Plan Operativo de creación de la Unidad de Delitos Informáticos del Ministerio Público

Dr. Santiago Acurio Del Pino
COORDINADOR DEL DEPARTAMENTO INFORMÁTICO
DEL MINISTERIO FISCAL DISTRITAL DE PICHINCHA

Hay algo en el mundo que es todavía más raro que los brillantes y las perlas: el buen juicio". **JEAN DE LA BRUYÉRE**

1.- El Delito Informático y su realidad procesal en el Ecuador

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

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

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

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

De acuerdo a la Constitución Política de la República, en su Título X, Capitulo 3ro al hablar del Ministerio Público, en su Art. 219 inciso primero señala que: "**El Ministerio Público prevendrá en el conocimiento de las causas**, **dirigirá y promoverá la investigación pre-procesal y procesal penal**. Esto en concordancia con el Art. 33 del Código de Procedimiento Penal que señala que "**el ejercicio de la acción pública corresponde exclusivamente al fiscal**". De lo dicho podemos concluir que el dueño de la acción penal y de la investigación tanto preprocesal como procesal de hechos que sean considerados como delitos dentro del nuevo Sistema Procesal Penal Acusatorio es el Fiscal. Es por tanto el Fiscal quien deberá llevar como quien dice la voz cantante dentro de la investigación de esta clase de infracciones de tipo informático para lo cual contara como señala el Art. 208 del Código de Procedimiento Penal con su órgano auxiliar la Policía Judicial quien realizará la investigación de los delitos de acción pública y de instancia particular bajo la dirección y control Ministerio Público, en tal virtud cualquier resultado de dichas investigaciones se incorporaran en su tiempo ya sea a la Instrucción Fiscal o a la Indagación Previa, esto como parte de los elementos de convicción que ayudaran posteriormente al representante del Ministerio Público a emitir su dictamen correspondiente.

Ahora bien el problema que se advierte por parte de las instituciones llamadas a perseguir las llamadas infracciones informáticas es la falta de preparación en el orden técnico tanto del Ministerio Público como de la Policía Judicial, esto en razón de la falta por un lado de la infraestructura necesaria, como centros de vigilancia computarizada, las modernas herramientas de software y todos los demás implementos tecnológicos necesarios para la persecución de los llamados Delitos Informáticos, de igual manera falta la suficiente formación tanto de los Fiscales que dirigirán la investigación como del cuerpo policial que lo auxiliara en dicha tarea, dado que no existe hasta ahora en nuestra policía una Unidad Especializada, como existe en otros países como en Estados Unidos donde el FBI cuenta con el COMPUTER CRIME UNIT, o en España la Guardia Civil cuenta con un departamento especializado en esta clase de infracciones. De otro lado también por parte de la Función Judicial falta la suficiente preparación por parte de Jueces y Magistrados en tratándose de estos temas, ya que en algunas ocasiones por no decirlo en la mayoría de los casos los llamados a impartir justicia se ven confundidos con la especial particularidad de estos delitos y los confunden con delitos tradicionales que por su estructura típica son incapaces de subsumir a estas nuevas conductas delictivas que tiene a la informática como su medio o fin.

Por tanto es esencial que se formen unidades Investigativas tanto policiales como del Ministerio Público especializadas en abordar cuestiones de la delincuencia informática trasnacional y también a nivel nacional. Estas

unidades pueden servir también de base tanto para una cooperación internacional formal o una cooperación informal basada en redes transnacionales de confianza entre los agentes de aplicación de la ley. Lo cual es posible aplicando la Ley de Comercio Electrónico Firmas Electrónicas y Mensajes de Datos.

La cooperación multilateral de los grupos especiales multinacionales pueden resultar ser particularmente útiles - y ya hay casos en que la cooperación internacional ha sido muy efectiva. De hecho, la cooperación puede engendrar emulación y éxitos adicionales.

