FISCALIA GENERAL DEL ESTADO

Informática Forense en el Ecuador

Una mirada introductoria

Dr. Santiago Acurio Del Pino

08/12/2009

La finalidad del presente documento es brindar una mirada introductoria a la informática forense a fin de sentar las bases de la investigación científica en esta materia, dándole pautas a los futuros investigadores de cómo manejar una escena del delito en donde se vean involucrados sistemas de información o redes y las posterior recuperación de la llamada evidencia digital

Introducción a la Informática Forense

Dr. Santiago Acurio Del Pino[1]

1.- Introducción

Increíblemente los delincuentes hoy están utilizando la tecnología para facilitar el cometimiento de infracciones y eludir a las autoridades. Este hecho ha creado la necesidad de que tanto la Policía Judicial, la Fiscalía y la Función Judicial deba especializarse y capacitarse en estas nuevas áreas en donde las TICs[2] se convierten en herramientas necesarias en auxilio de la Justicia y la persecución de delito y el delincuente.

Los hábitos de las personas han cambiado con el uso de las TICs, también las formas en que los delincuentes actúan y comenten sus actos reprochables, es así que el acceso universal a las tecnologías de la información y la comunicación brinda nuevas oportunidades para que gente inescrupulosa, delincuentes, pornógrafos infantiles, artistas del

[1] Director Nacional de Tecnología de la Información de la Fiscalía General del Estado, Profesor de la Universidad Católica del Ecuador. sacurio@hotmail.com
[2] Tecnologías de la Información y la Comunicación

engaño, quienes realizan toda clase de ataques contra la intimidad, fraudes informáticos, contra el tráfico jurídico probatorio, que atacan a la integridad de los sistemas computacionales y de red a nivel mundial, actúen de forma desmedida sin que los operadores de justicia puedan hacer algo, ya que estos han quedado relegados en sus actuaciones por la falta de recursos tecnológicos y capacitación a fin de lidiar con la evidencia digital presente en toda clase de infracciones y especialmente en los llamados Delitos Informáticos.

La comisión de infracciones informáticas es una de las causas de preocupación de los elementos de seguridad de muchos países en este momento dado que las mismas han causado ingentes pérdidas económicas especialmente en el sector comercial y bancario donde por ejemplo las manipulaciones informáticas fraudulentas ganan más terreno cada vez más, se estima que la pérdida ocasionada por este tipo de conductas delincuenciales supera fácilmente los doscientos millones de dólares, a lo que se suma la pérdida de credibilidad y debilitamiento institucional que sufren las entidades afectadas. Es por eso que en países como Estados Unidos, Alemania o Inglaterra se han creado y desarrollado técnicas y herramientas informáticas a fin de lograr tanto el descubrimiento de los autores de dichas infracciones así como aseguran la prueba de estas.

Una de estas herramientas es la informática Forense, ciencia criminalística que sumada al impulso y utilización masiva de las Tecnologías de la Información y de la Comunicación en todos los ámbitos del quehacer del hombre, está adquiriendo una gran importancia, debido a la globalización de la Sociedad de la Información[3]. Pero a pesar de esto esta ciencia no tiene un método estandarizado, razón por la cual su admisibilidad dentro de un proceso judicial podría ser cuestionada, pero esto no debe ser un obstáculo para dejar de lado esta importante clase de herramienta, la cual debe ser manejada en base a rígidos principios científicos, normas legales y de procedimiento.

Es necesario mencionar que son los operadores de justicia tanto como los profesionales de la informática, los llamados a combatir los delitos tecnológicos, ya que los primeros saben cómo piensa el delincuente y su *modus operandi*, mientras los otros conocen el funcionamiento de los equipos y las redes informáticas. Unidos los dos conforman la llave para combatir efectivamente esta clase de infracciones.

[3] Es una sociedad en la que la creación, distribución y manipulación de la información forman parte importante de las actividades culturales y económicas, es decir es un estadio del desarrollo social caracterizado por la capacidad de los ciudadanos, el sector público y el empresarial para compartir, generar, adquirir y procesar cualquier clase de información por medio de las tecnologías de la información y la comunicación, a fin de incrementar la productividad y competitividad de sus miembros, y así reducir las diferencias sociales existentes contribuyendo a un mayor bienestar colectivo e individual.

De lo expuesto se colige que es necesario contar dentro de los operadores de justicia con el personal capacitado en estas áreas para lidiar con esta clase de problemas surgidos de la mal utilización de la las Tecnologías de la Comunicación y la Información.

La finalidad del presente documento es brindar una mirada introductoria a la informática forense a fin de sentar las bases de la investigación científica en esta materia, dándole pautas a los futuros investigadores de cómo manejar una escena del delito en donde se vean involucrados sistemas de información o redes y las posterior recuperación de la llamada evidencia digital.

2.- La Investigación y la Prueba de los Delitos Informáticos

La prueba dentro del proceso penal es de especial importancia, ya que desde ella se confirma o desvirtúa una hipótesis o afirmación precedente, se llega a la posesión de la verdad material. De esta manera se confirmará la existencia de la infracción y la responsabilidad de quienes aparecen en un inicio como presuntos responsables, todo esto servirá para que el Tribunal de Justicia alcance el conocimiento necesario y resuelva el asunto sometido a su conocimiento.

Por ejemplo en delitos como el fraude informático o la falsificación electrónica, los medios de prueba[4] generalmente son de carácter material o documental, esto en razón de que esta clase de infracciones son del tipo ocupacional, (característica común en la mayoría de estas transgresiones). Esto significa que la persona o personas que cometen esta variedad de actos disvaliosos en un noventa por ciento (90%) trabajan dentro de las instituciones afectadas; en consecuencia la prueba de estos delitos se encuentra generalmente en los equipos y programas informáticos, en los documentos electrónicos, y en los demás mensajes de datos que utilizan e intercambian estas personas en su red de trabajo. Situación la cual hace indispensable que el investigador, cuente con el conocimiento suficiente acerca del funcionamiento de toda clase de sistemas informáticos, así como una sólida formación en cómputo forense y la capacidad para la administrar las evidencias e indicios de convicción aptos para lograr una condena en esta clase de infracciones.

Adicionalmente, estas conductas delictivas, eventos lesivos al orden jurídico, si bien pueden ser solucionados en parte a través de la normativa vigente en el Ecuador como la Ley de Comercio Electrónico y Mensajes de Datos y el Código de Procedimiento Penal, la particular naturaleza de los medios empleados para su comisión y

[4] Procedimiento que establece la Ley para ingresar un elemento de prueba en un proceso, por ejemplo las formalidades para brindar testimonio, o el contenido de un acta de reconocimiento.

fundamentalmente la falta de medios probatorios apropiados (Guía de Buenas prácticas en el manejo de evidencia digital, software y hardware especializado, personal capacitado), dificulta que se arribe a sentencias condenatorias[5].

Es necesario partir del principio de que la información constituye un valor económico con relevancia jurídico-penal, por ser posible objeto de conductas delictivas (acceso no autorizado, sabotaje o daño informático, espionaje informático, etc.) y por ser instrumento de comisión, facilitación, aseguramiento y calificación de los ilícitos tradicionales, llegando a ser un bien jurídico protegido, susceptible de protección legal propia y específica del ordenamiento jurídico imperante. Desde esa concepción, se han de identificar, reconocer y legalizar los procedimientos y herramientas técnicas especializadas en este tipo de infracciones para asegurar la prueba, otorgarle validez plena y constituirla en el fundamento para la valoración y decisión judicial, situación que como ya se señalo en líneas precedentes está relativamente regulado por la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y el propio Código de Procedimiento Penal vigente en nuestro país.

De lo expuesto es importante clarificar los conceptos y describir la terminología adecuada que nos señale el rol que tiene un sistema informático dentro del *iter criminis* o camino del delito. Esto a fin de encaminar correctamente el tipo de investigación, la obtención de indicios y posteriormente los elementos probatorios necesarios para sostener nuestro caso. Es así que por ejemplo, el procedimiento de una investigación por homicidio que tenga relación con evidencia digital será totalmente distinto al que, se utilice en un fraude informático, por tanto el rol que cumpla el sistema informático determinara donde debe ser ubicada y como debe ser usada la evidencia.

