de correo Electrónico
Argentina	●	●	●	●			
Bolivia					Proyecto		
Brasil		●	●				
Chile	●		●	●		●	
Colombia		●	●	●	●		
Costa Rica				●			
Ecuador	●	●	●		●		
Guatemala			●				
México				Proy.	●		
Panamá			●				
Paraguay					●		
Perú			●	●	●		●
República Dominicana			●				
Uruguay							Proy.
Venezuela			●	●			

Tabla.4.1 Leyes en países Latinoamericanos.

Fuente: Estadísticas de la Organización de Estados Americanos (OEA)

4.2.1. Legislación Informática de España

La legislación Española es una de las que mejor ha aplicado la ley en lo relacionado a los delitos informáticos, en especial en lo relacionado con pornografía infantil y propiedad intelectual.

Estos son algunos de los artículos más representativos de dicha ley.

CAPÍTULO XI

De los delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores:

Sección 1ª. DE LOS DELITOS RELATIVOS A LA PROPIEDAD INTELECTUAL.

Artículo 270.

Será castigado con la pena de prisión de seis meses a dos años o de multa de seis a veinticuatro meses quien, con ánimo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.

La misma pena se impondrá a quien intencionadamente importe, exporte o almacene ejemplares de dichas obras o producciones o ejecuciones sin la referida autorización.

Será castigada también con la misma pena la fabricación, puesta en circulación y tenencia de cualquier medio específicamente destinada a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de computador.

Artículo 278.

1. El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.

2. Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.
3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos.

CAPÍTULO III

Disposición general

Artículo 400.

La fabricación o tenencia de útiles, materiales, instrumentos, sustancias, máquinas, programas de ordenador o aparatos, específicamente destinados a la comisión de los delitos descritos en los capítulos anteriores, se castigarán con la pena señalada en cada paso para los autores.

Artículo 536.

La autoridad, funcionario público o agente de éstos que, mediando causa por delito, interceptare las telecomunicaciones o utilizare artificios técnicos de escuchas, transmisión, grabación o reproducción del sonido, de la imagen o de cualquier otra señal de comunicación, con violación de las garantías constitucionales o legales, incurrirá en la pena de inhabilitación especial para empleo o cargo público de dos a seis años.

Si divulgare o revelare la información obtenida, se impondrán las penas de inhabilitación especial, en su mitad superior y, además la de multa de seis a dieciocho meses.

4.2.2. Legislación Informática de Venezuela

Venezuela cuenta con una ley especial contra delitos informáticos, que tiene como objeto la protección de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos

mediante el uso de dichas tecnologías, en los términos previstos en esta ley.

Esta legislación divide y castiga a los delitos en cinco partes:

1. **De los Delitos contra los Sistemas que utilizan Tecnologías de Información**

   Condena de uno a cinco años el acceso indebido, de cuatro a ocho años el sabotaje o daño a sistemas, solo por mencionar algunos, pero también castiga delitos tales como: sabotaje o daños culposos, acceso indebido o sabotaje a sistemas protegidos, posesión de equipos o prestación de servicios de sabotaje, espionaje informático, falsificación de documentos, etc.

2. **De los Delitos contra la Propiedad**

   Los delitos que se encuentran enmarcados en esta categoría son: hurto, fraude, obtención indebida de bienes o servicios, manejo fraudulento de tarjetas inteligentes o instrumentos análogos, apropiación de tarjetas inteligentes o instrumentos análogos, provisión indebida de bienes o servicios, posesión de equipo para falsificaciones. Todos estos delitos pueden llevar a una pena máxima de 6 años y multas fijadas en unidades tributarias.

3. **De los delitos contra la privacidad de las personas y de las comunicaciones**

   En este apartado se describen los delitos como violación de la privacidad de la data o información de carácter personal, violación de la privacidad de las comunicaciones, revelación indebida de data o información de carácter personal, y en todos los casos puede ser penado de dos a seis años de prisión con sus respectivas multas económicas.

4. **De los delitos contra niños, niñas o adolescentes**

   En esta categoría se enmarcan delitos como difusión o exhibición de material pornográfico y exhibición pornográfica de niños o adolescentes, en ambos casos las penas pueden ir desde los dos años hasta los ocho años.