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

Es por tanto como manifiesta **PHIL WILLIAMS** Profesor de Estudios de Seguridad Internacional, Universidad de Pittsbugh[1], Es necesario contar no solo con leyes e instrumentos eficaces y compatibles que permitan una cooperación idónea entre los estados para luchar contra la Delincuencia Informática, sino también con la infraestructura tanto técnica como con el recurso humano calificado para hacerle frente a este nuevo tipo de delitos transnacionales.

Es por estas razones que el Ministerio Público tiene la obligación Jurídica en cumplimiento de su mandato constitucional de poseer un cuerpo especializado para combatir esta clase de criminalidad a fin de precautelar los derechos de las víctimas y llevar a los responsables a juicio, terminando así con la cifra negra de esta clase de infracciones.

2.- Unidad de Delitos Informáticos del Ministerio Público

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 perentoria 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.

---

[1] **WILLIAMS PHIL,** Crimen Organizado y Cibernético, sinergias, tendencias y respuestas. Centro de Enseñanza en Seguridad de la Internet de la Universidad Carnegie Mellon. **http://www.pitt.edu/~rcss/toc.html**

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 del Ministerio Público 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.

De acuerdo a lo dispuesto por el Art. 3 de la Codificación de la Ley de Ministerio Público, éste se ejerce por el Ministro Fiscal General y los demás funcionarios necesarios para el cumplimiento de las finalidades establecidas en la Constitución Política de la República y de la Ley.

En el Reglamento para la aplicación de la Ley Orgánica del Ministerio Público se menciona en la Disposición General Segunda que "*Las Direcciones Generales, Departamentos y más Unidades Administrativas creadas con posterioridad a la vigencia de la ley orgánica que se reglamenta se regirán al Reglamento orgánico funcional del Ministerio Público Vigente, en el marco de los principios de autonomía e independencia reconocidos por la Constitución Política y la ley*".

En el Art. 1 de la Codificación del reglamento Orgánico Funcional del Ministerio Público se señala en concordancia con el Art. 3 de la Codificación de la Ley de Ministerio Público, que la máxima autoridad en el Ministerio Público es el MINISTRO FISCAL GENERAL, y es él quien en uso de sus facultades y de acuerdo a los criterios de descentralización, eficacia y eficiencia, puede crear los Departamentos y Unidades Administrativas que sean necesarias para el cumplimiento de las funciones y la misión del Ministerio Público.

En consecuencia, el Ministerio Público del Ecuador en uso de sus facultades legales y reglamentarias debe crear la **UNIDAD DE DELITOS INFORMÁTICOS DEL MINISTERIO PÚBLICO**, **UDIMP**.

2.1.- Misión

La unidad tiene como misión fundamental investigar, perseguir y prevenir todo lo relacionado con la llamada criminalidad informática en todos sus espectros y ámbitos y en especial:

- Amenazas, injurias, calumnias. Por correo electrónico, SMS, tablones de anuncios, foros, newsgroups, Web.
- Pornografía infantil. Protección al menor en el uso de las nuevas tecnologías.
- Fraudes en el uso de las comunicaciones: By Pass.
- 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.

2.2.- Objetivos Generales

1. Investigar y perseguir a nivel procesal y preprocesal 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. Desarrollar en los miembros de la Unidad 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[2].
3. Contribuir a la formación continua de los investigadores; la colaboración de las más importantes instituciones públicas y privadas; la participación activa en los foros internacionales de cooperación con los diferentes Ministerios Públicos y las unidades policiales especializadas, además de la colaboración con la ciudadanía.

[2] 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.

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

2.3.- Objetivos Específicos.