Ahora bien para este propósito se han creado categorías a fin de hacer una necesaria distinción entre el elemento material de un sistema informático o hardware (*evidencia electrónica*) y la información contenida en este (*evidencia digital*). Esta distinción es útil al momento de diseñar los procedimientos adecuados para tratar cada tipo de

[5] Este hecho se evidencio dentro de la Audiencia de Juzgamiento que por el delito de Falsificación Informática se siguió en el Cuarto Tribunal Penal de Pichincha en donde y luego de analizar la teoría del caso con todos los participantes del proceso se logro pulir una estrategia eficaz para dicha Audiencia, tomando en cuenta que la carga de la prueba recae completamente en la Fiscalía, dicho lo cual se monto un escenario de análisis donde se examinaron los indicios de convicción con los cuales se sustento la acusación fiscal al igual que el grado de participación y la responsabilidad de cada uno los acusados en este Juicio. La audiencia se realizo sin muchas complicaciones pero se improviso mucho, no se aplico de forma rigurosa los principios de la Informática Forense en relación a la evidencia digital encontrada, pero a pesar de esto al final se demostró la existencia de la infracción y la responsabilidad de los encausados logrando una sentencia condenatoria.

evidencia y crear un paralelo entre una escena física del crimen y una digital. En este contexto el hardware se refiere a todos los componentes físicos de un sistema informático, mientras que la información, se refiere a todos los datos, mensajes de datos y programas almacenados y trasmitidos usando el sistema informático.

2.1.- Hardware o Elementos Físicos

SISTEMA INFORMÁTICO	
HARDWARE (Elementos Físicos)	**Evidencia Electrónica**
• El hardware es mercancía ilegal o fruto del delito.	• El hardware es una mercancía ilegal cuando su posesión no está autorizada por la ley. Ejemplo: en el caso de los decodificadores de la señal de televisión por cable, su posesión es una violación a los derechos de propiedad intelectual y también un delito. • El hardware es fruto del delito cuando este es obtenido mediante robo, hurto, fraude u otra clase de infracción.
• El hardware es un instrumento	• Es un instrumento cuando el hardware cumple un papel importante en el cometimiento del delito, podemos decir que es usada como un arma o herramienta, tal como una pistola o un cuchillo. Un ejemplo serían los snifers y otros aparatos especialmente diseñados para capturar el tráfico en la red o interceptar comunicaciones.
• El hardware es evidencia	• En este caso el hardware no debe ni ser una mercancía ilegal, fruto del delito o un instrumento. Es un elemento físico que se constituye como prueba de la comisión de un delito. Por ejemplo el scanner que se uso para digitalizar una imagen de pornografía infantil, cuyas características únicas son usadas como elementos de convicción

2.2.- Información

SISTEMA INFORMÁTICO	
INFORMACIÓN	**Evidencia Digital**
• La información es mercancía ilegal o el fruto del delito.	La información es considerada como mercancía ilegal cuando su posesión no está permitida por la ley, por ejemplo en el caso de la pornografía infantil. De otro lado será fruto del delito cuando sea el resultado de la comisión de una infracción, como por ejemplo las copias pirateadas de programas de ordenador, secretos industriales robados.
• La información es un instrumento	La información es un instrumento o herramienta cuando es usada como medio para cometer una infracción penal. Son por ejemplo los programas de ordenador que se utilizan para romper las seguridades de un sistema informático, sirven para romper contraseñas o para brindar acceso no autorizado. En definitiva juegan un importante papel en el cometimiento del delito.
• La información es evidencia	Esta es la categoría más grande y nutrida de las anteriores, muchas de nuestras acciones diarias dejan un rastro digital. Uno puede conseguir mucha información como evidencia, por ejemplo la información de los ISP's, de los bancos, y de las proveedoras de servicios las cuales pueden revelar actividades particulares de los sospechosos

En resumen el propósito fundamental de las categorías antes mencionadas es el de enfatizar el papel que juegan los sistemas informáticos en la comisión de delitos, a fin de que el investigador criminal tenga un derrotero claro y preciso al buscar los elementos convicción que aseguren el éxito dentro de un proceso penal. En estas condiciones para efectos probatorios son objeto de examen, tanto el hardware como la información contenida en este, para lo cual es necesario contar con el auxilio y el conocimiento que nos brinda la ciencia informática, y en particular de la Ciencia Forense Informática.

3.- Las Ciencias Forenses

Las Ciencias Forenses son la utilización de procedimientos y conocimientos científicos para encontrar, adquirir, preservar y analizar las evidencias de un delito y presentarlas apropiadamente a una Corte de Justicia. Las ciencias forenses tienen que ver principalmente con la recuperación y análisis de la llamada evidencia latente, como por ejemplo las huellas digitales, la comparación de muestras de ADN, etc. Las ciencias forenses combinan el conocimiento científico y las diferentes técnicas que este proporciona con los presupuestos legales a fin de demostrar con la evidencia recuperada la existencia de la comisión de un acto considerado como delictivo y sus posibles responsables ante un Tribunal de Justicia.

Las ciencias forenses han sido desarrolladas desde hace mucho tiempo atrás. Uno de los primeros textos y estudios en este campo los podemos ubicar en el año de 1248 DC, cuando el médico chino HI DUAN YU, escribió el libro "**COMO CORREGIR LOS ERRORES**", en el cual se explicaban las diferencias entre una muerte por ahogamiento y otra por una herida de cuchillo al igual que la muerte por causas naturales.

Posteriormente con el avance de la ciencia y la tecnología, las ciencias forenses han alcanzado un desarrollo inconmensurable, pero ese desarrollo a veces no ha ido de la mano del avance de la legislación penal. Esto en razón del retrazo en la incorporación de nuevos elementos de prueba y medios probatorios y sobre todo en la demora de la admisibilidad de nuevas evidencias o pruebas. Este es el caso por ejemplo de la prueba de ADN que fue admitida en un juicio recién en el año de 1996, pero su desarrollo y comprensión se logró desde la década de los ochentas.

Las ciencias forenses siempre están en constante cambio, siempre buscando nuevos métodos y procesos para encontrar y fijar las evidencias de cualquier tipo. Creando nuevos estándares y políticas. Son ochocientos años de experiencia como disciplina científica.

4.- La Informática Forense

Es una ciencia forense que se ocupa de la utilización de los métodos científicos aplicables a la investigación de los delitos, no solo Informáticos y 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[6]. En conclusión diremos que Informática Forense es "*la ciencia forense que se encarga de la preservación, identificación, extracción, documentación y interpretación de la evidencia digital, para luego ésta ser presentada en una Corte de Justicia*".

[6] **Sistema Informático**: Es todo dispositivo físico o lógico utilizado para crear, generar, enviar, recibir, procesar, comunicar o almacenar, de cualquier forma, mensajes de datos.

La informática forense es el vehiculo idóneo para localizar y presentar de forma adecuada los hechos jurídicos informáticos relevantes dentro de una investigación, ya sea de carácter civil o penal.

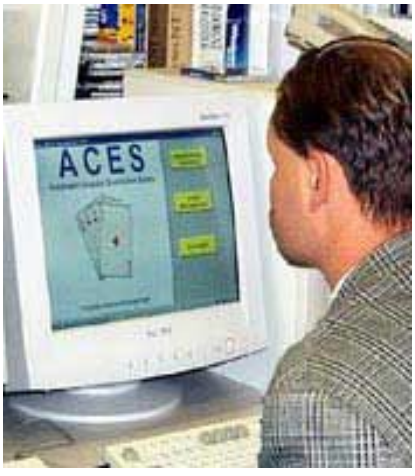
La ciencia forense es sistemática y se basa en hechos premeditados para recabar pruebas para luego analizarlas. La tecnología, en caso de la identificación, recolección y análisis forense en sistemas informáticos, son aplicaciones que hacen un papel de suma importancia en recaudar la información y los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

Históricamente la ciencia forense siempre ha basado su experiencia y su accionar en estándares de práctica y entrenamiento, a fin de que las personas que participan o trabajan en este campo científico tengan la suficiente probidad profesional y solvencia de conocimientos para realizar un buen trabajo en su área de experiencia. Esta situación debe ser igual en le campo de la Informática forense, es por tanto necesario que las personas encargadas de este aspecto de la ciencia forense tenga parámetros básicos de actuación, no solo en la incautación y recolección de evidencias digitales, sino también en su procesamiento, cumpliendo siempre con los principios del básicos del debido proceso.

El objetivo de la Informática forense es el de recobrar los registros y mensajes de datos existentes dentro de un equipo informático, de tal manera que toda esa información digital, pueda ser usada como prueba ante un tribunal.

De otro lado, esta ciencia forense necesita de una estandarización de procedimientos y de acciones a tomar, esto en razón de las características específicas que las infracciones informáticas presentan. Son entonces estas propiedades que contribuyen a la existencia de una confusión terminológica y conceptual presente en todos los campos de la informática, especialmente en lo que dice relación con sus aspectos criminales.

5.- Evidencia Digital



En derecho procesal la evidencia es la certeza clara, manifiesta y tan perceptible que nadie puede dudar de ella. De otro lado la evidencia digital es cualquier mensaje de datos almacenado y trasmitido por medio de un Sistema de Información que tenga relación con el cometimiento de un acto que comprometa gravemente dicho sistema y que posteriormente guié a los investigadores al descubrimiento de los posibles infractores. En definitiva son campos magnéticos y

pulsos electrónicos que pueden ser recogidos y analizados usando técnicas y herramientas especiales[7], no es otra forma de EVIDENCIA LATENTE, necesita para su recolección y preservación principios científicos y un marco legal apropiado.