5. **De los delitos contra el orden económico**

   En esta última clasificación se encuentra la apropiación de propiedad intelectual y la oferta engañosa, estos dos delitos pueden ser castigados de uno a cinco años y multa de cien a quinientas unidades tributarias.

4.2.3. Legislación Informática dictada por las Naciones Unidas

La Organización de las Naciones Unidas más que imponer una legislación lo que hace es especificar o unificar los criterios con respecto a las definiciones relacionadas con los delitos informáticos, entre los países integrantes.

En este sentido los tipos de delitos informáticos según las naciones Unidas son:

- **Fraudes cometidos mediante manipulación de computadoras**
  a. Manipulación de los datos de entrada.
  b. La manipulación de programas.
  c. Manipulación de los datos de salida.
  d. Fraude efectuado por manipulación informática.
- **Falsificaciones informáticas:**
  a. Como objeto.
  b. Como instrumentos.
- **Daños o modificaciones de programas o datos computarizados.**
  a. Sabotaje informático.
  b. Acceso no autorizado a servicios y sistemas informáticos.
  c. Piratas informáticos o hackers.

Asimismo, la ONU resume de la siguiente manera a los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

a. Falta de acuerdos globales acerca de qué tipo de conductas deben constituir delitos informáticos.
b. Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.
c. Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.
d. No armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.
e. Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.
f. Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

4.2.4. Legislación Informática en México

A continuación se detalla a breves rasgos lo que dicta la legislación Mexicana en lo que se refiere a delitos informáticos y como se castigan este tipo de delitos.

Libertad y privacidad

ACTA DE PRIVACIDAD DE 1974. Se refiere a la protección de la privacidad de los individuos cuyos datos personales figuran en bancos de datos del gobierno Federal. Sus mandatos básicos son los siguientes:

a. Prohibición de la existencia de bancos de datos secretos de información personal.
b. Posibilidad del individuo de conocer que información existe acerca de él y cual va hacer su uso.
c. Posibilidad del individuo de corregir o rectificar la información registrada sobre él.
d. Prohibición de utilizar la información personal sin el permiso del individuo para otro propósito diferente de aquel para el que fue recopilada.

e. Toda organización que recopile, use o distribuya información personal debe establecer los medios necesarios para asegurar su fiabilidad y prevenir los posibles abusos que se puedan realizar con la misma.

ACTA DE PRIVACIDAD EDUCACIONAL. Protege la información registrada en instituciones docentes públicas. Sus puntos principales son: Los datos solo pueden ser recopilados por aquellas personas u organismos autorizados por la ley.

1. Los estudiantes y sus padres han de tener posibilidad de acceso a las informaciones educacionales sobre ellos.
2. Solamente se permite la comunicación de esta información a las instituciones educativas públicas para usos administrativos y a las autoridades en algunos supuestos legales.

ACTA DE PRIVACIDAD FINANCIERA DE 1978. Proporciona protección a los individuos restringiendo el acceso del gobierno a las informaciones sobre clientes de los bancos e instrucciones financieras, estableciendo así un cierto grado de confidencialidad de los datos financieros personales.

ACTA DE LA LIBERTAD DE INFORMACIÓN DE 1970. Establece el derecho a la gente o individuos de acceder a los datos sobre ellos almacenados. Mencionaremos algunos artículos sobre los Derechos a la libertad informática.

1. Reconocen el derecho a la libertad:
   - El artículo 1 de la Declaración América de Derechos del Hombre:
     Todo ser humano tiene derecho a la libertad.
   - El artículo 3 de la Declaración Universal de Derechos Humanos, que afirma que:
     Todo individuo tiene derecho a la libertad.
   - El artículo 5 del Convenio Europeo de Derechos Humanos, de 1950, que establece que:

Toda persona tiene derecho a la libertad.