1. Recopilar los elementos de convicción necesarios (evidencia digital[3] y material) para iniciar los procesos penales correspondientes en contra de los responsables de la comisión de estas infracciones y posteriormente sustentar su acusación.
2. Brindar apoyo técnico especializado a las demás unidades del Ministerio Público en el campo de la informática forense.
3. Capacitar al personal técnico de la Unidad, acreditar a los Peritos Informáticos y formar en unión de la Policía Judicial a los investigadores especialistas en delitos informáticos.
4. Contar con un listado actualizado de los peritos informáticos a nivel nacional.
5. Crear en los diferentes distritos delegaciones de la Unidad de Delitos Informáticos, a fin de que se tenga un control nacional de esta clase de infracciones.
6. Impedir que los Ciberterroristas realicen cualquier tipo de extorsión a grupos financieros, esto a fin de recaudar fondos para financiar sus actividades ilícitas, con la finalidad de no ser victimas de delitos informáticos[4].
7. Mantener una base de datos de todas las investigaciones realizadas en la Unidad.

---

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

[4] Esto se hace haciendo pagos por protección, y así evitar ser atacadas informáticamente es decir inmunizarse contra posibles ataques o bien impedir la revelación datos personales nominativos de sus clientes a empresas competidoras.

2.4.- Conformación de la Unidad.

La Unidad de Delitos Informáticos del Ministerio Público, estará conformada por:

1. **COORDINACION 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[5]**:** Dr. Santiago Acurio Del Pino
FISCAL 1[6]**:** Dr. Borman Peñaherrera Manosalvas
FISCAL 2[7]**:** Dr. Marco Esquetini Proaño
SECRETARIO DE LA UNIDAD[8]**:** Sr. Gonzalo Núñez Velasco
AMANUENSE: Sr. Santiago Moreira
AMANUENSE: Sr. Xavier Torres
JEFE DE SECCION TÉCNICA FORENSE: Sr. Fabián Moreano[9].

2. **SECCIÓN DE INTELIGENCIA,** es la encargada de realizar recoger las informaciones, 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,** será la 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

---

[5] El Coordinador Nacional tendrá el Puesto de Jefe Departamental 3 de acuerdo al Distributivo de Personal del Ministerio Público.
[6] Actualmente se desempeña como Fiscal de delitos Financieros.
[7] Actualmente se desempeña como Fiscal de delitos contra la Vida
[8] Actualmente se desempeña como Secretario de la Unidad de Delitos contra la Vida en donde existen tres Secretarios.
[9] Para este puesto de la Sección Técnica y Forense tendrá el cargo de Ingeniero en Sistemas Distrital de acuerdo al distributivo de la Función Judicial. Bajo esta denominación el Sr. Moreano podrá seguir prestando sus servicios en el Departamento Informático del Distrito, a fin de optimizar el recurso humano capacitado

- **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 INFANTÍL:** 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 esta siendo difundido y transmitido a través de la Internet.

- **GRUPO 3: SEGURIDAD LOGICA Y TERRORISMO INFORMÁTICO (CIBERTERRORISMO[10]) :** 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.

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 auditoria 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:

[10] De acuerdo a **RAYMOND PÉREZ ORTA** podemos establecer que el Ciberterrorismo, es la forma de terrorismo que utiliza las tecnologías de información para intimidar, coercionar o para causar daños a grupos sociales con fines políticos-religiosos, para nosotros y siguiendo el concepto dado por 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 el envió de virus informáticos o instalando bongas lógicas, en definitiva provocando cualquier clase de daño informático que comprometa de forma grave a las instituciones de un estado a sus ciudadanos.

- **GRUPO DE APOYO TÉCNICO**
- **GRUPO DE ANALISIS 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[11], 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.

5. **SECCION 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, de igual forma se sugiere dentro de esta sección a Licenciado Fabián Páez con el cargo de Analista 4 de acuerdo al Distributivo de personal del Ministerio Público.