Para Miguel López Delgado la evidencia digital es el conjunto de datos en formato binario, esto es comprende los archivos, su contenido o referencias a éstos (metadatos[8]) que se encuentren en los soportes físicos o lógicos de un sistema comprometido por un incidente informático[9].

Otros autores como Anthony Reyes[10] se refieren a la evidencia digital como "**OBJETOS DE DATOS**" en relación a la información que es encontrada en los dispositivos de almacenamiento o en las piezas de almacenamiento multimedia, que no son más que cadenas de unos y ceros es decir de información binaria o digital grabada en un dispositivo magnético (como discos duros o los disquetes), en uno de estado sólido[11] o memoria solida (como las memorias flash y dispositivos USB) y los dispositivos ópticos (como los discos compactos y DVD).

Estos objetos de datos podemos encontrarlos en una gran cantidad de dispositivos tales como computadores personales, en IPODS, teléfonos celulares, los cuales tienen sistemas operativos y programas que combinan en un particular orden esas cadenas de unos y ceros para crear imágenes, documentos, música y muchas cosas más en formato digital. Pero también existen otros objetos de datos que no están organizados como archivos, son informaciones que están vinculadas a archivos como los metadatos antes mencionados, otros son fragmentos de archivos que quedan después de que se sobrescribe la información a causa del borrado de los archivos viejos y la creación de los archivos nuevos esto se llama SLACK SPACE, o espacio inactivo. También pueden quedarse almacenados temporalmente en los archivos de intercambio (SWAP FILE) o en la misma memoria RAM.

---

[7] **CASEY** Eoghan, Handook of Computer Investigation, Elsevier Academia Press, 2005

[8] El término meta proviene del griego y significa *junto a, después, siguiente*. Los metadatos pueden ser definidos como datos sobre los datos. Son como las etiquetas de un producto, nos brinda información relativa a este como, el peso fecha de caducidad, etc. **Tecnologías de la Información a la comunicación** ALONSO, Juan A. y otros, Editorial ALFAOMEGA y RA-MA, 2005

[9] **LOPEZ DELGADO,** Miguel, Análisis Forense Digital, Junio del 2007, CRIPORED.

[10] **REYES,** Anthony, Investigación del Cibercrimen, Syngress 2007.

[11] Más conocidos como SSD (Solid-State Drive) son dispositivos de almacenamientos de datos que usan una memoria solida para almacenar la información de forma constante de forma similar que un disco duro usando lo que se conoce como SRAM (Memoria de Acceso Randómico Estático) o DRAM (Memoria de Acceso Randómico Dinámico). Estas memorias simulan la interfaz de un disco magnético convirtiéndose en dispositivos de almacenamiento masivo.

5.1.- Fuentes de la Evidencia Digital

Algunas personas tienden a confundir los términos evidencia digital y evidencia electrónica, dichos términos pueden ser usados indistintamente como sinónimos, sin embargo es necesario distinguir entre aparatos electrónicos como los celulares y PDAs y la información digital que estos contengan. Esto es indispensable ya que el foco de nuestra investigación siempre será la evidencia digital aunque en algunos casos también serán los aparatos electrónicos.

A fin de que los investigadores forenses tengan una idea de donde buscar evidencia digital, éstos deben identificar las fuentes más comunes de evidencia. Situación que brindará al investigador el método más adecuando para su posterior recolección y preservación.

Las fuentes de evidencia digital pueden ser clasificadas en tres grande grupos:

1. **SISTEMAS DE COMPUTACIÓN ABIERTOS**, son aquellos que están compuestos de las llamadas computadores personales y todos sus periféricos como teclados, ratones y monitores, las computadoras portátiles, y los servidores. Actualmente estos computadores tiene la capacidad de guardar gran cantidad de información dentro de sus discos duros, lo que los convierte en una gran fuente de evidencia digital.
2. **SISTEMAS DE COMUNICACIÓN,** estos están compuestos por las redes de telecomunicaciones, la comunicación inalámbrica y el Internet. Son también una gran fuente de información y de evidencia digital.
3. **SISTEMAS CONVERGENTES DE COMPUTACIÓN,** son los que están formados por los teléfonos celulares llamados inteligentes o SMARTPHONES, los asistentes personales digitales PDAs, las tarjetas inteligentes y cualquier otro aparato electrónico que posea convergencia digital y que puede contener evidencia digital[12].

Dada la ubicuidad de la evidencia digital es raro el delito que no esté asociado a un mensaje de datos guardado y trasmitido por medios

[12] Se trata de una característica que presenta el actual desarrollo de las infraestructuras de red y de los dispositivos terminales, que les permite, pese a su naturaleza diversa, transmitir y recibir, en esencia, la misma información, todo ello girando en torno a la digitalización de los contenidos que se transmiten y conduciendo ineludiblemente a una transformación de la actividad económica que desarrollaban en forma separada las empresas de telecomunicaciones, de informática y de contenidos audiovisuales. **Ciberespacio, Sociedad y Derecho**, HERRERA BRAVO Rodolfo, en el Libro Derecho a las Nuevas Tecnologías, Editorial La Rocca, 2007.

informáticos. Un investigador entrenado puede usar el contenido de ese mensaje de datos para descubrir la conducta de un infractor, puede también hacer un perfil de su actuación, de sus actividades individuales y relacionarlas con sus víctimas.

5.3.- Evidencia Digital Constante y Volátil

En un principio el tipo de evidencia digital que se buscaba en los equipos informáticos era del tipo CONSTANTE o PERSISTENTE es decir la que se encontraba almacenada en un disco duro o en otro medio informático y que se mantenía preservada después de que la computadora era apagada. Posteriormente y gracias a las redes de interconexión, el investigador forense se ve obligado a buscar también evidencia del tipo VOLÁTIL, es decir evidencia que se encuentra alojada temporalmente en la memoria RAM, o en el CACHE, son evidencias que por su naturaleza inestable se pierden cuando el computador es apagado. Este tipo de evidencias deben ser recuperadas casi de inmediato.

De lo dicho se desprende que cuando se comete un delito cualquiera, muchas veces la información que directa o indirectamente se relaciona con esta conducta criminal queda almacenada en forma digital dentro de un Sistema Informático. Este conjunto de datos ordenados sistemáticamente y convertidos en información se convierte en evidencia digital. He aquí entonces que encontramos la primera dificultad en lo que se refiere a la obtención de esta clase de evidencia como prueba de la infracción cometida, esto debido a que los Sistemas Informáticos en donde se almacena la misma presentan características técnicas propias, en tal razón la información ahí almacenada no puede ser recuperada, recolectada, preservada, procesada y posteriormente presentada como indicio de convicción utilizando los medios crimínalisticos comunes, se debe utilizar mecanismos diferentes a los tradicionales. Es aquí que se ve la necesidad de utilizar los procedimientos técnicos legales y la rigurosidad científica que pone a disposición de los investigadores la ciencia Forense Informática a fin de descubrir a los autores y cómplices del delito cometido.

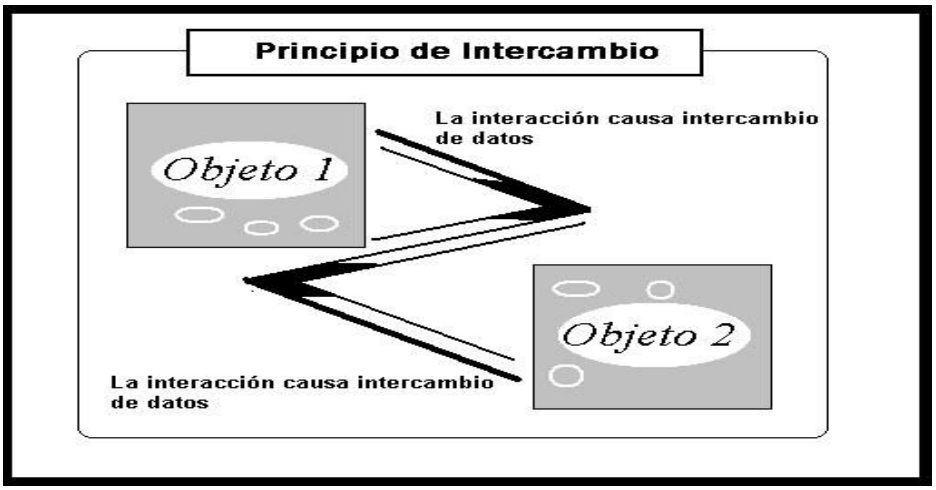
La falta de información especializada en esta área de investigación científica, la inexistente práctica y entrenamiento en la obtención, recolección, documentación y posterior análisis e interpretación de la evidencia digital, pueden permitir que se condene a un inocente y se deje libre a un culpable, situación que es inadmisible en un proceso penal, es por tanto necesarios que los operadores de justicia, es decir la Fiscalía, la Policía Nacional y la Función Judicial debe estar preparada para afrontar el reto de capacitar y entrenar al personal necesario para que lidien de forma óptima no solo con los Delitos Informáticos sino también con otra clases de delitos, aprovechando así las ventajas de utilizar la Informática Forense y la Evidencia Digital dentro de los procesos penales.