2. Reconocen el derecho a la seguridad personal:
   - El artículo 1 de la Declaración América de Derechos del Hombre:
     Todo ser humano tiene derecho a la seguridad de su persona.
   - El artículo 3 de la Declaración Universal de Derechos Humanos:
     Todo individuo tiene derecho a la seguridad personal.
   - El artículo 7 del Pacto de San José Costa Rica:
     Toda persona tiene derecho a la libertad y a la seguridad personal.
3. Reconocen el derecho a la intimidad:
   - Artículo 12 de la Declaración Universal de Derechos Humanos:
     Nadie será objeto de injerencia arbitraria en sus vidas privadas.
   - Artículo 17.1 del Pacto Internacional de Derechos Civiles y Políticos:
     Nadie será objeto de injerencia arbitraria o ilegal en su vida privada.

El derecho a la libertad informática o derecho a la autodeterminación informática es un derecho fundamental de muy reciente aparición. Está vinculado a la fuerte tecnología que ha experimentado la informática en los últimos veinte años. Lo cual ha permitido el almacenamiento, tratamiento y transmisión automatizada de una enorme cantidad de información personal. Crimen y fraude computacional.

4.2.5. Legislación Informática en Argentina

De acuerdo con los códigos vigentes, para que exista robo o hurto debe afectarse una cosa, entendiendo como cosas aquellos objetos materiales susceptibles de tener algún valor, la energía y las fuerzas naturales susceptibles de apropiación. **(Código Civil, Art. 2311).**

En lo que se refiere a daños infligidos la legislación informática propone:

- El **artículo 1072** del Código Civil argentino declara "el acto ilícito ejecutado a sabiendas y con intención de dañar la persona o los derechos del otro se llama, en este Código, delito", obligando a reparar los daños causados por tales delitos.
- En caso de probarse la existencia de delito de daño por destrucción de la cosa ajena, "la indemnización consistirá en el pago de la cosa destruida; si la destrucción de la cosa fuera parcial, la indemnización consistirá en el pago de la diferencia de su valor y el valor primitivo"**(Art. 1094).**
- Existe la posibilidad de reclamar indemnización cuando el hecho no pudiera ser considerado delictivo, en los casos en que "alguien por su culpa o negligencia ocasiona un daño a otro" **(Art. 1109).**
- Pero "el hecho que no cause daño a la persona que lo sufre, sino por una falta imputable a ella, no impone responsabilidad alguna" **(Art.1111).**
- En todos los casos, el resarcimiento de daños consistirá en la reposición de las cosas a su estado anterior, excepto si fuera imposible, en cuyo caso la indemnización se fijará en dinero" **(Art.1083).**

4.2.6. Legislación Informática en Estados Unidos

En Estados Unidos la legislación informática se adoptó en 1994, del **Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030),** que a su vez modificó al Acta de Fraude y Abuso Computacional de 1986.

Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y que no es un virus, un gusano, un caballo de Troya y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, a los sistemas informáticos, a las redes, información, datos o programas (18 U.S.C.: Sec. 1030 [a] [5] [A])[7]. La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus.

El Acta de 1994 diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus de aquellos que lo realizan con la intención de hacer estragos. Definiendo dos niveles para el tratamiento de quienes crean virus:

a. Para los que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa.
b. Para los que lo transmiten sólo de manera imprudencial la sanción fluctúa entre una multa y un año en prisión.

Esta ley constituye un acercamiento más comprometido con el creciente problema de los virus informáticos, específicamente no definiendo a los virus sino describiendo el acto, para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen. Diferenciando los niveles de delitos, la nueva ley da lugar a que se contemple qué se debe entender como acto delictivo.

Asimismo, en materia de estafas electrónicas, defraudaciones y otros actos dolosos relacionados con los dispositivos de acceso a sistemas informáticos, la legislación estadounidense sanciona con pena de prisión y multa, a la persona que defraude a otro mediante la utilización de una computadora o red informática.

4.2.7. Legislación Informática en Gran Bretaña.

Debido a un caso de hacking en 1991, comenzó a regir en este país la **Computer Misuse Act**[8](Ley de Abusos Informáticos). Mediante esta ley el intento, exitoso o no, de alterar datos informáticos es penado con hasta cinco años de prisión o multas.