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 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

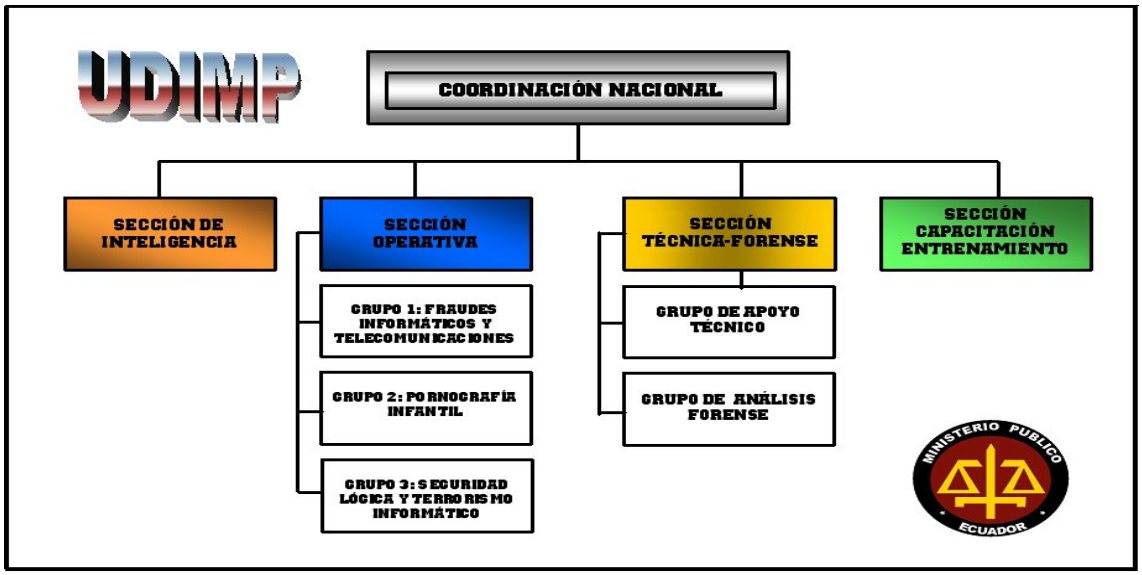
[11] **INFORMÁTICA FORENSE**, que es parte de la criminalística, es la ciencia que se ocupa de la utilización de los métodos científicos aplicables a la investigación de los delitos, en este caso en particular a los Informáticos donde se utiliza el análisis forense de las evidencias digitales, en fin toda información o datos que se guardan en una computadora o sistema informático. En conclusión diremos que Informática Forense es "*la ciencia Criminalísitica que se encarga de la preservación, identificación, extracción, documentación y interpretación de la evidencia digital*"**.**

de formar una red de Equipos de Respuesta de Incidentes ERI[12], los cuales formaran parte de la Unidad De Delitos Informáticos del Ministerio Público UDIMP. Los Incidentes de seguridad, son como cualquier evento no programado (anomalía) son 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.

2.5.- Coordinación Internacional

A fin de lograr un enlace expedito con los diferentes organizamos internacionales y multilaterales de cooperación en el tema de la Ciberdelincuencia, es necesario contar con los servicios de la Unidad de Asuntos Internacionales del Ministerio Público, para lo cual se sugiere como Jefe de dicha Unidad al Dr. Diego Bolaños[13], quien en combinación con el Coordinador Nacional de la UDIMP y el Señor Ministro Fiscal General trazarán las políticas de cooperación internacional en materia de delitos informáticos.

2.6.- Organigrama.



[12] *Un ERI,* o *equipo de respuesta a incidentes*, que no es más que una organización o grupo responsable de recibir, revisar y responder frente a notificaciones o descubrimientos de incidentes de seguridad. Un ERI puede ser tanto un equipo formalmente constituido, donde sus miembros responden a incidentes como su principal función de trabajo o un equipo *ad-hoc* que, en cambio, se reúne para tratar incidentes de seguridad en curso o inminentes.

[13] El Jefe de la Unidad de Asuntos Internacionales tendrá el Puesto de Jefe Departamental 3 de acuerdo al Distributivo de Personal del Ministerio Público

2.7.- Perspectiva del Proyecto

RECURSO HUMANO: El recurso humano que formará parte de la Unidad debe ser el mejor posible, tanto del Ministerio Público como de la Policía Judicial, deberá tener amplios conocimientos técnicos en el campo de la informática y afines, así como también conocimientos de Derecho, sobre todo en derecho penal informático, y procesal penal. Dicho personal debe estar en constante aprendizaje y entrenamiento dado que la tecnología informática y las modalidades comisivas de esta clase de infracciones cambian con el tiempo.