5.4.- La Dinámica de la Evidencia

La dinámica de la evidencia es la forma como se entienden y se describen los diferentes factores (humanos, de la naturaleza, de los equipos) que actúan sobre las evidencias, a fin de determinar los cambios que estos producen sobre ellas.

Podemos afirmar indudablemente que existen muchos agentes que intervienen o actúan sobre la evidencia digital, aquí se aplica el llamado principio de intercambio o de Locard[13]; el investigador forense se ve en la necesidad de reconocer la forma como estos factores pueden alterar la evidencia, y así tener la oportunidad de manejarla de una manera apropiada, evitando generalmente contaminarla, dañarla y hasta perderla por completo.

Los principios crimínalisticos, como el de Locard o de intercambio y el mismisidad[14] deben tenerse como instrumentos de la investigación en cualquier escena del crimen inclusive la informática. Esto se puede explicar por ejemplo en el caso de las bitácoras o LOGS del sistema operativo de un equipo informático utilizado por un Hacker o Cracker para romper las seguridades de un programa o vulnerar la integridad de un Sistema informático remoto. En dicha bitácora el investigador podría encontrará registrada dicha actividad ilegal. Ese es un ejemplo del principio de intercambio en acción.



Cuando en una escena del crimen se tiene que trabajar en condiciones adversas, como en incendios, inundaciones, derrames de gasolina o químicos peligrosos, es indispensable que el investigador tome las medidas de seguridad necesarias para asegurar en primer lugar su integridad física, luego deberá implementar el procedimiento más

[13] El principio de intercambio de Locard, menciona que cuando dos objetos entran en contacto siempre existe una transferencia de material entre el uno y el otro. Es decir que cuando una persona está en una escena del crimen esta deja algo de si misma dentro de la escena, y a su vez cuando sale de ella esta se lleva algo consigo.

[14] Una cosa es igual a si misma y diferente de las demás.

adecuado para incrementar las posibilidades de recuperar las evidencias de la manera más completa. De lo dicho podemos manifestar que los examinadores forenses nunca tendrán la oportunidad de revisar una escena del crimen en su estado original, siempre habrá algún factor que haga que la escena del crimen presente algunas anomalías o discrepancias.

Con la finalidad de explicar cómo funciona la dinámica de las evidencias, a continuación se expondrán algunas de las posibles situaciones en donde esta se ve afectada dentro de una escena del crimen:

1. **EQUIPOS DE EMERGENCIAS:** En el caso de un incendio, los sistemas informáticos pueden ser afectados por el fuego y el humo, posteriormente sometidos a una gran presión de agua al tratar de apagar este. Esto provoca que los técnicos forenses no puedan determinar a ciencia cierta si los sistemas informáticos encontrados en la escena estuvieron comprometidos, fueron atacados o usados indebidamente. En otras ocasiones los equipos de emergencia manipulan la escena cuando es necesario para salvar la vida de una persona.
2. **PERSONAL DE CRIMINALÍSITICA**[15]**:** En algunas ocasiones el personal de criminalística por accidente cambia, reubica, o altera la evidencia. Por ejemplo en el caso de que se quiera sacar una muestra de sangre de una gota precipitada sobre un disquete o disco compacto mediante el uso de un escarpelo, esto puede accidentalmente comprometer los datos e información almacenada en dichos soportes.
3. **EL SOSPECHOSO O EL IMPUTADO TRATANDO DE CUBRIR SUS RASTROS**: Cuando el Sospechoso o el imputado deliberadamente borra o altera los datos, registros u otros mensajes de datos considerados como evidencia dentro de un disco duro.
4. **ACCIONES DE LA VÍCTIMA**: La victima de un delito, puede borrar correos electrónicos que le causen aflicción o le provoquen alguna situación embarazosa.
5. **TRANSFERENCIA SECUNDARIA**: En algunas ocasiones, los sistemas informáticos usados en el cometimiento de un delito, son usados posteriormente por alguna persona de forma inocente, causando con ello

[15] Se tiene que minimizar todo rastro del investigador en la escena del delito. Una historia clásica en estos casos, es la del investigador forense que encontró una huella digital dentro de un caso de homicidio, al recuperar y preservar dicha huella creyó tener la pista necesaria para resolver el caso. Por tanto hizo comparar dicha huella digital con la base de datos de la Policía Judicial, al no encontrar un resultado, amplió la búsqueda a nivel nacional encontrándose que la huella encontrada en la escena era suya.

la destrucción y alteración de evidencia.

6. **TESTIGOS**: Un administrador del sistema puede borrar cuentas de usuarios sospechosas, las mismas que fueron creadas por un intruso, a fin de prevenir su acceso y utilización futura.
7. **EL CLIMA Y LA NATURALEZA**: Los campos electromagnéticos pueden corromper la información guardada en discos magnéticos.
8. **DESCOMPOSICIÓN:** En algunos casos la información almacenada en discos magnéticos, o en otros soportes puede perderse o tornarse ilegible para los sistemas de información, a causa del tiempo y de las malas condiciones de almacenamiento.

En resumen el investigador forense debe entender como los factores humanos, de la naturaleza y de los propios equipos informáticos pueden alterar, borrar o destruir evidencia, debe comprender como dichas variables actúan sobre la escena misma del delito, debe por tanto encaminar la investigación desde su etapa más temprana tomando en cuenta esos cambios, a fin de adecuar el mejor método para adquirir, preservar y luego analizar las pistas obtenidas, y así reducir de manera considerable los posibles efectos de la dinámica de la evidencia.

6.- Roles en la Investigación

La investigación científica de una escena del crimen es un proceso formal, donde el investigador forense, documenta y adquiere toda clase de evidencias, usa su conocimiento científico y sus técnicas para identificarla y generar indicios suficientes para resolver un caso. Es por tanto necesario dejar en claro cuáles son los roles y la participación que tiene 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.

6.1.- Peritos Informáticos

Por otro lado, se hace indispensable para la valoración de las pruebas o elementos de convicción la intervención de personas que tengan especiales conocimientos en materias especiales en este caso de la materia informática, personas que prestan un servicio especial al Fiscal y al Juez al momento ilustrar sobre las materias, técnicas o artes que son de su conocimiento, a fin de dichos funcionarios en función de dichas explicaciones puedan emitir su criterio en el momento adecuado (Dictamen Fiscal o la Sentencia)

De acuerdo a lo que dispone el Art. 94 del Código de Procedimiento Penal, "*son peritos los profesionales especializados en diferentes materias que hayan sido acreditados como tales, previo proceso de calificación de la Fiscalía*."

Peritos son las personas que por disposición legal y encargo Judicial o de la Fiscalía aportan con sus conocimientos los datos necesarios para que el Juez, el Fiscal o la Policía Judicial adquieran un grado de conocimiento para determinar las circunstancias en que se cometió una infracción. La presencia de los peritos en una diligencia es indispensable como lo manda el Art. 95 del Código de Procedimiento Penal, suscribir el acta y posteriormente llevarla a conocimiento del Fiscal y el Juez como informe pericial. En otras palabras el conocimiento del perito suple al del juez y el fiscal en cierta área del conocimiento del cual estos no son expertos, por tanto el perito entrega los elementos de convicción que permita al operador de justicia crear un razonamiento que desemboque en la resolución del caso propuesto, en fin aportan elementos que tanto el Fiscal como el Juez valoraran al emitir su resolución.

Jeimy Cano llama a los peritos informáticos forenses: "*investigadores en informática*" y los define como "*profesionales que contando con un conocimiento de los fenómenos técnicos en informática, son personas preparadas para aplicar procedimientos legales y técnicamente válidos para establecer evidencias en situaciones donde se vulneran o comprometen sistemas, utilizando métodos y procedimientos científicamente probados y claros que permitan establecer posibles hipótesis sobre el hecho y contar con la evidencia requerida que sustente dichas hipótesis*"[16]

Las condiciones que deben reunir las personas para ser peritos son:

[16] **CANO** Jeimy, Estado del Arte del Peritaje Informático en Latinoamérica. ALFA-REDI, 2005

a. Ser profesional especializado y calificado por la Fiscalía, poniendo a salvo un criterio, que es aquel de que no necesariamente el perito es un profesional en determinada rama, sino una persona experta o especializada en su respectivo campo de determinada materia. El Código de Procedimiento Penal faculta para que en ciertos casos de lugares donde se vaya a realizar una diligencia no existan peritos habilitados, el Fiscal nombrará a personas mayores de edad, de reconocida honradez y probidad que tengan conocimientos sobre la materia que van a informar.

b. Mayores de edad, los peritos deben tener la mayoría de edad que en nuestro país se fija en 18 años, porque a esa edad la persona ha alcanzado la madurez psicológica necesaria para prestar esta clase de asesoramiento a la Administración de Justicia.

c. Reconocida honradez y probidad, en cuanto a la calidad moral del perito, de proceder recto, íntegro y honrado en el obrar, el perito es un personaje esencialmente imparcial que cumple con su cometido y se desvincula del proceso.

d. Conocimientos específicos en la materia sobre la que debe informar, es decir los necesarios y específicos conocimientos para cumplir su cometido.