Esta ley tiene una sección que específica la modificación de datos sin autorización; Los virus están incluidos en esa categoría.

El liberar un virus tiene penas desde un mes a cinco años, dependiendo del daño que causen.

4.2.8. Legislación Informática en Holanda.

El 1 de Marzo de 1993 entró en vigencia la **Ley de Delitos Informáticos**,[9] en la cual se penaliza el hacking, el preacking[8] (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio), la ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no se entregaría), y la distribución de virus.

La distribución de virus está penada de distinta forma si se escaparon por error o si fueron liberados para causar daño.

Si se demuestra que el virus se escapó por error, la pena no superará el mes de prisión; pero, si se comprueba que fueron liberados con la intención de causar daño, la pena puede llegar hasta los cuatro años de prisión.

4.2.9. Legislación Informática en Francia.

En enero de 1988, este país dictó la **Ley relativa al fraude informático**[10], la cual prevé penas de dos meses a dos años de prisión y multas de diez mil a cien mil francos por la intromisión fraudulenta que suprima o modifique datos.

[8] Es el conjunto de mecanismos ilícitos por los cuales muchas personas vulneran la seguridad de los sistemas telefónicos tanto públicos, privados como celulares.

Asimismo, esta ley establece en su artículo 462-3 una conducta intencional y a sabiendas de estar vulnerando los derechos de terceros que haya impedido o alterado el funcionamiento de un sistema de procesamiento automatizado de datos. Por su parte el artículo 462-4también incluye en su tipo penal una conducta intencional y a sabiendas de estar vulnerando los derechos de terceros, en forma directa o indirecta, haya introducido datos en un sistema de procesamiento automatizado o haya suprimido o modificado los datos que éste contiene, o sus modos de procesamiento o de transmisión.

También la legislación francesa establece un tipo doloso y pena el mero acceso, agravando la pena cuando resultare la supresión o modificación de datos contenidos en el sistema, o bien en la alteración del funcionamiento del sistema (sabotaje).

Por último, esta ley en su artículo 462-2, sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la pena correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.

4.2.10. Legislación Informática en Chile.

Chile fue el primer país latinoamericano en aprobar una **Ley contra delitos informáticos**[11], la cual entró en vigencia el 7 de junio de 1993.

A continuación se transcriben las disposiciones de mencionada ley que tipifican los delitos informáticos:

La Ley No 19.223 contempla cuatro artículos, que si bien corresponden cada uno a un tipo de conducta distinta, se pueden clasificar en dos grandes figuras delictivas:

I. Sabotaje Informático.
II. Espionaje Informático.

Estas dos figuras se subdividen en categorías distintas, atendiendo al objeto contra el cual se atenta y/o al modus operandi.

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 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 la 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 incurriere en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado”.

4.2.11. Delitos informáticos: Aplicación Colombia

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

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

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. 4.2 Legislación en Colombia – Informática e información

Unidades de investigación que reciben todo el apoyo de organismos internacionales y países desarrollados, como es el caso de Estados Unidos, que le brinda a Colombia toda la ayuda que necesite para su lucha contra el narcotráfico, y la informática forense es uno de los organismos que recibe este tipo de ayuda, por eso es que Colombia es uno de los países de Latinoamérica más desarrollado en este aspecto.

En el campo jurídico, Colombia mantiene según la **tabla 4.2** las siguientes leyes decretos y acuerdos, relacionados con la informática y la información.

La Ley1273 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. (**Véase la Tabla 4.3**)

Se puede observar que las sanciones establecidas se orientan 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.

Como se mencionó antes, Colombia ha sido uno de los países que ha recibido la ayuda de los Estados Unidos para la persecución de actos criminales, y la rama de investigación de naturaleza informática, esto 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)[12] como parte de la Dirección de Investigación Criminal, que investiga las conductas delictivas que se derivan del uso de la tecnología y las telecomunicaciones, este organismo se sustenta con el apoyo de equipos de informática forense y personal profesional capacitado que

atienden incidentes informáticos presentes durante una investigación judicial.