El Perito Informático según la opinión del Profesor Jeimy Cano[14] requiere la formación de un perito informático integral que siendo especialista en temas de Tecnologías de información, también debe ser formado en las disciplinas jurídicas, criminalísticas y forenses. En este sentido, el perfil que debe mostrar el perito informático es el de un profesional híbrido que no le es indiferente su área de formación profesional y las ciencias jurídicas.

Con esto en mente se podría sugerir un conjunto de asignaturas y temas (básicos) que no pueden perderse de vista al formar un perito informático general, el cual debe tener por lo menos una formación en:

1. **ÁREA DE TECNOLOGÍAS DE INFORMACIÓN Y ELECTRÓNICA:**

- Lenguajes de programación
- Teoría de sistemas operacionales y sistemas de archivo
- Protocolos e infraestructuras de comunicación
- Fundamentos de circuiros eléctricos y electrónicos
- Arquitectura de Computadores

2. **FUNDAMENTO DE BASES DE DATOS ÁREA DE SEGURIDAD DE LA FORMACIÓN:**

- Principios de Seguridad de la Información
- Políticas estándares y procedimientos en Seguridad de la Información
- Análisis de vulnerabilidades de seguridad informática
- Análisis y administración de riesgos informáticos
- Recuperación y continuidad de negocio
- Clasificación de la información
- Técnicas de Hacking y vulneración de sistemas de información
- Mecanismos y tecnologías de seguridad informática

[14] **CANO JEIMY,** Inseguridad Informática: Un concepto dual de la Seguridad Informática. Universidad UNIANDES 1994.

- Concientización en seguridad informática

3. ÁREA JURÍDICA:

- Teoría General del Derecho
- Formación básica en delito informático
- Formación básica en protección de datos y derechos de autor
- Formación básica en convergencia tecnológica
- Formación básica en evidencias digital y pruebas electrónicas
- Análisis comparado de legislaciones e iniciativas internacionales

4. ÁREA DE CRIMINALÍSTICA Y CIENCIAS FORENSES:

- Fundamentos de conductas criminales
- Perfiles psicológicos y técnicos
- Procedimientos de análisis y valoración de pruebas
- Cadena de custodia y control de evidencias
- Fundamentos de Derecho Penal y Procesal
- Ética y responsabilidades del Perito
- Metodologías de análisis de datos y presentación de informes

5. ÁREA DE INFORMÁTICA FORENSE:

- Esterilización de medios de almacenamiento magnético y óptico
- Selección y entrenamiento en software de recuperación y análisis de datos
- Análisis de registros de auditoria y control
- Correlación y análisis de evidencias digitales
- Procedimientos de control y aseguramiento de evidencias digitales
- Verificación y validación de procedimientos aplicados en la pericia forense.

Establecer un programa que cubra las áreas propuestas en esta sección exige un esfuerzo interdisciplinario y voluntad política tanto del Ministerio Público, del Estado Ecuatoriano y de los Organismos Internacionales y de la industria para iniciar la formación de un profesional que eleve los niveles de confiabilidad y formalidad exigidos para que la justicia en un entorno digital ofrezca las garantías requeridas en los procesos donde la evidencia digital es la protagonista.

Dentro del campo de investigación forense es necesario dejar en claro los roles y la participación de ciertas personas dentro de una escena del crimen de carácter informático o digital, estas personas son:

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.
3. **INVESTIGADORES DE DELITOS INFORMÁTICOS**, 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.