La pericia es un medio de prueba específicamente mencionado por la Ley procesal, "*con el cual se intenta obtener para el proceso, un dictamen fundado en especiales conocimientos científicos, técnicos o artísticos, útil para el descubrimiento o valoración de un elemento de prueba*".

Un informe pericial, sus conclusiones u observaciones no son definitivos ni concluyentes, la valoración jurídica del informe pericial queda a criterio del Fiscal, Juez penal o Tribunal penal, quienes pueden aceptarlo o no con el debido sustento o motivación.

Se fundamenta en la necesidad de suplir la falta de conocimiento del Juez o del Fiscal, porque una persona no puede saberlo todo, sobre todo en un mundo tan globalizado, donde las ciencias se han multiplicado y diversificado, así como los actos delictivos.

El Perito debe regirse por los siguientes principios:

1. **OBJETIVIDAD:** El perito debe ser objetivo, debe observar los códigos de ética profesional.
2. **AUTENTICIDAD Y CONSERVACIÓN:** Durante la investigación, se debe conservar la autenticidad e integridad de los medios probatorios.
3. **LEGALIDAD:** El perito debe ser preciso en sus observaciones, opiniones y resultados, conocer la legislación respecto de sus actividades periciales y cumplir con los requisitos establecidos por

ella.

4. **IDONEIDAD:** Los medios probatorios deben ser auténticos, ser relevantes y suficientes para el caso.
5. **INALTERABILIDAD:** En todos los casos, existirá una cadena de custodia debidamente asegurada que demuestre que los medios no han sido modificados durante la pericia.
6. **DOCUMENTACIÓN:** Deberá establecerse por escrito los pasos dados en el procedimiento pericial.

Estos principios deben cumplirse en todas las pericias y por todos los peritos involucrados

El Perito Informático Forense según la opinión del Profesor Jeimy Cano[17] 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
- Concientización en seguridad informática

[17] **CANO** Jeimy, Estado del Arte del Peritaje Informático en Latinoamérica. ALFA-REDI, 2005

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 exige un esfuerzo interdisciplinario y voluntad política tanto de la Fiscalía, 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.

De lo dicho se colige que el PERITO INFORMÁTICO cumple un rol importante dentro de una investigación penal. En resumen y siguiendo al Profesor Jeimy J. Cano diremos que el PERITAJE INFORMÁTICO nace como la respuesta natural de la evolución de la administración de justicia que busca avanzar y fortalecer sus estrategias para proveer los recursos técnicos, científicos y jurídicos que permitan a los operadores de justicia (Función Judicial, Ministerio Público y Policía

Judicial), alcanzar la verdad y asegurar el debido proceso en un ambiente de evidencias digitales.

7.- Incidentes de Seguridad

Cuando se está a cargo de la Administración de Seguridad de un Sistema de Información o una Red, se debe conocer y entender lo que es la Informática Forense, esto en razón de que cuando ocurre un incidente de seguridad, es necesario que dicho incidente sea reportado y documentado a fin de saber qué es lo que ocurrió. No importa qué tipo de evento haya sucedido, por más pequeño e insignificante que pueda ser este debe ser verificado. Esto es necesario a fin de señalar la existencia o no de un riesgo para el sistema informático. Está tarea es de aquellas que es considerada de rutina por los Administradores de un Sistema de Información, pero a pesar de eso, esta tarea puede llevar a un computador en especial dentro de dicho sistema. Es por tanto necesario que los administradores y el personal de seguridad deben conocer los presupuestos básicos del manejo de la evidencia digital, a fin de que sus acciones no dañen la admisibilidad de dicha evidencia dentro de un Tribunal de Justicia, de igual forma deben mostrar la habilidad suficiente para recuperar toda la información referente a un incidente de seguridad a fin de proceder con su potencial análisis.

Un incidente informático en el pasado era considerado como cualquier evento anómalo que pudiese afectar a la seguridad de la información, por ejemplo podría ser una pérdida de disponibilidad, o integridad o de la confidencialidad, etc. Pero la aparición de nuevos tipos de incidentes ha hecho que este concepto haya ampliado su definición. Actualmente y citando a Miguel López diremos que un **Incidente de Seguridad Informática** puede considerarse como una violación o intento de violación de la política de seguridad, de la política de uso adecuado o de las buenas prácticas de utilización de los sistemas informáticos[18].

Es por tanto necesario a fin de comprender mejor el tema señalar algunos conceptos utilizados dentro de la seguridad informática, la cual es definida como *el conjunto de técnicas y métodos que se utilizan para proteger tanto la información como los equipos informáticos en donde esta se encuentra almacenada ya sean estos individuales o conectados a una red frente a posibles ataques premeditados y sucesos accidentales*[19].

La seguridad Informática a su vez está dividida en seis componentes a saber:

SEGURIDAD FÍSICA: Es aquella que tiene relación con la

[18] **LOPEZ DELGADO,** Miguel, Análisis Forense Digital, Junio del 2007, CRIPORED.
[19] El Autor

protección del computador mismo, vela por que las personas que lo manipulan tengan la autorización para ello, proporciona todas las indicaciones técnicas para evitar cualquier tipo de daños físicos a los equipos informáticos.

SEGURIDAD DE DATOS: Es la que señala los procedimientos necesarios para evitar el acceso no autorizado, permite controlar el acceso remoto de la información, en suma protege la integridad de los sistemas de datos.

BACK UP Y RECUPERACIÓN DE DATOS: Proporciona los parámetros básicos para la utilización de sistemas de recuperación de datos y Back Up de los sistemas informáticos. Permite recuperar la información necesaria en caso de que esta sufra daños o se pierda.

DISPONIBILIDAD DE LOS RECURSOS: Este cuarto componente procura que los recursos y los datos almacenados en el sistema puedan ser rápidamente accesados por la persona o personas que lo requieren. Permite evaluar constantemente los puntos críticos del sistema para así poderlos corregir de manera inmediata.

SEGURIDAD NORMATIVA (POLÍTICA DE SEGURIDAD): Conjunto de normas y criterios básicos que determinan lo relativo al uso de los recursos de una organización cualquiera. Se deriva de los principios de legalidad y seguridad jurídica, se refiere a las normas jurídicas necesarias para la prevención y sanción de las posibles conductas que puedan ir en contra de la integridad y seguridad de los sistemas informáticos.

ANÁLISIS FORENSE: El Análisis Forense surge como consecuencia de la necesidad de investigar los incidentes de Seguridad Informática que se producen en las entidades. Persigue la identificación del autor y del motivo del ataque. Igualmente, trata de hallar la manera de evitar ataques similares en el futuro y obtener pruebas periciales.

En los últimos años se ha puesto de manifiesto una creciente masificación del uso de Seguridad Informática en los entornos empresariales, pero a pesar de eso y dado que no existe nunca una seguridad total es decir los controles y políticas que se establecen no garantizan el cien por ciento de la seguridad, máximo si consideramos lo que algunos profesionales de la seguridad señalan como la existencia del llamado riesgo humano (HUMAN RISK[20]) tanto de quienes elaboran las políticas y los controles como también quienes las transgreden. Es por tanto que una amenaza deliberada a la seguridad de la información o de

[20] El riesgo humano siempre debe considerarse dentro de un plan de seguridad informática, ya que siempre nos hemos de hacer la pregunta ¿De qué nos protegemos?, pues la respuesta es nos protegemos de las personas. Es decir siempre existe un elemento que alienta al ser humano a ir en contra de los atributos funcionales de un sistema informático (la confidencialidad, la autenticación, el no repudio, la integridad, y el control de acceso), la ambición por el poder. Este poder reside en los datos y en la información que se encuentra en los actuales sistemas de información del mundo.

un entorno informático (que se verán más adelante), es una condición de ese entorno (una persona, una máquina, un suceso o idea) que, dada una oportunidad, podría dar lugar a que se suscite un incidente de seguridad (ataque contra la confidencialidad, integridad, disponibilidad o uso legítimo de los recursos). Con estas consideraciones las instituciones públicas y privadas deben implementar la política de seguridad que más les convenga a sus intereses. De igual forma cumplir con el análisis de riesgos del sistema a fin de identificar con anterioridad las amenazas que han de ser contrarrestadas, la necesidad de esto es vital, ya que estar consciente de las amenazas y los riesgos de un sistema y comprenderlas completamente hará que se aplique los procedimientos de seguridad apropiados para cada caso.