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 A 72 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 partes de las penas imponibles.
Atentados informáticos y otras infracciones: 1) Hurto por medios informáticos y semejantes 2) Transferencia no consentida de activos	

Tabla. 4.3. Ley de Delitos Informáticos – Ley 1273

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 otros, 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.

4.3. LEYES ECUATORIANAS E INTERNACIONALES

Si bien es cierto, la ley Ecuatoriana de Comercio Electrónico se realizó basada en leyes ya existentes en otros países, ésta se acopló a la realidad de nuestro país por lo tanto es una ley netamente territorial.

En este sentido el código penal Ecuatoriano sostiene que la ley penal es aplicable cuando la infracción ha sido cometida dentro del territorio, en este momento esto debe cambiar, teniendo en cuenta el nuevo escenario en donde se presentan este tipo de delitos que son de carácter transnacional, es decir delitos que se cometen en el Ciberespacio, un lugar donde no existen fronteras.

A primera vista se puede constatar que es difícil la persecución de estos delitos y su enjuiciamiento, ya que existe la posibilidad de cometer delitos informáticos desde lugares lejanos. Esto debido a los adelantos en telecomunicaciones y demás infraestructura, las cuales hacen que las distancias entre fronteras no existan y una persona puede realizar un acto delictivo en un lugar distinto al lugar de los hechos.

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

Pero en el caso de los delitos informáticos como se mencionó se debe aplicar el principio de universalidad y justicia mundial, este principio básicamente lo que dice es que la ley aplicable es la ley del país que primero capture al delincuente.

Este principio tiene la finalidad de reprimir delitos contra la humanidad, para esto es necesario firmar convenios internacionales y unilaterales con el fin de que cada país pueda sancionar al delincuente con su propia ley, sin importar el lugar donde el individuo haya cometido el acto ni tampoco la nacionalidad del mismo.

Como ya se mencionó los delitos informáticos en la mayoría de sus veces son de carácter transnacional, en especial el Ciberterrorismo, en este caso es necesario aplicar este principio de universalidad, por cuanto este tipo de ataques en estos momentos puede causar más daño que el terrorismo convencional.

4.4. OTRAS CONSIDERACIONES

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

Es indudable que los países latinoamericanos están tomando iniciativas que les permite desarrollar estrategias para el seguimiento de los delitos informáticos, algunos como Argentina y Colombia han elaborado y aprobado las respectivas regulaciones que protegen el bien jurídico; Ecuador cuenta ya con la entidad de certificación de las firmas electrónicas, la Ley de Comercio Electrónico, Firmas Digitales y Mensaje de Datos e iniciativas que permiten el seguimiento de ciertos aspectos tecnológicos como el proyecto "Libertador[9]", entre otros; debe embarcarse en un proyecto que permita delinear aspectos regulatorios sobre las tecnologías de la información.

Es indudable el avance tecnológico y la necesidad de establecer mecanismos que permitan la persecución de actos ilícitos cometidos utilizando medios tecnológicos.

Para lo que se debe preparar a una nueva generación de profesionales que den respuesta a la creciente necesidad de la sociedad de contar con asesores entendidos, y capaces de brindar sustento y respaldo legal a cada una de las actividades que se desarrollan con soporte de las tecnologías de la información.

[9] Proyecto para combatir el narcotráfico y el secuestro en el Ecuador

Todo esto no lo podemos lograr solos, por eso es necesario la búsqueda de apoyo internacional, en especial de países o entidades que ya tienen varios años de experiencia en estos temas

A continuación se destacan algunas recomendaciones por áreas, observadas tanto por el Doctor Santiago Acurio del Pino[10]como por la Licenciada Laura Alexandra Ureta[11]:

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

[10] Doctor Santiago Acurio del Pino, Director Nacional de Tecnologías de la Información
[11] Licenciada Laura Alexandra Ureta, Magister en Sistemas de Información Gerencial, ESPOL

	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 y probabilidad de ocurrencia de delitos informáticos 2. Difusión de medidas de salvaguarda tal como el cierre de brechas de seguridad, como medidas de prevención ciudadana ante delitos de índole tecnológico. 3. Concientización en las organizaciones de que las medidas de seguridad más que un gasto son una inversión que proveen mecanismo para evitar este tipo de delitos. 4. Concientización del efecto e impacto de los delitos informáticos sobre la sociedad.