RECURSO TÉCNICOS: Los recursos técnicos necesarios para la implementación del proyecto serán procurados a través de los organismos internacionales dedicados a la investigación, sanción y prevención de esta clase de infracciones, como por ejemplo: Computer Crime Unid del FBI, Unidad Nacional de Crimen de Alta Tecnología (NHTCU) del Reino Unido, la Brigada de Investigación Tecnológica de la Guardia Civil Española, Unidad de Delitos Cibernéticos de México, la Organización de Estados Americanos OEA y la Organización de las Naciones Unidas.

De igual forma se puede pedir apoyo a empresas nacionales, en especial a la asociación de Bancos Privados, la Corporación Ecuatoriana para el Comercio Electrónico CORPECE, la Superintendencia de Bancos entre otros.

RECURSOS LOGÍSTICOS: Los recursos logísticos podrán ser brindados tanto por el Ministerio Público como por la Policía Nacional, de igual forma estos pueden ser procurados ante organismos Internacionales a base de cooperación o a través del apoyo de las empresas nacionales.

RECURSOS ECONOMICOS Y FINANCIAMIENTO: El Recurso Económico y el financiamiento de la Unidad provendrán del presupuesto del Ministerio Público, y la Policía Judicial. Igualmente se contará con el apoyo económico de organizaciones Internacionales y nacionales.

3.- Glosario de Términos

- **ACTIVO PATRIMONIAL:** Conjunto de bienes y derechos que integran el haber de una persona física o jurídica.
- **BASE DE DATOS:** Conjunto completo de ficheros informáticos que reúnen informaciones generales o temáticas, que generalmente están a disposición de numerosos usuarios.
- **BROWSER (BUSCADOR):** El software para buscar y conseguir información de la red WWW. Los más comúnmente usados son Microsoft Explorer, Firefox y Opera.
- **COOKIE**: Es un archivo o datos dejados en su computadora por un servidor u otro sistema al que se hayan conectado. Se suelen usar para que el servidor registre información sobre aquellas pantallas que usted ha visto y de la información personalizada que usted haya mandado. Muchos usuarios consideran esto como una invasión de privacidad, ya que casi ningún sistema dice lo que esta haciendo. Hay una variedad de "anti-cookie" software que automáticamente borra esa información entre visitas a su sitio.
- **DIALUP (MARCAR)**: El método de conectarse con Internet vía la línea de teléfono normal mediante un modem, en vez de mediante una LAN (Red Local) o de una línea de teléfono alquilada permanentemente. Esta es la manera mas común de conectarse a Internet desde casa si no ha hecho ningún arreglo con su compagina de teléfono o con un ISP. Para conexiones alternativas consulte con su ISP primero.
- **DIGITAL SIGNATURE (FIRMA DIGITAL)**: El equivalente digital de una firma autentica escrita a mano. Es un dato añadido a un fichero electrónico, diciendo que el dueño de esa firma escribió o autorizo el Archivo.
- **DOCUMENTO ELECTRÓNICO:** Es la representación en forma electrónica de hechos jurídicamente relevantes susceptibles de ser presentados en una forma humanamente comprensible[15].
- **DOMAIN NAME (NOMBRE DE DOMINIO)**: Un nombre de dominio es su propiedad en el mundo cibernético. Esta propiedad, tal y como su homologo tangible, tiene valor dependiendo de su dirección y de su contenido. Usted puede cobrar a sus invitados o darles un tour gratis, o llevar un negocio paralelo como parte de la propiedad. Igual que una dirección de la 5 Avenida que es limitada y también más valorada que la inmensa mayoría de las demás direcciones, el valor de su dominio puede variar de unos cuantos dólares por ejemplo, algunos están en el millón de dólares. No le podemos decir que muebles, obras de arte, o negocio paralelo

[15] Definición dada por EDIFORUM.(Foro de Intercambio Electrónico de Datos)

debe tener en su propiedad en el mundo cibernético, pero su dirección es bien segura que realzara el valor de su contenido, o igual lo eliminara si ese nombre no atrae clientes. Técnicamente, es un concepto creado para identificar y localizar computadoras en Internet. Los nombres de dominio son un sistema de direcciones de Internet fácil de recordar, que pueden ser traducidos por el Sistema de Nombres de Dominio a las direcciones numéricas usadas en la red. Un nombre de dominio es jerárquico y usualmente acarrea información sobre el tipo de entidad que usa ese nombre de dominio. Un nombre de dominio es simplemente una etiqueta que representa un dominio, que a su vez es un subgrupo del total del espacio de nombres del dominio. Nombres de dominio en el mismo nivel jerárquico tienen que ser únicos: solo puede haber un .com al nivel más alto de la jerarquía, y solo un DomainMart.com en el siguiente nivel.