La integridad de un Sistema de Información puede verse afectada por la existencia de vulnerabilidades, en tal razón un buen sistema de seguridad informática seguido de la aplicación de los protocolos necesarios (normatividad informática). Harán que la actividad productiva de una empresa o su capital de conocimiento no sean afectados por posibles intentos de explotación de dichas vulnerabilidades (incidentes de seguridad).

En definitiva para que exista una adecuada protección a los sistemas informáticos y telemáticos se deben conjugar tanto la seguridad informática como la seguridad legal y así poder brindar una adecuada protección y tutela tanto técnica como normativa.

Es importante por parte de la persona que realiza la implementación tanto de la Seguridad Informática (Técnico en la materia), como quien realiza la Política de Seguridad, (Gerente de Seguridad y Abogado de la Empresa). Que el diseño del sistema debe hacerse de manera integral y conjunta en orden a poder asegurar una posible investigación en un ambiente Técnico y Jurídico que de solución a posibles problemas de seguridad informática y prevención de de Delitos Informáticos.

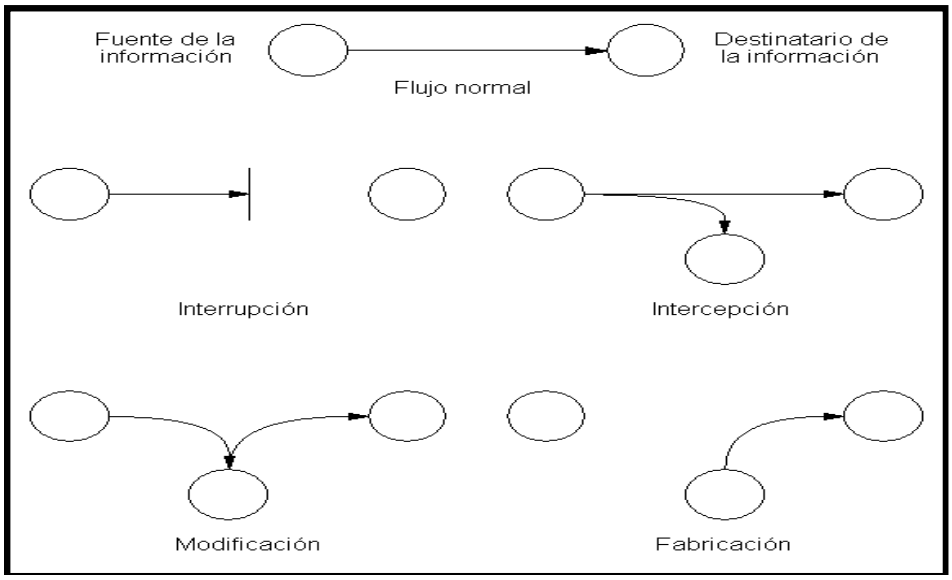
En conclusión es necesario que tanto los administradores del sistema y como los de seguridad en la red de una empresa, tengan el suficiente entrenamiento y habilidad en el uso de técnicas forenses, esto con la finalidad de que su actuación en un incidente de seguridad cumpla con los estándares de una investigación penal, ya que dicho incidente puede ser el resultado del accionar delictivo de una o varias personas, entonces la investigación de ese hecho saldrá de la empresa afectada para entrar en el campo criminal, en donde la Policía Judicial y la Fiscalía la llevarán adelante. Por tanto es esencial que el investigador forense que está envuelto en la obtención de la evidencia digital comprenda la naturaleza de la información, de su fragilidad, y de la facilidad que tiene en contaminarse. Si este se equivoca en la etapa preliminar de la investigación en la cual se identifica y obtiene la evidencia digital, sus errores y fallas de procediendo harán que esa evidencia se pierda o simplemente sea excluida como prueba durante el proceso judicial.

7.1.- Amenazas deliberadas a la seguridad de la información

Las amenazas cada vez más numerosas que ponen en peligro a nuestros datos, nuestra intimidad, nuestros negocios y la propia Internet ha hecho que la computación sea una tarea azarosa. Los riesgos familiares, como los virus y el correo indeseado, ahora cuentan con la compañía de amenazas más insidiosas -desde el llamado malware- , los programas publicitarios, y de espionaje que infectan su PC a los ladrones de identidad que atacan las bases de datos importantes de información personal y las pandillas de delincuencia organizada que merodean por el espacio cibernético.

Los incidentes de seguridad en un Sistema de Información pueden caracterizarse modelando el sistema como un flujo de mensajes de datos desde una fuente, como por ejemplo un archivo o una región de la memoria principal, a un destino, como por ejemplo otro archivo o un usuario. Un incidente no es más que la realización de una amenaza en contra de los atributos funcionales de un sistema informático[21].

Las cuatro categorías generales de incidentes son las siguientes



[21] Un sistema informático debe tener varios atributos funcionales que lo hacen podríamos decir resistente a una posible amenaza o ataque. Es por eso que para hacer frente a los incidentes de seguridad del sistema se definen una serie de atributos funcionales para proteger los sistemas de procesamiento de datos y de transferencia de información de una organización. Estos son considerados por varios profesionales de la seguridad informática como servicios de un Sistema Informático, personalmente los considero no como servicios sino como cualidades intrínsecas de los sistemas informáticos actuales, ya que si fueran solo servicios, se podrían suspender o quitar sin ningún problema, pero la realidad es otra, su falta u omisión causa mas de un problema grave al sistema al no tener estos atributos. Estos son la confidencialidad, la autenticación, el no repudio, la integridad, y el control de acceso.

INTERRUPCIÓN: un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad[22]. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de archivos, los ataques de denegación de servicios (DoD y DDoD)

INTERCEPCIÓN: una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad[23]. La entidad no autorizada podría ser una persona, un programa o un computador. Ejemplos de este ataque son pinchar una línea para hacerse con datos que circulen por la red (utilizar un SNIFFER) y la copia ilícita de archivos o programas (intercepción de datos, WIRETAPING), o bien la lectura de las cabeceras de paquetes para desvelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).

MODIFICACIÓN: una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad[24]. Ejemplos de este ataque es el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.

FABRICACIÓN: una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes espurios en una red o añadir registros a un archivo.

Estos ataques se pueden asimismo clasificar de forma útil en términos de ataques pasivos y ataques activos.

7.2.- Ataques pasivos

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación, que puede consistir en:

Obtención del origen y destinatario de la comunicación, leyendo las cabeceras de los paquetes monitorizados.

Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.

---

[22] La **Disponibilidad** hace referencia a que solo los usuarios autorizados, pueden acceder a la información y a otros recursos cuando los necesiten.

[23] La **Confidencialidad** se refleja en la utilización de información y de los recursos que solamente son revelados a los usuarios (personas, entidades y procesos), quienes están autorizados a acceder a ellos.

[24] La **Integridad** se refleja en que la información y otros recursos solo pueden ser modificados solo por aquellos usuarios que tiene derecho a ello. La exactitud y el detalle de los datos y la información está también garantizada.

Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos que se verán más adelante.

7.3.- Ataques activos

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

Suplantación de identidad[25]: el intruso se hace pasar por una entidad o usuario diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.

Re actuación: uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.

Modificación de mensajes: una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje "Ingresa un millón de dólares en la cuenta A" podría ser modificado para decir "Ingresa un millón de dólares en la cuenta B".

En cuanto a esto podemos hacer una referencia a los tipos de delitos informáticos que existen actualmente y que se refieren a este tipo de conducta que son los fraudes informáticos, a continuación se detallan estos tipos de delitos:

LOS DATOS FALSOS O ENGAÑOSOS (Data diddling), conocido también como introducción de datos falsos, es una manipulación de datos de entrada al computador con el fin de producir o lograr movimientos falsos en transacciones de una empresa. Este tipo de fraude informático conocido

[25] **PARASITISMO INFORMÁTICO (PIGGYBACKING) Y SUPLANTACIÓN DE PERSONALIDAD (IMPERSONATION)**, figuras en que concursan a la vez los delitos de suplantación de personas o nombres y el espionaje, entre otros delitos. En estos casos, el delincuente utiliza la suplantación de personas para cometer otro delito informático. Para ello se prevale de artimañas y engaños tendientes a obtener, vía suplantación, el acceso a los sistemas o códigos privados de utilización de ciertos programas generalmente reservados a personas en las que se ha depositado un nivel de confianza importante en razón de su capacidad y posición al interior de una organización o empresa determinada.

también como ***manipulación de datos de entrada***, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

MANIPULACIÓN DE PROGRAMAS O LOS "CABALLOS DE TROYA" (Troya Horses), Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

LA TÉCNICA DEL SALAMI (Salami Technique/Rounching Down), Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra. Y consiste en introducir al programa unas instrucciones para que remita a una determinada cuenta los céntimos de dinero de muchas cuentas corrientes.