Tabla 4.4. Recomendaciones por sector – Delitos Informáticos

4.5. BIBLIOGRAFÍA

[1] Delitos informáticos – Códigos penales,
http://www.portaley.com/delitos-informaticos/codigo-penal-197-201.shtml
http://www.portaley.com/delitos-informaticos/codigo-penal-270.shtml
http://www.portaley.com/delitos-informaticos/codigo-penal-386.shtml
http://www.portaley.com/delitos-informaticos/codigo-penal-263.shtml
http://www.portaley.com/delitos-informaticos/codigo-penal-248.shtml

http://www.portaley.com/delitos-informaticos/codigo-penal-169.shtml
http://www.portaley.com/delitos-informaticos/codigo-penal-205.shtml

[2] Pantin & Asociados, Legislación venezolana. Tomado de: http://www.pantin.net/

[3] Ley especial contra delitos informáticos, Venezuela, Gaceta Oficial Nª 37.313 de fecha 30 de octubre de 2001. Tomado de: http://fundabit.me.gob.ve/documento/LECDI.pdf

[4] Plan Operativo de creación de la Unidad de Delitos Informáticos del Ministerio Público. Tomado de: http://www.oas.org/juridico/spanish/cyb_ecu_plan_operativo.pdf

[5] Legislación nacional de los estados miembros de la OEA. Tomado de: http://www.oas.org/juridico/spanish/cybersp_legis.htm

[6] España, La informática forense. Tomado de: http://www.ciberjure.com.pe/index.php?option=com_content&task=view&id=3304&Itemid=9

[7] Estados Unidos, Fraud and Related Activity in Connection with Computers. Tomado de: http://www.justice.gov/criminal/cybercrime/1030_new.html

[8] Gran Bretaña, Computer Misuse Act 1990. Tomado de: http://www.opsi.gov.uk/acts/acts1990/ukpga_19900018_en_1.htm

[9] Holanda, De Wet Computercriminaliteit. Tomado de: http://www.iusmentis.com/beveiliging/hacken/computercriminaliteit/

[10] Francia, LOI N°88-19 DU 5 JANVIER 1988. Tomado de: http://www.securiteinfo.com/legal/loi88-19.shtml

[11] CHILE, LEY CHILENA DE DELITOS INFORMÁTICOS. Tomado de: http://www.rft.cl/informacion-informatica-y-negocios/delitos-informaticos

[12] COLOMBIA, Grupo Investigativo de Delitos Informáticos. Tomado de: http://delitosinformaticos.gov.co/

[13] Noticia: Venezuela contará con un Centro Nacional de Informática Forense, Lunes, 10 de Agosto de 2009. Tomado de: http://www.cnti.gob.ve/index.php?option=com_content&view=article&catid=44:nacionales&id=2708:venezuela-contara-con-un-centro-nacional-de-informatica-forense-&Itemid=88

[14] España, BRIGADA DE INVESTIGACIÓN TECNOLÓGICA. Tomado de: http://www.policia.es/bit/

[15] Policía Peruana, División de investigación de delitos de alta tecnología. Tomado de: http://www.policiainformatica.gob.pe/

[16] Policía Mexicana, policía cibernética de México. Tomado de: http://ssp.gob.mx

[17] Policía Nacional de Colombia, Grupo Delitos Informáticos. Tomado de: http://www.delitosinformaticos.gov.co/joomla/index.php?option=com_content&task=view&id=1&Itemid=2

[18] Policía Chilena, Brigada Investigadora del Ciber Crimen. Tomado de: http://www.investigaciones.cl/paginas/brigadas/bg-bricib/bg-bricib.htm

[19] Legislaciones de varios países. Tomado de: http://www.delitosinformaticos.com/delitos/

[20] Policías ecuatorianos estudian en España sobre cyberdelitos. Tomado de: http://www.eluniverso.com/2009/11/07/1/1360/policias-ecuatorianos-estudian-espana-sobre-cyberdelitos.html