- **FTP O FILE TRANSFER PROTOCOL (PROTOCOLO DE TRANSFERENCIA DE FICHERO)** Un estándar de Internet para transferir ficheros entre ordenadores. La mayoría de las transferencias FTP requieren que usted se meta en el sistema proveyendo la información mediante un nombre autorizado de uso y una contraseña. Sin embargo, una variación conocida como "FTP anónimo" le permite meterse como anónimo: no necesita contraseña o nombre.
- **HTML (HYPER TEXT MARKUP LANGUAGE)**: El lenguaje de computador usado para crear paginas de red para Internet. Aunque estándares "oficiales" de Internet existen, en la práctica son extensiones del lenguaje que compañías como Netscape o Microsoft usan en sus buscadores (browsers).
- **HTTP (HYPER TEXT TRANSPORT PROTOCOL)**: El conjunto de reglas que se usa en Internet para pedir y ofrecer paginas de la red y demás información. Es lo que pone al comienzo de una dirección, tal como "http:/," para indicarle al buscador que use ese protocolo para buscar información en la pagina.
- **INTERNET PROTOCOL (IP) NUMBERS O IP ADRESSES (PROTOCOLO DE INTERNET, NÚMEROS)**: Un identificador numérico único usado para especificar anfitriones y redes. Los números IP son parte de un plan global y estandarizado para identificar computadores que estén conectados a Internet. Se expresa como cuatro números del 0 al 255, separado por puntos: 188.41.20.11. La asignación de estos números en el Caribe, las Américas, y África la hace la American Registry for Internet Numbers.
- **INTERNET SERVICE PROVIDER (ISP) (PROVEEDOR DE SERVICIO DE INTERNET)** Una persona, organización o compagina que provee acceso a Internet. Además del acceso a Internet, muchos ISP proveen otros servicios tales como anfitrión de Red, servicio de nombre, y otros servicios informáticos.

- **MENSAJE DE DATOS:** Es toda aquella información visualizada, generada enviada, recibida, almacenada o comunicada por medios informáticos, electrónicos, ópticos, digitales o similares.
- **MODEM**: Un aparato que cambia datos del computador a formatos que se puedan transmitir mas fácilmente por línea telefónica o por otro tipo de medio.
- **SISTEMA TELEMÁTICO.** Conjunto organizado de redes de telecomunicaciones que sirven para trasmitir, enviar, y recibir información tratada de forma automatizada.
- **SISTEMA DE INFORMACIÓN:** Se entenderá como sistema de información, a todo sistema utilizado para generar, enviar, recibir, procesar o archivar de cualquier forma de mensajes de datos[16].
- **SISTEMA INFORMÁTICO:** Conjunto organizado de programas y bases de datos que se utilizan para, generar, almacenar, tratar de forma automatizada datos o información cualquiera que esta sea.
- **SOPORTE LÓGICO:** Cualquiera de los elementos (tarjetas perforadas, cintas o discos magnéticos, discos ópticos) que pueden ser empleados para registrar información en un sistema informático.
- **SOPORTE MATERIAL:** Es cualquier elemento corporal que se utilice para registrar toda clase de información.
- **TCP/IP: TRANSMISIÓN CONTROL PROTOCOL/INTERNET PROTOCOL:** Conjunto de protocolos que hacen posible la interconexión y tráfico de la Red Internet

[16] Definición entregada por La Ley Modelo de Comercio Electrónico de la UNCITRAL