FALSIFICACIONES INFORMÁTICAS: **Como objeto:** Cuando se alteran datos de los documentos almacenados en forma computarizada. **Como instrumentos:** Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color basándose en rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer reproducciones de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

MANIPULACIÓN DE LOS DATOS DE SALIDA.- Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición

de datos. Tradicionalmente esos fraudes se hacían basándose en tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

Degradación fraudulenta del servicio: impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes espurios. Entre estos ataques se encuentran los de denegación de servicio[26], consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc.

7.- Procedimiento de Operaciones Estándar

Cuando se va revisar una escena del crimen del tipo informático es necesario tener en cuenta un procedimiento de operaciones estándar (POE), el mismo que es el conjunto de pasos o etapas que deben realizarse de forma ordenada al momento de recolectar o examinar la evidencia digital. Esta serie de procedimientos se utilizan para asegurar que toda la evidencia recogida, preservada, analizada y filtrada se la haga de una manera transparente e integra. La transparencia y la integridad metodológica (estabilidad en el tiempo de los métodos científicos utilizados) se requieren para evitar errores, a fin de certificar que los mejores métodos son usados, incrementado cada vez la posibilidad de que dos examinadores forenses lleguen al mismo dictamen o conclusión cuando ellos analicen la misma evidencia por separado. A esto se lo conoce como reexaminación.

Una de las mejores Guías Prácticas de manejo de evidencia digital es la de los Jefes y oficiales de Policía del Reino Unido publicada en 1999, en base a los principios de la Organización Internacional de Evidencia Informática (SWGDE).

Estos principios establecen lo siguiente:

[26] **ATAQUES DE DENEGACIÓN DE SERVICIO**: Estos ataques se basan en utilizar la mayor cantidad posible de recursos del sistema objetivo, de manera que nadie más pueda usarlos, perjudicando así seriamente la actuación del sistema, especialmente si debe dar servicio a mucho usuarios Ejemplos típicos de este ataque son: el consumo de memoria de la máquina víctima, hasta que se produce un error general en el sistema por falta de memoria, lo que la deja fuera de servicio, la apertura de cientos o miles de ventanas, con el fin de que se pierda el foco del ratón y del teclado, de manera que la máquina ya no responde a pulsaciones de teclas o de los botones del ratón, siendo así totalmente inutilizada, en máquinas que deban funcionar ininterrumpidamente, cualquier interrupción en su servicio por ataques de este tipo puede acarrear consecuencias desastrosas.

1. El funcionario de la Fiscalía o de la Policía Judicial nunca debe acudir solo al lugar de los hechos, este tipo de actividad debe ser realizada como mínimo por dos funcionarios. Un segundo funcionario, por un lado, aporta seguridad personal y, por otro, ayuda a captar más detalles del lugar de los hechos. Los funcionarios deberían planear y coordinar sus acciones. Si surgen problemas inesperados, es más fácil resolverlos porque "dos cabezas piensan más que una.
2. Ninguna acción debe tomarse por parte de la Policía o por sus agentes que cambie o altere la información almacenada dentro de un sistema informático o medios informáticos, a fin de que esta sea presentada fehacientemente ante un tribunal[27].
3. En circunstancias excepcionales una persona puede tener acceso a la información original almacenada en el sistema informático objeto de la investigación, siempre que después se explique de manera razonada cual fue la forma de dicho acceso, su justificación y las implicaciones de dichos actos.
4. Cuando se hace una revisión de un caso por parte de una tercera parte ajena al mismo, todos los archivos y registros de dicho caso y el proceso aplicado a la evidencia que fue recolectada y preservada, deben permitir a esa parte recrear el resultado obtenido en el primer análisis.
5. El oficial a cargo de la investigación es responsable de garantizar el cumplimiento de la ley y del apego a estos principios, los cuales se aplican a la posesión y el acceso a la información almacenada en el sistema informático. De igual forma debe asegurar que cualquier persona que acceda a o copie dicha información cumpla con la ley y estos principios.

Estas guías son hechas para cubrir la gran mayoría de temas y situaciones comunes a todas las clases de sistemas informáticos existentes en estos momentos. Estas guías no asumen por completo que la investigación se realizará absolutamente sobre evidencia digital, se debe tomar en cuenta que solo es una parte de la averiguación del caso. El investigador tiene que ver toda la escena del crimen, debe poner sus sentidos en percibir todos los objetos relacionados con la infracción, es así que por ejemplo la guía advierte de que no se debe tocar los periféricos de entrada de la computadora objeto de la investigación, como el teclado, el ratón, en los cuales se puede encontrar huellas digitales que pueden ayudar a identificar a los sospechosos.

[27] Una regla universal de la informática forense es "no cambies nada de una escena del delito", el objetivo de la informática forense como se ha mencionado es reconocer, colectar, analizar y generar un reporte en base a la evidencia que no ha sido ni alterada y cambiada en ninguna forma, de ahí la importancia de este principio.

Es importante darse cuenta que estas guías y procedimientos se enfocan mayormente en la recolección de evidencia digital y un poco en el análisis de esta. Asimismo las nuevas tecnologías que van apareciendo con el tiempo no son cubiertas por estas guías.

Para finalizar se debe tomar en cuenta que cada caso es diferente, por eso es difícil tener un estándar que abarque en profundidad cada uno de los aspectos del análisis forense informático. Sin embargo es necesario siempre usar una metodología de trabajo definida para organizar y analizar la gran cantidad de datos que se encuentra en los sistemas de información y las redes de telecomunicaciones. La ciencia forense en general usa la reconstrucción del delito para definir dicha metodología de trabajo.

8.- Investigación en la Escena del Delito.

La escena del delito es el punto de partida de una investigación forense, aquí se aplican los principios crimínalisticos como el de transferencia y el de mismisidad, explicados anteriormente; aquí se da inicio al procedimiento pertinente de acuerdo a la infracción cometida. En muchos de los casos el investigador forense no es el primero en llegar a la escena del delito, a veces llega después de un tiempo de cometido este, como un experto secundario, pero aún así debe estar consciente de su entorno de trabajo, igual como si hubiera sido el primero en llegar.

Los Investigadores que llegan primero a una escena del crimen tienen ciertas responsabilidades, las cuales resumimos en el siguiente cuadro:

- **OBSERVE Y ESTABLEZCA LOS PARÁMETROS DE LA ESCENA DEL DELITO**: El primero en responder debe establecer si el delito todavía se está cometiendo, tiene que tomar nota de las características físicas del área circundante. Para los investigadores forenses esta etapa debe ser extendida a todo sistema de información y de red que se encuentre dentro de la escena. En estos casos dicho sistema o red pueden ser blancos de un inminente o actual ataque como por ejemplo uno de denegación de servicio (DoS).
- **INICIE LAS MEDIDAS DE SEGURIDAD**: El objetivo principal en toda investigación es la seguridad de los investigadores y de la escena. Si uno observa y establece en una condición insegura dentro de una escena del delito, debe tomar las medidas necesarias para mitigar dicha situación. Se deben tomar las acciones necesarias a fin de evitar riesgos eléctricos, químicos o biológicos, de igual forma cualquier actividad criminal. Esto es importante ya que en una ocasión en una investigación de pornografía infantil en Estados Unidos un investigador fue muerto y otro herido durante la revisión de una escena del crimen.
- **FACILITE LOS PRIMEROS AUXILIOS**: Siempre se deben tomar las

medidas adecuadas para precautelar la vida de las posibles víctimas del delito, el objetivo es brindar el cuidado médico adecuado por el personal de emergencias y el preservar las evidencias.

- **ASEGURE FÍSICAMENTE LA ESCENA**: Esta etapa es crucial durante una investigación, se debe retirar de la escena del delito a todas las personas extrañas a la misma, el objetivo principal es el prevenir el acceso no autorizado de personal a la escena, evitando así la contaminación de la evidencia o su posible alteración.
- **ASEGURE FÍSICAMENTE LAS EVIDENCIAS**: Este paso es muy importante a fin de mantener la cadena de custodia[28] de las evidencias, se debe guardar y etiquetar cada una de las evidencias. En este caso se aplican los principios y la metodología correspondiente a la recolección de evidencias de una forma práctica. Esta recolección debe ser realizada por personal entrenado en manejar, guardar y etiquetar evidencias.
- **ENTREGAR LA ESCENA DEL DELITO**: Después de que se han cumplido todas las etapas anteriores, la escena puede ser entregada a las autoridades que se harán cargo de la misma. Esta situación será diferente en cada caso, ya que por ejemplo en un caso penal será a la Policía Judicial o al Ministerio Público; en un caso corporativo a los Administradores del Sistema. Lo esencial de esta etapa es verificar que todas las evidencias del caso se hayan recogido y almacenado de forma correcta, y que los sistemas y redes comprometidos pueden volver a su normal operación.
- **ELABORAR LA DOCUMENTACIÓN DE LA EXPLOTACIÓN DE LA ESCENA**: Es Indispensable para los investigadores documentar cada una de las etapas de este proceso, a fin de tener una completa bitácora de los hechos sucedidos durante la explotación de la escena del delito, las evidencias encontradas y su posible relación con los sospechosos. Un investigador puede encontrar buenas referencias sobre los hechos ocurridos en las notas recopiladas en la explotación de la escena del Delito.

[28] La cadena de custodia es un sistema de aseguramiento que, basado en el principio de la "mismidad", tiene como fin garantizar la autenticidad de la evidencia que se utilizará como "prueba" dentro del proceso. La información mínima que se maneja en la cadena de custodia, para un caso específico, es la siguiente: a) Una hoja de ruta, en donde se anotan los datos principales sobre descripción de la evidencia, fechas, horas, custodios, identificaciones, cargos y firmas de quien recibe y quien entrega; b) Recibos personales que guarda cada custodio y donde están datos similares a los de la hoja de ruta; c) Rótulos que van pegados a los envases de las evidencias, por ejemplo a las bolsas plásticas, sobres de papel, sobres de Manila, frascos, cajas de cartón, etc.; d) Etiquetas que tienen la misma información que los rótulos, pero van atadas con una cuerdita a bolsas de papel kraft, o a frascos o a cajas de cartón o a sacos de fibra; e) Libros de registro de entradas y salidas, o cualquier otro sistema informático que se deben llevar en los laboratorios de análisis y en los despachos de los fiscales e investigadores.

8.1.- Reconstrucción de la Escena del Delito

La reconstrucción del delito permite al investigador forense comprender todos los hechos relacionados con el cometimiento de una infracción, usando para ello las evidencias disponibles. Los indicios que son utilizados en la reproducción del Delito permiten al investigador realizar t res formas de reconstrucción a saber:

- *Reconstrucción Relacional*, se hace en base a indicios que muestran la correspondencia que tiene un objeto en la escena del delito y su relación con los otros objetos presentes. Se busca su interacción en conjunto o entre cada uno de ellos;
- *Reconstrucción Funcional*, se hace señalando la función de cada objeto dentro de la escena y la forma en que estos trabajan y como son usados;
- *Reconstrucción Temporal*, se hace con indicios que nos ubican en la línea temporal del cometimiento de la infracción y en relación con las evidencias encontradas.

A fin de ilustrar lo señalado en las líneas precedentes tomemos como ejemplo una investigación de un acceso no autorizado. Cuando sucede este incidente uno en primer lugar desea saber cuáles son los sistemas de información o redes se comunicaron entre sí, cual fue la vulnerabilidad que se explotó para obtener este acceso no autorizado y cuando se produjo este evento.

Con estos antecedentes empezamos a realizar la reconstrucción relacional en base a la localización geográfica de las personas y de los equipos informáticos involucrados en el incidente, también se busca cual fue su interrelación en base a las líneas de comunicaciones existentes y a las transacciones o intercambio de información hechas entre sí. Esta reconstrucción de tipo relacional es muy útil en casos de Fraude Informático ya que nos puede revelar información crucial dentro de la investigación, al crear un patrón de comportamiento conectando las transacciones financieras fraudulentas con una persona o una organización en particular. De igual forma en la investigación por el acceso no autorizado se crea una lista de las direcciones IP de los sistemas de información comprometidos con las direcciones IP donde se realizó las conexiones, buscando la fuente y el destino de estas, logrando un diagrama de cómo los equipos informáticos interactuaron entre si.

El investigador forense realiza la reconstrucción funcional del hecho, estableciendo el funcionamiento de un sistema o aplicación específica y como estos fueron configurados en el momento del delito. En algunas ocasiones es necesario determinar cómo un programa de computación o sistema funciona para tener un mejor entendimiento del delito en si o de una evidencia particular. Cuando una plataforma UNIX es comprometida usando un rootkit, el examinador tiene que reiniciar el sistema y analizar una copia exacta del sistema expuesto y su operatividad con sus componentes, lo cual puede crear una puerta trasera

en el sistema, capturar contraseñas o esconder evidencias relevantes.

La línea de tiempo del incidente ayuda al investigador a identificar patrones e inconsistencias en la escena, guiando a éste a más fuentes de evidencia. Antes de realizar esta línea temporal el investigador debe tomar en cuenta las diferentes zonas horarias y las discrepancias temporales de los relojes de los sistemas de información examinados.

9.- Fases de la Investigación Forense.

El objetivo principal de la Investigación Forense Informática es la recolección, preservación, filtrado y presentación de las evidencias digitales de acuerdo a los procedimientos técnicos y legales preestablecidos, como apoyo de la Administración de Justicia.

9.1.- Recolección

Este primer paso es fundamental para la investigación, aquí el investigador forense debe identificar a todos los objetos que tengan valor como evidencia para posteriormente recolectarlos. Normalmente estos objetos serán mensajes de datos, información digital contenidos en discos duros, flash memory's y otros artefactos que almacenan información digital, también pueden incluir los respaldos de emergencia, en fin el investigador debe tener bien en claro cuáles son las fuentes de la evidencia a fin de identificar a esta y la mejor manera de recolectarla.

9.2.- Preservación

La preservación es la parte de la investigación digital forense que se enfoca en resguardar los objetos que tengan valor como evidencia de manera que estos permanezcan de forma completa, clara y verificable. Aquí se utiliza técnicas criptográficas como códigos de integridad (función hash, checksums) y la más prolija documentación.

La fase de preservación interviene a lo largo de todo el proceso de investigación forense, es una fase que interactúa con las demás fases.

9.3.- Filtrado

También conocida como la fase de análisis en la investigación forense, es donde el investigador busca filtrar todos los objetos recolectados y preservados de la escena del delito a fin de separar los objetos que no tienen valor como evidencia de los que si.

En esta fase el investigador utilizar una serie de instrumentos y técnicas para localizar y extraer la evidencia para luego ponerla en el contexto de la investigación.

9.4.- Presentación

Esta es la fase final de la investigación forense informática, es cuando se presentan los resultados, los hallazgos del investigador.

La presentación debe ser entendible y convincente, es decir aquí se debe reseñar los procedimientos y las técnicas utilizadas para recolectar, preservar y filtrar la evidencia de manera que exista certidumbre en los métodos usados, aumentado así la credibilidad del investigador en un contra examen de los mismos.

10.- 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 70 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 IV, Capitulo 4to, en la sección décima al hablar de la Fiscalía General del Estado, en su Art. 195 señala que: "**La Fiscalía dirigirá, de oficio o a petición de parte 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 de la Fiscalía, 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 de la Fiscalía 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 de la Fiscalía 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 de la Fiscalía especializadas en abordar cuestiones de la delincuencia informática e informática forense. 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.

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[29], 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 la Fiscalía 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.

11. - Bibliografía

- **HANDBOOK OF COMPUTER CRIME INVESTIGATION, FORENSIC TOOLS AND TECHNOLOGY:** Eoghan Casey, Elsevier Academic Press, 2005
- **DERECHO DE LAS NUEVAS TECNOLOGÍAS:** Mariliana Rico Carrillo Coordinadora, Ediciones La Rocca, 2007.
- **COMPUTER EVIDENCE COLLETION & PRESERVATION:** Christopher L.T. Brown, Charles River Media, 2006.
- **ESTADO DEL ARTE DEL PERITAJE INFORMÁTICO EN LATINOAMÉRICA:** Jeimy Cano, ALFA-REDI, 2005.
- **CRIMEN ORGANIZADO Y CIBERNÉTICO, SINERGIAS, TENDENCIAS Y RESPUESTAS:** Phil Williams, Centro de Enseñanza en Seguridad de la Internet de la Universidad Carnegie Mellon. http://www.pitt.edu/~rcss/toc.html
- **ANÁLISIS FORENSE DIGITAL**, López Delgado Miguel, Junio del 2007, CRIPORED.
- **TECNOLOGÍAS DE LA INFORMACIÓN A LA COMUNICACIÓN** Alonso Juan A**.** y otros**,** Editorial ALFAOMEGA y RA-MA, 2005
- **CIBERESPACIO, SOCIEDAD Y DERECHO**, Herrera Bravo Rodolfo. En **DERECHO DE LAS NUEVAS TECNOLOGÍAS:** Mariliana Rico Carrillo Coordinadora, Ediciones La Rocca, 2007.

[29] **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